Moderated Discussion: Are we addressing the "real" issue?

Moderator: Mark Feher
AECL
Chalk River, ON

1. INTRODUCTION

Session 5 was a moderated discussion on the topic of "Are we addressing the "real" issue. The Moderator opened the session with the following question areas to stimulate discussion.

Questions Part 1:

Is the concept of alarms and alarm systems still valid? Are we designing for physical features rather than information that has to be conveyed? Are we addressing the essential annunciation needs or are we attempting to implement patch-work solutions to solve specific problems?

Is the design process so firmly established in organizations that a major change is required to result in different and improved approaches?

Will the cost of increasing scrutiny for Software QA make advancement impossible or too costly?

What is the role of overview displays in accident management and how do imbedded alarms play a role? Is the need for reliable signals adequately addressed (or can it be)?

Questions Part 2:

Should we include automated diagnosis and decision making with annunciation?

What is the role of the operator? Is the operator some one who only follows fixed procedures, or is he/she a responsible authority, or both?

Does the focus on safety-first divert the attention away from other important issues, such as operational efficiency?

Does the concept of "hard-wired" annunciation still apply given advancements in reliability of computer systems?

How do we shorten the design and implementation time period cost effectively while still improving the performance?

Questions Part 3:

Does the discussion of problems with existing systems in order to identify areas for improvement result in retrofit for change to existing facilities demanded by regulators?

How can innovations in the design of annunciation (or other) systems be credibly linked to the economic benefits for the change?

Complex design leads to support for complex design, which in turn leads to more complexity - why not simplify the design in the first place?

2. SUMMARY OF THE DISCUSSIONS

This summary represents highlights of statements made and does not necessarily reflect consensus of opinion amongst the participants.

- The role of annunciation includes two levels of information: overview and detailed.
- The level of quality assurance (QA) required of computerised annunciation systems should be based on the impact of the system on safety and a probabilistic model for failure (reliability).
- The concept of reliability is not being applied in the same way for hardware versus software systems.
- For reliability estimates to be adequate for truly assessing safety, the estimate must be based on a measure of the closed loop reliability of the system as a whole (which includes humans).
- The use of hard-wired back-up technology for computerised systems requires that the back-up system be integrated into normal operational use. This restricts the capabilities of the computerised system to achieve its full potential. Designs are targeting highly reliable computer systems such that the primary systems can be available and used for more than 99% of the operation.
- Several experiences have shown a trend where Regulatory scrutiny of software systems is delaying or denying design changes that would otherwise improve operational performance and therefore overall plant safety.
- There appears to be considerable overlap between "annunciation systems" and "plant display systems". The issue should not be "how we design annunciation systems" but "how we represent all the information about the plant to the operating team".
- We need more objective measures of performance to address overall reliability of the system (including the human operator).
- Annunciation around the world is being described in different ways; an operator aid, a key part of safety critical actions, and everything in between.
- Is the concept of software categorization for QA and regulatory needs "real" in the context of the whole system without closing the loop with the human operator in the system?

3. CONCLUSIONS

As with many discussions in the nuclear industry, the topic of Quality Assurance and software qualification diverted attention from key topics in improving the information systems for nuclear power plant operators. Although QA is important and reliability is needed, we must focus more attention on designing more operationally effective systems if we are in fact going to achieve high overall reliability. With limited resources available, the QA and regulatory process may be a net contributor to reduced reliability. We need to resolve the question of reliability and level of quality assurance in order to benefit from innovations.

It is clear that the concept of annunciation has undergone considerable change over the past several years. The definition of annunciation is almost as diverse as the options to implement it. The presentations over the week have clearly identified the need to alert operational personnel by redirecting their attention to important "information" about the plant. The nature of the information (problems, faults, successful versus unsuccessful changes of state, detection of events, procedural requirements, etc.) has resulted in a confusion of terminology that is masking the more creative discussions about how to better represent information to enhance operational effectiveness. The research, development, design, and regulatory community need to focus more on describing the issues in terms of information needs and use rather than focusing on the terminology used to describe it.

The nuclear industry has generated wonderful new ideas and technologies that we should all better understand and learn how to exploit for maximum benefit. There is overwhelming consensus on the problems with existing designs and there is clear evidence, as presented this week, that the industry is turning the corner and has resolutions for many of them.

In closing, let us recognise the need to develop and learn new technology, but let us not lose sight of the need to select technology and tools based on well understood operational and performance needs and not on the existence of the technology itself.