Designing To Avoid Human Error Consequences

S.L.N. Chen-Wing and E.C. Davey
Atomic Energy of Canada Ltd., Canada

Abstract: AECL and CANDU utilities have developed a process for minimizing human error in plant operations and maintenance. Recent plant operational experience demonstrates that human error is a key contributor to operating inefficiencies, equipment damage, and significant plant events. To improve plant operation and safety, plant designers and utilities are placing renewed emphasis on approaches to prevent the occurrence and limit the effects of human error. One aspect of the multi-faceted approach to addressing error involves the choice of features that are incorporated into plant systems.

This paper discusses the systematic approach developed, outlines the principles and general process adopted for avoiding human error in design, and describes design solutions that are representative of specific application principles. It is expected that application of the recommended approach will result in plant designs with decreased risk of human error occurrence and consequence.

1. INTRODUCTION

This paper outlines a design strategy for minimizing human error in plant operations and maintenance. Current plant operational experience has demonstrated that human error is a key contributing factor to operating inefficiencies, equipment damage and significant plant events. To improve plant operation and safety, plant designers and utilities are placing renewed emphasis on approaches to prevent the occurrence and limit the effects of human error.

Addressing human error in a systematic way has become a utility priority due to evolving production and safety demands for (Heuertz and Herrin, 1997):

- Reduced probability of safety challenges,
- Increased capacity factors and production,
- Lower operations and maintenance costs,
- Increased tolerance of operational errors, and
- Increased assurance for protection of plant investment.

Recent operational experience and industry studies have consistently shown that human performance related problems, including human error are key contributing factors in about one half of all significant events at nuclear power plants (INPO, 1991). Current error occurrence and consequence rates have the potential to become limiting factors to further improvements in plant operations and safety.

As a consequence, a multi-faceted approach to addressing error is being practiced. Human error is best addressed with overlapping error occurrence prevention and reduction, and consequence prevention and reduction means. Such a layered defensive strategy is consistent with the "defense in depth" approach to safe operation, characteristic of the nuclear industry and other complex technical systems. One form of defense involves the feature choices made by designers that are incorporated into plant systems.

2. INTEGRATING HUMAN FACTORS INTO DESIGN

The development of specific guidance for addressing human error was undertaken as one component of a three year program to establish a generic approach to integrating human factors into plant design or design changes. The program was funded as a co-operative project among CANDU plant utilities and AECL. The objectives of the program were to:

- Develop generic approaches to the issue of human factors licensing concerns balanced with practical and cost-effective solutions, and
- Develop a process that utilities and AECL design staff can use to ensure the operational

effectiveness of plant and control center designs.

A broader description of the program, recommended design approach, and supporting guidance can be found in a previous conference paper (Feher, Davey, and Howard, 1995). Practical experience with application of the approach has been gained both in an operational assessment of a retrofit Critical Safety Parameter display system for the Ontario Hydro Pickering B station, and in the development, design, and regulatory review of a new control room for the CANDU 9 plant.

A sub-objective of the program was the development of guidance and tools that would assist designers in limiting the potential impact of human errors by controlling the sources of error and consequences of human error in system operation.

3. THE NEED FOR GUIDANCE

There are two reasons why guidance is required:

1. Human error is a key causal factor in plant events. If, as an industry, we are to improve safety and production, future plant designs and refinements must be designed to be more resilient to error occurrence and more accommodating of error consequence.
2. Formalizing good design practices for all designers to use leads to completeness and consistency in design practice.

3.1 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 and slips) 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 must be operated with the recognition that breakdowns in operation will occur as a result of human error. Thus, specific defenses in design, operations and personnel selection and training must be applied to minimize the occurrence and limit the consequences of human error. Equipment design and interfaces which minimize the potential for misunderstanding and control interference, and support recovery from errors, will promote reliable system performance.

3.2 A Review of Existing Human Error Guidance.

An initial review of the human error literature revealed an extensive discussion of the problem (i.e., types of human error, methods for predicting human error, and methods for analyzing designs and tasks for human error potential). Human error types and analytical methods are well documented (Reason, 1990; Kirwan, 1994; Kirwan and Ainsworth, 1992). The references cited are illustrative of previous work that is fairly complete in describing methods for predicting human error and for analyzing designs and tasks for human error potential. In contrast, we found little ‘solution oriented’ material covering: human error prevention and reduction principles, strategies and means for linking these tools to the existing design process, and concise summaries of design solutions that have demonstrated success in considering human error concerns. The best source of this material, that we located, was the work of Norman (1988). However, industry-relevant examples with the ties drawn to the design process were not available. To address this design guidance need a systematic approach to dealing with human error concerns during the design stage was established. This approach is consistent with the manner in which other design issues and uncertainties are addressed.

3.3 Role of the Design Guidance.

The design guidance developed consists of a set of design feature guidelines and a description of a

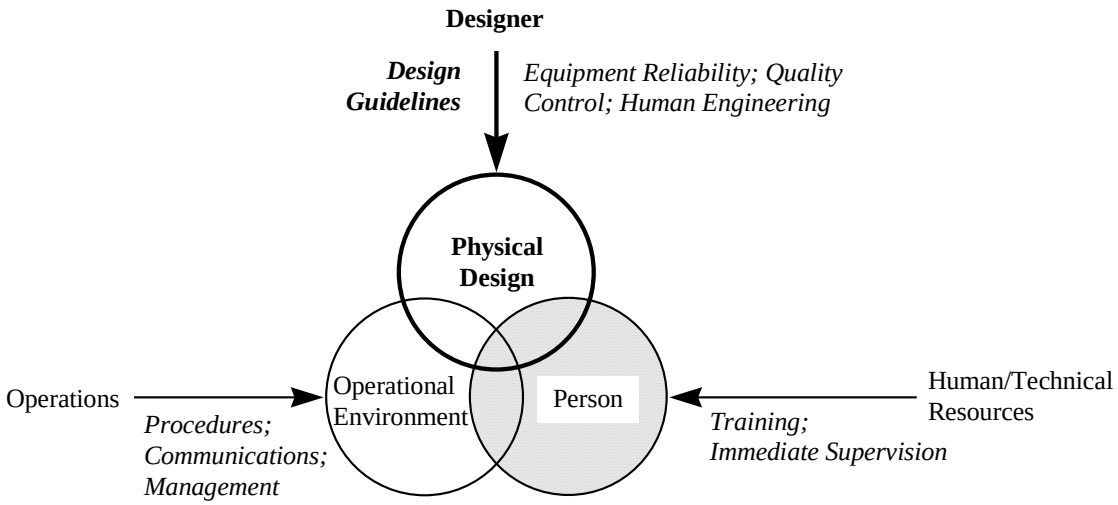

Figure 1: The designer's influence on human error in system operation.

process for how the guidelines may be applied in support of engineering design. The guidance organizes the findings and good practices from the literature and industry experience into a concise document, available for designer reference.

In reducing human error, designers represent one of three groups that provide error reduction measures, as indicated in Figure 1. Each group may apply specific error reduction, defensive practices, and features, associated with their domains of influence and consistent with overall system operational objectives. Designers are responsible for only one of the three areas, specifically equipment design. To improve the robustness of designs, designers have been encouraged to develop an awareness of the defensive mechanisms employed in the other two areas in order to ensure that design choices support and complement the human error defensive mechanisms applied within the operational environment and personal sub-system areas.
For example, common operational practices applied to reduce the incidence of human errors include:

- Monitoring Oversight
- Procedural Compliance
- Self Check Practice
- Independent Verification
- Three-Way Communication Strategy

In the personal sub-system area, examples of common practices applied to reduce the incidence of human error include:

- Personnel Selection
- Training
- Refresher Training
- Fitness for Duty

4. HUMAN ERROR GUIDANCE.

The design guidance developed consists of two forms: design principles and a three-step process for systematically addressing human error in design. The relationships between the guidance developed, human error occurrence and consequence in system operation, and conventional engineering design and design change processes are shown in Figure 2. The three-step process was mapped to the designers' existing design or design change process (that of the project or station).

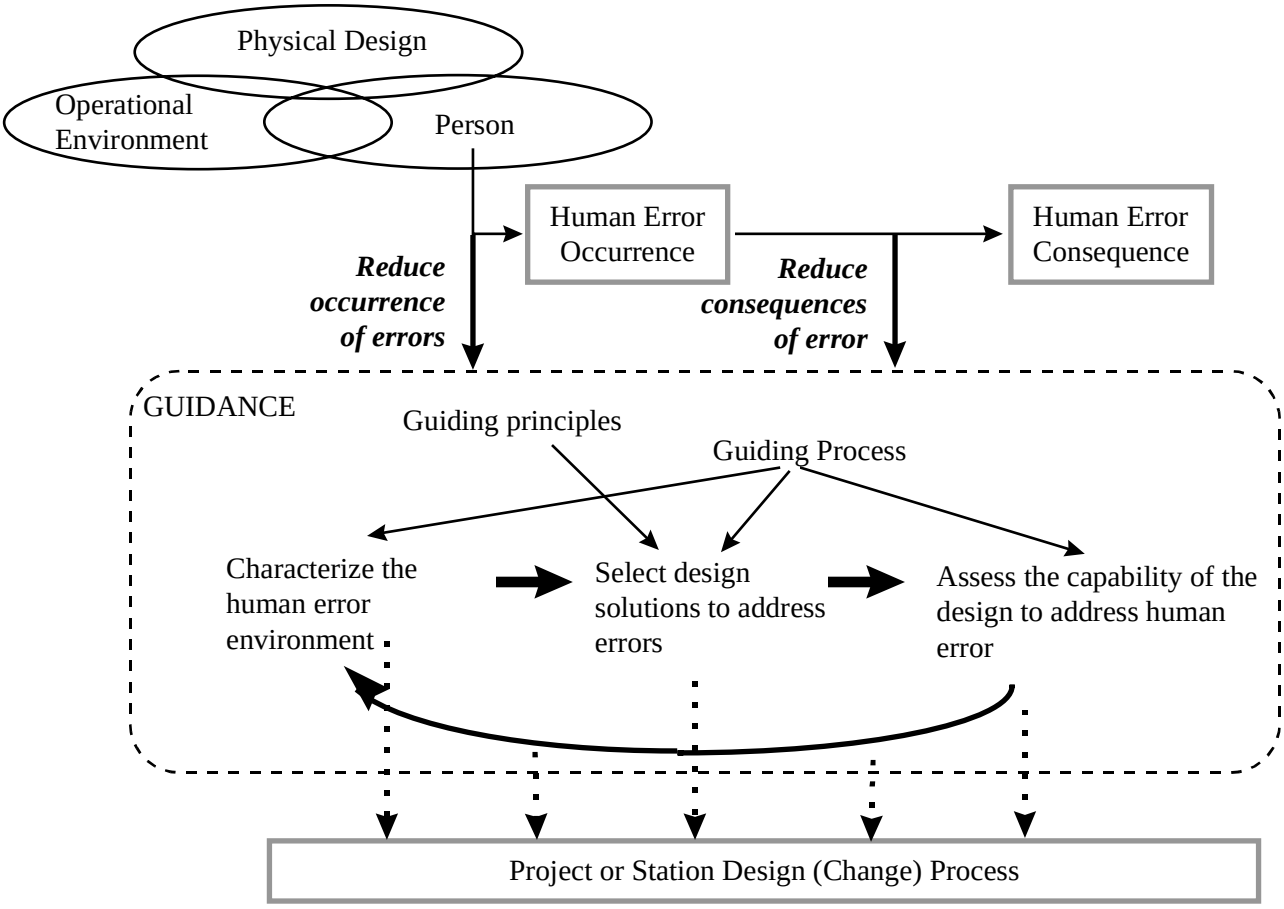

Figure 2: The role of guidance in addressing human error in design activities.

4.1 Guiding principles for addressing human error.

This section describes a number of principles which, if applied, can not only reduce the incidence of and consequence of human error but can result in more robust and understandable designs. These principles have been drawn from the work of several groups but most closely reflect a definition and organization developed by Norman (1983)

1. *Make goals and system state visible*—Interfaces should make accessible, information in a form so that system state can be easily related to system operational goals.
2. *Provide a good conceptual model*—It is important that operators be able to develop a good conceptual model of the plant systems from training, from the design of the interface between the operator and the plant, and from observations of system operation. The information from these three sources should be consistent and complementary to reduce the possibility of operating errors.
3. *Make the acceptable regions of operation visible*—Directly indicating the acceptable, unacceptable, and desired regions of system operation in process and state displays can act as a visual aid. This reduces dependence on user memory recall and the need for dynamic context dependent determinations. The adequacy of plant process state can thus be judged more readily against performance targets.
4. *Make process and automation behavior predictable*—Errors have a better chance of being detected if the normal behavior of plant processes and automation is predictable.

5. *Employ affordances*—Apply design features that visibly convey the possibilities for action.
6. *Make the options for functional control visible*—Errors in planning and action execution can be minimized if controls are visible so that the possibilities and limits for action are known.
7. *Provide appropriate feedback*—Always provide feedback for an operator's actions. Feedback can take many forms. As a minimum, feedback should convey the impact of the operator's action on the overall state of the system.
8. *Ensure a close relationship between a control and its function*—To reduce the demand on an operator's memory, there should be a clear relationship between the location and mode of operation of a control and its function.
9. *Build-in constraints*—The user's actions should be limited to acceptable ranges of control possibilities to guard against errors.
10. *Make error recovery easy*—Given that errors will occur, the system should be forgiving and allow the operator to readily detect and recover from these errors..
11. *Make interfaces consistent*—Consistency (and standardization) allows users to apply existing knowledge to new tasks, This reduces the burden of interface characteristics that must be learned and remembered. Minimizing the secondary tasks associated with task performance can reduce the incidence of operating error.

4.2 Addressing human error in the design process.

This section outlines a three-step process for addressing human error which can be incorporated into the design process (see Figure 3).

4.2.1 Characterize the human error environment.

To address human errors, one first needs to characterize their potential for occurrence and consequence for the operating situations encompassing system operation. Characterizing the human error environment involves:

- Identifying operational and design requirements,
- Determining operational and functional context for system operation and possible human error occurrence,
- Understanding the operator's needs in support of task performance, and
- Evaluating the human error potential for the system operation and environment examined.

Information for the evaluation may be based primarily on either:

- Observation or operational experience (e.g., examination of past incidents and errors, observation of system operation, simulated system operation, walk-throughs, and talk-throughs), or
- Analytical prediction of anticipated events.

Adaptation of several analytical techniques from the human reliability field can assist in assessment of human error potential. Most techniques are based on

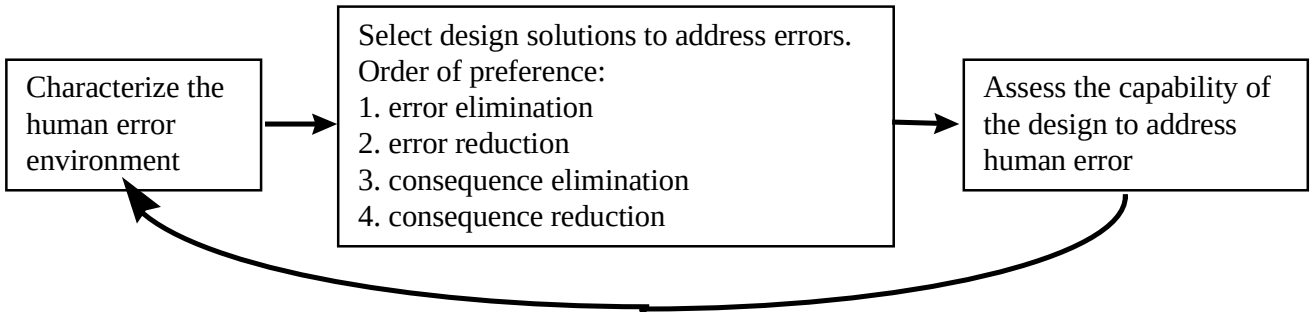

Figure 3: Process for addressing human error.

analysis of:

- Events (e.g., Barrier analysis, fault trees, event trees), or
- Task analysis (e.g., Hazard and Operability analysis, Technique for Human Error Rate Prediction).

These methods assist the designer in identifying potential human errors and in focusing on areas of weakness in designs.

4.2.2 Select design solutions to address errors.

Once the error environment is characterized, particular design solutions can be selected to achieve error reduction objectives. By matching expected error causing situations with appropriate design solutions, one can address potential human error occurrences or consequences.

A design solution strategy that preferentially deals with error occurrence first and error consequences second is recommended. Design solutions should be applied, in the order of preference as outlined below:

1. Eliminate Error Occurrence

This is the first preference, where design features known to be a source of human error are eliminated (e.g., lack of feedback, lack of differentiation, inconsistent or unnatural mappings). Design choices available for error elimination include:

- Replacement of error inducing design features (e.g., physical device separation, physical guards, application of validity and range checking).
- Restructuring of task so the error prevalent behavior is no longer performed (e.g., by information filtering, only the information needed for the task is provided).
- Automate to change the role of human involvement in support of task performance.

2. Reduce Error Occurrence

Consider this approach if complete error elimination is not possible or feasible through design choices. Design features which can reduce error occurrence include:

- Identification (e.g., device labeling).
- Affordances (i.e., visually convey acceptable choices).
- Constraints (i.e., build in constraints to limit operation to acceptable ranges).
- Coding (i.e., aid in choice differentiation and selection).
- Consistency.
- Feedback (i.e., convey device and system state directly in the interface).
- Predictability (i.e., design system responses so that operators can associate specific control actions with system response).

3. Eliminate Error Consequence

The third approach is to eliminate error consequences. There are three categories of design features that reflect the components of the consequence prevention strategy:

A. Error detection design features (to promote detection prior to consequence occurrence):

- Feedback (i.e., status information in relation to operational goals and potential side-effects of an action).
- Alert of Unacceptable Device States (e.g., visual/auditory feedback of off-normal or unacceptable device states).
- Confirmation (i.e., support of self checking and independent verification practices).
- Prediction (i.e., providing information on the outcome of an action prior to its implementation, or with sufficient time for correction).

B. Error recovery design features (to enable recovery prior to consequence occurrence):

- Undo (e.g., facilities for reversing recent control actions to allow promote error recovery).
- Guidance (i.e., alternative forms of guidance for cases where reversing a recent control action is not the preferred action).

C. Consequence Prevention Design Features

- Interlocks
- Margins and Delays (i.e., these features can provide more time to unacceptable consequence realization thus increasing the chances of error detection and recovery prior to consequence occurrence)
- Fail Safe Features

4. Reduce Error Consequence

If errors and consequences can not be completely eliminated, consider measures that enable consequence reduction. This may be achieved through application of additional design features that allow operators or automation to recognize the occurrence of an error consequence, and to take action to mitigate the consequences. Examples include:

- Margins (i.e., apply larger design margins to allow some consequences to be accommodated by normal system function and capacities).
- Engineered Mitigating Systems (e.g,, automatic special safety systems actions, such as CANDU Automatic Stepback and Setback).

  Human Intervention (i.e., operations team can readily adapt to both predefined and undefined operating situations).
- Response Teams (i.e., organizational structure is prepared and coordinated to deal with the predefined consequences).
- Consequence Prediction (e.g., aids can assist operations staff in predicting the extent of consequences of operating actions and assist in selection and execution of mitigating actions).
- Backup Replacement Function (i.e., provision of equipment and/or human intervention to mitigate consequences).

4.2.3 Assess the impact of the design and track operational performance.

The third stage of the process is the assessment of the impact of the selected human error defensive measures.

The scope of the plant and control center design to be assessed should be defined. Error-related issues should then be identified—the likelihood of particular error-occurring modalities, and the related design features. Error related issues are any changes or designs that could lead to a change in the likelihood of human error. The analytical techniques discussed in Section 5.2.1 may be applied at this stage again, now that the design exists.

Assessing the impact of designs (changes) on error can assist in reducing errors and consequences. This can be proactive or reactive. Both positive (error-reducing) and negative (error-increasing) characteristics should be noted.

The long term use of the system, as well as the immediate impact, should be tracked. This will help to determine new error modes that may develop, through system use, that warrant further design modification.

5. CONCLUSION

The methodology defined in this paper can assist designers in assessing the impact of a plant or control center design and supporting tasks, or to assess the impact of proposed design changes, on the potential for human error. Application of this recommended design approach leads to designs that are less error prone and are more forgiving of operational errors.

6. ACKNOWLEDGEMENTS

The development of human error design guidance was sponsored by the CANDU Owners Group under Project WPIR 1659. The authors would like to acknowledge the support and direction offered by

Sherry Howard, Carolyn McIntyre and Archie Campbell of the Ontario Hydro Pickering Nuclear generating station.

The authors would also like to acknowledge the contributions of Fiona Bremner.

7. REFERENCES

Feher, M., Davey, E., and Howard, S. (1995) *Increasing Operational Effectiveness and Reducing Regulatory Risk of Control Centre Changes.* Paper presented at the Second COG Computer Conference, Markham, Ontario, 1995 October 1-3.

Heuertz, S. and Herrin, J. (1997) *Human Error Prevention in the Nuclear Industry*, Seminar at the IEEE Sixth Conference on Human Factors in Power Plants, Orlando, Florida, 1997 June 8-13.

INPO (1991) *An Analysis of 1990 Significant Events*, Institute of Nuclear Power Operation report INPO-91-018. Atlanta, (GA):INPO.

Kirwan, B. (1994) *A Guide to Practical Human Reliability Assessment*, London (UK):Taylor & Francis.

Kirwan, B.I., Ainsworth L.K., Eds. (1992*) A Guide To Task Analysis*, London (UK):Taylor & Francis.

Norman D.A. (1988) *The Psychology of Everyday Things*, New York (NY):Basic Books.

Reason, J. (1990) *Human Error*, Cambridge (UK):Cambridge University Press.