MASTER

On the Role of Systems Safety in Maintaining "Affordable" Safety in the 1980's

H. Hollister
Scientific Advisor to the
Assistant Secretary for Environment
Department of Energy
Washington, DC 20585

and

C. A. Trauth, Jr.
Supervisor of Special Projects
Sandia Laboratories
Albuquerque, NM 87185

SAND79-1671 C

ON THE ROLE OF SYSTEMS SAFETY IN MAINTAINING "AFFORDABLE" SAFETY IN THE 1980'S

H. Hollister*
Scientific Advisor to the
Assistant Secretary for Environment
Department of Energy
Washington, DC 20585

and

C. A. Trauth, Jr.
Supervisor of Special Projects
Sandia Laboratories
Albuquerque, NM 87185

*Presented to the Fourth
International System Safety Conference
San Francisco, CA
10 July 1979

ABSTRACT

Historically, the Department of Energy and its predecessors have used and supported the development of systems safety programs, practices, and principles, finding them by and large adequate, effective, and managerially efficient.

Today, increasingly complex environmental, safety, and health problems and issues are facing us all, we are turning to increasingly complex and detailed regulation as the primary governmental answer, and it is increasingly doubtful that such an approach will give us management of these issues and problems that is either effective or efficient.

The above account presents us -- you in systems safety, all of us in society -- with a ready-made challenge, and that is to develop and apply systems safety principles and practices more broadly to total operational systems and not just to hardware and to environmental and health protection and not just to safety, so that the total universe of environmental, safety, and health can be managed effectively and efficiently with encouragement of innovation and creativity, using a relatively brief and concise, but adequate, regulatory base.

ON THE ROLE OF SYSTEMS SAFETY IN MAINTAINING "AFFORDABLE" SAFETY IN THE 1980'S

INTRODUCTION

By way of background, the Department of Energy (DOE) is currently responsible for the protection of facilities valued at well over 30 billion dollars, for the health and safety of approximately 20,000 Federal employees and over 160,000 prime contractor employees, and for the protection of the public and the environment from hazards associated with the activities of these many persons. These activities are diverse, ranging from oceanography to stratospheric sampling, and from solar and conservation R&D to the production of radioisotopes and electrical power.[1]

The department still has something of the character of a loose federation of organizations acquired from various Federal agencies during its formation.[2] Thus, broad, programmatic generalizations are not wholly valid. Nevertheless, with this caveat, there is a strong systems safety tradition within the DOE, arising from the Atomic Energy Commission (AEC) and its nuclear programs. In fact (as many of you here today surely know), the AEC was involved in the early efforts to develop the field of systems safety. Our weapons program[3] has strong elements of systems safety management, failure modes and effects analysis, quality and reliability control and assurance, and human factors and human engineering. Thus, a significant part of the DOE has historically been committed to a strong systems safety program, and we are now striving for uniform application of systems safety concepts to all activities.[4] Within this context, it is a pleasure to be here to lend support to the Systems Safety Society's efforts to determine the role of systems safety in the coming decade.

CONCERN FOR THE 1980's

Safety during the 1980's will carry a high potential cost. During the past century, we, as a society, have moved gradually away from concern with hazards of the following types:[5]

- Hazards that were largely simple and easily recognized
- Hazards that generally impacted only individuals or small groups of people in fairly immediate and recognizable ways
- Hazards that were controlled to a large extent by the persons who might be harmed

- Hazards that had associated benefits that were generally recognized and attained by individuals

We have in turn moved gradually toward a concern for hazards of this type:

- Hazards that are often very complex and hard to recognize or understand
- Hazards that may impact many thousands of people over long times
- Hazards that are often controlled by persons other than those who may be harmed
- Hazards that have benefits whose value to persons "at risk" is only indirect and not easily measured

Over the same time, another change of immense importance has taken place: our increasing use of governmental regulation to control our activities--not only for safety but for environmental and health protection and for economic activity as well.[6] Regulation has perhaps become society's primary vehicle for expressing a "consensus" opinion on the acceptability of perceived risk from technologically related hazards. It represents means of controlling risk to vast numbers of persons who individually cannot exercise reasonably direct control over hazards and who may not even understand the complex issues involved. Thus, in a sense, such regulation is a manifestation of the freedom in our society to govern our individual destinies.

In what may appear to be a paradox, regulation can, and often does, limit our freedom as well. Overprescriptive detail in regulation can stifle creativity and inhibit achievement, bringing with it high costs, inefficient use of resources, and so forth. In the extreme, regulations themselves, collectively or individually, can become so complex that compliance is uncertain or even impossible.

Consider this: The DOE has activities in nearly all of the 50 states. We require that we and our major contractors comply with virtually all Federal and State environment, safety, and health laws and regulations.[7] We are required under the terms of the DOE Organization Act to assure such compliance.[8] This would appear to mean that we must have a working knowledge of an estimated 18,000,000 pages of requirements.[9] The scope of the problem increases when local regulations, which we also deem mandatory as applicable, are added to this list. To completely assure compliance with such a collection of requirements is some task, one whose value might, in fact, be questioned. Indeed, as we struggle with this approach to assurance,

one might wonder whether our whole assurance machinery won't break down. A systems matter, indeed. What is true for DOE is clearly true for the nation as a whole.

What of the 1980's? To appreciate what is coming, it should be observed that the volume of all Federal regulation is currently increasing approximately geometrically. It is not unreasonable to assume that environment, safety, and health regulation, on a national scale, is doing likewise. During the coming decade, it appears that the body of requirements may be on its way to becoming so detailed, complex, and uncoordinated that it itself will become a major impediment to the achievement of intended or reasonable environment, safety, and health objectives. Better, more efficient ways of achieving them are evidently badly needed. We will need to manage more efficiently as a nation.[11]

What price safety in the 1980's? We don't know, but we believe that, for a set of reasonable policies [illegible], it can vary from "reasonable" to "unaffordable," depending upon the efficiency and effectiveness with which our society learns to manage its environment, safety, and health affairs. Do not misunderstand: there is no question that a free society must express its consensus opinion about the acceptability of perceived risk in this complex age, or that we, as good citizens, must respond to this opinion. Basically, we expect this consensus to continue to be expressed through regulation. At issue is how we, as a nation, can most effectively, or efficiently, do this.[11]

A ROLE FOR SYSTEMS SAFETY IN THE 1980'S

This brings us to a discussion of systems safety. We come to it with the AEC perspective that was mentioned earlier. In our opinion, the AEC had a good operational safety record. In some cases, and with considerable hindsight, its record in the environment and health protection areas is, perhaps, equivocal. The excellent AEC safety record stemmed from a commitment to systems safety principles: A structured, systematic, administrative approach designed to identify hazards, understand and control them, with an inclusion of professional expertise in safety, reliability, human factors, and quality control and assurance. The AEC record did not stem from the fact that it was regulated. In many respects it was not. To use Walinsky's words in Newsweek not long ago, "in matters of real importance, regulation ... is meaningless. If your son is to undergo back surgery, you care little whether the doctor will be penalized if he inadvertently severs his spinal cord. You want a surgeon skilled enough not to bungle the job," that is, a real professional.[12]

With our AEC background, it is not unnatural that we should put forward the following hypothesis: efficient management of our environment, safety, and health affairs, nationally, can be achieved through a strong commitment, at all levels, to three things:

- The use of the regulatory/legal system to set performance[13] objectives for limitation and control of hazards
- The use of a systems safety philosophy, suitably modified to incorporate environment and health protection and operational, as well as technological (design or hardware) activities, to achieve these objectives through the establishment of systems safety programs
- The development of associated assurance programs to assure that ES&H protection programs are adequate and truly followed in order that society, through its overall regulatory approach, can have confidence that its ES&H objectives are being attained

In setting forth this hypothesis, we are encouraged by the results of a study of ES&H assurance[14] being conducted for the DOE by Sandia Laboratories.

Some illustrations. Let us first touch on the Three Mile Island incident. This incident was, as we're sure you know, characterized by several equipment malfunctions, including a water pump and pressure relief valve failure, interspersed with possible human engineering errors, including easily misunderstood gauges and administrative system deficiencies which permitted cooling system valves to remain closed after servicing. It appears that the regulatory approach, highly detailed, failed -- which, given our historical tendencies, probably implies still more detailed regulation. A systems safety program addresses the deficiences as they are currently perceived. Indeed, a thorough commitment to such a program would, in our estimation, lead to better performance.[15]

A second example arises from a recent unpublished study of OSHA accident data.[16] An attempt was made to answer the question, "What percentage of the reported accidents might have been prevented by an OSHA inspection just before their occurrence?" This clearly is one measure of the efficacy of compliance with detailed regulation. The answer was "about 25 percent." This assumes that the inspections would have found the OSHA deficiencies, that is, it represents an upper limit. An early part of the Sandia study[17] sought to answer the somewhat similar question, "What percentage of serious incidents might have been prevented by a program to assure that environment, safety, and health plans are adequate and properly

implemented?" The criteria for adequacy were general ones related to systems safety. In this case, the maximum answer was 96 percent. The two studies are not really comparable: types of accident/incidents considered were different ("all lost time" versus "serious"), and the data-base sizes were very dissimilar--not comparable but suggestive.

For the last example, we would like to describe a recent DOE accident. If you read Jack Anderson's column, you will know all about the strategic petroleum reserve program, the objective of which has been to store 1 billion barrels of crude oil, in various ways, by the year 1983. Crude oil is currently being stored under pressure in salt formations along the Gulf Coast. At one such site (West Hackberry, LA), oil containment devices failed under the pressures generated during an operation to remove piping to the salt cavern. Over 67,000 barrels of oil escaped from the repository, catching fire from nearby machinery as it did so. One person was killed and a second badly injured. In addition, an environmental threat was posed by the approximately 31,000 barrels of the oil that ran into a nearby lake. Here, the issues were almost exclusively systems safety oriented: failure to recognize the failure mode, poor choice of temporary containment equipment, poor quality backup devices, poor safety procedures, and so forth. So far as we know, no regulations were violated. This, then, is a case where reliance upon regulation to stay out of trouble was inappropriate. It was not a "routine" operation. A good systems safety program would clearly have addressed the relevant issues, and accident investigation recommendations directed that such a program be instituted.[18]

These examples may or may not convince you that our hypothesis has merit; if so, it seems to us that the 1980's offer us all quite a challenge:

- To develop and broaden the use of the systems safety philosophy to more fully cover not only safety per se, but environmental and health protection, not only hardware, but comprehensive operational activities

- To develop and use techniques, acceptable to the public, for assuring program performance (including a priori performance measures, i.e., leading indicators, not just accident/incident statistics)

- To consider how current ES&H requirements might be modified so as to be expressed as performance objectives to be met within this broad systems safety context and to commit ourselves to the achievement of such objectives

- To strive for improved environment, safety, and health performance using such a structured systems approach

- To effectively communicate the efficacy and advantages of, and performance associated with, such an approach in thorough and open ways

What price safety in the 1980's? We still don't know, but we strongly suspect that it may depend largely upon all of us.

Notes and References

1. Because of the diversity in activities, there is, of course, a diversity of hazards.

2. In its formation, the Department of Energy has acquired activities and organizations from the Atomic Energy Commission (via the Energy Research and Development Administration), the Department of Interior, the Department of Defense, and the Federal Energy Administration.

3. Systems safety has been emphasized in areas other than weapons, as well. These include various reactor development programs (both civilian and naval), space power programs, magnetic fusion programs, and special "major acquisition" efforts.

4. In this regard, there are several new Department of Energy Orders, or parts thereof, which require various systems safety program elements that are either in place or nearly so. These include Order 5481.1, "Safety Analysis and Review System," which, for example, specifically references MIL-STD-882A, "Systems Safety Program Requirements;" Order 5482, "Environment, Safety and Health Appraisal Program," to assure adequacy and use of programs; and specific chapters of Order 5480, "Department of Energy Environment, Safety and Health Program," such as Chapter II, "Quality Assurance."

5. These lists are paraphrases of fairly common thoughts in the "risk literature." See, for example, Of Acceptable Risk: Science and the Determination of Safety by William W. Lowrance, published by William Kaufmann, Inc., 1976.

6. "We hold these truths to be self-evident." For a discussion of the fundamental characteristics of society that lead to the use of regulation, see, for example, "Preliminary Indicators of the Public Acceptance of Risk," a monograph by Jay B. Sorenson, Professor of Political Science, University of New Mexico, Albuquerque, NM. Available from the author.

7. See Department of Energy Order 5480, Note 4.

8. Among other things, the Department of Energy Organization Act of 1977, Public Law 95-91, has as its purpose, "to ... assure incorporation of national environmental protection goals ... and ... the goals of ... assuring public health and safety" (emphasis added).

9. This is a very crude estimate which may be very misleading (either way). Basically the number is unknown, which is informative in itself. The estimate assumes that one-fourth of the approximately 900,000 pages of the Code of Federal Regulations is ES&H-related: yielding 225,000 pages. It then is assumed that mandatory first, second, third, etc., references to regulations (ANSI standards, for example, at about 20,000 pages) and to statutes, the statutes themselves, ES&H-related treaties, appropriate guidance material, torts, committee and conference reports, hearing outcomes, and so forth total an additional 125,000 pages, knowledge of which is necessary. Finally, it is assumed that, on average, states do no less than the Federal government, making the total package contain 51 times 350,000 pages or 17,850,000 pages.

10. The "volume" of regulation is only one measure of regulatory and management complexity. Others include multiple regulation of the same hazards by many agencies and a lack of a centralized overview of ES&H-related regulation.

11. We particularly do not wish to be misunderstood on this point. The public "dictation" of ES&H goals in our society is essential in this age of complex hazards. Our concern is not with this inherent right: it is with the management of ES&H affairs, nationally. We both subscribe to the goals implied by current regulation -- and wish only to find efficient ways of meeting them.

12. Adam Walinsky, "Nuclear (T)error," in "My Turn," pp 26-27, Newsweek, May 7, 1979.

13. Here we have in mind the use of only such detail in regulation as is needed to make objectives clear.

14. Several comments are appropriate here. Reliable and believable assurance is needed on behalf of the public. It appears that some assurance of a commitment to good programs will be more reassuring -- and provide more meaning and flexibility -- than the existence of detailed regulations, conformance with which is not (or is at best, poorly) assured. The Department of Energy has been sponsoring a systems research project aimed at examining precisely this possibility. For reference to this work, see A. C. Ellingson, C. A. Trauth, Jr. and M. S. Tierney, A Proposed Standard for ES&H Assurance Programs,

SAND79-0240 (Albuquerque: Sandia Laboratories, March 1979) and the references given therein. These are available from the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161.

15. Neither of us has kept up with very recent developments in this area. Early reports, e.g., the testimony of Herman Dieckamp, president of the General Public Utilities Corporation, before the Subcommittee on Nuclear Regulation of the Senate Committee on Environment and Public Works, 23 April 1979, would seem to strongly support this assertion.

16. Personal communication to one of us (CAT). Allusion to the results of this study may be found in the "Interagency Task Force on Workplace Safety and Health -- First Recommendations," 1 August 1978, p II-2.

17. See Note 14. The specific document dealing with this issue is C. A. Trauth, Jr., A. C. Ellingson, L. M. Jercinovic, and D. E. Farr, A Study on the Application of Quality Assurance, Human Factors and Reliability Principles to the Prevention of Major Environment, Safety and Health Incidents, SAND78-2176 (Albuquerque: Sandia Laboratories, December 1978). This is available from NTIS.

18. See "Report on the Explosion, Fire, and Oil Spill Resulting in One Fatality and Injury on September 21, 1978, at Well 6 of Cavern 6 at the West Hackberry, LA, Oil Storage Site of the Strategic Petroleum Reserve," DOE/EV-0032, U.S. Department of Energy, November 1978.