BNL-NUREG--44385

DE90 010013

# THE IMPORTANCE OF HUMAN PERFORMANCE AND PROCEDURES IN LIMITING SEVERE ACCIDENT RISKS

By

James C. Higgins
Engineering Technology Division
Brookhaven National Laboratory
Upton, NY 11973



Prepared for Presentation at

American Institute for Chemical Engineers
Spring 1990 Health and Safety Symposium

Safe Procedures and Accident Prevention in Chemical Industries
Session 7

January 1990

UNPUBLISHED

# 1. OVERVIEW OF HAZARDOUS INDUSTRIES

Modern technology has created a number of potentially hazardous industries, such as the nuclear and the chemical industry. Individual plants in such hazardous industries are designed using the principle of "defense in depth" and are fitted with various redundant safety features(1) to protect against and mitigate accidents. Due to the nature of the technology and the many safeguards that have been incorporated into these industries, the plants are often quite complex. As a result of all the safeguards built into the plants, multiple failures must occur before significant adverse consequences could develop. An often held view, particularly by plant operators, is that severe accidents with adverse consequences will not happen. However, failures at these plants, particularly human and management type failures, are often interdependent and can fail multiple safeguards at the same time.

The defense in depth and redundancies built into modern complex industrial plants can be effective in protecting against severe accidents. However, proper and safe operation requires vigilance on several organizational levels such as: the company that operates the plant (e.g., utility or chemical company), the corporate oversight, and the regulators. As vigilance drops, overconfidence can develop, and plants may no longer strive for good performance. In this situation, certain factors arise, which predispose a plant for a major accident. Once enough of these factors are present, all that is needed is an appropriate (and often trivial) initiating event to begin the sequence of events leading to the accident.

*This work was in part sponsored by the U.S. Nuclear Regulatory Commission.

## 2. MAJOR ACCIDENTS IN HAZARDOUS INDUSTRIES

As one examines selected major accidents from hazardous industries in retrospect, the factors which were present to "set up" the accident can be identified. Also, there are often key decisions and actions taken during the course of the accident (after the initiating event) which exacerbate the event and take one further along the path toward significant consequences. These actions, that were taken by the plant operators, can also be identified by analyses of the accident, after the fact.

Three of the significant accidents that have occurred in the chemical and nuclear industries in the last decade, were reviewed (see Appendix A) to identify these key issues which first of all predispose the plant to an accident, and secondly, those factors that provide the impetus to continue the accident along its course. The issues or factors seemed to fall naturally into four areas: Design, Organization and Management, Maintenance, and Operations (Human Performance). The first three areas are those that generally occur before an initiating event and predispose the plant to the accident. The Operations area includes human performance actions that occur both before and during the accident. It is important to note, however, that even the during-accident actions are heavily influenced by training provided, and procedures written, before the onset of the accident.

Appendix A to this paper provides the breakdown of the major causal factors for the three selected accidents: Three Mile Island, Bhopal, and Chernobyl. These were developed from a number of reports (2-15) issued on the

accidents. Naturally, there is some disagreement among experts as to the most important causes of the accidents. Also, no attempt was made to include every quoted cause or to prioritize the causes or factors. Chernobyl was interesting and different than the other two in that the design and operations factors were so significant that no maintenance problems were necessary to create the severe accident.

## 3. PROBABILISTIC RISK ANALYSIS

Besides post-accident analysis of real events, another method for determining the susceptibility to risk of complex industrial plants is through probabilistic risk analysis or PRA. These analyses are being used more often for U.S. nuclear power plants (NPPs). Regarding the four key areas affecting accidents that were noted above, current PRAs can reasonably address three of them: Design, Maintenance, and Operations (Human Performance). Research is currently underway at Brookhaven National Laboratory to determine the effect of Organization and Management issues on a PRA.

A PRA is a comprehensive, integrated analysis of the plant, systems, components, and the personnel who operate the plant. In the PRA, failure probabilities are assigned to equipment based on data analysis. The human actions which are modelled in the PRA as human errors are also quantified via a Human Reliability Assessment (HRA). HRA methods have continuously improved over the last decade, but are still somewhat subjective and uncertain.

Regarding the three key areas affecting accidents that PRAs do address, consider first plant design. A PRA can illustrate design weaknesses in a plant and provide insights into effective design improvements. A PRA also can identify the important plant safety features, which could then be verified to have no design errors. Second, consider the area of maintenance. PRA importance or sensitivity analyses can be used to illustrate the risk importance of having certain key components or systems out of service for maintenance. This is useful in scheduling and prioritizing maintenance in the plant.

The third area affecting accidents is operations or human performance. PRA sensitivity analyses also can be used to show the overall importance to risk of human actions and to identify those particular actions which are most important. Toward this end, BNL has performed three studies over the last several years (16, 17, 18) to determine the sensitivity of risk to human error and to develop insights relative to the results. These studies have primarily used core melt frequency (CMF) and accident sequence frequency as the risk measures. The results have shown that CMF is quite sensitive to human error, but that both the baseline CMF and its risk sensitivity vary noticeably between plants. Interesting and different results were obtained regarding the risk increase from degraded human performance and the risk decrease from enhanced human performance. Also, insights were developed into the areas that may benefit from improved human performance and improved human action modeling in the PRA.

## 3.1 Overall Sensitivity

The most recent of the three sensitivity studies completed by BNL was for the LaSalle PRA, currently being completed by SANDIA National Laboratories for the U.S. NRC. LaSalle is a recent vintage Boiling Water Reactor (BWR). The PRA model contained 83 human errors. BNL established somewhat conservatively large ranges over which the human error probabilities (HEPs) would be varied. Figure 1 shows the effect on CMF as all HEPs were increased or decreased together by a constant factor (not to exceed an HEP = 1.0).

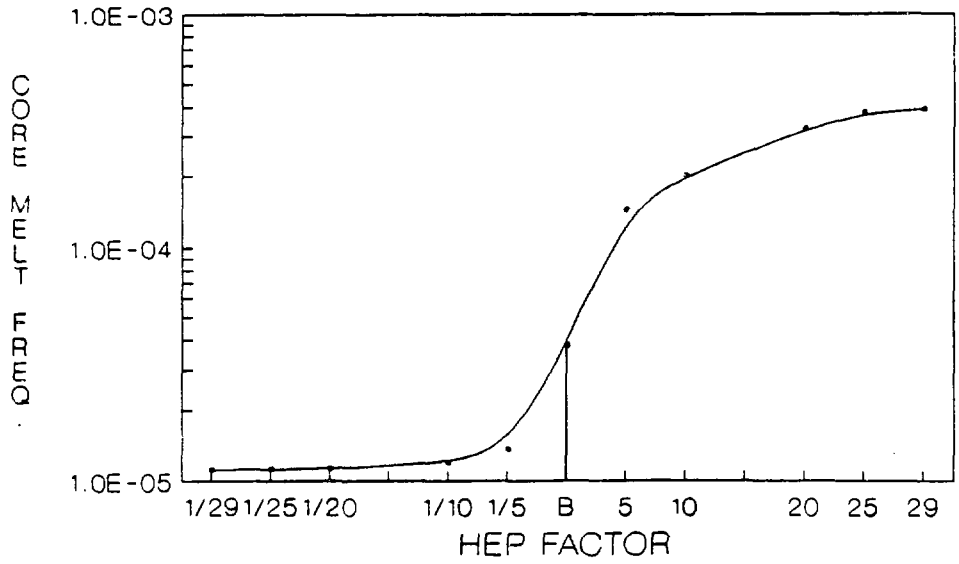
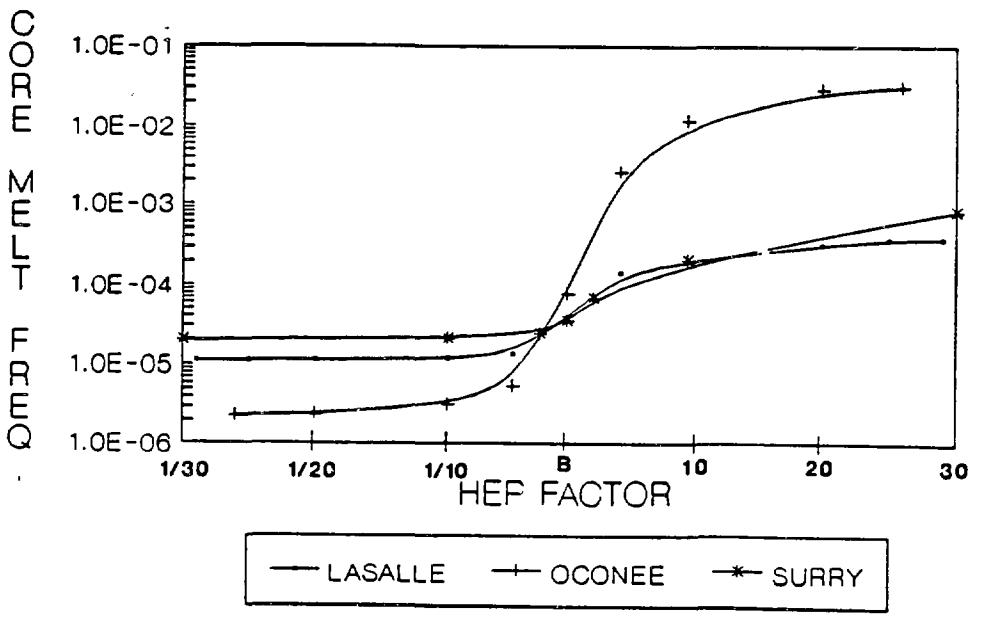



Figure 1. Overall CMF sensitivity to human error at LaSalle

Overall CMF at LaSalle varies about one and one-half orders of magnitude, as the HEPs vary over their full range. Most of the variation in CMF, however, occurs when HEPs are varied by a factor of only 5. Thus, we see that CMF can increase noticeably if HEPs were to degrade due to some common cause factor. Part of the reason for the CMF rise flattening out is due to many of the HEPs reaching a ceiling of 1.0. Likewise, we see that lowered HEPs, for

example, due to enhanced human performance, will lower the overall CMF, although the change is not as significant as in the increasing HEP direction.

The two other plants analyzed were Pressurized Water Reactors: the Surry plant (using the original WASH-1400 PRA) and the Oconee plant (using the 1984 NSAC-60 PRA). Figure 2 shows the sensitivity results from all three studies on one plot, even though the PRA and HRA models were quite different and the method of determining the ranges over which HEPs were varied was also slightly different.




NOTE: PRAs and studies had differences.

Figure 2. CMF sensitivity - LaSalle/Oconee/Surry

Of the three plants, Oconee shows by far the greatest sensitivity, about four orders of magnitude in CMF. Oconee also, however, modeled the most human errors of the three plants (223 errors). Currently, work is underway at BNL to determine the causes of the large difference in sensitivity between Oconee

and LaSalle (e.g., plant design, PRA model, HRA model, etc.). All the plants do show a notable effect on risk (CMF) as HEPs are varied.

## 3.2 Categories of Human Performance that Contribute to Risk Sensitivity

The human errors appearing in the PRA were coded in various categories such as: personnel, timing of error, location, activity, etc. This categorization allowed an analysis, which only varied the HEPs of specific types of errors. This is more realistic than varying all HEPs together and also shows which types of errors affect risk most significantly. Figure 3 shows the analysis for the category "timing of error" at Oconee. In this analysis, errors were classified as "pre-accident" (such as valves mispositioned or miscalibration) and "during-accident" (such as failure to manually initiate High Pressure Injection or failure to recover Feedwater). This figure shows that the risk is predominantly sensitive to the during-accident errors.

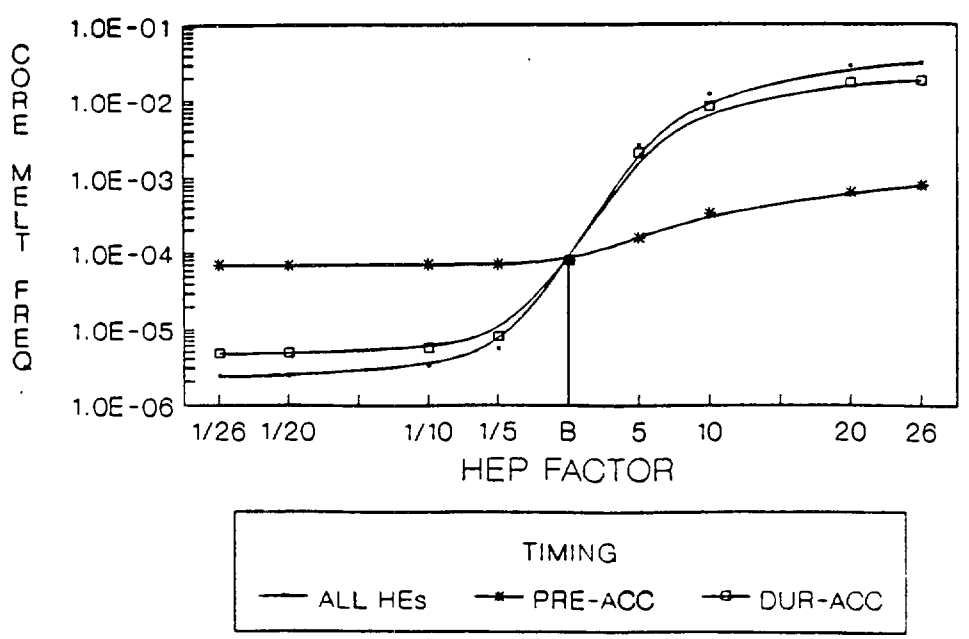



Figure 3. CMF sensitivity at Oconee - timing category

Results from other sensitivity studies on the categorized human errors for the Oconee and LaSalle plants produced the following insights:

- Recovery actions, which are a subset of the during-accident errors, are particularly important. Recovery actions involve efforts to recover and return to service failed components or systems.

- Operations-related errors dominate the risk. Qualitative analyses also determined that the specific operations errors identified would best be addressed by improved procedures and operator training.

- Errors by both licensed reactor operators (ROs) and non-licensed auxiliary operators (NLOs) were important. Particularly important errors were complex recovery actions, involving both ROs and NLOs. This points out the importance of good team or shift performance, good shift communications capabilities, clear procedures, and training in accident mitigation efforts.

These results would allow one to focus efforts into fruitful areas for improvement of human performance which would in turn limit risk. The analyses identified particular errors that were important and which could be addressed by procedures and training. Areas where improved modelling would be beneficial can also be identified. The results, however, should be used with some

caution since only a few plants have been analyzed with these techniques and PRA models are quite plant specific.

## 4. CONCLUSIONS

Due to the defense in depth concept and redundancy in safety systems utilized, complex industrial plants, such as nuclear power plants (NPPs) can be operated safely. This capability has been demonstrated by many years of safe operation by numerous NPPs in the U.S. and abroad. However, the occurrence of severe accidents has also demonstrated that constant vigilance in a number of areas is necessary to ensure continued safe operation. The areas noted as particularly important are Design, Organization and Management, Maintenance, and Operations (Human Performance).

Detailed PRA sensitivity analyses were performed for three different NPPs to determine the overall importance to risk of human performance and the relative importance of different types of actions. These calculations have shown that overall risk is very sensitive to human performance, particularly as performance degrades. Specific types of actions found to be important were: actions taken during the course of an accident, operations unit actions, actions to recover failed equipment, and actions of both licensed reactor operators and non-licensed auxiliary operators. The primary methods of ensuring successful operator performance throughout all of these types of actions is through operator training and via good procedures for the accident situation. Detailed analyses of this nature for chemical facilities should also prove beneficial. However, one should not be left with the impression

that a PRA is a panacea for catastrophe prevention. Rather, a PRA is only one element of a complete risk management program that is very useful for identifying appropriate areas for safety improvement.

## 5. REFERENCES


1) Safety Series No. 75, INSAG-3, "Basic Safety Principals for Nuclear Power Plants," IAEA Nuclear Safety Advisory Group.

2) P. Shrivastava, "Bhopal: Anatomy of a Crisis," Ballinger, Cambridge, Massachusetts, 1987.

3) Chemical and Engineering News, "Bhopal - Special Report," December 2, 1985.

4) High Technology, "Beyond Bhopal: Toward a 'Fail-Safe' Chemical Industry," Gordon Graff, April 1985.

5) "Investigation of Large-Magnitude Incidents: Bhopal as a Case Study," Adhok S. Kalelkar, Arthur D. Little, Inc., May 1988.

6) Newsday, December 30-31, 1984, and March 21, 1985.

7) "Sources of Common Cause Failures in Decision-Making Involved in Man-Made Catastrophies," Edwin L. Zebroski, EPRI.

8) IEEE Spectrum, "Special Report: Designing and Operating a Minimum-Risk System," June 1989.

9) Nuclear News, Special Report "Chernobyl: The Soviet Report," October 1986.

10) B.A. Semenov, "Nuclear Power in the Soviet Union," IAEA Bulletin Vol. 25, No. 2, June 1983.

11) NUREG-1250, Revision 1, "Report on the Accident at the Chernobyl Nuclear Power Station," December 1987.

12) NUREG-1251, Final Report, "Implications of the Accident at Chernobyl for Safety Regulation of Commercial Nuclear Power Plants in the United States," 2 volumes, April 1989.

13) John G. Kemeny (Chairman), "Report of the President's Commission on the Accident at Three Mile Island," October 1979.

14) Mitchell Rogovin (Director), "Three Mile Island, A Report to the Commissioners and to the Public," January 1980.

15) NRC Investigation Report Number 50-320/79-10, "Report of Special Investigative Team from NRC's Office of Inspection and Enforcement of Accident at TMI-2," October 25, 1979.

16) NUREG/CR-1879, "Sensitivity of Risk Parameters to Human Errors in Reactor Safety Study for a PWR," June 1981.

17) NUREG/CR-5319, "Risk Sensitivity to Human Error," April 1989.

18) NUREG/CR-5527, "Risk Sensitivity to Human Error in the LaSalle PRA," February 1990.

## APPENDIX A

## CATEGORIZATION OF CAUSAL FACTORS FOR THREE MAJOR INDUSTRIAL ACCIDENTS

### Major Causal Factors

**Accident: Three Mile Island (TMI)**

Design

- Poor human factors design of Control Room for accident situation including alarms, instrumentation, controls. Some examples are Power-Operated Relief Valve (PORV) indication, sump indication, core thermocouples, and radiation monitoring.
- Insufficient attention to small break loss of coolant accidents (SLOCAs).
- Inability to deal with large amount of hydrogen generated.
- Babcock + Wilcox (B+W) design very sensitive to transients (e.g., once through steam generators).

Maintenance

- Power-operated relief valve (PORV) leakage for months before accident.
- Iodine filters in poor condition.
- Condensate polisher problems - led to initiating event.
- Out of calibration and out of service equipment; for example, feedwater block valves closed.
- Multiple equipment problems (on key equipment) in prior 6-month to accident.

Organization and Management

- Mindset that serious accident could not happen.
- Assumed compliance with NRC regulations assures safety.
- Procedures and training for normal transients sufficient.
- NRC and industry focussed on design as opposed to operations and operations experience.
- No training for solid pressurizer with SLOCA out of top (led to securing high pressure injection).

Accident: TMI
(Continued)

- Poor feedback of operating experience (e.g., Davis-Besse accident).
- Never less than 52 alarms lit in control room during normal pre-accident operation.

Operations (Human Performance)

Pre-accident

- Need for improved Emergency Operating Procedures (deficient LOCA and pressurizer procedures).
- No good status on shift turnover in control room. RCS unidentified leakage > 1 gpm (technical specification limit) for six days before accident.

During-accident

- Failure to isolate stuck open PORV (even when tail pipe temperature >130°).
- Securing of High Pressure Injection (HPI).
- Did not recognize saturation conditions in core.

Accident: Bhopal

Design

- Many paths for water entry to Methyl Isocyanate (MIC) tank.
- Scrubber and flare tower designed only for process vent, not runaway reaction.
- Scrubber operation was manual, not automatic.
- Water curtain had insufficient pressure to reach release point.
- No safety instrumentation/alarms on MIC tank.
- Site communication depended on messengers.

Maintenance

- MIC tank chiller OOC for months.
- Flare tower shutdown for repairs.
- MIC tank leaks (meaning water and impurities could enter).
- Maintenance practices had potential to allow water entry to MIC tank.

Organization and Management

- Many, many major problems.
- Little corporate attention to plant.
- High personnel turnover, low morale, union problems.
- Lack of emergency procedures and plans.
- Toleration of negligence.
- All operators and supervisor on tea break together around accident time.
- Instrumentation unreliable.
- Culture at plant at time of accident led to need of plant operators to initiate cover up of accident.

Accident: Bhopal
(Continued)

Operations (Human Performance)

- Sensed small MIC leaks early on night of accident, but took insufficient action.
- Tank 610 (MIC tank) filled to 75-80% vice <50%.
- Vent gas scrubber in standby for over a month before accident.
- Turned off MIC release alarm that would warn community.
- Practices allowed contamination of MIC.

Accident: Chernobyl

Design

- No containment.
- Positive reactivity coefficient (from voids).
- Rods on initial insertion added positive reactivity.

Maintenance

- No maintenance factors noted in reports.

Organization and Management

- Little or no training on simulator or for accident situations.
- Culture that adherence to procedures not needed.
- No safety review of test procedure.
- Little or no management control over test.

Operations (Human Performance)

- Reducing operational reactivity margin below limit by pulling rods.
- Operation at too low and unstable power levels.
- Excessive water flow in core.
- Blocked automatic scram signals (from turbine generators, water level, steam pressure).
- Switched off Emergency Core Cooling System (ECCS) and blocked them from operations for nine hours.