THE 4TH INTERNATIONAL TOPICAL MEETING ON
NUCLEAR THERMAL HYDRAULICS, OPERATIONS AND SAFETY
April 6-8, 1994, Taipei, Taiwan

HUMAN RELIABILITY ANALYSIS IN SUPPORT OF A LEVEL 1 PRA FOR SURRY DURING MIDLOOP OPERATIONS

J. C. Lin, D. C. Bley
PLG, Inc.
4590 MacArthur Blvd., Ste. 400
Newport Beach, California 92660-2027
(714) 833-2085

T-L Chu
Brookhaven National Laboratory
Dept. of Advanced Technology
32 Lewis Ave., Bldg. 130
Upton, Long Island, NY 11973
(516) 282-5730

SCOPE

The objectives of this Level 1 probabilistic risk assessment (PRA) are to evaluate the important accident sequences initiated during midloop operations and to compare the qualitative and quantitative results with those for accidents initiated during power operations. The primary types of human actions analyzed in this study involve the dynamic operator actions and recovery actions that take place during the accident sequence following an initiating event. Two parts of the human actions were analyzed: failure to diagnose and failure to perform the action.

The scope of the Level 1 PRA for Surry during midloop operations includes internal, fire, and flood initiating events. The major categories of dynamic operator actions taken during the accident sequence following an initiating event are: providing makeup to the reactor coolant system (RCS), restoring residual heat removal (RHR) cooling, establishing steam generator reflux cooling, establishing primary feed and spill, establishing gravity feed from refueling water storage tank (RWST), establishing high pressure recirculation, establishing recirculation spray, and cross-connecting RWSTs. All categories are not applicable to all initiating events and all plant operating states (POS).

DIFFERENCES BETWEEN SHUTDOWN CONDITIONS AND POWER OPERATIONS

To evaluate human actions in the shutdown conditions, the following important differences from the power operation case must be recognized. Due to the different decay heat levels, the time windows available for operator diagnosis and action performance are different if the timings of accident initiation relative to the reactor shutdown time are different. This implies that the operator performance may be different for the same action responding to the same event initiated at different times after shutdown. For the same reason, greater times are available for recovery actions. Because of the relative lack of instrumentation and emergency procedures and the need to consider possibilities for loss of containment integrity that are unique to plant shutdown conditions, there is a greater uncertainty in the behavior of the operators. Due to the many operator actions involved during the accident response to events initiated in shutdown conditions, more dependencies may exist among the preceding and subsequent actions.

SURRY DESIGN AND PRACTICE

Surry has implemented administrative and response procedures for shutdown conditions, and a training program for operators. The plant has loop isolation valves, which permit draining a loop for maintenance without maintaining drained conditions in all three loops. Plant policy is to minimize time drained to midloop. If extensive reduced inventory work is required, the plan is to off-load the core.

The RHR system provides no other service (such as safety injection) and is completely inside containment. No automatic trip function is provided for the RHR isolation valves so a major cause of interruption of cooling at other plants is eliminated. Two independent, permanently installed level systems are provided. One is a standpipe with local indication by flags on the standpipe. The other is an ultrasonic sensor on one loop. Both are monitored and alarmed in the control room. The RHR pump piping and valves are configured so that if one pump vortexes and becomes air bound, the other pump remains flooded. After level is restored, the pump lineup can be shifted from the control room, and the standby pump can be started without first venting the air bound pump.

- **SURRY PLANT PROCEDURES AND TRAINING**

The keynote procedure for shutdown conditions is AP-27.00, "Loss of Decay Heat Capability." According to plant personnel, this procedure has been in the plant for 4 years, and the operators have performed simulator drills for shutdown conditions, including midloop operations, for that entire time.

The procedure follows the standard Westinghouse Owners Group format of defining the entry conditions (initiating events), then sequentially diagnosing the event and restoring stable conditions. Loss of inventory problems are addressed first, followed by other causes for interruption of cooling. Restoration is orderly: first, trying to recover normal modes of RHR cooling; next, checking time until boiling, protecting personnel, isolating containment, and trying steam generator cooling (reflux cooling if drained); and, then, moving on to feed and spill, use of a charging pump from the opposite unit, and gravity feed.

The operators are well trained on this procedure. The simulator drill scenarios and critiques were reviewed. The operators train on all of the basic scenarios that were analyzed. In addition, they have a sense of the potential importance of these actions and indicate that they would not wait long in a configuration that failed to yield the expected temperature reduction. The procedure is based on vendor and utility thermal-hydraulic analyses for shutdown conditions.

Additional procedures apply during shutdown. There are general operating procedures that guide cooldown, depressurization, and draining operations. These provide detailed requirements for maintaining control of the shutdown machine. There are special procedures, such as OC-28, "Operational Check, Assessment of Maintenance Activities for Potential Loss of Reactor Coolant Inventory," and a reduced inventory checklist that provide special guidance for reducing the chance of loss of cooling events when RCS maintenance can lead to reduced inventory conditions. Other procedures have been expanded to provide a focus on shutdown conditions. For example, in AP-40.00, "Non-Recoverable Loss of Instrument Air," if the unit is shut down on RHR, the first step requires use of a portable air bottle and fitting to reopen the containment isolation valves in the component cooling water system that supplies the RHR heat exchanger. We found the bottles and fitting in the Appendix R locker, as expected.

Similarly, the blackout, loss of AC power, loss of intake canal level, main control room isolation, and fire procedures provide important guidance.

SURRY PLANT OPERATIONAL STAFFING

Crew staffing for the two-unit plant includes the following:

— **Three to Four Senior Reactor Operators (SRO).** At least one SRO is required in the control room at all times; usually, two will be there.

- One Shift Supervisor (SRO) for both units.
- Two to three Assistant Shift Supervisors (SRO).

— **Four to Five Licensed Reactor Operators (RO).** Three in the control room and one to two outside; after shutdown, a second RO is shifted to the shutdown plant.

— **Eight Auxiliary Operators (AO).**

— **One Shift Technical Advisor (STA).** The STA is assigned to licensing, not operations. STAs are not licensed. They take the same licensed operator requalification training (LORT) and testing. STAs perform calculations (shutdown margin, mass balance, etc.) and know technical bases for operations; e.g., ultrasonic level detector, critical safety function monitoring, etc.

During Alert or higher emergency action levels, the Technical Support Center (TSC) must be called to action. Approximately 15 to 20 people staff the TSC, including the plant superintendent, the emergency manager, and four or five department heads. During the daytime, the center is manned within about 15 minutes; at other times, when people must be called in, less than 1 hour is required. A review of plant procedure EPIP-1.01, "Emergency Action Level Table (Tab A) System Shutdown, or Assessment System Shutdown," indicates that, for cold shutdown conditions as midloop, the TSC will be called to duty for the following conditions:

— Unavailability of secondary system cooling capability.

— Loss of service water or component cooling or RHR.

— RCS T> 140°F.

QUALITATIVE AND QUANTITATIVE ANALYSIS

A variety of methods have been used to quantify the reliability of operators in responding to accidents and in carrying out procedures. All of these methods demand a substantial effort to describe qualitatively the full scenario facing the operator, the use of judgment based on experience, and care with regard to dependencies. Due to the unique conditions associated with the shutdown operations (e.g., unusual and changing plant configuration, accident response actions not specifically covered by procedures, training, and simulator exercises, lack of appreciation for hazards during shutdown, etc.), heavy reliance on experience-based expert judgment is required. Since the success likelihood index method (SLIM) provides a structured methodology for applying judgment consistently,[1, 2] it has been considered to be especially applicable to shutdown events analysis. This methodology is based on the assumption that the likelihood of operator error in a particular situation depends on the combined effects of a relatively small set of performance-shaping factors (PSF) that influence the operator's ability to accomplish the action. PSFs account for both the plant conditions, or scenarios, under which the action must be performed, and the psychological and cognitive state of the individuals performing the action. To permit a direct ranking of the contributors to human error, the rating scale used must increase as the likelihood of failure increases. Therefore, a failure likelihood index (FLI) method (i.e., an adaptation of the SLIM) is used in this analysis.

The approach to evaluating human actions and recovery actions that follow an initiator is to, first, qualitatively define the event scenario, required action, important factors affecting operator performance, and the consequences of the action not being successful. Relatively detailed qualitative descriptions of all relevant information that could affect operator performance were prepared. This is because such actions are beyond direct experience and relevant statistical data. Therefore, most practical estimates of human error rates (HER) are strongly influenced by the experience and judgment of the experts performing the analysis. It is essential that these experts base their evaluations on the most complete and accurate descriptive information available. Table 1 gives an example page of these qualitative descriptions.

Then, a set of seven PSFs were selected to characterize the most important elements that affect the successful completion of the operator actions. These factors include preceeding and concurrent actions, plant interfaces, time adequacy, availability of procedures, task complexity, training and experience, and stress level. These seven PSFs cover most conditions that the operator is expected to encounter. Because of the decreasing decay heat levels, timing of the accident scenario initiation is very important to the time available for operator response or recovery actions during the transient prior to core damage and significant radioactive material release. These time windows are based, in large part, on the thermal-hydraulic analyses that have been performed for Surry in the Pressurized Water Reactor (PWR) Low Power and Shutdown Accident Sequences Program. They were considered for both diagnosis and action performance.

The qualitative evaluations of the actions and the important factors that affect operator performance were used to derive the HERs. To quantify the HERs, the PSFs were rated in the following two ways: a weight that ranks the relative importance of each PSF for influencing the reliability of the human action, and a score that rates the degree to which the PSF helps or hinders the operator to perform the action. For each action evaluated, an FLI is obtained by summing the product of the preceding weight and score for each PSF. This numerical index represents the overall belief of the positive or negative effects of the PSFs. It is converted to an HER for the action by assuming that it follows the relationship

$$\log_{10}(\mathrm{HER}) = (a * \mathrm{FLI}) + b$$

where a and b are calibration constants obtained by evaluating well-defined actions with "known" or "accepted" error rates from analysis for other PRAs. The calibration procedure ensures that the error rates are realistic and consistent with available data, observed human behavior, and the results from comparable expert evaluations of similar activities.

A ranking of contributors to the human error rate is accomplished by multiplying the weight of the PSF by the numerical score of the PSF. Because the score increases as the failure potential increases, the product of the weight and the rating becomes a direct measure of the relative contribution of that PSF to the human error rate of that action. The uncertainties of the HERs are estimated from the uncertainties in the ratings of the PSFs and the uncertainties associated witl the calibration tasks.

Table 2 illustrates a sample calculation of the HERs. For example, action code A-F1AR6-XHE-S-8 addresses the operator action to establish the steam generator reflux cooling following a loss of RHR due to water damage to all 4-kV and 480V buses by a large turbine building flood during midloop operation in a refueling outage. The weights assessed for the seven PSFs are 4, 2, 4, 2, 4, 4, and 3. These weights were normalized and presented along with the action scores in Table 2. In accordance with the relationships discussed in the preceding, the FLI and the HER were calculated to be 7.22 and 0.22, respectively.

RESULTS AND FOLLOW-UP ANALYSIS

The results of this study indicate that the dominant cause of core damage is operator failure to mitigate the accidents. This is primarily because, during shutdown operations, most of the automatic actuation features for accident mitigation are disabled, very few procedures are currently available for accident mitigation, and a significant fraction of the mitigation equipment is removed from service. However, due to the long period of time during which a potential shutdown accident sequence may be initiated, significant uncertainty and conservatisms are involved in the analyses of plant thermal-hydraulic and operator responses. A a result, there is a very large uncertainty in the human error probabilities used in this study.

In a follow-up phase of this study, a refined approach that defines several time intervals after shutdown to better account for the decay heat level at which the initiating event occurs is used. It is shown that the dynamic operator actions taken in response to shutdown initiating events depend much more on the time interval during which the initiating event occurs than on the types of outage (i.e., refueling outage and drained maintenance outage) and the POSs; i.e., 6 and 10 for midloop operations.

REFERENCES

1. D. E. EMBREY, "The Use of Performance Shaping Factors and Quantified Expert Judgment in the Evaluation of Human Reliability: An Initial Appraisal," Brookhaven National Laboratory, prepared for the U.S. Nuclear Regulatory Commission, NUREG/CR-2986, May 1983.

2. D. E. EMBREY, et al., "SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment," Brookhaven National laboratory, prepared for the U.S. Nuclear Regulatory Commission, NUREG/CR-3518, Vols. 1-2, March 1984.

Table 1. Example Page of Qualitative Descriptions of Dynamic Human Actions Evaluated for the Surry Shutdown PRA

SRA(B,3,4,5)R6:

Operator establish steam generator bleed and feed (reflux cooling) following a loss of RHR at mid-loop in POS 6 of refueling.

PRECEDING EVENTS

- 4 days since reactor shutdown.
- Loss of RHR due to
  - over-draining (RA),
  - failure to maintain RCS level (RB),
  - unrecoverable RHR failure (R3),
  - operating RHR train failure (R4), or
  - recoverable RHR failure (R5).
- For the action event of establishing SG reflux cooling, Operators have successfully diagnosed that a loss of RHR has occurred and referred to 1-AP-27.00 (Loss of Decay Heat Removal Capability).
- Restoration of RCS level has failed (for RA(B)R6-XHE-S-16) or Restoration of RHR cooling has failed after successfully restoring level (for RA(B,4,5)R6-XHE-S-9).

INDICATIONS OF PLANT CONDITIONS

- Low RCS level (for RA(B)R6-XHE-S-9(16)), restored RCS level (in the event of failure to restore RHR cooling; for RA(B)R6-XHE-S-9)), and slowing decreasing RCS level.
  - Control room RCS standpipe level 1-RC-LI-100A (may not be accurate if RCS boiling starts).
  - Control room cold shutdown RCS level narrow range 1-RC-LR-105.
    (ultrasonic indication of RCS level within the loop, i.e., from middle to top of the loop; may be partially unavailable if vital bus is unavailable)
  - RCS standpipe level local indication.
  - Shutdown cooling low level annunciator B-C-8.
- RHR pump motor amperage oscillation (for RA(B)R6-XHE-S-9(16)).
- Excessive RHR pump noise (for RA(B)R6-XHE-S-9(16)).
- No RHR flow
  - Control room RHR flow indication 1-RH-FI-1605.
  - RHR heat exchanger low flow annunciator B-C-6.
- Incore thermal couples for RCS temperature monitoring (may be partially unavailable if vital bus is unavailable).

PROCEDURAL GUIDANCE

- 1-AP-27.00 Loss of Decay Heat Removal Capability
  - Steps 26, 27, and 28 and Attachment 5, Part 4: Maintain SGs near 33% NR level and dump steam using SG PORVs or main condenser to control RCS temperature.

TRAINING AND EXPERIENCE

- Operators train on this scenario during simulator drills.

CONCURRENT ACTIONS/COMPETING FACTORS

- Restoration of RCS level (for RA(B)R6-XHE-S-9(16)).
- Restoration of RHR cooling (for RA(B,4,5)R6-XHE-S-9).

INDICATION OF SUCCESSFUL COMPLETION/IMPACT OF SUCCESS

- SG pressure is stable or slowly decreasing.
- SG level is slowly decreasing if water is not feeding into the SGs.
- WR hot leg temperatures are stable or slowly decreasing.
- WR cold leg temperatures are at saturation for SG pressure.
- RCS level is stable.
- Successful decay heat removal is established.

IMPACT OF FAILURE/ADDITIONAL CUES

- *SG pressure is increasing if steam dump is unsuccessful.*
- SG level is decreasing if no water is provided to the SGs.
- As RCS heats up RCS temperature increases; loss of subcooling and alarms.
- Boiloff would lead to decreasing RCS levels.

TIME CONSTRAINTS

- At 4 days into the outage, boiling would occur within about 21 minutes and core uncovery could occur as early as 144 minutes.
- Establishing SG reflux cooling should only take a few minutes if instrument air and semi-vital bus are available and if providing water to the SGs is not necessary.

Table 2. Example Page for PSF Ratings and HERs for Flood Initiating Events

Action Code	Preceding & Other Actions Weight	Preceding & Other Actions Score	Plant Interfaces Weight	Plant Interfaces Score	Time Adequacy Weight	Time Adequacy Score	Procedures Weight	Procedures Score	Complexity Weight	Complexity Score	Training & Experience Weight	Training & Experience Score	Stress Weight	Stress Score	FLI	P(fail)	LOG(P(fail))
Rated Actions																	
MAX															7.87	1.0E+00	0.00
D-F1AR6-XHE	0.00	1	0.24	5	0.18	10	0.12	2	0.12	5	0.24	5	0.12	9	6.00	1.3E-02	-1.89
D-F1AR10-XHE	0.00	1	0.24	5	0.18	5	0.12	2	0.12	5	0.24	5	0.12	8	5.00	1.2E-03	-2.91
D-F1AD6-XHE	0.00	1	0.24	5	0.18	10	0.12	2	0.12	5	0.24	5	0.12	10	6.12	1.7E-02	-1.77
D-F2AR6-XHE	0.00	1	0.24	4	0.18	8	0.12	3	0.12	4	0.24	3	0.12	7	4.71	6.2E-04	-3.20
D-F2AR10-XHE	0.00	1	0.24	4	0.18	5	0.12	3	0.12	4	0.24	3	0.12	6	4.06	1.4E-04	-3.86
D-F2AD6-XHE	0.00	1	0.24	4	0.18	9	0.12	3	0.12	4	0.24	3	0.12	9	5.12	1.6E-03	-2.79
D-F3R6-XHE	0.00	1	0.24	5	0.18	9	0.12	3	0.12	5	0.24	4	0.12	9	5.71	6.4E-03	-2.19
D-F3R10-XHE	0.00	1	0.24	5	0.18	5	0.12	3	0.12	5	0.24	4	0.12	8	4.88	9.4E-04	-3.03
D-F3D6-XHE	0.00	1	0.24	5	0.18	10	0.12	3	0.12	5	0.24	4	0.12	10	6.00	1.3E-02	-1.89
A-F1AR6-XHE-S-8	0.17	9	0.09	8	0.17	7	0.09	4	0.17	5	0.17	7	0.13	10	7.22	2.2E-01	-0.66
A-F2AR6-XHE-F-4	0.20	7	0.10	6	0.15	6	0.10	4	0.10	8	0.20	5	0.15	9	6.45	3.7E-02	-1.44
A-F2AR10-XHE-F-4	0.21	7	0.11	6	0.11	4	0.11	4	0.11	8	0.21	5	0.16	8	6.11	1.6E-02	-1.79
A-F2AD6-XHE-F-3	0.19	7	0.10	6	0.19	8	0.10	4	0.10	8	0.19	5	0.14	9	6.81	8.5E-02	-1.07
A-F2AR6-XHE-G-5	0.19	9	0.10	6	0.14	7	0.14	4	0.10	6	0.19	5	0.14	10	6.81	8.5E-02	-1.07
A-F2AR10-XHE-G-4	0.19	9	0.10	6	0.14	5	0.14	4	0.10	6	0.19	5	0.14	9	6.38	3.1E-02	-1.51
A-F2AR6-XHE-GR-4	0.16	9	0.08	7	0.16	8	0.12	5	0.16	8	0.16	6	0.16	10	7.72	7.1E-01	-0.15
A-F2BR6-XHE-S-8	0.18	8	0.09	8	0.18	6	0.09	3	0.14	3	0.18	7	0.14	10	6.59	5.1E-02	-1.29
A-F3R6-XHE-S-8	0.18	9	0.09	8	0.18	6	0.09	3	0.14	3	0.18	7	0.14	10	6.77	7.8E-02	-1.11
MIN															0.00	1.1E-08	-7.98
Calibration Actions																	
NSAC84: DE1-LC	0.09	2	0.18	6	0.18	3	0.18	4	0.09	2	0.18	2	0.09	2	3.27	1.0E-05	-5.00
NSAC84: MC4-LOCA	0.09	6	0.18	3	0.18	8	0.18	8	0.09	6	0.18	9	0.09	8	6.91	1.0E-01	-1.00
NSAC84: RT1-LOCA	0.11	3	0.11	4	0.22	5	0.11	5	0.11	0	0.22	4	0.11	2	3.56	1.0E-04	-4.00

X Coefficient 1.0138
Std Err of Coef. 0.1767

Regression Output:

Constant	-7.98
Std Err of Y Est	0.506
R Squared	0.971
No. of Observations	3
Degree of Freedom	1

Legend:

D - Diagnosis
A - Action Performance
R6 - 1st Midloop Operation during Refueling Outage
R10 - 2nd Midloop Operation during Refueling Outage
D6 - Midloop Operation during Drained Maintenance
F1A - Large Turbine Building Flood
F2A - Large Aux Building Flood with RWST
F2B - Large Aux Building Flood without RWST
F3 - Large Safeguard Area Flood
R - Restoration of RHR
F - RCS Feed and Spill
S - SG Reflux Cooling
G - RWST Gravity Feed
GR - Additional Recovery during Gravity Feed