Journal of Hazardous Materials, 15 (1987) 123-135
Elsevier Science Publishers B.V., Amsterdam — Printed in The Netherlands

RISK ASSESSMENT: CONTROLLING HAZARDOUS MATERIALS

CAROLYN D. HEISING

Department of Industrial Engineering and Information Systems, Northeastern University, 360 Huntington Avenue, Boston, MA 02115 (U.S.A.)

(Received April 1986; accepted September 1986)

Summary

Recent events such as the Bhopal chemical plant accident in India and the Chernobyl nuclear plant accident in the Soviet Union have demonstrated that technologies have the potential to release hazardous materials to the environment with catastrophic consequences. This paper discusses probabilistic risk assessment (PRA), and suggests that this methodology can be useful in the regulatory arena. This conclusion is based both on previous experience (e.g. the Reactor Safety Study) and growing interest in the methodology from many different sectors, including regulatory agencies such as EPA, NASA, OSHA, and NRC, the military, in addition to the private sector, such as insurance companies. Since human error is a major contributor to accident risk in large technologies, this paper also discusses at some length how such error may be quantified in risk assessments, as well as how risk may be reduced through improved management practices. Finally, regulatory developments in this area, and future directions for change, are also highlighted.

I. Introduction

Recent events have shown that our society is increasingly faced with many issues in controlling the risks of technologies, particularly those technologies with the potential to release hazardous materials into the environment. Whether these materials be in the form of radioactive fission products, as in the case of nuclear power plants, poisonous chemicals, as in the case of most chemical plants, or explosive mixtures, as in the case of rocket engines, these materials and the technologies that produce and/or utilize them must be regulated in such a way as to minimize the hazard to workers and the public alike [1].

Fortunately, the rise of these potentially hazardous technologies has also been accompanied by the concurrent rise of engineering analysis methods for safety estimation and design improvement. These methods include reliability analysis tools, such as fault and event trees, failure modes and effects analysis (FMEA tables), reliability block diagrams, in addition to other methods [2–4].

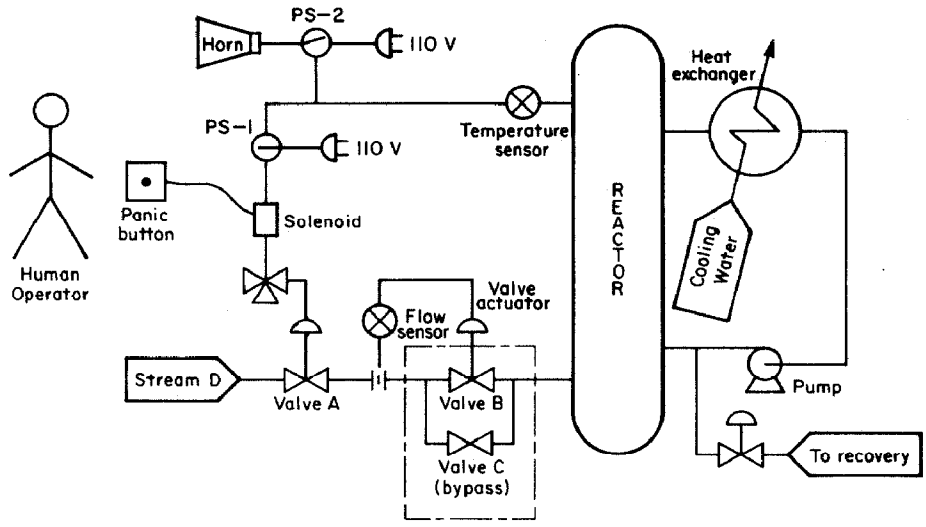

Fig. 1. Schematic diagram for chemical reactor system [8].

Moreover, new methods of risk analysis are being developed that increase our understanding of technological systems [5–6].

In this article, we focus on examples where risk analysis study results have affected the design of engineering facilities. The treatment of human error is particularly highlighted, since most major accidents in technological facilities have involved a significant degree of human error [1]. Finally, the impact of risk assessment in the regulatory process is discussed, and conclusions follow.

II. A tutorial in risk assessment — the chemical reactor

One might ask how can we design our facilities so as to reduce the probability of catastrophic accidents. The methodology of probabilistic risk assessment (PRA) permits us to design our plants safely, and can be used in conjunction with probabilistic safety goals to enchance public safety [7].

For example, consider the chemical reactor system shown in Fig. 1. Suppose we wish to conduct a realiability–risk study on this plant for purposes of quantifying the level of safety inherent in the design. We may wish to do this for many reasons, one being that this plant may be under regulatory review. If we can demonstrate that the current design meets a regulatory standard, we may be free to continue operating the system. If not, we may need to redesign (or modify) the system so that it *does* meet regulatory standards.

To perform the risk study, we use fault tree analysis, a procedure widely used in risk assessment [4]. One of the significant accident scenarios we envision in this system is one where the reactor catastrophically "runs away" and

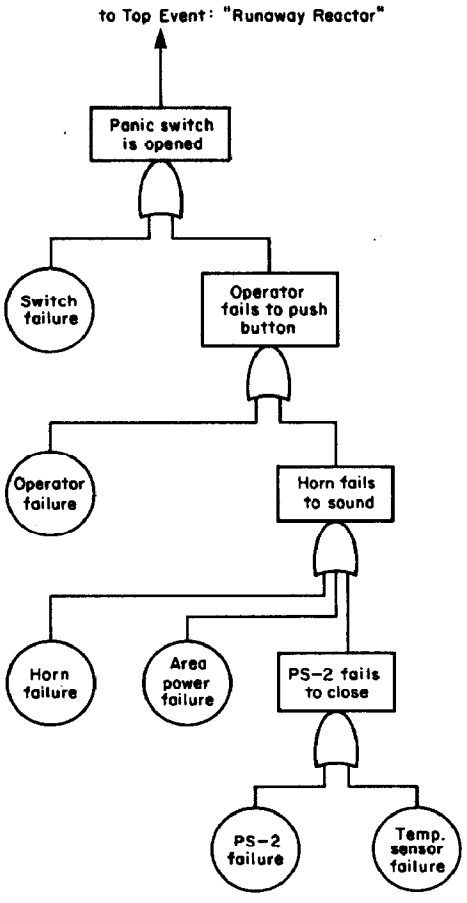

Fig. 2. Inclusion of human error in fault tree analysis.

explodes, releasing any hazardous chemicals that may be contained inside.* In such a scenario, the human operator becomes a significant "component" of the system in that he is responsible for a series of actions that must take place in order to prevent a catastrophic release. As is shown in Fig. 2, it is possible to place the operator failure directly into the fault tree. In order to quantify the fault tree, it is necessary to assign a value to the probability of human error. This leads us to our next topic — human error models and data.

*In this hypothetical chemical reactor, the temperature increases with the feed rate of the flow-controlled stream D. Heat is removed by water circulation through a water-cooled exchanger. Normal reactor temperature is 200°F (93°C), but a castastrophic runaway will start if this temperature reaches 300°F (149°C). In view of this situation: (i) the reactor temperature is monitored, (ii) rising temperature is alarmed at 225°F (107°C) with a horn that annunciates this problem to the operator, (iii) an interlock shuts off stream D at 250°F (121°C) stopping the reaction (see solenoid and valve A in Fig. 1), and (iv) the operator can initiate the interlock by pushing the panic button.

III. Human error models and data

Previous studies have shown that the human contribution to system failure can be large [1, 9, 10]. System safety analyses can evaluate the impact of human errors by appropriate modelling techniques [11, 12]. Human error data, though sparse and soft, do exist for quantifications and evaluations.

It is perhaps useful to begin with an explanation of basic terms applicable to human error analysis: (i) human engineering–human factors, describes the discipline concerned with designing machines, operations, and work environments so that they match human capacities and limitations, (ii) man–machine system and interfaces, denotes a system in which people have a monitoring and–or control function; interface refers to points of interaction between people and components in a system, (iii) human reliability, is the probability that a job or task will be successfully completed by personnel at any required stage in system operation — the probability of successful performance of the human activities necessary for either a reliable or an available system. Included in this definition is the probability that a system-required human act, task or job will be completed successfully within a required period of time, and (iv) human reliability analysis, a method by which human reliability is estimated.

In addition to these basic definitions, it is useful to identify five major categories of human error: (i) error of omission — a person fails to perform the task or part of the task, (ii) error of commission — a person performs the task step incorrectly, (iii) extraneous act — a person introduces some task or step that should not have been performed, (iv) sequential error — a person performs some task or step out of sequence, and (v) time error — a person performs the task or step within the allotted time, either too early or too late.

The general method for analysis and quantification of human performance consists of: (i) identification of all interactions of people with systems and components — the "man–machine interfaces", (ii) analysis of these interfaces to see if they are adequate to support the tasks that people have to perform, (iii) identification of potential problem areas in equipment design, written procedures, plant policy and practice, people skills, and other factors likely to result in human error, (iv) decisions on which problems have sufficient potential impact on the system to warrant changes, (v) development of candidate solutions for the problems, and (vi) evaluation of the estimated consequences of these changes to ensure that they will improve system reliability and safety and that no additional serious problems will result from them. This procedure is called "man–machine systems analysis" [11].

There are three types of probability that are important in performing an analysis of human error: (i) basic human error probability (BHEP), (ii) conditional human error probability (CHEP), and (iii) joint human error probability (JHEP). The BHEP is the probability of a human error on a task which is considered as an isolated entity unaffected by any other task. The CHEP is

the probability of human error on a specific task given failure, or success, on some other task (five levels of dependence are defined in the human reliability handbook: zero, low, moderate, high and complete dependence). The JHEP is the probability of human error on all tasks which must be performed correctly to achieve some end results (this is the probability of most interest in reliability work and is determined by using both BHEPs and CHEPs).

The most useful human error data is actuarial — human error probabilities (HEPs) of the known number of errors of a given type divided by the number of opportunities for that error to occur:

$$\text{HEP} = \frac{\text{Number of errors of a given type}}{\text{Number of opportunities for the error}} \quad (1)$$

If a data-based estimate is not available, an estimate derived from information on similar tasks can be used if the tasks are similar in terms of the types of human behaviors involved. The HEP per hour can be obtained if required; for most availability calculations, the interest is in the probability of at least one error per task per hour [11].

The human reliability model (or technique for human error rate prediction (THERP)) was developed at Sandia in 1964 to estimate the quantitative influence of human failure on the reliability of nuclear weapon systems and components [11]. Applications of the model have involved estimates of the probabilities that system-required tasks will be executed correctly within specific time limits. There are other human reliability methods and models, but none of them have had as much extensive practical application. The steps in THERP are to: (i) define system failures of interest (these pertain to system functions which may be influenced by human errors and for which error probabilities are to be estimated), (ii) list and analyze the related human operations, (iii) estimate the relevant error probabilities, (iv) estimate the effects of human errors on the system failure events (this step usually involves integration of the human reliability analysis with a system reliability analysis), and (v) recommend changes to the system and recalculate the system failure probabilities, an iterative process.

III. Stress and the lognormal distribution in human reliability studies

The distribution of the logarithms of the human error probabilities for various tasks is often normal. The rationale for this assumption is that performance of skilled persons tend to "bunch up" toward the lower human error probabilities.* Data supports the use of a lognormal distribution for the per-

*Use of the lognormal is common place in reliability studies, since the long tail of the skewed distribution provides for "conservatism" in the calculations of systems reliability [3,4]. This provision is of particular significance for human reliability calculations, as more uncertainty pertains to these quantitative estimates of human performance [11].

formance of skilled people. In one study, an analysis of human performance data revealed lognormal type distributions for simple tasks and slightly skewed distributions approaching the normal for more complicated tasks [11]. A lognormal distribution was reported in a British study of the time taken to respond to a simulated alarm signal superimposed on normal tasks in a nuclear power plant [11]. In an unpublished followup study in Danish research reactors, similar results were found [11]. The parameters of the applicable lognormal distribution are, of course, speculative. Swain hypothesizes that for most tasks, a lognormal probability density function (pdf) with a standard deviation of 0.42 would provide a suitable fit [11]. This standard deviation four-to-one was obtained by assuming a range ratio between the 95th and 5th percentile on the dimension of error probabilities. Swain concludes that, for human reliability analysis of operations, the assumption of normal, lognormal, or other similar distributions usually will make no significant difference in the results of the analysis. In some cases, this insensitivity may result from a well designed system which has so many recovery factors that the effect of any one human error on the system is not substantial. However, if some very different distributions such as the exponential or extreme value were used, it is possible that different results can be obtained. For computational convenience, one might wish to assume the same distribution for human failure as the one used for equipment failure. A sensitivity analysis would reveal whether any significant differences will be obtained with different assumptions.

In conjunction with the use of the lognormal to model human error probabilities, it is important to show how stress can influence human error probabilities. In WASH-1400 [3], a large loss-of-coolant accident (LOCA) was used as an example of a situation resulting in very high stress levels for the operators (Fig. 3). Human error probabilities were estimated for an operator from the first moments of a large LOCA until the operating crew could establish control of the situation (Fig. 4)*. The rationale for this curve is (WASH-1400, p. III-61 [3]):

"Following a LOCA, human reliability would be low, not only because of the stress involved, but also because of a probable incredulity response. Among the operating personnel the probability of occurrence of a large LOCA is believed to be so low that, for some moments, a potential response would likely be to disbelieve panel indications. Under such conditions it is estimated that no action at all might be taken for at least one minute and that if any action is taken it would likely be inappropriate. With regard to the performance curve, in the study the general error [probability] was assessed to be 0.9 at five minutes after a large LOCA, to 0.1 after thirty minutes, and to 0.01 after several hours. It is estimated that by seven days after a large LOCA there would be a complete recovery to a normal, steady-state condition and that normal error [probabilities] for individual behavior would apply." *

*It is interesting in light of the Chernobyl event to consider the fact that several nuclear plant personnel panicked during the early stage of the event, and fled the area of the reactor. Such behavior, of course, must ultimately be considered in any risk study.

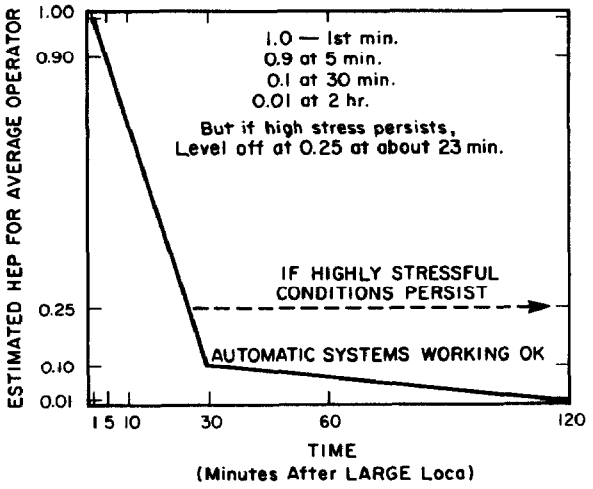

Fig. 3. Hypothetical relationship between performance and stress (based on Fig. III 6-1 from WASH-1400 [3]).

The consequences of human error can be large. All of the major accidents that have recently occurred, including Chernobyl, Bhopal and Three Mile Island, have involved significant human error. Of course, there are varying degrees of what constitutes "human error", but the human reliability methods adequately account for this range of errors and their consequences [11]. The issue of greatest concern here is the possibility for a sequence of human errors

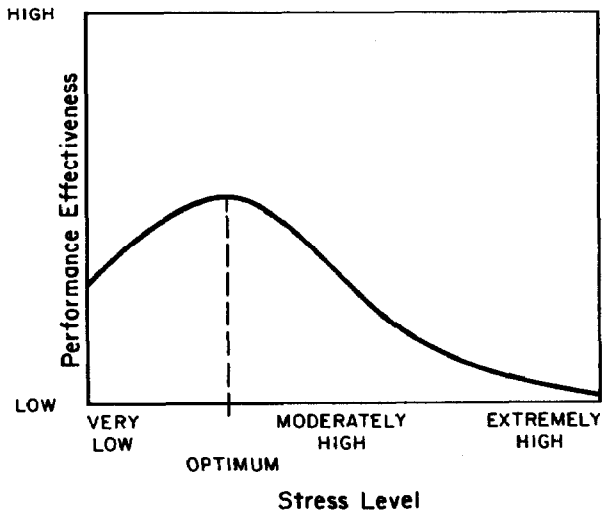

Fig. 4. Estimated human performance after a large LOCA [11].

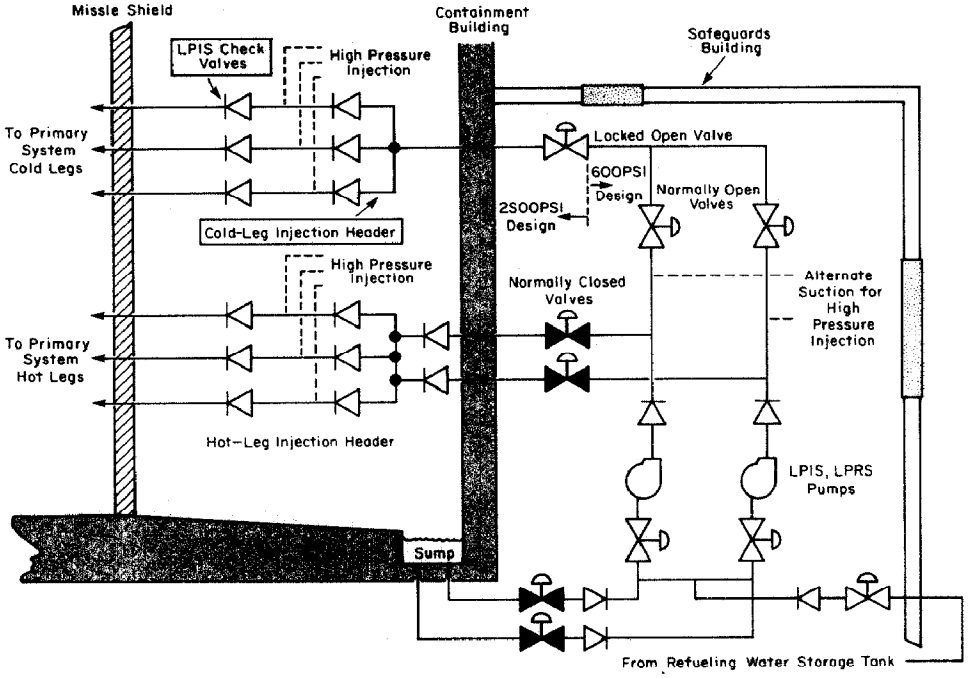

Fig. 5. The "V" sequence in PWR systems with ECCS systems housed outside primary containment [3].

that can lead to a major accident. The dependency relations between human errors is therefore very important to study and quantify.

IV. Directions for change: results of risk studies

Risk studies provide a useful service in that results of such studies point to directions for change in system design that can significantly reduce risk and improve system reliability. One very famous example of such an improvement came about as a result of the Reactor Safety Study (WASH-1400 [3]). The Surry pressurized water reactor (PWR) was analyzed for possible catastrophic failure. It was found that the emergency core cooling system (ECCS) was primarily housed outside of the containment structure (a massive, six foot thick steel reinforced concrete building housing the reactor). Penetrations through the containment were thus necessary by way of pipes connecting the safety equipment housed in the auxiliary building with the reactor primary coolant system (Fig. 5). Since the reactor maintains an extremely high pressure (2000 psi), the pressure drop across the connecting pipes, and thus the containment penetrations, was very high. This pressure drop, or "ΔP", permits the possibility of a loss-of-coolant accident (LOCA) through the pipe pene-

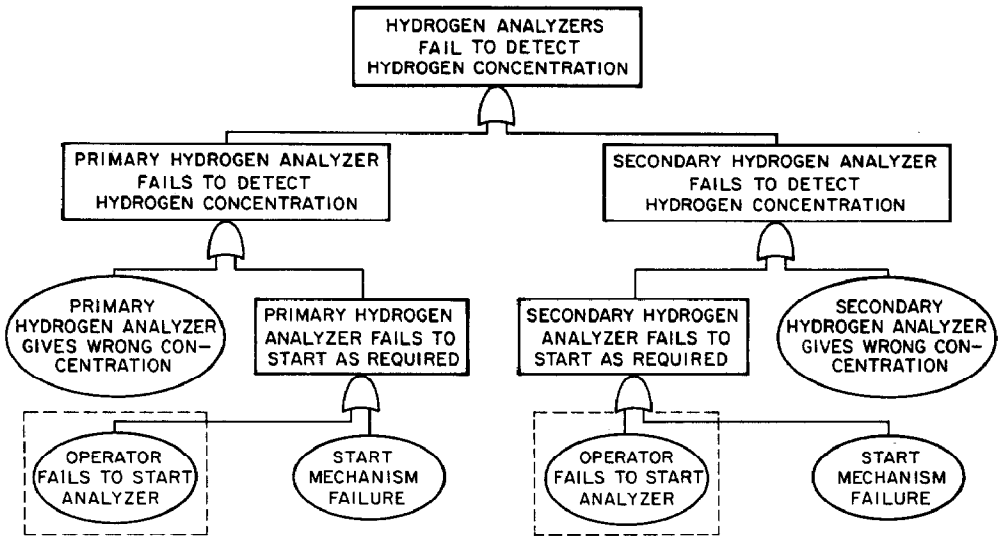

Fig. 6. Operator failure in fault tree for hydrogen analyzers [13].

trations directly bypassing containment. Such an accident, termed the "V" sequence in WASH-1400, was found to be a dominant sequence in the study. This sequence had never been identified prior to the Reactor Safety Study, and signaled an important direction for design change with corresponding reductions in catastrophic risk.

Another direction for change became obvious from this same systems analysis. In the reliability study of the Surry emergency core cooling system (Fig. 5), it was found that human operators had to be relied upon to "switch over" from the injection mode to the recirculation mode of the ECCS. Since there was a rather significant failure probability assigned to human error for this switchover task, the "direction-for-change" spelled out by the study was to remove the operator entirely from this system. In today's systems, as a result of this finding, the switchover is performed automatically without requiring human intervention.

Finally, the third example to be provided comes from a study performed by the author for the Yankee Atomic Company [13]. In that work, we were asked to analyze the reliability of a stand-by hydrogen control system that would be used only under emergency conditions in the case of a LOCA. In performing the fault tree analysis as part of the overall system reliability assessment, we found that human operators were again a major component of the system (Fig. 6). In assessing the failure probabilities to be assigned to the operator in the fault tree, we visited the particular plant in question, and thoroughly inspected the system layout and operator requirements. What we found was that for the secondary hydrogen analyser, because of the way the system was designed, the

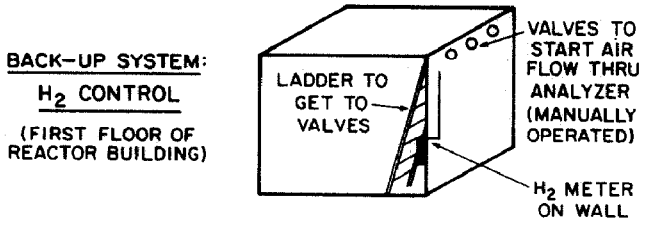

Fig. 7. Physical layout for hydrogen control back-up system secondary analyzer [14].

operator failure probability was equal to one. This meant, in our judgement, that there was no way that the operator could operate the secondary analyser because of major mistakes in the system design. We recommended to the plant that changes be made to correct these problems [14]. (Later, the entire hydrogen control system was replaced by a nitrogen inerting system.)

From these three examples, it is clear that risk study results have led to significant plant redesign and modification to reduce public and financial risk. Human error in both maintenance and operations can be minimized through application of human reliability analyses methods. These methods are available now. Unidentified accident sequences have been determined through reliability studies suggesting that future designs should be analyzed with these methods. Thus, risk analysis methods can help minimize the potential for future major accidents in both nuclear and other facilities alike.

V. Regulatory considerations: human error contribution to risk and directions for effective risk management

It is quite clear from our discussion that methods exist to model and quantify the human error contribution to accident risk, particularly for those accidents that can lead to the environmental release of hazardous materials. Nonetheless, it is imperative that regulators consider the more global aspects of risk management within the context of the organizational climate to be found at a particularly facility. In reviewing the many major accidents that have occurred recently and over the years, it has become apparent to many researchers that engineering failures may indeed be "man-made" [15]. In view of this conclusion, we must ask from a legal and regulatory perspective what can be done to reduce the human error element in the development of these events; this is the question that many in both the government and private industry are asking today [16].

After the accident at Three Mile Island (TMI), the nuclear power industry formed the Institute of Nuclear Power Operations (INPO) in Atlanta, Georgia. This industry-supported organization acts as a "watchdog" on electric utilities operating nuclear plants, and was formed to maintain standards of excellence across the industry. Now, after the Chernobyl event, the Interna-

tional Atomic Energy Agency (IAEA) is drafting guidelines for safety of nuclear plants worldwide, to improve the mechanism for accident reporting. The Soviet Union has also responded to Chernobyl by creating a board of inquiry to look into Western safety standards more carefully, perhaps for future implementation. These examples indicate that a learning process takes place after major accidents that can help prevent future such events.

Beyond this learning process, it is interesting to speculate on the future management of our technologies. My view is that, worldwide, industry is heading toward adopting the management principles first put into practice by the Japanese shortly after World War II. These are the management principles based on the concept of "quality systems", including statistical methods for quality control as the primary tool for ensuring consistant high-level performance. One of the chief architects of this management approach is Dr. W. Edwards Deming. His treatise on quality, productivity and competitive position is a forerunner of all future technological management systems [17].

The Deming management philosophy can be shown to result in a significant reduction in risk, both public and financial. Preliminary work in this area by the author [19] has shown that the Deming approach to management leads to a reduction in the probability of various events occurring, thus reducing plant risk. This risk reduction is particularly significant for the human reliability events that contribute to accident sequences as the Deming management philosophy leads to a different performance standard for those individuals involved in plant maintenance and operation. Moreover, one major American utility known for its progressive management style has recently adopted this philosophy and is planning to compete in the near future for the Deming Prize.

From the regulatory standpoint, it is evident that industry is becoming self-regulating, since the financial risk associated with major accidents greatly dominates any public risk by several orders of magnitude [18]. This conclusion is particularly valid for nuclear plants, but is most likely also valid for other major technologies. Thus, the future for hazardous material control has less to do with government regulations then with internal industrial self-regulation as the pressures from corporate insurance companies, public interest groups, and capital investors make their desires for improved safety and reliability known to the technological management. Clearly, none stands to benefit more from improved risk management then the groups most at risk — the stock and bond holders of the technological corporations themselves.

The role for government will thus become one of providing greater incentives for those who most quickly adopt the new management philosophy. This incentive will be primarily financial and may take the form of reduced licensing times for new projects. Reduced interference in operating facilities may also occur as the well-managed projects will increasingly be considered exemplary, just as they are today in Japan.

The quality improvement process is an ongoing evolutionary process that

continues to reduce risk while increasing plant and employee productivity. It is quite clear that the future direction of our technologies will be that shown to us by the Japanese — the direction of the quality management system.

VI. Conclusions

It is clear that worldwide, technology will increasingly be controlled by advanced organizational management systems. These systems will be based on similar structures already taking shape in Japan and elsewhere. Probabilistic risk assessment will be one of the many statistically based quality assurance tools that will be integral to these advanced management systems. These tools, along with an overall commitment to the principles of quality assurance, will result in major technological risk reductions. Thus, the risk we currently face from possible environmental releases of hazardous materials will be substantially reduced to smaller and smaller levels. The role of the government in regulating our technologies will be less integral to future risk reduction, since industry itself will continue to move in its current direction of self-regulation. By adopting the new management philosophy, the contribution to risk from human error will also be substantially reduced as we move to train our personnel in these methods. Thus, contrary to those who would wish our technologies eliminated, it is in this way that technology will continue to fulfill its promise of continuing to improve our standard of living.

Acknowledgements

I would like to thank Mr. Roger Batstone of the Office of Environmental and Scientific Affairs of the World Bank in Washington, DC, for inviting me to speak at the 1985 World Bank Symposium on the Bhopal chemical plant accident. This paper is based on that presentation. Also, I thank the General Electric Company and the Center for the Integration of Engineering and Manufacturing (CIEM) at Northeastern University for their support of my work on quality management systems during the 1985–86 academic year.

References

1 C. Perrow, Normal Accidents: Living With High-Risk Technologies, Basic Books, Inc., New York, 1984.
2 S. Kaplan et al., Methodology for probabilistic risk assessment of nuclear power plants, PLG-0209, Pickard, Lowe and Garrick, Inc., June 1981.
3 Reactor safety study, WASH-1400, US Nuclear Regulatory Commission, 1975.
4 Fault Tree Handbook, NUREG-0492, US Nuclear Regulatory Commission, January 1981.
5 N. Siu and G. Apostolakis, Modelling the detection rates of fires in nuclear plants: development and application of a methodology for testing imprecise evidence, Risk Anal., 6(1) (1986)43–60.

6 C.N. Guey and C.D. Heising, Development of a common cause failure analysis method: the inverse stress-strain interference (ISSI) technique, Structural Safety, 4 (1986) 63-77.
7 D. Okrent, G. Apostolakis and N.D. Okrent, On the usefulness of quantitative safety goals for state regulation of energy systems, J. Hazardous Materials, 10 (1985) 279-316.
8 E.J. Henley and H. Kumato, Fault tree construction and decision tables, In Reliability Engineering and Risk Assessment, Prentice-Hall, 1981, Chap. 2, pp. 76-78.
9 W.J. Parkinson, Sensitivity analysis of the reactor safety study, MS Thesis, MIT, February 1979.
10 R.E. Hall, P.K. Samanta and A.L. Swoboda, Sensitivity of risk parameters to human errors in reactor safety study for a PWR, NUREG/CR-1879 (BNL-NUREG-51322), Brookhaven National Laboratory, January 1981.
11 A.D. Swain and H.E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, Sandie National Laboratories, October 1980.
12 C.D. Heising and E.I. Patterson, Plant specification of generic human-error data through a two-stage Bayesian approach, Reliability Eng., 7(1) (1984) 21-52.
13 C.D. Heising and J. Lepervanche-Valencia, An evaluation of accident hydrogen control in BWRs, Nucl. Eng. Des., 64 (1981) 319-329.
14 C.D. Heising, The use of PRA techniques to assess and improve reactor operations, ANS Trans., 39 San Francisco, CA, November 1981, p. 859 (invited paper).
15 C.D. Heising, E. Frankel, E. Vanmarcke and H. Irwig, Engineering failures: man-made?, In Comparison of Risks Resulting From Major Human Activities, Proc. of the SFRP Annual Congress/Xth Regional Conference of IRPA, Avignon, France, October 18-22, 1982.
16 J. Perrolle, Policy guidelines for the protection of employees from reproductive hazards in the chemical industry, Northeastern University, Dept. of Sociology, June 1985.
17 W.E. Deming, Quality, productivity, and competitive position, MIT, Center for Advanced Engineering Studies, 1982.
18 C.D. Heising and V.P. George, Nuclear financial risk: economy-wide cost of reactor accidents, Energy Policy, 14(1) (February 1986) 45-52.
19 C.D. Heising, Developing methods for the computerized control of large, technological systems for improved safety, quality, and productivity, Final Rep., GE/CIEM Grant Program, Northeastern University, June, 1986.