REFLECTIONS ON SYSTEM SAFETY

AND

THE LAW

Mr. Daniel F. Hayes, Sr.
Assistant
NASA Director of Safety

NASA Headquarters
Washington, D.C.

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

HOW SAFE IS SAFE?

The question "How safe is safe?" will be frequently directed to those who work at preventing accidents. The question will often take these forms: How far do we have to go with these precautions? how much money or effort shall we spend to prevent accidents? do we need "redundancy," "back-up," "guards," "fail-safe," "emergency procedures," "more training?" if we provide backup for an operation, shall we backup the backup? If we do, how much safer is it? If we spend money to reduce the hazards all the way, is it worth it? Is the benefit worth the risk? This last question has become a most serious one for business men today in the light of increasing awareness of the public and attending claims consciousness. While still not taken as a national policy, it is becoming more and more recognized that "accidents can be prevented." And so--how much prevention?

We safety managers have a notion that we know what is safe. No doubt! Experience teaches us to know better than some others what is safer, and only perhaps what is unsafe. But "safe" and "unsafe" are general, abstract, unquantified, relative terms. Here-to-fore we have been successful only to the extent that we have given more attention to eliminating or controlling conditions from which accidents can arise which are discernible to a trained eye.

The unconscious desire of specialists is to prevent change in their specialty--(A quotable quote from one of the cases)--"To a specialist "change" means unlearning a section of knowledge, a painful process!"

With the development of additional attention and emphasis on safety and the greater urgency technologically, socially and politically, we are refining the search to prevent accidents with the more diligent application of engineering methods and the stricter use of logic and of computer selected information. Thus conditions that were formally called "accident causes," are found out or discovered, and anticipated, and the potential for loss eliminated, controlled, or otherwise negated. We find that many so-called accident causes were not unforeseeable and unpredictable! We didn't search with sufficient diligence! Thus system safety analyses become, not panaceas, but only aids to anticipating what was formerly unanticipated. The probabilities have been qualified and quantified. The result of these efforts permitted us to send men to the moon and bring them back safely. They can be used in many other applications with similar success.

THE ANSWER IS LAW

But this search still does not answer the question fully--how safe is safe? It only tells us that asking "what if?" often enough and providing the answers will make our hardware, process or management safer. In fact, to be able to go all the way, will require more than human clairvoyance. I submit that in any given situation the question of whether this process has been followed to an adequate degree will usually be explored in a court of law.

Safety is a state of being free from or the absence of danger. Danger is a positive word and means that there is a potential for harm or loss. (Incidentially, the word for "safe" in Russian is the equivalent in English of "danger" (oposnosti) plus the prefix "without" (bez) which makes it "safe" i.e., without danger.) Harm is damage or hurt. And, unless the hurt is to the perpetrator himself, there can be a claim for negligence. When negligence is alleged in a court action to be the cause of the damage, we are all set for a determination of "how safe is safe" because the law will want to know among other things "How diligently did the responsible person look for the causes of harm and what did he do about them."

Throughout the cases of negligence, definitions and court determinations are generally consistent. In general "negligence is an act or omission in violation of duty to exercise ordinary care by reason of which injury to person or property occurs."*

Courts always imply that the negligence or failure to do or not do was what a reasonable or prudent person would do or would not do under the circumstances.

PRUDENT PERSONS WILL ANALYSE

It is my purpose to advance the idea that in some circumstances "what a reasonable or prudent person would have done under similar

*Sec. 32, 38 AM. Jurs. P643.

circumstances" will be to make a systems analysis. So far I have been unable to find adjudicated cases where this has happened, though I've been told it has.

If there are any, they are rare, so far. However, one does not have to stretch the imagination to realize that under many circumstances, now developing in products safety, technical operations, complex machinery, aircraft, pollution and other modern situations, negligence will consist "in" not having looked as systematically as one could have. "The policy of the law has relegated the determination of such questions to the jury (i.e., was he a reasonably prudent man?), under proper instruction from the court." When products and processes become too complex for a jury to understand or too technical for a judge to comprehend, some other means than rhetoric may be needed. What is "ordinary care" may be quite difficult to explain. The search for negligence has already been extended all the way back to defects in design. Such cases put a strain on laymen and technical terms before the judge. What better way in a technical situation to demonstrate to a jury how diligently one has sought out and eliminated those circumstances which could cause actionable harm or loss? Particularly is this so when the expression "the analysis applies throughout the life cycle of the system" is honestly applied.

From a case in the books--"A reasonably prudent man will neither neglect what he can foresee nor waste his anxiety on events that are barely possible..." [What is barely possible has only been occasionally quantified in legal thinking. Not so, in a system analyses. In some analyses, the "barely possible" is actually put into numbered probabilities.] Continuing the quotation--"but he, the reasonable man, will order his precautions by the measure of what appears likely in the known course of things, whether the particular act or acts charged in the petition were performed or omitted and whether the performance or omission of some of them was a breach of legal duty."*

This, in legal terms, describes what one does in a logic analysis!

Having made an analysis the step by step documentation required in practically every Safety Analysis Report, Operations Readiness Review, Fault Tree Analysis, Failure Mode and Effects Analysis, etc., provides recorded proof that one was diligent, not negligent.

The day may be here already, considering the advances in technical knowledge and techniques for retrieval of hazard information and accident experience, that a man or person (corporation) may be considered negligent if he has not used a system analysis in the degisn of a product to offer to the public.

If this theory is to be of value, the question of admissibility of such proof will have to be considered. This will be touched later.

THE LAW CHANGES

Argument for use of system safety techniques as a legal instrument is supported by several considerations. These techniques are certainly new tools. They have accompanied the growth of recent technologies--atomic energy, aircraft, space. But law and lawyers use new tools, too. The needs of a changing society will be reflected in the decisions in the courts. This growth and change in the law is most interestingly dealt with in a book titled "How High is Up" by Loth & Ernst.* They trace, in some of those fields, the manner in which law has adapted itself to modern new problems beginning with the legal concept "caveat emptor" i.e., "buyer beware." They show how this concept was changed in a few years, by reason of the "Cardozo Revolution," to a 180^{0} attitude and is now "caveat vendor", (seller beware).

They, Loth & Ernst, show that concepts of liability in aviation brought about vast changes in the law regarding ownership of land and air, and the effects on the posture of society in respect to noise, vibration, comfort, right of way, personal injury.

In McPherson v. Buick, 1916 Judge Cardozo said, "on the basis that science perfected previously undreamed of safeguards against inanimate objects and also much more damaging objects the vendor has a responsibility and a liability if he was placing a dangerous object on the market." Later interpretations placed liability on aircraft manufacturers, based on

*Sec. 38-28 Am Jurs. P645

*Bobbs-Merrill Co., Inc., NYC, LIB CONG. 64: 15-665

the lack of reasonable care in the design and control of quality. I dare to predict that the law will recognize and use, logic techniques, technological advances in the storage of accident information, system safety analyses, the tests and measurements and requirements for documentation that the space industry has developed.

It is not unreasonable to expect that in the field of negligence, warranty, breach of contract and rules of evidence, the law will adapt to more systematic assistance in seeking out the truth in appropriate cases, by the very means used to assure safe hardware.

AS EVIDENCE

The books say "Proof which is addressed directly to the sense of the court or jury without interposing the testimony of witnesses--is the most convincing " The presentation of charts, diagrams or tables which makeup the analysis would, no doubt require the engineer or persons qualified to be present. Diagrams or charts showing the basic assumptions of steps and stating the manner in which a system safety analysis was made and the controls which were applied will probably be allowed as evidence. The witnesses would be required to be authenticated by the presiding judge.

Let us look at another aspect of system safety and evidence. How well would the documentation required a system safety analysis serve the lawyers?

"In general where a map, or a drawing is offered as embodying in itself, the knowledge of the witness to which he, in this form deposes, the verifying witness must be shown to have personal knowledge of the facts so as to qualify him to testify to their correct representations. . ." It is my feeling that the step-by-step documentation not only provides the witness with a most potent method of recall, but it also demonstrates that nothing within the power of the intellect has been overlooked in the search for safety, and that there was diligence.

TESTS

"The courts, though they do not favor experiments and tests by the jury itself, now very generally permit relevant experiments, demonstrations or tests by others in court or permit evidence of experiments performed out of court. . ." This would seem to say that tests made as part of a hazards analyses, where the probability (or improbability) of failure is to be demonstrated, would surely be admissible. Similarly, tests which frequently became part of a system analysis will probably be admissible.

RISK VERSUS BENEFIT

The queries "What is safe?" or "How unsafe is unsafe?" are also tied into the construction which may be put on the concept of "benefit versus risk."

Ernst in "How High is Up" says "So law must always strike a balance between risk and recklessness." He mentioned this (he said) because it struck him as exceptionally plain in considering atomic energy." But use of atomic energy is not the only situation where this question is being posed. We see it frequently, for instance, with respect to environmental pollution, now considered as a great risk. Here it would seem that the law, when faced with this dilemma, risk vs benefit, will be greatly aided when the engineer or scientist applies his informed logic before hand, in respect to what the risk is, that is to be balanced. So it is possible that the precise quantification of hazards by technical analysis may more clearly help to determine the values of risk and benefit for the law as well as for the engineer.

ACCIDENTS FEED THE LAW

In the field of atomic energy there have been relatively few successful litigated claims for damage. In fact, few accidents. I can speak here with some knowledge, since I wrote the first complete repertoire of all accidents involving nuclear energy, which is now an Atomic Energy Commission biannual report. At the time there was no collected history, and I was somewhat surprised that the report sold over 7,000 copies at the Government Printing Office. The whole application of a new energy source and its integration into society is an instance where the lack of accidents, due to the rigid requirements written into the law relating to its use, the extreme caution exercised in the

manufacture and control of these hazardous materials and the experience with other kinds of energy deprived the courts of precendent on which to base decisions. (This further supports the thesis that until there is loss or damage we have no measure of what is safe or unsafe.) It will be interesting in the future as to what weight will be given by the courts to the extreme care exercised in the control of this hazard including the Safety Analysis Review system of analysis.

When accidents do not occur, both plantiff and defendent are left without a good measure of the relationship of benefit and risk. For the question of excessive risk is going to depend on what the courts decide is excessive, that is, whether the controls were or were not what a reasonable man would have done--and whether even so, the public benefit prevails.

STRICT LIABILITY

In certain situations a product or process is held to be hazardous without further proof to the contrary. This raises a speculation. In the doctrine of strict or absolute liability the person who puts a hazardous product on the market without performing certain actions such as warnings and specific instruction to the buyer will be considered negligent per se. However, it would seem the absolute liability might someday be successfully fought off and the trend turned, shifting the liability back from the vendor and giving him a chance to plead benefit to the public and the absence of unevaluated hazard. The law makes its changes in small steps. The application of new methods of engineering analysis are also steps usually in the direction of greater precision and sounder logic and safety. Perhaps these technical steps toward greater perfection will be the occasion for new legal approaches. It may be possible to avoid throwing up one's hands and saying "This machine is too dangerous to allow man to use it." It was only a few years ago that the possibility of atomic energy for power was abhored--today there are many nuclear power plants on the line in spite of the fears of the public and the experience is good.

When I became interested in the relationship between system safety analyses and the law, I had not looked at a law book in many years. Consequently, changes were very apparent to me, and the possibilities of changing from absolute liability back to a defensive position by reason of an engineering procedure that looks at, identifies and eliminates hazards would seem quite real. "There are few constants in the law but continued change. . ."*

Given a hypothesis or doctrine of strict liability there must also be a corrollary that says "you may do something or offer a product in the first place." That is, you are not prohibited to do so, but if you do so, the law says you must be prepared to be liable for it. In other words you are deprived of defenses normally available as to being a reasonable man. I submit again, subject to argument of course, that here is an ideal situation for use of logical analysis of risk. By using (and perhaps by usage) a system safety analyses will allow you and the court to arrive at a more precise idea of the true hazard, correct and control them and provide proof that the previous strict liability is not to be assumed.

APPLIED TO THE ENVIRONMENT

The National Environmental Policy Act of 1969, P.L. 91-190, 1970 imposes requirements on all Government agencies to interpret and administer their policies, regulations and public laws in accordance with the policies set forth in the Act. Those policies relate to conservation and use of the environment, and assuring safe, healthy, productive, esthetic and culturally pleasing surroundings, and other purposes. These requirements will fall on industry to an increasing degree.

To accomplish these purposes the Congress states under Sec. 102 of the Act that the agencies shall--

"(A) utilize a systematic, interdisciplinary approach which will insure the integrated use of the natural and social sciences and the environmental design arts in planning and in decision making which may have an impact on man's environment;

(B) identify and develop methods and procedures, in consultation with the Council on Environmental Quality established by Title II of this Act, which will insure that presently unquantified environmental amenities and

*Effective Research - Price & Bittner, 1953, Prentice-Hall, NYC

values may be given appropriate consideration in decision making along with economic and technical considerations;

(C) include in every recommendation or report on proposals for legislation and other major Federal actions significantly affecting the quality of the human environment, a detailed statement by the responsible official on--

(i) the environmental impact of the proposed action,

(ii) any adverse environmental effects which cannot be avoided should the proposal be implemented,

(iii) alternatives to the proposed action,

(iv) the relationship between local short-term uses of man's environment and the maintenance and enhancement of long-term productivity, and

(v) any irreversible and irretrievable commitments of resources which should be involved in the proposed action should it be implemented."

It is the five specifics under (C) that deserve our attention when pursuing the subject of the title of this paper.

As written, those requirements paraphrase quite suitably the basis for a systems analysis. The objective of a systems safety analysis is to avoid an undesired event, in this case one which will pollute the environment. In a systems analysis of a piece of hardware this event is equivalent to a failure resulting in damage or loss of a mission.

The methods available such as Fault Tree, FM & Effects, Gross Hazards Analysis could be used to identify the events which will bring the pollution about.

The selection of available alternatives to the proposed action as required in this law will become possible when, in the analysis they are pin pointed.

The commonly used term in the analyses of space systems is "trade off." It accurately described item (IV) relationship above.

And finally item (V) is a statement of the residual hazards and the requirement on which management decisions must be made.

The usual hard requirement in a system analysis is that each step is documented, and that the whole analysis provides for sound management decisions.

The administration of the requirements of the Environmental Act place an added burden on almost every project or activity of any importance and--it would seem that system analysis would provide a simple and effective procedure to assure that a given project meets the intent of the law.

Summary

The final answer to the question of safeness is stated by the courts. What is "safe" changes with experience.

As technology advances new tools are developed. The new system safety analyses (methods) are such tools.

The law and lawyers use new tools.

The needs of society will be reflected in decisions of the courts.

These decisions change the law step by step.

It is not unreasonable to expect that the law eventually adapts its decisions as to what is or is not safe to the real world, and better engineering analyses will be defense against liability all the way back to design.

If, in the real world we find system analyses useful, so also will the courts, and they can find them so in negligence, warranty, breach of contracts, evidence.

SESSION I

QUESTIONS AND ANSWERS

DR. CLARK: I am interested in the problem of liability of the vendor from the last speaker. On what basis do you say, at the present time, that this is the situation, when you notice that the percent of defective sales that are going to qualify a builder for settlement, are less than 1%? The National Commission on Product Safety has identified .05% as the typical quality reliability insurance plus settlement costs.

MR. HAYES: I don't think I quite understand your question--or did I just hear the first part of it.

DR. CLARK: Why do you say it is up to the vendor today, that the manufacturer is taking the responsibility for its product?

MR. HAYES: I think you all find that those cases that have resulted in very large settlements and where the cases are completely litigated, (i.e. not settled out of court), that the responsibility in many cases today ends up on the vendor.

DR. CLARK: This is a very small percent of sales! The real responsibility remains on the buyer.

MR. HAYES: All right, I buy that but we are talking about litigated cases. Many airplane cases end up in placing the negligence on the designer of the airplane. This is becoming more and more frequent. It is my point, that adequacy of design is important now in law suits and the courts look at how the manufacturer designed the product to determine whether or not the manufacturer is liable when it is involved in an accident.

DR. CLARK: We were very impressed in the National Commission on Product Safety with what a small percent of the product failures end up in liability suits. Most of these things of course get settled out of court, but it is a very small percent that ends up as the manufacturer's responsibility.

MR. HAYES: Yes, but I think if those products happened to be pressure cookers or other hazardous devices or vehicles that get into the public's hands and create the accidents, I think you will find a larger percentage.

MR. BOLGER: It would be interesting to see how the settlements went too.

QUESTION: Concerning the supervisors reporting on accidents, you seem to indicate that this supervisor knows what the problems are in this management system and you infer a great deal of validity to what this man is saying, how do you know that what he is saying is that valid?

POPE: I don't know that I can take your question and give you the answer that you're looking for. The only thing that the aligned supervisor knows is that things are going wrong. What we've done is, we coded, we have a coding system, and we have given him a number of questions which he can respond to, we literally lead him towards. For example, if he thinks personnel is not giving him a problem or he has a problem, he then has a whole series of things he looks at under personnel and one of them would be staffing. If he has a lifting problem, he can say, well we can go out and train them how to lift, yes, but I should have an extra man there too. He not only puts in that he has a condition of lifting but he also puts in that he has a personnel problem related to staffing. Then, when we go to the computer and ask how many staffing problems we have had in accident situations related to personnel, we then can go back to personnel with a cause and a cost, we go by cost, and say to our personnel function that has something to do with staffing, do you realize that there is a staffing problem generally in this particular area of the organization which is shown by the number of cases that we've got that came out, not necessarily lifting but staffing was the problem in many other instances too. These people are not happy with their staffing situation and it has cost us this amount of money because of it; therefore, you have a responsibility, a concern to solve that particular problem, not me.

QUESTION: I would like to ask Mr. Pinkel about the datafax accessibility. Is it accessible at the present time only to NASA contractors and NASA personnel?

MR. PINKEL: Anyone can request the information he wishes to have. It is available to the community at large, really. No charge is involved.

MR. BOLGER: That is the intent of it isn't it? It is to be used for the nation as a whole, right?

MR. PINKEL: It is for the nation as a whole. Of course, the interest is steered to the aerospace community, but anyone has a right to it.

QUESTION: Would the information be inaccessible to any lawyer to get information for a law suit?

MR. PINKEL: We can't keep a citizen from having access to the bank.

MR. BOLGER: That poses the problem of who is going to put information in it, Right?

MR. LEDERER: Then he can be sure of his facts before he distorts them.

MR. PINKEL: We'll distort them a little first, Jerry.