N72-25960

PRECEDING PAGE BLANK NOT FILMED

WHY SYSTEM SAFETY PROGRAMS CAN FAIL

Mr. Willie Hammer

Member

Senior Technical Staff
Hughes Aircraft Company

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

As a participant of the first Air Force-Industry Conference on System Safety in 1963, I remember the aims and claims of the proponents of this new concept; the presentations on why System Safety programs were necessary; and other (hopeful) assurances that System Safety programs would minimize the number of accidents involving new systems. After eight years, I believe we have neither achieved the aims nor fulfilled the claims. This paper will try to indicate why not, and why they can continue to fail. My experience has been with DOD activities, procedures, specifications and standards, and my comments are predicated on that experience. NASA personnel will probably be able to correlate those comments related to DOD with their own practices and problems.

Let's start at the beginning, with the initial requirement for a System Safety program in a Statement of Work.

The item which can contribute most to failure of a System Safety program is ambiguity, lack of clear definition, use of obsolete requirements, and pure typographical errors in a poor Statement of Work.

This leads me to a set of axioms regarding contractors efforts. They apply to contractors for ditch-digging, the aerospace industry, or any other activity. They are not intended to be derogatory; they are merely basic facts of life which everyone should understand.

Axiom #1 - No contractor will accomplish a task unless he is specifically and contractually required to do so.

Axiom #2 - No contractor will include in a proposal for a contract any uncalled for effort which will increase his cost so he might not be awarded the contract.

Axiom #3 - Any requirement which is not clearly stated will be interpreted to the best advantage of the contractor.

Axiom #4 - A contractor will pay more attention to a requirement which stipulates a penalty for noncompliance, than to a requirement for which no penalty is indicated.

When MIL-STD-882 was being coordinated, some engineers argued (and won) that no other specifications or standards should be referenced; they should be included in the Statement of Work. Frequently they are not. Some Statements of Work still refer to specifications and standards which have long been rescinded. Add typographical errors, and the problems grow even more complicated. I have seen AFR 127-100, Responsibilities for the Explosives Accident Prevention Program (which involves relationships between the Air Force and the Armed Services Explosive Safety Board), with which the contractor has no concern, cited when AFM 127-100, Explosives Safety, was meant. Axioms #1 and 3 apply in such cases.

An especially miserable requirement I have seen in a Statement of Work is: "The principles in AFSC DH 1-6 will be observed." What principles? I found one ------- and it was wrong. (In Design Note 4B2: Fuel/Propellant Equipment, it states: "Component design and selection must be based on the fail-safe principle, i.e., failure will cause minimum system degradation." Actually, the fail-safe principle is: first and foremost to prevent injury; secondly to prevent damage; and lastly, to prevent system degradation.)

Next I would like to propound "Hammer's Law": The probability of failure of a System Safety program varies directly as the square of the time from system concept until a firm, clear, funded System Safety requirement is issued in a Statement of Work. If the requirement isn't in early, there may be problems; if it is left until the end of development, don't expect much. It is easier to guide designers into safe practices than it is to change prepared designs.

Another detriment to the success of any System Safety program is the use of "weasel" words in Statements of Work, specifications, standards and other criteria. Safety requirements are indicated and then qualified by a following phrase, such as "as far as practicable" or "if practical". Or a paragraph will state: "Designers should consider the following:" and then list requirements. The designer considers them and then decides he'll stick to Axioms 1 to 4. If the procuring activity believes there is a valid requirement, it should be stated clearly, firmly and without qualification. If the contractor cannot meet the requirement or wants to deviate, he should request approval from the procuring activity.

Unless the safety requirements are stated clearly, and where they are readily apparent as firm requirements, some of them will be overlooked by designers. The Air Force has

placed much of its reliance for this on AFSC DH 1-6, which I believe failed miserably. The best document I have seen to this purpose is the Navy's MIL-S-23069(Wep), Safety Requirements, Minimum, For Air Launched Guided Missiles. It was issued in 1961 and requires updating and other revisions, but even now is very useful.

The next major problem to accomplishment of a good System Safety program is MIL-STD-882 itself. The original System Safety specification, which applied solely to the Air Force, was MIL-S-38130. It was prepared in the Directorate of Aerospace Safety at a time when the Air Force was receiving new missiles and putting them into operational use with little prior warning of their hazards, and with inadequate safeguards. Some of the propellants were considered so toxic, reactive, and explosive that the Air Force hardly wanted information on them revealed to the general public. MIL-S-38130 was therefore prepared to alert Air Force safety people against the next hazards coming down the pike; and secondly, to permit safeguards to be provided during development. The Gross Hazard, and now Preliminary Hazard, analysis was stipulated; primarily for the alerting process, and then to initiate action to provide safeguards. This procedure has generated problems and should be updated.

I have contended for a long time that any system (or product) will have only a limited number of factors which will directly cause injury or damage. I call these "primary" hazards. There are numerous and various contributory factors to each of these, but the primary hazards are limited. This is true whether an aircraft, space station, skateboard, tank, radar or washing machine is being considered.

Figure 1 is a Safety Consideration Tree for a submarine, prepared to illustrate this contention. It is indicative of what can be done. People more knowledgeable of submarines can probably improve it. The block on "Injury" can be expanded in a manner similar to the one on "Damage". The trees are easy to prepare, and should be prepared by the procuring activity for each system for whose development it is responsible. After a few iterations and reiterations, some fine trees will result. Information derived from them can be put to many uses:

a. The various factors which can affect safety and which must be considered in the development of a system or product are readily apparent. There will be no need for a Preliminary Hazard Analysis. The first advantage to this is that it will eliminate a sore point for competing contractors. No contractor likes to point out that hazards exist in his system. A contractor with the better System Safety engineer might be able to point out more hazards, making his design appear more dangerous, than that of a competitor with a less knowledgeable System Safety engineer. With this method, the contractor will not have to make a Preliminary Hazard Analysis. He can get on with his more detailed analyses.

b. MIL-STD-882 now requires a Preliminary Hazard Analysis be prepared for use in the next phase of development. If one wasn't prepared in the previous phase, a problem arises. With the concept I envision, the procuring activity will indicate the problem areas which they have established from the Safety Consideration Trees; the contractor indicates in his proposal how he will handle them; the procuring activity either approves or requests more satisfactory information until it does approve; and things get started immediately, in the current program. This method can be used even in the Concept Phase where the contractors would be required to indicate their provisions for safety for each of the problem areas, in their system specifications. This is the point at which incorporation of safety requirements is needed most. Remember Hammer's Law!

c. When contractors are given the same firm requirements on which to estimate and prepare their System Safety efforts, they will be more comparable. The effort, manpower and cost of each task can be broken down and evaluated more easily. The procuring activity will also find proposals easier to evaluate if they are consistent in substance.

There are other advantages to use of a method such as this:

- *Data files can be established using the same coding as that shown on the trees.
- *The Armed Services can ensure that each factor or problem is covered by a suitable

requirement for safety in a military specification or standard.

*Personnel working on any program can be assigned to those problems which they are most capable of handling.

*It is a logical method of attacking safety problems, instead of waiting until a problem jumps out of the bushes.

MIL-STD-882 creates more problems. The use of the four hazard categories is a case in point. Those categories generate more problems than they are worth. First of all, they require clarification if they are to be used for any purpose. What is meant by "major system damage" or "severe injury"? If the various categories are defined well enough by each procuring activity to indicate clearly what they want them to mean, you will have a Preliminary Hazard Analysis.

The second problem with the four hazard categories is that too much time is spent trying to decide into which category each problem falls; and then to justify the choice. There are other reasons for which the categories should be eliminated (they overlap, detract from the effort of minimizing and controlling hazards, etc.) which will not be discussed here.

MIL-STD-882 applies to System Safety programs; it has no technical safety requirements, such as MIL-STD-454. If the technical requirements are not included in the Statement of Work, or by the contractor himself (watch out for Axiom #2), they will not become criteria to be observed. A solution is to require the System Safety Program Plan to be submitted as part of the contractor's proposal. Even better, this proposal should be submitted as a separate line item.

One more point about MIL-STD-882 and the Plan: AFSC Form 1664 for Contract Data Requirements states that the Appendix to MIL-STD-882 "shall be used" when preparing the Plan. Since the Appendix and the text of the standard do not jibe, it generates problems. Contractors observe the four axioms I have presented; but when a requirement is presented, they are very conscientious about its observance. So when a requirement says "shall" they want it that way, even if we System Safety engineers say that MIL-STD-882 cites it as a sample, and that it is not very good, they still want it that way because the 1164 says "shall."

I don't have many gripes about managers, especially when I realize they are acting within the four axioms I pointed out. Other than that I can only say that contractor (and maybe procuring activity managers too) have a hard time understanding that System Safety engineering extends beyond the safety considerations of design, reliability, maintainability, and human factors engineers. And very frequently it requires a redirection of their thinking when we indicate that System Safety includes minimizing damage of hardware, which was formerly a responsibility of reliability.

Often, this results in a failure to support the System Safety program properly. Another management solution is to appoint one or two men as a System Safety organization, and to direct that representatives in various design groups, systems engineering, test, reliability, maintainability, and other functional areas will perform the necessary System Safety tasks for their organizations. From what I have seen, it doesn't work. Everyone may be very conscientious about it, but such an arrangement does not work.

The last problem I have encountered with managers is that many believe that any requirement involving probabilities, such as a quantitative safety analysis to determine whether a specified level is being met, should be handled by the reliability engineers. Perhaps they believe System Safety is an extension of the hard hat-hard shoe school of safety and that System Safety engineers know nothing about the more theoretical aspects of engineering.

Some of these problems with management may actually be due to the System Safety engineer:

a. Many have not gotten beyond the 1963 stage when talks were common on "Why System Safety Is Needed." (If there is no System Safety requirement in the Statement of Work for a contract, there is no point in bringing up "Why System Safety Is Needed." Begin looking for work elsewhere.) System Safety engineers have done little to advance this discipline to a point where it can be recognized as something different from reliability and human factors. (Perhaps like Moses in the desert after the Exodus from Egypt, we need a new more energetic generation to take over, to forget the past, and accomplish new things.)

b. Many System Safety engineers don't know where to start a program or analysis. They then do either of two things: wait for something to rise up out of the bushes with which they can struggle; or they get onto the paperwork and meeting treadmill. They attend meetings and then write memoranda on the safety aspects. In between, they review the masses of papers which deluge them if they on the paper route. To these people, the approach I have indicated may be helpful in trying to figure out which way to go.

c. Some System Safety engineers are ardent proponents of checklists (I used to be one). Actually, checklists are ineffective for many reasons. Generally they are too late: the design has been agreed upon and frequently accomplished; often they are too general (DH 1 - 6 is in this category); and lastly, if they are not based on firm requirements (Axiom #1), it is generally difficult to have the designs changed.

This paper has gotten rather long. In summation, I will say that if there is one thing which can make a System Safety program fail, it is lack of clarity:

*Lack of clear requirements by the procuring activity.

*Lack of clear understanding of System Safety by other managers.

*Lack of a clear methodology to be employed by System Safety engineers.

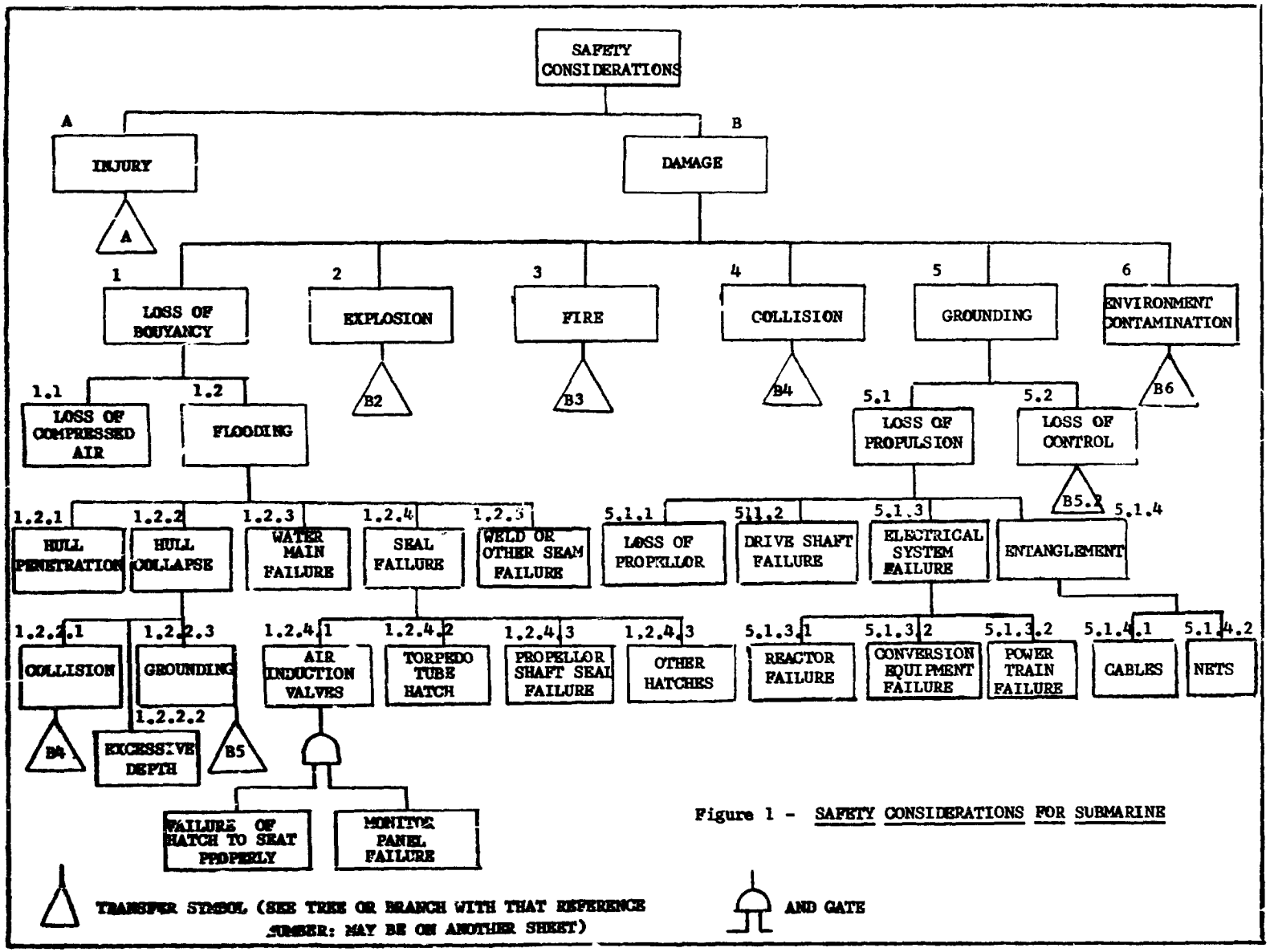

Figure 1 - SAFETY CONSIDERATIONS FOR SUBMARINE

FIGURE 1