ABB
ASEA BROWN BOVERI

May 29, 1992
LD-92-072

Docket No. 52-002

Attn: Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Subject: System 80+™ Human Reliability Analysis Methods

References: 1. ABB-CE Letter LD-92-038, March 25, 1992
2. ABB-CE Letter LD-92-064, May 8, 1992

Dear Sirs:

This letter transmits a description of the human reliability analysis methodology used in the Probabilistic Risk Assessment. This transmittal fulfills the Reference 1 commitment for submittal by May 31, 1992. Reference 1 also included a commitment to submit, by May 31, a description of how the PRA was used in the design process, but that description has already been submitted (Reference 2).

If you have any questions, please call me or Mr. Stan Ritterbusch at (203) 285-5206.

Very truly yours,

COMBUSTION ENGINEERING, INC.

C. B. Brinkman
Acting Director
Nuclear Systems Licensing

CBB/ser
cc: J. Trotter (EPRI)
T. Wambach (NRC)

ABB Combustion Engineering Nuclear Power

Combustion Engineering, Inc.
1000 Prospect Hill Road
Post Office Box 500
Windsor, Connecticut 06095-0500

Telephone (203) 688-1911
Fax (203) 285-9512
Telex 99297 COMBEN WSOR

D032 1/1

HUMAN RELIABILITY ANALYSIS METHODOLOGY

Introduction

The objective of the Human Reliability Analysis (HRA) for SYSTEM 80+ is to identify the critical operator actions in responding to accidents and transients, and to quantify the impact of failure to perform these actions on the probability of core damage. Since observational studies and simulator experiments can not be used to identify and quantify the sources of human error, for design certification the analysis will be based on existing plant data. These methodologies, however, will be used at a later stage of the System 80+ design and construction process to validate the results of this analysis.

System 80+ is an evolutionary plant design based upon the System 80 design. Therefore, the procedures and types of actions, e.g. opening and closing valves, are very similar to those required in currently operating plants. The ergonomic design of the controls and displays, however, will be different. This has a significant impact on the performance shaping factors that will be used in this analysis. Previous databases of human error probabilities have considered only the use of conventional types of technology. While the same types of error will exist in the advanced evolutionary control room, the error rates should be reduced. This is because a goal of the design is to reduce the possibility of human error by improving the design of the information presented to the operators.

The "Handbook of Human Reliability Analysis" (Ref. B) gives a table of "Estimated decreases in HEPs resulting from the application of good ergonomics practices to nuclear power plants." This table presents a series of factors with which the analyst can modify the accepted HEPs to take into account good ergonomic design. However, it is necessary to make clear that this is an expert judgement and not a factor necessarily backed up by some rigorous analysis. Since the use of the control room features will be essentially the same as in a conventional control room, expert judgement is considered acceptable.

One of the driving assumptions of this analysis is that the operators are performing, or think they are performing, in a manner that ensures the safety of the plant. Malevolent actions, for example, sabotage, will not be discussed (Ref A). The actions should conform to those in a procedure, or where deviations occur, it is because the operator, or the expert judge, believes that the actions performed instead are better than the actions prescribed in the procedure.

The HRA Team

The HRA team that was used for the SYSTEM 80+ HRA included people who have held, or hold, Senior Reactor Operator (SRO) licenses, people who have held Reactor Operator (RO) licenses, a human factors specialist with advanced formal training in Human Factors Engineering (HFE), engineers with intimate knowledge of the plant design, transient analysts and PRA engineers.

The HRA team used an iterative closed-loop process for this analysis. While the primary responsibility for the direction of the analysis lay with the Human Factors Specialist and the PRA engineers, each member of the team was involved in the review process so as to maximize the possibility for incorporation of each persons experience and knowledge, and to minimize the possibility of overlooking any aspect of the analysis.

Methodology

The basic methodology that was employed during this analysis is a version of the Systematic Human Action Reliability Procedure (SHARP) endorsed by the Electric Power Research Institute (Ref C). SHARP consists of seven separate steps that, when performed sequentially, and with full documentation, achieve a robust and reproducible analysis. The seventh step of SHARP is to document the HRA results. Since this is an intrinsic part of the entire analysis, this step is incorporated in every aspect of the

procedure.

The six steps of the procedure are:

Step 1 (Definition)	From the event trees and supporting documentation, the HRA team develops a comprehensive qualitative description of the human interactions for each initiating event.
Step 2 (Screening)	The human interactions are screened, using expert judgement, in order to identify the most important human interactions that directly mitigate, or contribute to, core damage.
Step 3 (Breakdown)	Each key interaction, identified at step two, is broken down into the goal, and the tasks and subtasks which are required to achieve that goal.
Step 4 (Representation)	The subtasks and tasks are then explicitly modelled to identify the actions that the operator may take, the errors of commission and omission, and the associated performance shaping factors that may impact that action, such as level of knowledge, stress, level of experience, ergonomic design etc.
Step 5 (Impact Assessment)	The impact of these errors is then evaluated and added to the system logic trees, similar to step 2
Step 6 (Quantification)	The Human Error Probabilities (HEPs) are evaluated

and added to the PRA

STEP 1

The first part of step 1 is to review the initiating events. This allows the team to familiarize themselves with the plant and the possible design differences that have been incorporated into System 80+ that may affect operation (e.g. the placement of the Refueling Water Storage Tank inside containment). The next part of step 1 is to identify and qualitatively describe the actions taken by the operators to mitigate these events. This is done to identify all the interactions that the operators have with the system. This description is not as detailed as a Task Analysis but could potentially provide the basis of a qualitative link analysis for use later in the HRA or in the design activities.

The Combustion Engineering Emergency Procedure Guidelines (Ref D) were the primary input to this stage of the analysis. These are a set of generic Emergency Procedure Guidelines that were generated from many man-years of operating experience. They describe the mitigation strategies that should be used for Nuclear Power Plants that utilize a Combustion Engineering Nuclear Steam Supply System. They are intended to be the basis for plant specific technical guidelines from which the emergency operating procedures will be written. These guidelines make no reference to specific setpoints but describe a strategy that is appropriate for System 80+. They refer to generic systems that are aspects of CE's design. Where the redesign of a system caused a change in the usage of that particular system, this was identified. The qualitative descriptions reflect expert judgement as to the use of these new features of System 80+ and the improvements therein.

Chapter 15 of CESSAR DC provides the analysts with analyses performed on the response of the system 80+ design to particular transients. These provided more

detailed information about the response of the plant to the various transients.

Another important source of information that was used extensively is the design documentation available for Nuplex 80+, the advanced control complex design for System 80+. These documents defined the control panels, the layout, the information presentation methodology and the control design. This information is vital in order to understand the operating philosophy and to identify the potential sources of human error. A prototype was available to give the analysts a visual aid with which to evaluate certain actions.

These sources of information are vital as they are used to establish the reason that an operator would perform a particular action. This "motivation" or purpose behind each of the actions gives the analyst an insight into the possible "errors of commission" that may occur.

Once these actions have been identified, the analysts must pursue the interactions by classifying them into one of five different categories. The 5 different types of human interactions are:

Type 1 is defined as:	Interactions consisting of testing and maintenance actions that improve or degrade system availability.
Type 2 is defined as:	Interactions that initiate accidents.
Type 3 is defined as:	Interactions that involve the success or failure of following rules/procedures.
Type 4 is defined as:	Interactions that aggravate the accident situation.

Type 5 is defined as: Interactions that consist of recovery actions.

Type 2 human interactions are assumed to be covered within the initiating event frequency data. Therefore this HRA methodology does not deal with Type 2 human interactions. Type 1 human interactions can be quantified separately from the procedural mitigation actions and are considered in step 5 and 6 of this methodology. The methodology described here deals primarily with Types 3, 4 and 5 human interactions. For the purposes of this discussion type 4 is treated as special case of type 3 as all the actions taken should or will be associated with some form of procedure. Type 5 interactions are those associated with the recovery of a particular system, e.g restoration of A.C. power.

These classifications aid in the later stages of the analysis since these bring direct bearing on the action's impact on analysis. Once these elements are identified, the analysts move on to step 2.

STEP 2

The number of human interactions that can come from the step 1 is potentially huge. Not all of these interactions have a direct implication for core safety. Some have implications for investment protection with respect to equipment damage. Others can potentially lead to a return to normal operation. The procedures in use today try to mitigate the accident and to do so in a way that will preserve the plant for a return to normal operation, if possible, and also to retain certain of the safety systems undamaged by the accident.

Screening is a very important part of the HRA process in that it allows the analysts to reduce the number of human interactions that are analyzed to those that potentially affect the safety of the plant. Screening allows the analysts to concentrate their efforts on the analysis of the key interactions.

The technique that has been chosen is called Judgmental Screening. This facilitates the introduction of expert judgement of operations staff early into the HRA process. Expert judgement is used to identify the actions taken by the operators that will ultimately lead to, or directly mitigate, core damage. The introduction of expert judgement and operator experience at this level of the analysis, while under the direction of the HR analysts, brings a level of validity to the screening process that would otherwise be absent if one of the more quantitative methods were employed. That is, the mathematical methods may achieve the same or similar results. However, judgmental screening allows operations staff experience to evaluate which action would actually be the most important, and reflect the kinds of trade-offs that actually happen in a real-life accident situation.

For each of the actions identified in step 2, steps 3 and 4 will be performed together and provide its own feed-back loop to ensure that every possible task within that action is addressed.

STEP 3

Once the appropriate human interactions have been identified, the break down of these interactions into tasks, and subtasks, affords the analyst more insight into the contributors of error. Each of the human interactions is probably, prior to this step, described in high level terms. For example, the operators will initiate safety injection at the ESF panel. This interaction contains a myriad of smaller tasks and subtasks, associated with verifying the line up of the safety injection valves, verifying that available inventory exists, manually actuating the momentary actuation switch that switch on the pumps and verifying that, after all of this is done, safety injection is actually working the way it should be. In the System 80+ plant control room, most of this may be taken care of by intelligent symbol representations. That is the intelligence designed into the data processing system will be able to display an aggregate symbol that will represent the operation of safety injection within alarm limits. But procedures will probably require

the operator to back up these indications by verifying everything with the discrete indicators.

Once the breakdown has been completed, performance shaping factors can be identified. These are factors that influence the performance of a human interaction with respect to error. These factors can be quantified and provide a means to modify the Human Error Probability (HEP) to produce a number more appropriate for the particular situation. The performance shaping factors that are used for this methodology are:

Availability of necessary indication
Accuracy of indication
Training
Workload
Annunciated
Stress/Arousal
Level of Experience
Quality/availability of procedures
Ergonomic design of display/control

STEP 4

The objective of this step is to select and construct the most appropriate representation for the tasks and subtasks that were the output of step 3. Of the various options available to the analysts, it was decided to use a combination of Operator Actions Trees (OATs) and Human Reliability Analysis trees (HRA trees). The representations should reflect a qualitative logic structure within which the analysts could identify potentially important successes and failures. These can be analyzed and quantified for their impact on the system logic.

Typically it has been difficult to evaluate errors of commission. It is easy to postulate

many possible different actions that could be performed instead of the correct act but these need to be justified given the indications and the motivation that the operator may have at a particular time. A by-product of the representations is the ability to identify this class of human errors known as "acts of commission". These are the alternative actions that could be performed given the stimuli and information available at the decision-making stage. These can potentially be the cause of more errors and have their own class of omission errors.

A technique that has been employed when appropriate is the "confusion matrix". This method allows the diagnosis portion of any task to be represented as a matrix. If the available indications can lead the operator to diagnose the state of the system as being one state when it actually another this can lead to a whole group of actions which may aggravate the situation. For example a small LOCA, under some conditions, can be mistaken for a steam line break. The confusion matrix gives a rationale for representing operator actions which stem from the response to the wrong accident.

STEP 5

The identification of the human interactions may have new implications for the system's analysis. At this point in the procedure, these new impacts are assessed with respect to the systems analysis. The representations of the previous steps, especially the OAT, may describe alternate operator actions that could impact the frequency of core-damage based on the systems response to the operator actions.

Type 1 human interactions, associated with test and maintenance errors, are incorporated into the event trees by the PRA engineers. These errors affect the availability of systems that are either automatic, and used in the accident mitigation, or manual and utilized by the operator. Therefore they are part of the original systems analysis.

The output of this step is a revised set of system event and fault trees. These should

incorporate the operator actions and possible acts of commission, that lead alternatively to success and failure. These may incorporate changes in the assessment of dependencies, system reliabilities or sequence quantification.

STEP 6

One of the main goals of PRA/HRA is to quantify the probability that the operators will fail to perform the critical actions (i.e. to determine the human error probability).Literature on the subject (Ref A and Ref) suggests that the best source of human error frequency data comes from simulator studies on a plant specific simulator. This is not feasible for design certification for System 80+. Therefore generic industry data was used. The data sources used include "The Handbook of Human Reliability Analysis (Ref B), The NUCLARR database (Ref E) and existing PRAs.

Since the control room is an evolutionary design, i.e. fundamentally the operating characteristics should be the same but the hardware and the "look and feel" have been updated and improved, the types of errors should be the same. If the types of error are the same then, assuming that this error has certain components to it, the components should be same but their magnitude may be different. For example, if the probability of reading a display incorrectly is 10^{-3} , some proportional of this may be attributed to the assumed visual acuity of the operator, another proportion to the ergonomic design of the display and the rest to the type of data being monitored. For a redesigned meter the components will be the same but the magnitude will be different. There a correctional factor would be used to make this number appropriate for use with the new display.

This is the argument used to justify the use of correctional factors to take into account the ergonomic design of the control room. It is just this approach used for the quantification of human error for Nuplex 80+ and System 80+.

Each of the branches in the trees that have been developed at Step 4 has an error

associated with it. These are modified by the Performance Shaping Factors that have been identified in step 3, including those for the improved control room ergonomics. The various failure paths can then be evaluated and these are then added to evaluate a total probability of failure (or success).

Reference

A. Bell, B.J. and Swain, A.D. "A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants" NUREG/CR-2254

B. Swain, A.D. and Guttman, H.E. "Hand Book of Human Reliabilify Analysis with Emphasis on Nuclear Power Plant applications" NUREG/CR-1278

C. Hannaman, G.W. and Spurgin, A.J. "Systematic Human Action Reliability Procedure (SHARP)" EPRI NP-3583

D. "Combustion Engineering Emergency Procedure Guidelines" Prepared for the C-E Owners Group, CEN-152.