N72-25985

INTEGRATING A MULTIFACETED SYSTEM SAFETY PROGRAM FOR A LARGE COMPLEX SYSTEM

By

Mr. W. W. Malasky
Manager
Assurance Engineering
Litton Systems, Inc.

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

INTRODUCTION

Man's concern with safety dates back to earliest pre-historic times, when his primary objective was survival against his enemies and the elements. However, as is the case with many other disciplines, the greatest advances made in System Safety have occurred in recent times. In the main, these advances have come about through efforts focused upon two classes of activity. One engaged in by relatively few people but of great interest to the general public, relates to man's recent extensions of his travels into new and unfamiliar environments - into the depths of the ocean, through the atmosphere at great heights and speeds, into outer space and onto the surface of the moon. The other interfaces with larger numbers of people and is concerned with the prevention of hazardous events that are potentially catastrophic to many, such as inadvertent nuclear explosion, of either a military device or a commercial power generating station, or loss of a large passenger aircraft.

The areas of System Safety Technology which have benefited the most as a result of these recent advances are:

1. The development of techniques for the identification of inherent problems so that all hazards associated with a given undertaking can be determined. This aspect of System safety Technology is discussed only peripherally in this document.
2. The formalizing of interfaces between System Safety and other technologies. This aspect will be dealt with at some length.

The need for such formalization in a large, complex system can be illustrated by considering a large ship such as LHA. This ship has many of the qualities associated with a city in that large numbers of people work, are housed, engage in recreational pursuits, are fed and are tended to medically. It has the qualities of an industrial complex by virtue of the various shops it contains. It has many of the problems usually associated with military operations, such as armament activity, storage of large quantities of combustibles and the need to conduct aircraft operations during good and inclement weather conditions. Finally, safety interfaces that relate to ecology and pollution must now be considered in a more formal fashion. In relation to this latter interface it can be considered that the ironclad rule usually accorded to ships' captains is now being challenged as a consequence of the pre-dawn collision between two oil tankers that occurred on 18 January 1971 which spilled nearly 900,000 gallons of oil into the ecologically sensitive San Francisco Bay.

INTERFACE WITH SYSTEM EFFECTIVENESS

The disciplines that conventionally relate most intimately to System Safety are Reliability (R), Maintainability (M), Quality Assurance (Q), Human Factors (H), and Value Engineering (V). Unification of these, and other, disciplines with System Safety can be achieved through various techniques. The one chosen for use in this presentation is system effectiveness, E, which is defined as

> The measure of the extent to which a system may be expected to achieve a set of stated system objectives.

In general form the functional relationship between E and the "ilities" listed can be written.

$$E(t) = f\left[\left(\frac{S}{\frac{a}{S_s}}\right), \left(\frac{R}{\frac{a}{R_s}}\right), \left(\frac{M}{\frac{a}{M_s}}\right), \left(\frac{Q}{\frac{a}{Q_s}}\right), \left(\frac{H}{\frac{a}{H_s}}\right), \left(\frac{V}{\frac{a}{V_s}}\right)\right] \qquad 1$$

since E is a function of t, and where

a is the achieved level of each parameter at some specified time in the system's life, and

s is the specified level established for that parameter.

The functional relationship expressed by equation (1) needs to be written as an explicit expression if a value of E is to be obtained at some point in time. However, no single explicit expression can be proposed, for E(t) depends upon factors that are unique to each system.

$$E(t) = f\left[\left(\frac{S_a}{S_s}\right)^{k_1}, \left(\frac{R_a}{R_s}\right)^{k_2}, \left(\frac{M_a}{M_s}\right)^{k_3}, \cdots\right] \qquad 2$$

$$0 \leq k_i \leq 1$$

Because of the considerable complexities in establishing and measuring the various parameters that comprise equation (2), it is necessary to obtain values for E by a process of optimization. This is discussed later.

INTERFACE WITH RELIABILITY

System Safety is more closely related to and allied with reliability than with any of the other disciplines defined by E. The basis for this strong interface becomes apparent upon examination of fundamental definitions. The generally accepted definition of Reliability is

> The probability that a system performs its intended function for a specified period of time under a set of specified conditions.

A definition for Safety that fits most requirements is

> Freedom from those conditions that can cause injury or death to personnel, damage to, or loss of, equipment or property.

Disregarding, for the moment, the fact that the definition for safety is qualitative rather than probabilistic in nature, it is evident that hazards which occur without causing injury or death to personnel, can fall into either the safety or reliability domain Further, it is also evident that injuries and fatalities can result from the inability of a system to perform its intended function, a reliability concern. Conversely, the occurrence of a hazard which affects only personnel, a safety concern, can, as a secondary effect, be responsible for preventing a system from performing its intended function, thereby degrading the reliability of the system.

One problem is brought about by the fact that the components of E are almost never completely independent of each other. Another relates to the fact that the components have different "utility values", k_i. When these are known, equation (1) can be written.

In order to define an interface between safety and reliability which can be operated upon by conventional scientific methods, it is necessary that both domains be quantified using compatible units. In the safety domain quantification is accomplished by assigning probabilities to events and then combining these individual probabilities into an overall probability. In most general terms, all safety calculations are derivable from the expression

$$P(S) + P(F) = 1 \qquad 3$$

where

- S is the set of events that describe safe performance
- F is the set of events that describe unsafe performance
- P(S) and P(F) are probabilities of the occurrence of S and F respectively

Having transformed safety into probabilistic terms, mathematical operation is carried out through manipulation with sample points, sets and events. It is possible to represent the S and F sets by means of a Venn diagram such as the one shown in figure 1. In this figure, the rectangle, I, is presumed to contain a finite number of sample points. These define the safe event, S, the unsafe event, S, the reliable event, R, and the unreliable event, R. In turn, each of these four events consist of

a defined collection of sample points, and each is a subset that is wholly contained in the universe, I. The interface between safety and reliability is represented by the lined area found between the arc acb, the extension of the safety event into the reliability event, and the arc dbb, the extension of the reliability event into safety. Two implications, readily apparent from an examination of figure 1 are:

1. R, the unreliable event, which is represented by all of the area outside the R event, includes sample points that are in the safe event.
2. Similarly, S, the unsafe event, represented by all the area outside S, includes sample points that are contained in R.

It might be presumed from an examination of figure 1 that the common goal of both safety and reliability is to expand the intersection of S and R, $S \cap R$, until $S \cap R = I$. This would be valid goal under the circumstance that I is comprised only of events in S and R. Complications arise when events and other disciplines must be included in I.

INTERFACE WITH RELIABILITY AND MAINTAINABILITY

Suppose now that maintainability considerations, which are also closely allied with the safety domain, are now inserted in I as shown in Figure 2. Maintainability is a characteristic of System Design, installation and operations which may be defined, for both hardware and human systems as

> The probability that the system will be retained in, or restored to, a specified condition within a given period of time, presuming that maintenance is performed in accordance with a set of prescribed procedures and allocated resources.

In turn, the term maintenance may be defined as

> All actions necessary for retaining this system or restoring it to a specified condition.

Since this definition of Maintainability is already expressed as a probability, its interface with Safety and Reliability can be expressed by means of a Venn diagram. In this, Figure 2, all the relationships between S, R and their compliments are the same as in Figure 1. The interface between M and S is represented in Figure 2 by the arc cdf, and the interface between M and R is represented by the arc ecs. The area common to all three events, S R M, is represented by the cross-hatched area bounded by the arcs c, cd and db. Perhaps the most obvious relationship observable from Figure 2 is that not all the sample points in the subset $M \cap R$ relate to the S event. This is due to the fact that the fundamental role of maintainability is to increase system life, without necessarily enhancing safety. As a consequence, the utility of maintainability to the system, reflected by the value of E, is enhanced as:

1. It becomes more expensive to replace the system rather than to keep it maintained.
2. Achieving longer system life through improved reliability or redundancy of parts becomes less cost effective than carrying out maintenance activities.

Consider now the safe event in relation to the R and M events shown in Figure 2. Let the sample points in S be divided into two subsets, one relating only to equipment damage, S_E, and one relating only to personnel injury, S_P. It is clear that S_P can occur even when S_E does not. For example, consider the case in which the life support system of a submarine is damaged during submerged operations. Presuming that a monitor and alarm system exists and that it can provide adequate warning time, there can be various sample points in S_P that may be selected such that the safe event can nevertheless occur.

Some sample points, in the area defined by $S \cap M$, presume that maintenance is possible, while others, in $S \cap R$, presume that the equipment to be used for contingency, escape or rescue is reliable. The following guidelines are offered in assigning sample points to $S \cap M$, $S \cap R$ or $S \cap R \cap M$.

1. Direct removal and replacement of faulty equipment, or the repair by personnel in situ, is contained in $S \cap M$.
2. Switching to a redundant equipment through remote means such as telemetry or in situ by attending personnel, is contained in $S \cap M$.

3. Switching to redundant equipment through the use of built-in, self checking circuits is contained in S∩M∩R.
4. Redundancy used in majority voting, for use in a fail safe configuration for replicated elements is contained in S∩R.

The process of idealizing the interrelationship described by Figure 1 involved an expansion by R and S sample points in I such that S∩R I. Although, in Figure 2, there are sample points located both in M and in R which permit the event S to occur, this process of idealizing can be extended to R∩S∩M by permitting the union of either R or M to fill the universe. That is,

$$(S \cap R) \cup (S \cap M) = I$$

It is clear that, even when there are as far as three variables, there will be advantages and disadvantages to selecting one of the two possible intersections for expansion in I. Increasing the number of variables that interact within I emphasizes still further the need for increasing the intersection of S with other parameters through the process of optimization.

SYSTEMS SAFETY IMPLIES OPTIMIZATION

It has been noted that the application of scientific methodology to safety requires the ability to quantify. Further, it is considered that scientific methodology applied to system safety implies optimization. To offer evidence for this point of view consider first the meaning of the term System Safety. First, a system may be defined as

> A device, scheme or procedure which behaves in accordance with some description, its function being to operate on information and/or energy and/or matter in some time reference in order to yield information and/or energy and/or matter.

This definition places no restriction upon the size or complexity of the device, scheme or procedure under consideration. Large systems such as the LHA, are usually comprised of some composite of operational and support equipment, personnel, facilities and software which are used together as an entity to perform or support a specified role. The operational role for a function performed by a given system is often referred to as its "mission". A system may be described by specifying

1. Its inputs and outputs as function of time.
2. All the possible conditions (states) of the system; i.e., the system phase space.
3. A descriptive model relating inputs, outputs, and system space as a function of time.

System inputs for LHA includes, among hundreds of others, operational plans, contingency operational plans, qualification and training requirements of crew members, maintenance and overhaul activities and a description of weather conditions. The system model includes considerations such as the rate of fuel consumption as a function of speed and range as a function of pitch and roll and alternate modes of operation in response to potential hardware and personnel problems. A definition for System Safety which relates all necessary factors is

> An optimum degree of safety, established within the constraints of operational effectiveness, time, cost and other applicable interfaces to safety, that is achievable throughout the life cycle of the system.

This definition does not imply that one, unique optimum is appropriate for the life of a system, although this possibility is not unacceptable. Rather, the definition establishes a requirement that sytems analysis techniques be applied to the domain of safety, and that these techniques include a quantification of safety over the entire life of the system based upon all facets of the system. As such, optimization is the essence of System Safety. It may be defined as

> The application of mathematics and simulation techniques for identification, examination and calibration of the interaction between and among the elements of the system.

OPTIMIZING SYSTEM SAFETY

Achieving an "optimum degree of safety" requires that choices be made among the various alternative means available for arriving at a chosen objective. Various "alternative

means" may be found within the domains of those disciplines defined by E or wholly within the domain of safety. This latter circumstance is illustrated by Figure 3 and is taken from the domain of hazard analysis. On the left hand side are the kinds of hazard analyses that are performed, generally successively in time, on a large system. On the right are shown the logical flow of hazard analysis outputs as a function of time. At one extreme, at t=0, are those tasks which imply the prevention of hazardous occurrences, and at the other extreme are those safety activities which are intended to minimize the effects of a hazardous occurrence. Although included for completeness, the tradeoffs between alternative means in one discipline are not as difficult as the selection of trade-offs among differing disciplines. Examples of alternate means which could be selected as optimum between various disciplines include configurations:

1. Of minimum complicity, as such that minimum demands are placed upon human skills for operation or maintenance.
2. Such that the failure of any one component can not lead to failure of the system or to personnel fatality.
3. Which provide an indication of those components that have become degraded and, consequently, are likely to fail.

It is apparent that no intelligent evaluation of alternative means can be made without relating to system objectives. If the domain of human safety is not involved, there is no hesitancy in permitting the system output to range over the domain of all possibilities in order to establish an optimum. System safety, however, is not free to trade-off all possible variations in system output. Specifically, it is considered undesirable in our culture to equate the value of human life in terms as inanimate equipment or money. Similarly, the notion that risks may be intentionally taken as part of the operation of a non-military system, based upon a schedule of compensation for injury or fatalities that may occur is equally undesirable in our culture. The suggestion that such an attitude is not rigorously pursued has, particularly in recent times, brought about confrontation between various elements of our society and the creation of a host of new industry and government agencies oriented towards resolving these differences. System safety cannot help but find itself at the focus of such considerations, and can make a valid contribution toward enhancing safety in our society through techniques that are useful for integrating multi-faceted programs for large, complex systems.

REFERENCES

J. E. Bylin, When Ships Don't Pass in the Night, The Wall Street Journal, 9 March 1971

S. W. Malasky, System Safety, Sparten Books (publication date to be announced)

J. F. McCloskey, and F. N. Trefethen, Operations Research for Management John Hopkins Press, 1956

F. E. Hohn, Applied Boolean Algebra, McMillian Company, 1960

R. M. Wilmotte, The Management and the Risk, IEEE Spectrum, April 1971, pp. 31-35

S. W. Malasky, Value Engineering Aspects of Safety in Manned Space Programs, Journal of Value Engineering, May 1966

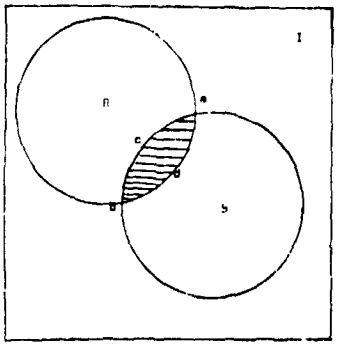
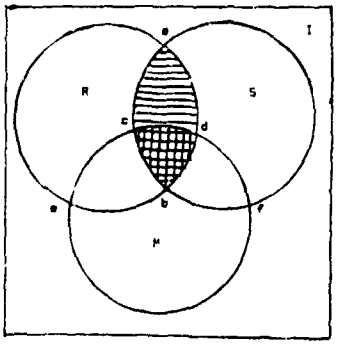


Figure 1 Reliability-Safety Venn Diagram



Reliability-Safety-Maintainability Venn Diagram

FIGURE 1

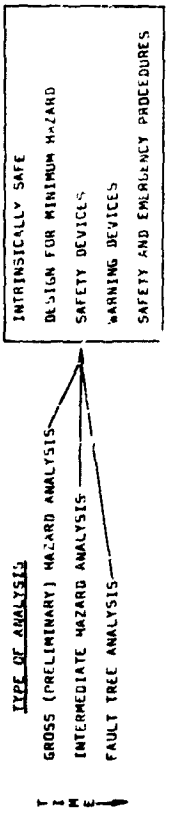


FIGURE 2