

OPERATIONAL VALIDATION - CURRENT STATUS AND OPPORTUNITIES FOR IMPROVEMENT

Eric Davey
Crew Systems Solutions
Deep River, Ontario, Canada K0J 1P0

ABSTRACT

The design of nuclear plant systems and operational practices is based on the application of multiple defenses to minimize the risk of occurrence of safety and production challenges and upsets. With such an approach, the effectiveness of individual or combinations of design and operational features in preventing upset challenges should be known.

A longstanding industry concern is the adverse impact errors in human performance can have on plant safety and production. To minimize the risk of error occurrence, designers and operations staff routinely employ multiple design and operational defenses. However, the effectiveness of individual or combinations of defensive features in minimizing error occurrence are generally only known in a qualitative sense. More importantly, the margins to error or upset occurrence provided by combinations of design or operational features are generally not characterized during design or operational validation.

This paper provides some observations and comments on current validation practice as it relates to operational human performance concerns. The paper also discusses opportunities for future improvement in validation practice in terms of the resilience of validation results to operating changes and characterization of margins to safety or production challenge.

BACKGROUND

This paper summarizes observations and opinions of the author concerning current industry emphasis and limitations in human performance validation practice. The paper draws on over 15 years of industry application experience with both research, initial design and retrofit projects. The willingness of utility, design and regulatory colleagues to share and discuss their project validation experience over the years has been most helpful in developing the author's perspective.

Validation is a design confirmation activity intended to determine the degree to which the integrated use of equipment, operational aids, and formalized work practices by trained users leads to achievement of pre-defined performance goals. Validation, as currently practiced, is a culminating activity, generally occurring just prior to the commissioning of a system for active service. The definition and conduct of validation activities is set out in industry human factors engineering regulatory standards [1,2] and project specific program plans.

THE NATURE OF HUMAN ERROR

Human errors can occur in the operation of technical systems for a number of reasons. Errors can be directly attributed to technical system design, environmental, and personnel factors. While the technical system design can be controlled to eliminate and/or reduce human error occurrence, the control of environmental factors and the way the system is used by personnel is often less controllable. For example, the occurrence of errors due to personal factors (i.e., Mistakes - errors in intent, and Slips - errors in attention) cannot be entirely eliminated through improved training or optimal interface design. Humans are prone to errors due to: limited attentional resources; biases; and modification of rules and models of system operation with time, based on experiential knowledge.

As a consequence, technical systems should be operated with the recognition that the occurrence of operating errors may present ongoing challenges to achievement of operational goals. As part of validation, the effectiveness of selected defenses in preventing error occurrences, and promoting error detection and safe recovery should be characterized.

CURRENT VALIDATION EMPHASIS AND LIMITATIONS

As a design confirmation activity, the current emphasis in validation practice is placed on demonstration of expected performance in a representative operational setting. Due to the effort and resources required for such integrated tests, budget and schedule constraints often limit the validation scope undertaken. Consequently, validation effort focuses only on a few of the operational situations likely to be encountered during actual system in-service use. Thus, system performance may not be assessed and confirmed in all operational situations in which the system is likely to be operated.

While the adoption of formal validation practices as part of human factors engineering programs over the past ten years has been a positive step forward, several aspects of current practice limit the validity and application of current validation results, for example:

- Variability in Application - Validation is most rigorously applied to 'identified' system changes under the auspices of human factors program plans. Many changes in operating practice, procedures, and workplaces with equivalent operational impact are implemented and placed into service with much less formal operational testing.

- Performance Measures and Criteria - Frequent reliance on general or global measures of task success, and subjective or opinion-based assessment, rather than very task-specific and objective measures and criteria.
- Situational Validity - Operational validation is often undertaken in environments that do not truly mimic those to be experienced in operational practice, thus discounting the validity and transferability of results (e.g., task performance in isolation of normal workplace burdens and distracters, or assessment with optimally trained staff).
- Error and Upset Prevention Effectiveness - Little emphasis is placed on characterizing and confirming the effectiveness and margins provided by human performance related defensive design and operational features.

NEW CHALLENGES

Two additional aspects of design confirmation activities are presenting new challenges to industry designers, operations and regulatory staff:

- Judging the Sufficiency of Defence-in-Depth Design Features

Designers and operations staff routinely employ multiple design and operational features to promote correct operating actions and minimize the occurrence of errors. Examples of these features that are used singly or in combination include:

- Labeling to provide unambiguous information and device identification to promote location and correct selection,
- Visual coding to promote correct information or control identification and selection,
- Grouping of information and controls according to system or function affiliation to promote visual location and correct selection,
- Warnings and Cautions to alert users to the consequences and side effects of operating actions or the consequences of operating errors before actions take place,
- Procedures and written guidance to specify permitted operating actions and action sequences,
- Self-check operating practices for 'on-task' confirmation of information or device control selections or actions,
- Affordances to assist users in recognizing device control possibilities,
- Constraints to limit action possibilities to acceptable choices and ranges,

- Independent verification of information or device control selections or actions to provide enhanced assurance of correct operating choice.
- Undo capabilities to permit users to reverse operating actions and recover from errors,
- Interlocks that physically prevent user actions that may result in unsafe or uneconomic consequences, and
- Indications of feedback from process parameters or equipment states resulting from operating actions to provide confirmation of successful operating action success.

The error prevention effectiveness of many of these features can be situationally dependent, being a function of the type of task action, error possibilities and characteristics of the operating environment. Thus, an understanding of these three factors is required to determine the specific error prevention effectiveness of an individual interface or operating feature.

Generally, such level of information detail is not readily available and the human error prevention effectiveness of individual or combinations of features is only known in a qualitative sense. Thus, judgments of the sufficiency of error prevention features can not be made with specific assurance.

- The Continuing Relevance of Validation Results During Operational Changes

Operational environments change as a result of utility continuous improvement initiatives. Thus, some conditions under which a system is required to operate may change substantially across the system's operating lifetime. In such circumstances, a point may be reached where the initial system performance validation is no longer relevant. Consequently, the system performance may require re-validation to justify continued in-service use.

To address this challenge, designers, operations staff and regulators need to begin identifying the factors that are most critical to maintaining validation relevance for projects that they undertake. Likewise, the merits of alternative ways for characterizing and/or maintaining the operational relevance of system validation results should be explored. Solutions could include:

- Envelope Definition - This involves the adoption of validation approaches that confirm operational performance within a defined envelope of operating conditions rather than for bounding or single scenario situations. As long as key in-service operating conditions remain within the envelope of validated

performance, the original validation of the system performance would remain relevant.

- **Periodic Re-validation** - This approach is dependent on repeated confirmations of system performance across the system's service lifetime. Either time-based or operating envelope excursion criteria could be used to provide the basis for re-qualification frequency.
- **Ongoing Confirmation** - Continuous confirmation of system performance against actual in-service operating conditions would provide a means to maintain validation relevance as operating conditions change. In this case, collection and interpretation of operating data could be used to continuously confirm system performance so that the validation results would remain up-to-date.

SUGGESTIONS FOR IMPROVEMENT

To improve the effectiveness of industry validation practice, the following suggestions for enhancing operational understanding, design application, and operational confirmation are offered:

- **Improved Understanding of Human Error**
Human error remains a key contributing causal factor to plant operating events, yet there is a weak characterization of error types and occurrence frequency in plant operations. To develop effective defenses, a fundamental understanding of current human error characteristics (e.g., types, frequency, prerequisite conditions, and visibility) should be developed. The necessary data could be gathered using industry wide anonymous reporting systems such as those pioneered by the United States Federal Aviation Authority and currently employed by some American nuclear utilities.
- **Characterization of Defenses**
To characterize the effectiveness of error prevention, detection and recovery features, specific tests of feature performance with representative tasks and error challenges should be conducted. An industry test matrix could be developed that would permit results to be shared and allow for comparison of results based on single and combinations of features from a number of organizations. These combined results could then serve as design guidance and practical assessment criteria in future industry projects.
- **Broadening Assessment Emphasis**
The current assessment emphasis should be moved beyond simple operational confirmation to encompass confirmation of design and operational defense effectiveness. Such an assessment extension would provide evidence for sound assurance of the effectiveness of human error defenses on each application project.

- Characterization of Margins

Establishing and maintaining operating margins provides assurance that plant operating conditions remain distanced from operational or safety challenges. Where margins are employed, confirmation of actual operating values with design intent should be characterized during validation. This can provide an additional measure of design assurance and a means for longterm tracking changes in feature effectiveness prior to failure.

- Ongoing Performance Assurance

The most comprehensive demonstration of the degree to which equipment features, operating practices, and staff skills support achievement of operational objectives is through routine tracking of operational performance. Definition of objective measures and assessment criteria would allow system performance to be characterized over its service life, thus providing assurance the system remains supportive of achieving operational objectives in spite of ongoing operational changes. This would require an additional shift in validation emphasis from one-time, pre-operations limited tests to on-going operational experience tracking.

To re-confirm error prevention, detection and recovery effectiveness using routine operating experience would require collection of information on the types of errors that occur, their frequency and the degree of feature effectiveness in mitigating their challenge.

The examination of recordable operating events representative of major system performance challenges and breakdowns would not be sufficient for demonstrating the effectiveness of human error defenses. While the occurrence of events offer confirmation of instances of performance failure, the absence of events can not confirm the effectiveness of human error defenses without an understanding of the type and frequency of human error initiated challenges.

CONCLUSIONS

This paper has outlined some of the limitations with current industry validation practice, discussed two evolving validation challenges, and offered suggestions for improvements to validation practice. Validation in its current or enhanced form is expected to remain a key tool for demonstrating design confirmation in the nuclear industry.

ACKNOWLEDGMENTS

The author wishes to thank CANDU utility, design and regulatory staff who have shared their experiences, insights and concerns with respect to industry validation practice over the past ten years.

REFERENCES

1. Guide to Human Factors Verification and Validation Plans. Canadian Nuclear Safety Commission draft Regulatory Guide C-278, 2001 March.
2. J. O'Hara, W. Stubler, J. Higgins and W. Brown. Integrated System Validation: Methodology and Review Criteria. United States Regulatory Commission report NUREG/CR-6393, 1997 January.