N72-25972

SYSTEM SAFETY EDUCATION FOCUSED ON SYSTEM MANAGEMENT

Mr. Vernon L. Grose
George Washington University

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

Student Contribution

The GWU course is purposely designed to utilize and integrate the diversity of experience represented by the students attending the course. This position is in contrast to courses where the instructors supposedly have all knowledge on the subject "wrapped up in a box with a blue ribbon around it." Rather than "pipe knowledge in a straw to naive students," the instructors view classroom discussion as a learning experience every bit as valid as formal lecturing

The diversity of backgrounds possessed by graduates of previous classes makes this point obvious. Students from at least seven categories have completed the course:

Commercial Industries - American Mutual Liability Insurance Company, Ebasco Services, Incorporated (major contractor), De Leuw, Cather & Company (engineering contractor for the Washington Mass Transit), and Western Electric.

Aerospace Industries - General Dynamics, Ling-Temco-Vought, Martin Marietta, McDonnell Douglas, and Vitro Laboratories.

Federal Government - Federal Highway Administration, Atomic Energy Commission, Bureau of Mines, Federal Aviation Agency, National Transportation Safety Board, National Bureau of Standards, and National Aeronautics and Space Administration.

Foreign Governments - Department of Social Action (Mexico) and British Aircraft Corporation.

City/County Governments - Chicago Transit Authority, New York City Transit System, and Montgomery County (Maryland).

Military Services - Numerous branches within the Army, Navy and Air Force

Universities - Johns Hopkins University and The George Washington University.

APPROACH TO SYSTEM SAFETY

The GWU course starts off by defining the problem. As Figure 1 states, "We are trying to do well that which we do not understand." Furthermore, we will never understand that which we must do well. Dr. Raymond M. Wilmotte reaffirms this statement in different language:[1] "The uncertainties that remain (in any complex decision) are never zero."

The reason for this pessimistic outlook is quite simple. The complexity of most situations faced by decision-makers today is far beyond any single individual's capability to comprehend them in depth. Yet we are precluded the luxury of simply wringing our hands in despair--we must still press forward and make decisions.

"Systems" Characteristics

The systems approach, regardless of its application, has at least eight characteristics as shown in Figure 2. Since system safety can be described as "the systems approach applied to safety," these eight traits apply directly to system safety. Further, these characteristics differentiate system safety from other safety activities.

A description of each characteristic is repeated from an earlier publication:[2]

Methodical - The systems approach involves a definite method. This method consists of an orderly procedure or way of solving complex problems. All the steps involved in problem-solving are arranged in a consistent and orderly manner.

Objective - The systems approach is also objective; i.e., the steps in the problem-solving method are free from personal bias to the greatest extent possible. Personal opinion must be identified as such. By maintaining this discipline, the results of each step in the problem-solving process can be verified or confirmed by someone other than the person who performed the step.

Quantitative or Measurable - Almost without exception, each element in the problem-solving process results in a quantitative expression. At the very least, there must be some measurement possible to weigh the validity of the conclusion reached. Because any end product produced by the systems approach is obviously a compromise, it is necessary to weigh the relative merits of each element in the system by some means other than personal opinion. This need to compare alternatives dictates that measurability be

one of the characteristics of the systems approach.

Analytical - The systems approach employs a rational division of the whole system into its constituent parts to find out the nature, proportion, function, and interrelationship of these parts as they contribute to system objectives. This analytical function frequently leads to solving system problems by means of mathematical models or equations. Thereby, the elemental variables can be related and traded off with respect to each other.

Subsystem Interdependence - Another characteristic of the systems approach is a constant recognition that any given element or subsystem is dependent on all the other elements in the system. Should the function, dimension, or description of a subsystem be revised, such a revision will affect every other element to varying degrees. This interdependence must not only be acknowledged but must be accounted for in the systems approach.

Parallel Analysis of Elements - Somewhat related to the interdependence of all elements and subsystems in the systems approach is the concept of treating all elements in parallel rather than in series. In contradistinction to the Western civilization concept of time as being a chronological series of events, each one of which must be complete before the next can take place, the systems approach demands that the end event be considered at the same time as the initiating event in order to properly balance the allocation of resources toward solution of the problem. This is commonly known as "womb-to-tomb" thinking.

Inputs and Outputs in Clear Language - Another important characteristic of the systems approach is the requirement that both inputs and outputs, at all levels in the system, be described in unambiquous language. The key to this requirement is that it removes subjective judgment both as to what is expected in the way of outputs and what is available in terms of inputs to the system. One of the reasons for insisting on the quantitative indices discussed earlier is that numbers do reduce ambiguity.

In simplest terms, a "system" can be defined as "any complete entity consisting of hardware, software, personnel, data, services and facilities which transforms known inputs into desired outputs." Therefore, a system has no meaning unless both inputs and outputs have clear and universal understanding.

Self-Containment/Closed Loop - Since a system has been defined as a "complete entity," this means that a system has individual existence and that it lacks none of its requisite parts. It is complete in itself. A corollary is that the system must be free from any isolated or "orphan" elements which do not contribute to system objectives. Outputs of every element or subsystem must ultimately become part of the system output rather than independent of it. In a sense, this is a restatement of the fact that everything within the system is interdependent.

The Role of the Human

One difficult that must be acknowledged in the field of safety is the high pe ·entage of social behavior involved in hazard analysis and prevention. Therefore, the emphasis on human behavior is quite pronounced in the GWU System Safety course. Whether it be called human factors, human engineering, or just plain human awareness, the role of the human is accented heavily.

Figure 3 illustrates the interface that exists between physical and social sciences. Skirting the traditional battle over whether social sciences are "scientific," predictability (which is a cornerstone of scientific endeavor) is an elusive characteristic, at best, in the social sciences. To illustrate this difference between physical and social sciences, the specific gravity of sulfuric acid (H_2SO_4) has been, is, and will continue to be 1.834, whereas you and I had not been, are not, and never again will be the same persons we were when we awoke this morning!

There will always be a mixture of physical and social forces in any system. However, the mixture ratio will influence the applicability of the systems approach. The higher the percentage of systems effort which involves the physical sciences, the greater the applicability.

The spectrum of system problems in Figure 3 runs from greatest applicability on the left end to least on the right. System safety, as an activity, would probably fall about where "auto safety" is shown. We can do much to make

cars safer--crash helmets, harnesses, inflatable bags for crashworthiness. But in the end, can the automobile be made totally safe if the human is ignored? Obviously not. We can never make people wear seatbelts, helmets or chest protectors. Further, we cannot stop them from driving after they have been drinking! My good friend and colleague, Chuck Miller, has said that we probably should start to design cars to be driven by drunk drivers because there is no way to stop people from driving while drunk.

This pragmatic outlook of accepting the world as it is, rather than idealistically teaching "what ought to be" distinguishes the GWU course from some others.

System Management Foundation

System safety may be the foremost among those activities where moral arguments must be translated or converted into specific tasks. Furthermore, this "conversion into tasks" must ultimately result in specific safety tasks which are described in the language of management--yes, that dirty but real world of cost, performance and schedule!

In a letter dated 14 January 1971, General George S. Brown, Commander of the Air Force Systems Command, said in part:

> "Reports of the USAF Inspector General continue to reflect that systems safety within AFSC is unsatisfactory. There are several underlying problems in this area, including the need to train systems safety engineers. To overcome these problems we must have added management emphasis on systems safety at all levels." (Italics added)

The System Safety course at the George Washington University is based firmly on a SYSTEM MANAGEMENT foundation for a number of compelling reasons:

1. Management and professional system safety personnel both have one basic modus operandi-- "accomplishing through others." While they both may occasionally get in, roll up their sleeves, and "do" something, this is a rare exception. Learning how to step back from the daily rush of detail activity to view the "big picture" of the systems approach is vital to effective system safety work. Further, if the system safety professional accepts a role as simply an "engineer," "analyst," or "investigator," he cannot hope to accomplish his mission because these "doing" roles are only partials of a whole picture.

2. A corollary to the first reason is that since system safety personnel "assure that a system is safe" rather than personally "make the system safe," they must have a 1:1 communication link with management. How can they hope to communicate with top management if they take less than a system management viewpoint? How will they know the system management viewpoint if they have not studied it?

3. One of the major advances of MIL-STD-882 over earlier system safety specifications was in pioneering the concept that system safety was far larger in scope than just "engineering." To state this idea another way, you could be the best safety engineer, analyst or investigator in all the world and still be no more effective in achieving system safety than if you were in Tibet, if you fail to comprehend system management.

4. A primary precept of system safety is that no area or activity in the system development process is free from creating hazards. Therefore, since system safety personnel must be sensitive to all sources of hazards (and management is a hazard source as shown in the Venn diagram of Figure 4), it is imperative to start the study of system safety on the base of system management, the most pervasive activity in system development.

It is no accident that management is listed prior to science and engineering in this definition used in the GWU course:

> "System safety is the optimum degree of hazard elimination and/or control within the constraints or operational effectiveness, time and cost, attained through the specific application of management, scientific and engineering principles throughout all phases of a system life cycle."

The interrelationship of man, machine, media, and management in Figure 4 contains 15 different categories; e.g., man/media, machine/management, media/man/machine/management, etc. Each one of those categories is a source for system hazards which must be either eliminated or controlled.

Using rapid rail transit as an example in Figure 5, management is prominent as a factor in contributing to hazards. As a warning, it should be obvious that Figure 5 ignores the interaction between the factors listed; e.g., possible interaction between passenger vehicle seat versus stand ratio and accident investigation procedures.

Likewise, most of the individual events shown in the Fault Tree illustration in Figure 6 have resulted from management decisions; e.g., policies, procedures, design selections or accepted risks. Note also the high percentage of events in the Tree that are social rather than physical in content.

Figures 4, 5, and 6 are not meant to be exhaustive and complete but to simply trigger further thought and expand the analyst's thinking regarding hazard sources. In fact, the GWU course is often described as a "mind expander." An attempt is made to open up new ways of thinking about hazards, followed by devising methods to either eliminate or control the identified hazards.

Integrative Aspect

A prime thesis of the GWU course is that system safety is not another "specialty" but an integrative activity among the already-too-many specialties. Figure 7 depicts system safety as the "mortar between the bricks" that makes possible a strong wall (system). In other words, the philosophy of the course is that system safety personnel should not be "out-designing the designer." Rather, they should be concentrating their attention on the many interfaces created between functions whenever a large and complex system is divided up into smaller units.

As Figure 7 shows, "design" is separated from "testing," and when this division occurs (necessary as it may be), there are inevitable problems often overlooked by both designers and test engineers. This interface is typical of those areas where system safety personnel will realize the greatest payoff in terms of hazard potential.

FOCUSING FOR MANAGEMENT DECISION

The system safety professional has only one ultimate "reason for being"-- to provide top management with one of two inputs for management decision: (1) the system under consideration is safe enough, or (2) the system under consideration still has the following identified hazards which are neither eliminated nor controlled satisfactorily to meet the system objectives.

As stated earlier, safety is basically a moral argument; i.e., "No one should get killed or injured and there should be no property loss as a result of operating this system." Unfortunately, there are literally millions of moral arguments of equal conviction. Management has no way to handle moral arguments. They do not fit nicely into equations, calculations, or profit/loss ledgers. They must be converted into a new language.

How can safety then be translated into management language? What is the language of management? Management language is three-dimensional-- cost, performance and schedule. To bridge the gap then between a moral argument and the world of cost, performance and schedule, there must be a methodology.

In a nutshell, the methodology required has five basic steps:

1. All possible hazards must be identified.
2. These identified hazards must be ranked first for their severity.
3. These identified hazards must be ranked secondly for their likelihood of occurrence.
4. These identified hazards must be ranked thirdly for the cost, in resources, of either eliminating or controlling them in the system.
5. The rankings of steps 2, 3, and 4 must be combined into a single ranking of management consequence; i.e., where the most severe which will occur most frequently and can be eliminated for the least resource expenditure are on top.

Each of the five basic steps required to translate the moral argument for safety into language that any manager can understand is discussed briefly.

Step 1 - Identify Hazards

This is the function of the various analytical techniques such as Hazard Mode and Effect Analysis (HMEA), Gross Hazard Analysis, and Fault Tree Analysis. Equally essential with

these techniques are analysts with inquisitive, imaginative, and indefatigable minds. Ironically, some system safety courses cover only this first analytical step.

Step 2 - Rank Hazards for Severity

Continuing to use rapid rail transit as an example, Figure 8 is a conversion of the four hazard levels of MIL-STD-882 into rail transit effects. Rather than having everyone decide what a "critical" hazard is, the translation has been made so that there is universal understanding of this level. If there were 478 hazards identified in Step 1, then every one of the 478 should have either an A, B, C, or D assigned to it.

Step 3 - Rank Hazards for Likelihood

After all 478 identified hazards have been categorized for severity, they must be ranked for probability of occurrence. One example of how this might be accomplished is shown in Figure 9. The reason that the four levels of probability are in a logarithmic scale is because the human response to sensory stimuli, according to Fechner's Law, is logarithmic. Perception of probabilities is probably similar to sensory perception. When this step is complete, all 478 identified hazards should have two letters assigned-- one for severity and one for probability.

Step 4 - Rank Hazards for Elimination/Control Resources

The third letter to be assigned each of the 478 hazards should be from a table such as shown in Figure 10. This step requires an intermediate conversion of various resources (e.g., policy, procedures, manpower, technology, facilities, materials, and schedule) into a dollar equivalence prior to selecting a code letter. Nevertheless, this estimate of the amount of resources is essential in order to speak management's language. Now all 478 hazards have three letters assigned.

Step 5 - Rank Hazards for Management Consequence

Once three code letters (one each from Steps 2, 3, and 4) have been assigned to all 478 identified hazards, the focusing for management consequence is achieved by combining the three individual code letters into one overall index of significance. The Hazard Totem Pole shown in Figure 11 lists these code combinations in order of consequence for management decision.

Obviously, there are never enough resources to completely eliminate every possible hazard. For this reason, management must set a "decision point" or cutoff level in the Hazard Totem Pole. This decision point is drawn at that significance ranking code below which all remaining hazards will be ignored. The decision point may be established by either (1) the reduction of hazard significance to a level which management considers adequate or (2) the depletion of resources available for application to hazard elimination or control.

To illustrate this decision point, management could decide that it will eliminate and/or control all hazards in the first 7 levels or categories in the Hazard Totem Pole; i.e., all the AJP, AJQ, AKP, BJP, AJR, AKQ, and ALP hazards. This would mean that 31 of the 478 identified hazards will require resources to be allocated by management for purposes of eliminating or controlling the hazards. (Note that there were no AJQ or AKQ hazards.)

It is important to also note that while management will be committing resources for the first 7 levels in the Hazard Totem Pole, they will, by this very action, be deliberately ignoring all remaining 57 levels in the Hazard Totem Pole (which contain the remaining 447 hazards!). Therefore, the decision point becomes that point which separates action from inaction regarding hazards.

RESOLUTION OF HAZARDS

MIL-STD-882 describes a series of actions for satisfying safety requirements of a system design. The series is known as "system safety precedence." This precedence is shown in logic diagram format in Figure 12.

Continuing the rapid rail transit example where management has now decided to eliminate or control 31 of the 478 identified hazards in the Hazard Totem Pole, a decision must be made on HOW to eliminate or control them. Figure 12 shows four alternatives (numbered 1 through 4) for this decision.

With the exception of those hazards which can be eliminated very economically early in the design stage, the four alternatives of Figure 12 are numbered in a hierarchy of decreasing effectiveness as well as decreasing cost. Therefore, the lower the number in the hierarchy, the more effective the choice will be in satisfying system safety requirements even though there may be higher cost associated with the action. (A more detailed discussion of this concept appears in Reference 3.)

The dotted lines in Figure 12 illustrate something not discussed in MIL-STD-882. Two conditions, both of which are undesirable, are shown in dotted lines. First, a system can be tolerant to identified hazards without the knowledge of either designers or operators. Secondly, the system can be intolerant to identified hazards, either unknowingly (most serious) or knowingly. Hazards which are knowingly intolerable are often described as "accepted risks." Those risks are the ones for which insurance is purchased.

REFERENCES

1. Wilmotte, Raymond M., "Communication of Risk," "Proceedings of the Second Government/Industry System Safety Conference, Goddard Space Flight Center, 26-28 May 1971.

2. Grose, Vernon L., "Constraints on Application of Systems Methodology to Socio-Economic Needs" Proceedings of the First Western Space Congress, 27-29 October 1970, Santa Maria, California.

3. Grose, Vernon L., "System Safety in Rapid Rail Transit," as presented to the Rail Transit Conference, sponsored by the American Transit Association and the Institute for Rapid Transit, San Francisco, California, 13-16 April 1971.

THE PROBLEM

Trying to do well that which we do not understand

Figure 1

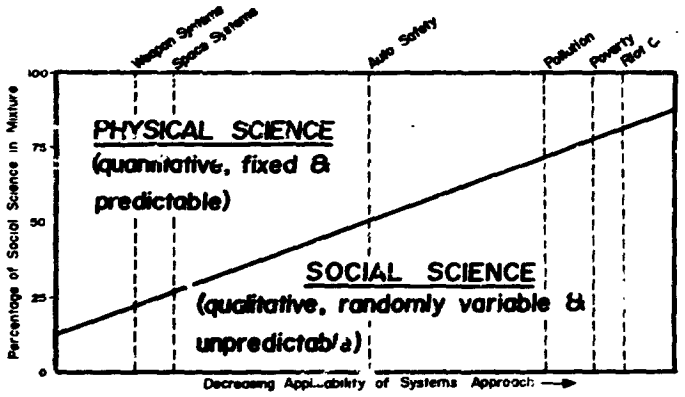
SYSTEM SAFETY EDUCATION FOCUSED ON SYSTEM MANAGEMENT
Vernon L. Grose

- Methodical
- Objective
- Quantitative or Measurable
- Analytical
- Subsystem Interdependence
- Parallel Analysis of Elements
- Inputs & Outputs in Clear Language
- Self-Containment/Closed Loop

"SYSTEMS" CHARACTERISTICS

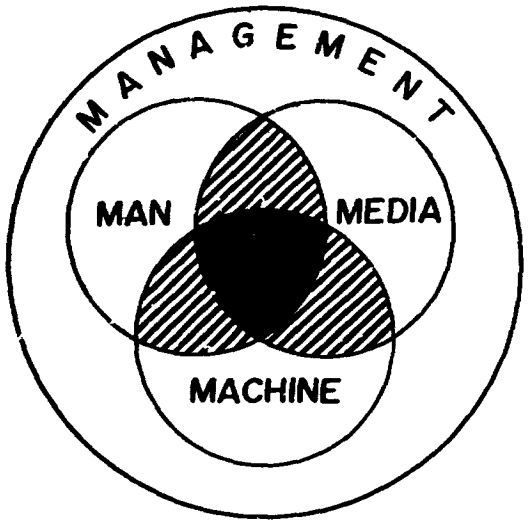
Figure 2

SYSTEM SAFETY EDUCATION FOCUSED ON SYSTEM MANAGEMENT
Vernon L. Grose



The Science "Mixture Ratio" in the Systems Approach

Figure 3



Interrelationship of System Safety Factors

Figure 4

SYSTEM SAFETY EDUCATION FOCUSED ON SYSTEM MANAGEMENT
Vernon L. Grose

SYSTEM SAFETY

"The Strength Between Functions"

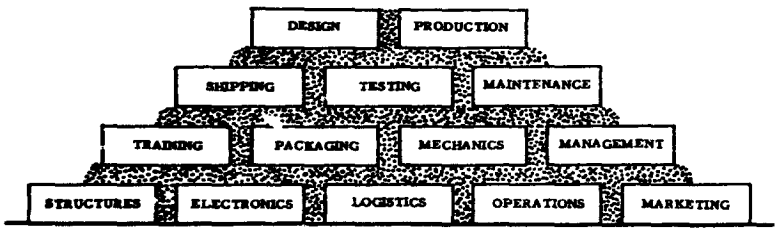
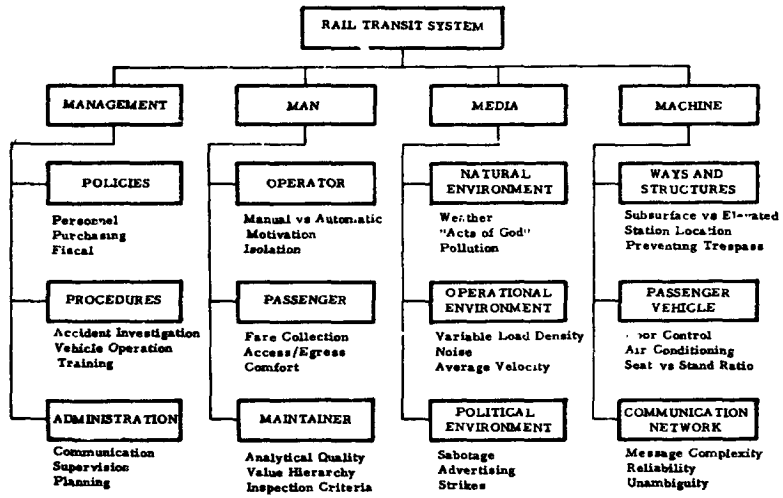


Figure 7

SYSTEM SAFETY EDUCATION FOCUSED ON SYSTEM MANAGEMENT
Vernon L. Grose



TYPICAL SYSTEM SAFETY FACTORS IN RAPID RAIL TRANSIT

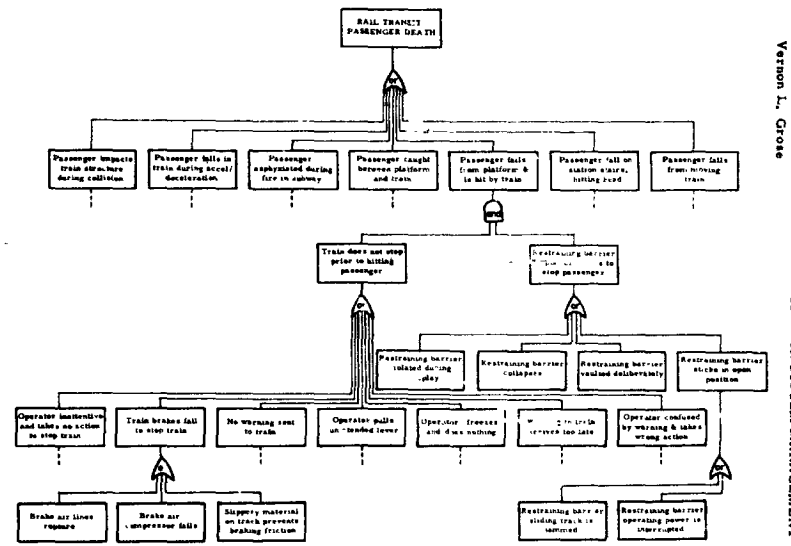
Figure 5

CODE	MIL-STD-882 HAZARD LEVEL	EFFECT ON SYSTEM OBJECTIVES	EFFECT ON FUNCTIONAL CAPABILITY	EFFECT ON PERSONNEL SAFETY
A	Catastrophic	Rail transit rendered impossible-- Mission is lost	No portion of rail transit system can be salvaged-- Total loss	Personnel suffer death or multiple injuries by factors in Code B
B	Critical	Rail transit impaired seriously-- Mission accomplished only by auxiliary methods	Two or more major sub-systems of rail transit are damaged-- This condition requires remote depot maintenance	Personnel injured either: (1) operating the transit system, (2) maintaining the system, (3) being transported by system, or (4) being in vicinity of the transit system
C	Marginal	Rail transit is possible by utilizing available redundant operational options	No more than one component or subsystem damaged. This condition is either repairable or replaceable within one hour on site	Personnel-injuring factors in Code B can be controlled by either automatic devices, warning devices or special operating procedures
D	Negligible	No measureable effect on rail transit mission	No apparent damage to the rail transit system	No injury to personnel

HAZARD SEVERITY FOR RAIL TRANSIT SYSTEM

Figure 8

SYSTEM SAFETY EDUCATION FOCUSED ON SYSTEM MANAGEMENT
Vernon L. Grose



Rail Transit Fault Tree Illustration

Figure 6

SYSTEM SAFETY EDUCATION FOCUSED ON SYSTEM MANAGEMENT
Vernon L. Grose

CODE	DESCRIPTION OF SITUATION
J	Hazard of interest will occur within 10 cumulative hours of operation
K	Hazard of interest will occur within 100 cumulative hours (4 cumulative days) of operation
L	Hazard of interest will occur within 1000 cumulative hours (41 cumulative days) of operation
M	Hazard of interest will occur within 10,000 cumulative hours (14 cumulative months) of operation

HAZARD PROBABILITY FOR RAIL TRANSIT SYSTEM

Figure 9

CODE	CALCULATED DOLLAR EQUIVALENCE*
P	Less than $1000 required to eliminate/control this hazard
Q	$1000 - 10,000 required to eliminate/control this hazard
R	$10,000 - 100,000 required to eliminate/control this hazard
S	Over $100,000 required to eliminate/control this hazard

*Calculated dollar value of all resources (revision of policy, procedures, manpower, dollars, technology, facilities, materials, and schedule) required to either eliminate or control the hazard of interest.

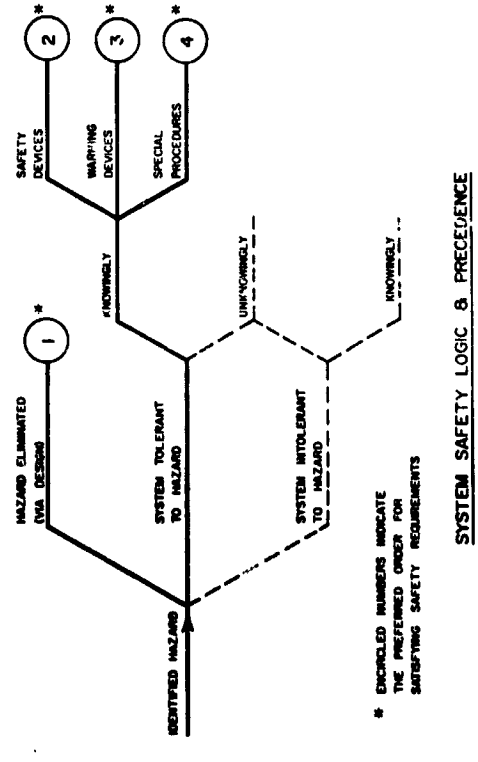
HAZARD ELIMINATION/CONTROL RESOURCES

Figure 10

Hazard Significance Ranking	Code Combination			Number of Rail Transit System Hazards
	Hazard Severity	Hazard Probability	Hazard Resources	
1	A	J	P	3
2	A	J	Q	None
3	A	K	P	1
4	B	J	P	16
5	A	J	R	7
6	A	K	Q	None
7	A	L	P	4
8	B	J	Q	22
64	D	M	S	2

HAZARD TOTEM POLE

Figure 11



SYSTEM SAFETY LOGIC & PRECEDENCE

Figure 12

SECTION III

QUESTIONS AND ANSWERS

QUESTION: I would like to ask the panel if there is any concerted effort in the educational field to incorporate a system safety engineering course in all undergraduate engineering programs -- aeronautical, industrial, electrical, etc.

DR. JOHNSTON: We can only speak for the industrial engineering department. As far as I know Texas A&M has none. Actually what we are looking at in a system safety engineering course as far as for a person working on a degree in mechanical engineering or something at the undergraduate level, this would have to be an elective. What we are doing at Texas A&M is trying to make people in all the engineering disciplines aware, probably more so toward product safety and product liability. We are getting more and more people to come in and take the courses as electives, but as far as a requirement, I would say there is no attempt to put it into the undergraduate discipline across the board. Most all of the people that take or get a B.S. in industrial engineering will take a course in system safety engineering as it is offered.

MR. GROSE: Gene I don't know if you care to respond to this or not, are you aware of any activities at USC where they have tried to introduce this?

EUGENE HOLT: I don't think that is necessarily a good idea. Outside of a system safety curriculum or a safety program, the only way to incorporate system safety engineering into EE or ME courses, I think would be in each basic course and that would be rather hard to do. I think because of the basic structure of universities and the way curriculums are established, etc. it would be hard to do that. It is a good idea but at present it is not workable I am afraid.

JACK MANSFIELD (GWU): It is about the same answer you just got from Gene Holt. This was discussed very recently at a system safety society meeting here in Washington. As a matter of how to get this into an undergraduate, should something be put in. I think it will not come by the university taking the initiative on it. If it comes it is going to be by societies or conferences or things making recommendations and putting a little pressure on universities to get something like this as a part of some undergraduate course. I don't think a complete course itself would be of value because it would be an elective almost certainly and would not cover a great many people. A portion of a few hours of this type of thing in some other undergraduate course would be an effective thing at least as a beginning and as I say it is going to have to come from pressure outside.

GEORGE CRANSTON: I have a question that is related to the one that was just asked. I want to put it in a little different way I think. We have been told by the educators this morning that we do not have a philosophy of system safety or asking us if we have a philosophy of system safety - that is a legitimate question, but I want to turn the question around after what I have heard and ask them if they have a philosophy of education in our university system and the reason I ask this, from what I have heard it appears that every course is a special course started to meet some special need of some special organization. What we have heard today is the philosophy of that particular course to meet that need, but we have not heard a philosophy about how do we educate people generally in this field.

ANSWER: I think to the common layman it would seem an easier task than it really is to break through the structures at universities. You have to understand the curriculum committees to start with. University curriculum committees are a very strange kind of thing. You approach them with a new idea, no matter how firmly and strongly you believe in it you have to convince them and sometimes they are very hard to convince. It is very true, Mr. Cranston, that these are special interest kind of courses that we have discussed this morning and unfortunately, that is the level we are at right now. I agree with you, we need to do something about that and to motivate. I think maybe an aroused and intelligent public

will do that. Societies will do that if we will continue to motivate people, it might happen.

MR. GROSE: I think you can leave that one open, George, as a rhetorical question.

DR. BALL: This is a comment related to the last question and then a direct question. A couple of weeks ago the National Academy of Engineering held a two day conference on consumer products. Dr. Carl Clark will be speaking on this subject tomorrow and this first workshop was on safety. One of the recommendations that came out of that workshop had to do with the education of the people who are designing and will be designing consumer products such as mowing machines, bicycles, etc. It seems to me that the essence is to teach the design decision-making process. I think it is quite impractical for every aspect of design decision-making to be taught in a separate course so my comment would be that there is a tremendous need in the consumer products area, that the essence is to teach the design decision process, to teach the design and to take into account all aspects of design decision-making including the safety. My question would be to what extent are you teaching the design decision process, have you included safety in this area, not as a special course, not as an option, but simply as an inherent and integral part in the design decision process?

ANSWER: In fairness I think to that question, those present here today are not in the decision making position in the university in order to do that. I think it is one of those things that we are obliged to do though from a professional point of view, to urge that this be done inside university structures. It suffers from all the ills of any bureaucracy I'm sure and it only responds very lethargically to any impulse that comes from society, and I think it is one of those things that conferences like this are essential in proposing as well as professional societies and other people like Ralph Nader. Mr. Nader even has his own way of making himself known but the point is that I agree with what you say, Les, that the decision-making process is sufficiently broad that we cannot afford specialized courses. We do need to focus one more time because the university process has been one of division and separating it to specialties when in actuality I'm sure we need an integrated type of teaching in the universities.

JERRY LEDERER: I have three different comments. First of all, about ten years ago I got the Deans of some of the countries foremost engineering schools together to discuss putting into the curriculars some safety and especially human factors and I was told that there just isn't time. Some universities such as Cornell had increased their engineering course to 5 years to put in humanities as they thought the students should have something on humanities. They had gotten to the point where they are giving them almost entirely engineering. There isn't time, they said, to do this. I would think that at least they could give a couple of electives per semester to get the students thinking about this. The second thing is that we have heard all through this conference that it is the executive who makes the decisions, the businessman. How many universities, if any, have a lecture or two lecturers in their schools of business administration so that you can get the men who become the administrators to recognize there is such a problem. I wouldn't call it safety, I'd call it risk management, part of the management picture. The third item is in connection with the use of system safety for accident investigation. The idea was advanced that you could use those same logic diagrams to conduct the investigation. Also you can use the logic diagrams that were involved in the design to help with the investigation. If you can go back to those logic diagrams, I would think it would facilitate the investigation of an accident enormously in many cases, where structural problems are concerned or systems problems come up, failure of systems and things like that.

QUESTION: I'm not sure that there is such a thing as a non-Government-related industry any more, but if there is such a thing, is there any indication that this side of industry is accepting the concept of system safety as well as the educational side and providing opportunities in form of jobs and salaries that would lure the people from engineering into the system safety side of the house?

ANSWER: I'll respond and I don't know of any. I would just simply say this. I am reasonably certain that the recent emphasis on product reliability is causing the civil sector of the economy to respond to the idea that there are risks that must be addressed and our experience in our particular course is that the students attending from other than aerospace or military part of the economy say that there is a ground swell. It may not be great yet, but it is perceptible and I think we are going to see increasing interest in that area.

COMMENT: I have an observation, I recently read a report that the President of Honda Motor Company that makes the automobiles in Japan has been accused of murder due to reported 16 or 17 deaths which supposedly are due to a design deficiency in the automobile. They are accusing the President of that Company of murder. Obviously, Japan has kind of a strange legal system but those kinds of activities might motivate the consumer product people to respond.

JOHN FRENCH/MSC: I'd like to make one comment. In keeping abreast of system safety activities it would appear appropriate that you visit some of the NASA Centers. I'll speak for Manned Spacecraft Center specifically because we have been involved in system safety from a management and engineering technique standpoint. I would like to welcome any of you gentlemen to come down and discuss these things with us.

C.O. MILLER: Vern, addressing the last two questions, I might mention a visitor we had at the Board a couple of weeks ago. He was a Professor of Engineering from a Midwest University. He had never heard of the term "System Safety" and frankly I don't really know what prompted his visit other than he said, "I've been worried that our people have been coming out of the engineering schools without an appreciation for the hazards that can be designed into a program." I then broke into my standard three-hour lecture on system safety. The point is, I think there is an awareness, well outside the DoD environment on this particular problem as typified by this man. What I gained from it, and I would offer a challenge to not only you on the stage but the people in the audience, I wonder why we don't go back in our memories to our undergraduate days and say for example in aeronautical or say an aerodynamics course, how would we go back to our professor and say, where could you in this course, within its existing framework, introduce some thoughts about system safety?

I submit that I could do this. I could go back in and talk to them about stall spin accidents and where in his course, just as he teaches it today, in an analytical sense or any of a number of other ways, he could come up and engender a feeling in this undergraduate that you ought to look at the hazards. I believe every single one of us, if we chose to, could go back into our own undergraduate field and introduce ideas like this but it is a monumental task.

MR. GROSE: Do you have a practical way, Chuck, to suggest how this might be done. Should we all go back to our own schools as alumni?

MR. MILLER: I think it would be a tremendous challenge to the system safety society to do just this on a local basis.

MR. SHAW/TRW: One of the means obviously of broad education is availability of the literature. Most everyone in the engineering game recognizes it gets obsolete pretty quick and it is a habit of most of the brotherhood to read widely. Coupling that with the idea of the old academic principle of publish or perish, I'd like to raise the question, do any of you gentlemen know of texts available or being prepared at this time on the general subject of system safety?

MR. GROSE: Willie Hammer who spoke yesterday morning is writing a book about it. Willie's book, he tells me, is within 9 months of publication. I have reason to believe there are other books in the mill but I don't have dates.

MR. HOLT: I would like to get a plug out of this. In collaboration with Mr. Richard L. Reeb, who is system safety manager of McDonnell-Douglas Astronautics in Huntington Beach, California, he and I, he is writing a management section and I am writing an engineering section, we're trying to write a book. We don't have any dates but we've got quite a few pages together now -- it's looking good.

COMMENT: I might add one thing too, Bill Rogers at TRW has one in preparation. I have no idea of the date there either.

R. ALTGELT/EATON CORPORATION: I would like to know whether there is a science we might call safety economics that would say, to put it into example form, that one accident would take on the average one-man life and we could show that in the course of a year say X men's lives are taken by this typical accident occurring, and we could show that it would take Y-men's lives of people who are working in factories to eliminate this or eliminate a percentage of this. So far I have been dodging the dollar aspects of it and I recognize a man's life snuffed out isn't the same as the man-life consumer in the shop to add another aspect, conceivably there would be some man-lives that would be lost in industrial accidents producing this apparatus; but I'm wondering, then of course the insurance companies would come in and assign a dollar value to the man-lives and premiums that they have to put out and industries could perhaps be faced with law suits, which could be assigned a dollar value. I'm wondering if there is a science that approaches safety in this way, dollars loss versus dollars spent to prevent, or lives lost versus lives spent to prevent?

ANSWER: I would think that all of our courses try to take this approach. Basically, we try to show the economics whether we are talking about designing a system or probably the specific course would be in our industrial safety-type courses where we talk about cost of accidents, accident elimination and budgeting for safety. I think this is our philosophy inherent in all of our courses. It's the name of the game, really.