REQUIREMENTS FOR SYSTEMS SAFETY PROGRAMS AS DELINEATED

BY

MIL-STD-882

Dr. C. O. Miller, Director
Bureau of Aviation Safety

National Transportation Safety Board
Department of Transportation

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

FOREWORD

As part of the Second NASA Government-Industry System Safety Conference, this paper was prepared to inventory the development and features of the currently best known system safety requirements document, MIL-STD-882, "System Safety Program for Systems and Associated Subsystems and Equipment...," dated July 15, 1969. NASA officials requested me to prepare it and, although I have not been in mainstream Department of Defense (DOD) efforts to implement the standard recently, I was in an active advisory capacity to DOD during the Standard's formulation and, indeed, its predecessors, the MIL-S-38130 series. Presumably, this would provide a degree of objectivity at least in assessing the successes - and failures - of the Standard thus far.

Unfortunately, this is not necessarily the case. I remain biased! I firmly believe there is a need within the management work structure of any reasonably complex system for a defined and implemented system safety program. The "whys" of this need have been chronicled elsewhere by others as well as myself. In any case, some implementing process is required.

As a result, this paper merely reiterates certain development history of MIL-STD-882 and attempts to spell out the role of the Standard through, among other ways, identifying its norms, its strengths, and its weaknesses. Further, of course, there are some considerations for the future.

This paper is not to be construed as representing an official position of the National Transportation Safety Board although the record has clearly shown the Board's endorsement of the system safety concept.

C. O. Miller

N72-25974

REQUIREMENTS FOR SYSTEM SAFETY PROGRAMS AS DELINEATED BY MIL-STD-882

EVOLUTION OF SYSTEM SAFETY PROGRAM REQUIREMENTS

In January 1946, Amos L. Wood of the Boeing Company presented an Institute of Aeronautical Sciences (IAS) paper regarding a recommended air safety program for aircraft manufacturers. He emphasis "continuous focus of safety in design... advance analysis and post accident analysis... accident preventive design to minimize personnel error... safety work, most effective when it is not fettered by administrative organizational pitfalls." (1)*

In February 1948, William I. Stieglitz wrote:

> "Safety must be designed and built into airplanes, just as are performance, stability and structural integrity... Every engineer cannot be expected to be as thoroughly familiar with all the developments in the field of safety anymore than he can be expected to be an expert aerodynamicist... (thus) A safety group must be just as important a part of a manufacturer's organization as a stress, aerodynamics, or weights group... (although) A safety program can be organized in numerous ways and there is probably no one best way." (2)

While the obscurations inherent in history preclude totally accurate revelation of who said what to whom first, these quotations represent the two earliest statements of what can be considered the cornerstone system safety principle. Namely, that at some level of system complexity, management is most effective and efficient if it were to require a specialized approach to safety as well as safety being simply everyone's job.

That this has come to pass is not a matter of argument, it is a matter of record. (3) The military services implemented this philosophy in their operational segments in the early 1950's. In this same time frame, many aircraft manufacturers established flight safety engineering groups (and without government requirements!). The aircraft complexity barrier was being faced and a number of ility functions were being called upon to supplement heretofore normal management division of work to provide a functional, economical, reliable, maintainable, available and sufficiently safe system so that a mission could indeed be performed.

Then, in oozed systems management. This not only called for a life cycle look and a better description of what comprised a system, but it produced a plethora of contractural documents.** Missile and space vehicle development in the late 1950's required this approach not only because of the aforementioned complexity problem being carried over and amplified from aircraft development, but also the loss of a single vehicle became an economic and mission degradation that simply would not tolerate less than an all out accident prevention effort. And the mood of the times dictated more clearly defined documentation during the engineering phases, including safety programming, as it had been implemented a decase earlier in the aviation operational world.***

Highlights of such specification predecessors to MIL-STD-882 are summarized below:

MIL-S-23069 (WEP) "Safety Requirements, Minimum, for Air Launched Guided Missiles" October 31, 1961

> This oft forgotten document broadly identified life cycle requirements for a system safety program. Its implementation, however, was minimal, at

*Number in parenthenses refer to references noted at end of paper.

**An interesting analogy is possible here. "Plethora" is defined in the medical sense as "a disease caused by an excess of red corpuscles in the blood or an increase in the quantity of blood in the body." This led one writer to observe"... a person in plethora (is) dying from too much health" (Sheridan as quoted in the World Book Encyclopedia Dictionary, 1963). Consider the "health" of the aerospace industry today... too much documentation???

***It has also been argued, perhaps not too facetiously, that in missiles, you no longer have a pilot to blame for the vehicle's loss, so why not go further upstream to the system's design?

least at its beginning. The Navy organization then, as now, was not conducive to life cycle system safety implementation efforts.

BSD Exhibit 62-41 "System Safety Engineering: Military Specification for the Development of Air Force Ballistic Missiles" June 1962

This USAF Ballistic Systems Division document was noteworthy on several counts. First, it was the initial definitive system safety specification that was implemented in major aerospace programs. Almost of equal significance, it was the first time such an engineering effort received the unqualified support of the head of the procuring agency who literally directed BSD contractor management personnel to get with the program, so to speak, or forget doing business with BSD. (4)

MIL-S-38130 (USAF) "General Requirements for Safety Engineering of Systems and Equipment" September 1963

Actually, Commander Donald Layton USN made major attempts to translate BSD Exhibit 62-41 into a broader based system safety engineering specification applicable to all DOD aerospace systems. However, he encountered in-house resistance by the BuWeps Industry Material Reliability Board which preferred to wait for a broader program that would encompass safety, reliability, maintainability and other similar requirements under one heading. (5) Concurrently, Lt. Col. James McConnel of the USAF Systems Command Headquarters aggressively shepherded the document through Air Force channels as a cleaned-up version of BSD 62-41. What it contained was basically four requirements:

(1) A safety management program
(2) Criteria to produce a reasonable level of safety
(3) Hazard analysis
(4) Program milestone reporting

MIL-S-58077 (MO) "Safety Engineering of Aircraft Systems, Associated Subsystems and Equipment; General Requirements for" June 30, 1964

This Army specification was a virtual verbatim issuance of MIL-S-38130. Interestingly enough, the Army was the first service to apply its specification to a new aircraft program, the Armed Aerial Fire Support System (AAFSS). (6)

MIL-S-38130A (DOD) "System Safety Engineering of Systems and Associated Subsystems, and Equipment, General Requirements" June 6, 1966

In the 1964-5 time period the Air Force Systems Command (AFSC) continued leadership in system safety by not only requesting an updating of MIL-S-38130, but also developing a System Safety management guide and a System Safety design handbook (ultimately published as References 7 & 8). Concurrently, a decision was made to implement the system safety approach DOD-wide as part of a continuing program of interservice standardization of requirements documentation. (9) AFSC was named Office of Primary Responsibility (OPR) for the task. The result was MIL-S-38130A (DOD). It subsequently was introduced into many programs both new and underway.

At this point the reader might ask "why all this discussion on the history of system safety and particularly the specification and current standard development?" The answer is so simple as to often be overlooked by the newcomer to system safety and MIL-STD-882. There is a decade or two of specific technological and managerial experience that has shaped MIL-STD-882, time which has demonstrated the need for such a programmed approach, time which has seen senseless waste of men and other resources that could have been avoided by an improved systems approach to safety.

Does this mean MIL-STD-882 is a model document? Far from it as will be discussed subsequently. It simply means some very astute and high ranking management types, both inside and outside the government, had fully adopted the system safety principle by the time the decision was made to go to a "standard." Indeed, the combined talents of many people offered a check and balance into what had preceded the standard and what got into the standard itself.*

MIL-STD-882... ITS CHARACTERISTICS

Like any Military Standard, MIL-STD-882 must be considered as the uniquely defined type of document that it is. For example, a Military Standard does not connote the preciseness of every yardstick being 36 inches long. Nor does it connote some minimum acceptable level of performance as is generally the case with "standards" issued by the Federal Aviation Administration. A standard is, by DOD definition, as follows:

> "A document that establishes engineering and technical limitations and applications for items, materials, processes, methods, designs, and engineering practices. (10)

Engineering standards, further, are "documents created primarily to serve the needs of designers and to control variety... define terms, establish codes and document practices, procedures and items selected as standard for design, engineering, and supply management operations." (11)

Military standards are not to be used as the direct medium for imposing administrative requirements on contractors. Rather, standards function in procurement through the medium of specifications. (12) Specifications are in turn defined as:

> "A document intended primarily for use in procurement, which clearly and accurately describes the essential technical requirements for items, materials, and services including the procedures by which it will be determined that the requirements have been met." (10)

Accordingly, MIL-STD-882 is more a guide than a directive at least until program management decides to follow it. Then it becomes a matter of further delineation, through specifications or otherwise, to implement a specific program tailored to the system under consideration including where that system is in its life cycle.

To be more precise in what MIL-STD-882 comprises, consider it in two ways: first, the problems inherent in MIL-S-38130A which were corrected and, second, what are the Standard's basic features.**

During its application, MIL-S-38130A was revealed to be limited if not dificient in that it:

(1) Did not adequately define terms necessary for its understanding.
(2) Was limited to the engineering phase of the life cycle only thus negating optimum effectiveness of total system safety management practices.
(3) Entailed excessive emphasis on the analytic process to the exclusion of other tasks.
(4) Produced further confusion between safety and reliability engineering efforts particularly because of a failure to delineate between the two in the analytic process.
(5) Failed to acknowledge the role of training in the accident prevention process.
(6) Failed to provide for safety data communication and interchange between the customer and contractor and within the customer's own organizational segments.
(7) Failed to provide for a safe and acceptable disposal of equipment and material at the completion of their usefulness.

*Not to be forgotten in this entire discussion are other events in the evolution of system safety such as the direction of the concept into the SST program by the FAA in 1965, the Apollo 204 fire that launched NASA into system safety, the National Transportation Safety Board's recommendations regarding system safety in surface modes of transportation, etc. While not directly bearing on MIL-STD-882, these non-DOD developments in system safety are further testimony of the acceptance of system safety principles.

**It can be argued that MIL-S-38130A was neither specific enough as a specification nor sufficiently encompassing as a standard. Another reason for establishing the standard was the desirability to place in the documentation hierarchy a top document under which various detail system safety specifications could develop logically.

As will become apparent in a moment, these shortcomings were corrected for the most part in the published MIL-STD-882.

Like all military standards, of course, MIL-STD-882 is couched in governmentese language. However, when all the confusion factors are eliminated, what the document really says is this:

(1) It tells why the standard is in existence, i.e., to provide for a system life cycle program for safety with the planning function being used as the overview control document. Observe this goes well beyond engineering per se... a fact often not recognized by the casual student in the field.

(2) It defines terms which, in their finality, look simple. In actual fact, however, they bear careful study. The nuances existent in the use of the word system (rather then systems) or the need to distinguish between different levels of contractors are but examples of where meanings must be fully appreciated before many other parts of the standard fall into place.

(3) It provides requirements within constraints present in any "standard" type document as discussed earlier. These include:

a. A System Safety Program Plan (SSPP).
b. Specific tasks in different phases of the life cycle.
c. An explanation of what safety organization is present to implement the program.
d. Milestone and program review points.
e. Detail consideration of hazards and the analysis thereof, to include corrective action or control processes available.
f. Safety data production and interchange.
g. Testing considerations, both in verification of given safety performance and insuring test programs being performed safely.
h. Training program inputs.
i. Special consideration of ground storage and handling problems including system close-out requirements.

(4) It provides, albeit brief, a relationship to associated disciplines, particularly to system engineering.

In addition, the sample System Safety Program Outline (Appendix A to the Standard) infers other tasks that might be expected within the scope of an SSPP, e.g., accident investigation planning and procedures, audit programs, establishment of system safety groups, etc.

In summary, MIL-STD-882 is a document which says "You ought to consider a system safety program, plan for it, and here are some of the prime considerations when you do." It is the basis for good dialogue with management when they face their difficult decisions about safety. It is the system safety practitioner in his relationship to management what the blueprint is to the designer in his relation with his management or with the manufacturing department.

A long-time colleague, Vernon L. Grose, also put it succinctly this way:

"A System Safety Program Plan is a mechanism to translate a generalized standard into a language that management understands in terms of cost, performance, and schedule." (13)

Enough said for the objectives and good points. What about the problems with MIL-STD-882? And it does have some, or at least the system trying to use it does!

MIL-STD-882 ... ITS PROBLEMS

Without attempting any rank order listing, let us consider various adverse comments involving MIL-STD-882 derived from a number of personal interviews and a review of a particularly critical analysis of the standard appearing in the Journal of Quality Technology, October 1970. (14) Before proceeding, however, it is of interest to note that as of May 1, 1971, the OPR for the Standard, AFSC Hdq (IGFS) had not received a single written criticism as requested routinely in all standard documents and appended to each release (DD Form 1426). This followed, among other communications, a specific request for such comments at the USAF-sponsored System Safety Conference in Las Vegas, February 1969.

Nevertheless, listed below are the problems encountered and personal editorial-type views of this author noted under "Comment."

1. The Standard is too confusing... is not easily understood.
Comment: Perhaps true; however, a standard in safety cannot be expected to be understood or appreciated by persons not well versed in the field any more than a powerplants engineer could be expected to fully comprehend a standard in electromagnetic radiation. In other words, one should know the business before trying to criticize it! Still, the challenge remains to put the Standard in words a broader-based population can grasp.
2. There are minimal numbers of trained and/or experienced personnel in the system safety field and unfortunately non-qualified engineers are often assigned to system safety tasks both at the contractor or at the procuring agency.
Comment: A very valid point and one closely allied with the previous item. The solution rests not only with more and better system safety literature and training, but also with continued professionalism by those in the field. Further, the pseudo safety expert, (who) got that way because his boss merely told him to put on a system safety hat) must be recognized and exposed for what he is.
3. Each program must have a safety effort delineated for its own peculiar needs.
Comment: That's correct and as it should be, albeit more ingenuity and hard work may be involved than to simply follow MIL-STD-882 in checklist fashion. But, since when do we accomplish progress in our aerospace field "by the numbers" or, even more importantly these days, do it within reasonable economic limits without ingenuity and hard work?
4. The Standard or other documents do not relate system safety to other disciplines.
Comment: Another valid point, although the place for such delineation probably does not belong in MIL-STD-882 but rather in something like MIL-STD-499, "Military Standard, System Engineering Management." (MIL-STD-499 is only under trial use today by the USAF.) In any case, the distinctions have been made in various contributions to the technical literature.
5. Duplication of efforts "ilities" or between system safety efforts and designers is encouraged by MIL-STD-882.
Comment: Even discounting the fact that planned duplication of some effort (e.g. critical hazard analyses) may often be a wise management technique, the problem suggested here has arisen. It does so because contractor and/or customer organizational segments have parochial interests which preclude cooperation between different organizational segments. Or, as covered more in the next item, the documentation requirements are conducive to separate reporting.
6. Information is developed for contract satisfaction rather than for use at the time of its inception or downstream.
Comment: This may well tie in with the people experience problem described earlier but in any case is considered by many to be the principal problem associated with MIL-STD-882. For example, if timing of hazard analyses are not predicated upon their contributing to the design or their output does not tell a usable story to downstream personnel, what really has been accomplished? Answer: A paper exercise ... and it has happened.
7. In contractural arrangements with some parts of DOD a single integrating contractor is not designated thus, making system safety integration a bureaucratic nightmare.
Comment: A serious problem: As to just how serious, the DOD agencies can only answer for themselves.
8. Implementation of a total life cycle system safety program within most military organizational structures is difficult because of excessive administrative barriers between development and using commands. The arsenal approach simply does not provide for a life cycle approach to anything including safety.
Comment: This has been a long standing problem which can be overcome to

some degree by formation of a strong system safety group early in the program and not letting it become degraded with time. This would seem to be dependent upon the initiative of operating command personnel even more than those at the development end of the spectrum.

9. System safety cannot be quantified and, therefore, the hazard analyses can never become a part of management's prime effort in maintaining a high benefit to cost ratio for its efforts.
   Comment: This myth continues to surface periodically but fortunately aerospace technology has seemed to come around to the real world pleaded for on this subject by system safety types for many years. Witness DOD Instruction 7041.3, "Economic Analysis of Department of Defense Investments," which states "An economic analysis is not required... when it can be shown that an analysis would not... result in increased decision effectiveness." (15) Actually, the principal contribution of hazard analysis is to make people think before the accident instead of afterwards... not the paper result.
10. System safety costing difficulties are continuing. No one seems to have found an adequate formula for what should be a direct charge, vis a vis an overhead charge, for system safety. Further, all too often, unqualified people at the negotiating table are discussing safety-generated work items.
    Comment: Once again, an old problem but one that is faced by anyone operating at the marketplace today. Resolution would seem best achieved when solution to the next item listed is forthcoming.
11. Safety tasks suggested by MIL-STD-882 are not definitive enough.
    Comment: This would seem to be a valid criticism and will remain so until more "how-to-do-it" technology is documented and understood by all. The design safety handbooks on hand and/or underway by some of the services are a major step in this direction. However, as indicated earlier system safety tasks are not uniquely those associated with design, and the total collection of such material in text form is still on the distant horizon.
12. The feedback loop to system safety of a given system via the accident/incident investigation process does not seem to be well established.
    Comment: As noted earlier, the outline SSPP acknowledges accident/incident investigation as a part of the program. But what about an effective closing of the loop back to the designer, the production man, the manager, etc., of the specific results of the investigation conducted by either the manufacturer or the customer? Is it really being done? Answer: No!
13. The fear of litigation has not only restricted information interchange concerning accident/incident investigations (applies to 12 above) but also has inhibited accomplishment and dissemination of information associated with hazard analyses.
    Comment: Sooner or later all firms and agencies will realize that a far greater risk is incurred concerning their possible culpability if it can be shown they did not use state-of-the-art analytical techniques at their disposal when the product was designed, tested, or turned over to the operator. And such techniques can be described in courtrooms today by any number of qualified consultants. What exists today in this regard is the psychological roadblock in the minds of most technologists concerning anything related to legal proceedings.
14. Several questions about the logic used involving the term "hazard":
    a. Why a "system safety hazard?" (Section 4.2.4 of MIL-STD-882)
       Comment: Does it mean a hazard to safety?
    b. A Category I hazard is called "Negligible," that is, it will not result in personal injury or damage.
       Comment: The question remains if it won't cause injury or damage, how can it be called a hazard?
    c. The Category IV hazard is of most concern.

Comment: Number four out of how many? (Besides, it is the exact opposite numbering logic than that used by NASA, although at one time during discussion regarding the Standard, NASA's logic was the same.

These comments regarding "hazard" approach the nit-picking category but are troublesome questions that could stand some editorial correction.

Observe that some if not most of the basic problems described could be dismissed as being non-relevant to the Standard itself, and, in fact, simply described as faults of the system in which the Standard operates. But let us take a lesson from our own system safety methodology. If something has problems, you do not just look at any single piece of the action to effect corrective measures. You also look at the interrelationships wherever they exist and try to make corrections wherever possible within existing fiscal and time constraints. In the end, then, your individual components start looking better as well as the total system performance.

SUMMARY AND REMARKS

System safety in general and MIL-STD-882 in particular will not remain static since the overall aerospace business will not remain static. The emphasis placed on the evaluation phase of system procurement by DOD is one example of change being felt now.(16) Another is a programmed detailed review of MIL-STD-882 to be performed in the next few months by a committee representing the military services safety centers.

It would seem that during these dynamics, it is encumbent upon the workers in system safety to continue their professionalism and dedication to the accident prevention task. Then, too, the system managers should try to be open-minded enough to try to understand the contribution that can be made by utilization of the principles outlined in MIL-STD-882 albeit they should not be satisfied unless they are convinced a system safety approach contributes positively to their mission. This is something that can only be accomplished by their association with qualified people in the field.

Of all the problems encountered in research for this paper, the item most frequently illuminated was the lack of appropriate people at the decision points where system safety was needed or used. This is not just a matter of education in the sense of people having a general association with the principles of system safety. It is also a matter of a better understanding of the "how-to's" of system safety... the specific safety tasks that must be delineated for a given program, man-loaded in the work allocation process, scheduled with the other work, and assessed as to their effectiveness by measures valid for the tasks that have been performed.

Whoever said "Safety is a responsibility, not a task" was living in a philosophical dream world.(17) You do not achieve accident prevention by just appealing to people's ethical values, you get out and work using proven accident prevention techniques. In this regard, most of the educational programs in existence concerning system safety are just that, education rather than training. The sponsors cannot seem to afford to pay for or allocate the time of their people to have each task subject covered in depth. An exception to this might be thought of in terms of the Fault Tree analysis course at the University of Washington. However, Fault Tree is just one analysis technique among dozens that might be used. There are many tasks besides analysis, and recognizing this, one begins to appreciate the magnitude of the job of training people in the system safety discipline, let alone educating those on the periphery.

Appreciating the above problem, there becomes a need for more manuals and, yes, specifications, when the techniques are reasonably solidified. Another possibility would be a series of Aeronautical Recommended Practices (ARP's) by the Society of Automotive Engineers (SAE) or similar publications by the EIA G-48 Committee.* In any case, the discipline must be documented in every expanding fashion with constantly improving professionalism if it is to compete in the marketplace for management's dollars.

One thing is to have a MIL-STD, and even a series of explanatory directives such as AFSCM 127-1, (7) or the Army's AMCP 385-23. (18)

*Electronics Industries Association, System Safety Engineering Committee, G48.

It is quite another thing to have something quite specific to implement.

Finally, as a major finding of this little study, a question is posed. Do we want paper or progress? All too often in the implementation of MIL-S-38130, MIL-S-38130A, and even MIL-STD-882 thus far, too many people seem to think the objective was to turn in a specified number of documents so that a box could be checked off for contract progress reports. A disproportionate amount of time has been spent figuring out the paper flow compared to expeditious resolution of the dirty details of what the paper contained. Fortunately for all of us, this "easy way out" has not always been the case and things are improving. Ask some of the aircraft manufacturers of those weapon systems to which MIL-STD-882 has been applied.

In conclusion, the two decades or so of effort leading up to MIL-STD-882 has not all been fun and games. Nor will the next two decades be such while we advance man's ability to control those forces of destruction that, in increasing fashion, he himself has created. But we will be working at it.

REFERENCES

(1) Wood, Amos L., "The Organization and Utilization of An Aircraft Manufacturer's Air Safety Program." The Boeing Company, Seattle, Washington. Presented at the Institute of the Aeronautical Sciences Meeting, New York, January 1946.

(2) Stieglitz, I., "Engineering For Safety." Aeronautical Engineering Review, February 1948.

(3) Miller, C. O., "The Role of System Safety in Aerospace Management" University of Southern California, Los Angeles, California, August 1966.

(4) Personal communication with Lt. Col. (Ret.) George Ruff, 1965, (considered by many to be the author of BSD Exhibit 62-61)

(5) U.S. Navy, Letter to the Assistant Chief for Research, Development, Test and Evaluation from the Intra-Bureau Systems Effectiveness Policy Committee, RAAV 02/39, Washington, D.C., April 9, 1964.

(6) Hamilton, Col. R. M., and Capt. R. W. Newton, "The Army Evaluation of MIL-S-58077, and Those Agencies Involved in Its Implementation." Annals of Reliability and Maintainability, Vol. 4 (Washington, D.C.: Spartan Books, July 1965).

(7) U.S. Air Force Systems Command, "AFSCM 127-1, Safety Management" January 1, 1967.

(8) U.S. Air Force, Systems Command, "DH-1-6, System Safety" July 25, 1967.

(9) U.S. Department of Defense, DDR and E Memorandum, "Safety Engineering Requirements for Systems and Equipment - Specification Consolidation and Tri-Service Coordination," August 5, 1965.

(10) U.S. Department of Defense, "Standardization Policies, Procedures and Instructions," (Glossary)

(11) Supra (Paragraph 2-103)

(12) Supra (Paragraph 2-103 and 1-204)

(13) Personal communication with V. L. Grose, April 1971.

(14) Bailey, Peter H. G., and Eugene R. Christie, "Review of Standards and Specifications," MIL-STD-882, System Safety Program for Systems and Associated Subsystems and Equipment" Journal of Quality Technology, Volume 2, No. 4, October 1970.

(15) U.S. Department of Defense Instruction 7041.3, "Economic Analysis of Proposed Department of Defense Investments," February 26, 1969 (Part III Bla).

(16) Letter to DOD activities by David Packard. "Policy Guidance on Major Weapon System Acquisition," May 28, 1970.

(17) As quoted anonymously in the Flight Safety Foundation Aviation Safety Exchange 70-402/403, Arlington, Virginia, 1970.

(18) U.S. Army Materiel Command AMCP 385-23, "Management System Safety," July 1967.