ABSTRACT

SAFETY AND THE SMALL SATELLITE BUILDER
BY JAMES S. (SID) SMITH

EXPANDING HORIZONS
SAFETY CONSULTING SERVICES

The importance of safety and the early understanding and incorporation of safety requirements into all phases of the small satellite's life can not be over-emphasized. Safety is an engineering discipline, a mind set, a concious practice of all involved in the small satellite. There are numerous safety requirements which must be complied with and there are numerous processes and procedures which the small satellite must be subjected to. Being aware of the requirements and procedures and assuring their accomplishment is a total project responsibility. Risk cannot be totally eliminated, but it can be managed and controlled. This paper was written to provide some information on the steps to successful Risk Management and Risk Acceptance.

INTRODUCTION

The aerospace accidents which occurred last year have given all of us a heightened awareness of the need to emphasize safety. The accident showed dramatically and conclusively the rapidity with which a disaster can happen. The accident should have provided a lesson in the importance of systems integration and analysis of the requirement to thoroughly understand the interaction of components and the overall synergy of systems. This paper was written to discuss, define and clarify the systems safety aspects of small satellites and their environments.

OVERVIEW

This paper has been prepared in three sections with the intent to provide some systems safety philosophy and understanding; a discussion of requirements, their meanings and application methods; and a summation with background information.

SCOPE

The intended scope of this paper is the coverage of systems safety for small satellites. However, totally necessary to any discussion of satellite safety is an accompanying discussion of booster interfaces and interactions and ground processing methods, procedures and support requirements. All are totally interrelated and all requirements have been written with the total integrated system in mind.

DISCUSSION

Perhaps the single most important factor in the incorporation of safety requirements into a product is that they be incorporated during the initial design phase. This of course implies that the designers have a thorough knowledge of safety requirements and an understanding of the rationale for why the requirements were formulated. All too often - usually when no one person has been assigned safety responsibility - the satellite developer learns after hardware has been produced that some change will be required to satisfy a safety requirement. This situation creates turmoil throughout all levels of management, increases the cost and frustrates the customer.

Safety requirements are based upon several factors with the prevention of death or injury and the prevention of damage or loss of property being the major drivers. Operational responsibility is the determinant for whose requirements must be met. If the satellite is to be processed and launched by the Department of Defense, one set of requirements must be met. If the satellite is to be launched aboard a Space Shuttle and processed by NASA, another set of requirements

must be met. There is a third case when a satellite is launched on a NASA booster and processed through NASA facilities - such as Wallops Island and even a fourth case where a spacecraft is processed in a NASA or DOD facility and launched by NASA on a DOD installation - the NASA Delta launch pad (SLC-2) at Vandenberg AFB is an example of this case. The safety issue of satellites launched on commercially developed/owned boosters is just now being addressed and will undoubtedly have a number of variations too.

Safety requirements are found in a number of different types of documents and become applicable when the launch/processing agency so directs. Requirements may be in the form of MIL-Standards; Government regulations; American National Standards Institute standards; Boiler, Electrical and Fire Codes; and various NASA Handbooks, Specifications and Manuals. With the large number of documents from which to draw requirements, conflicts are not uncommon. Usually, conflicts are resolved by applying the "whichever is the most stringent" rule to the design. Unfortunately, application of this rule is often needlessly expensive. When this case occurs, negotiation to the "common sense" application level is required. In order to successfully reach a negotiated settlement, the developer must have a thorough knowledge of the intent of the requirement and be able to show that the system complies with the intent.

DEFINITIONS AND REQUIREMENTS

Key terminology which the safety engineer/safety manager must become familiar with includes risk management, risk acceptance and hazard reduction. All are components of each other. All define the boundaries of the safety program and measure its effectiveness.

Risk management is the combination of designs, procedures and verifications which enable the operator of systems to function safely.

Hazard reduction is the methodology for reducing hazards and consists of the following elements which should be applied to systems in order of precedence:

a) Design for Minimum Hazard - design out the problem.
b) Safety Devices - when the hazard cannot be designed out, control it with automatic safety devices which are incorporated into the design.
c) Warning Devices - when neither design nor safety devices can control hazard warning devices capable of detecting and providing notice to operators in sufficient time to allow the use of emergency procedures or corrective actions to return the system to a safe condition.
d) Special Procedures - Used when design, safety and warning devices cannot be used to control hazards.

Risk acceptance is the acknowledgement that there is a risk in operating the system but that the risk has been quantified through verification methods and that the system can be safely operated.

Safety analyses are narative assessments of the methods used for controlling hazards. Safety analyses are prepared in preliminary and final forms and cover both design and operations. The safety analyses are used in conjunction with drawings, procedures, and supporting analyses to prove the safety of the system to launch and processing agencies. References for preparation of the safety analyses are found in Data Item Descriptions DI-SAFT-80101, DI-SAFT-80102 and DI-SAFT-80103 (Ref. 1) for NASA expendible and DOD programs. NASA Shuttle programs use JSC 13830 (Ref. 3) as the reference guide for the preparation of safety analysis reports. If the program is sponsored by the Air Force Space Division, the Safety Assessment Reports will be collected in the Accident Risk Assessment Report (Ref. 2).

The systems safety program plan is used to define the system safety program which will be used in support of the development effort. The plan will show functional interfaces and describe organizational responsibilities. A systems safety program plan is required to the DOD but is optional to NASA. For the developer's own use and general guidance, a system safety program plan should be prepared even though it may not be required. Data Item Description DI-SAFT-80100 (Ref. 1) system safety program plan should be used as a guide.

PROCEDURES

The importance of incorporating safety requirements into the design and the early analyses for verification of incorporation cannot be over emphasized. To assure the timely incorporation of safety requirements safety should be a key item on the agenda of all design reviews. The person responsible for safety should make a presentation which details his understanding of the requirements, his methods for assuring their incorporation, and his role in the verification process. He should also describe acceptance criteria and his methods for evaluating acceptance.

Both the DOD and NASA have established phased safety reviews for STS payloads which are conducted during the course of the design effort and evaluate the incorporation of safety requirements through the maturity of the program. Entry into the process will be accomplished either by submitting the safety data to the NASA Johnson Space Center safety office for NASA sponsored payloads, or, DOD sponsored payloads will be processed by and the data submitted through the sponsoring Systems Program Office (SPO).

A more informal process exists for payloads which are to be launched on expendable boosters and is normally conducted by the launch and processing agency to determine that the system can be processed and launched without causing injury to personnel or damage to facilities or equipment. Payloads processed for launch on either the Eastern Test Range or the Western Test Range must comply with the requirements of each range's safety requirements regulations (Refs. 4 and 5).

Payload builders having NASA sponsorship will be required to submit their safety data to the sponsoring NASA organization at the respective

test range and that sponsor will perform the interface activities between the payload builder and the DOD launch agent. Payloads which are to be launched on DOD boosters will provide their data directly to the Safety Office at the respective test ranges.

After a review of the data by the appropriate agencies, DOD or NASA Safety Review Teams or Test Range Safety personnel, the operator is given written approval to process, launch and operate the satellite. The approval may be granted as requested or with conditions stipulated.

SUMMARY

Safety must be considered for all phases and all aspects of the small satellite just as surely as it must be considered for large satellites, boosters, and support equipment. Safety requirements are usually common sense application of good engineering design. System safety is systems engineering using a different set of criteria. The safety manager is a member of the design team and is responsible for assuring that safety requirements are incorporated during design and that all engineers understand the safety requirements and acceptable methods for applying them. Safety verification is part of overall systems testing and must be considered when developing test plans and procedures.

Safety approvals are a key element of operations and are frequently time consuming. Therefore, an approval cycle must be incorporated into system schedules. The documentation required to support the approval process is logical and readily developed during the design process.

REFERENCES

1. MIL Standard 882B, Mar 30, 1984, Systems Safety Program Requirements

2. MIL Standard 1574A, Aug 15, 1979, Systems Safety Program for Space and Missile Systems

3. JSC 13830A, May 16, 1983, Implementation Procedure for STS Payloads System Safety Requirements

4. Eastern Space and Missile Center Regulation (ESMCR) 127-1, July 30, 1984, Range Safety

5. Western Space and Missile Center Regulation (WSMCR) 127-1, May 15, 1985, Range Safety Requirements, Range Safety Regulation

All documents may be obtained through your sponsor or from the agency which is responsible for the document.

BIOGRAPHICAL SKETCH

Mr. Sid Smith (Colonel USAF) retired from the U.S. Air Force in 1985 after 24 years of experience in all aspects of Space and Missile System Engineering and Operations. Specific positions of responsibility include:

- Deputy Missile Combat Crew Commander Atlas F ICBM
- Gemini and Apollo Flight Controller
- Upgrade Program Systems Engineer for the Minuteman III Weapon System
- DOD Accident Prevention Manager for all DOD STS Launched Payloads
- Commander Air Force Western Test Range

Since January of 1987 Mr. Smith has been an independent safety consultant and is the owner of Expanding Horizons Safety Consulting Services. Customers for his services include:

Aerospace Corporation, El Segundo, CA and Vandenberg AFB
- Safety transition work and definition of Space Test Range Safety (on orbit safety)

Astro Aerospace Corporation, Carpinteria, CA
- Safety Analyses, Safety Planning Engineer training for the Deployable Mast Subsystem - a NASA program, and for MILSTAR - a DOD program

Webb Murray and Associates, Inc., Houston, TX
- Proposal preparation for the Vandenberg AFB Systems Safety Support Contract. Fire Protection Systems Design marketing to Santa Barbara County and the local oil industry

Mr. Smith was the first DOD recipient of the NASA Silver Snoopy Award which is an award presented by the Astronaut Office to individuals who have made significant contributions to the safety and reliability of Manned Spaceflight.