N72-25975

INTEGRATING SYSTEM SAFETY INTO THE BASIC SYSTEMS ENGINEERING PROCESS

Mr. John W. Griswold
Reliability & System Safety Manager

Aerospace Group
The Boeing Company

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 1971

INTRODUCTION

In any undertaking there is always a competition for resources. Decisions must be made for each expenditure of time and money. Functional and specialty groups compete for the funds necessary to do the best possible jobs within their specialty.

No one gets all the money they want and each element of a total system, be it management or technically oriented, must prepare the best possible argument for their position. Dedicated specialist groups are becoming more sophisticated in their approach and have given up on the motherhood approach in favor of hard facts determined from detailed analyses.

The system safety function is no different from other specialist groups in its need to compete for limited resources. Although man is inherently reluctant to settle for less than the ultimate in safety, a program manager is sooner or later faced with the decision as to how safe is safe enough.

The combination of all specialist groups inputs into a balanced program is essential. The systems engineering process is a method that defines the system and its functions, integrates the requirements of all of the subfunctions, sets priorities for funds and time to carry out the tasks and directs the combination of all engineering efforts to complete the program. By definition the system safety effort thereby becomes a part of the systems engineering process.

The term systems engineering has been used to describe many different things. To properly respond to the title of this paper, a baseline description of systems engineering must be established since system safety is one of the subfunctions in the systems engineering process.

Although many of the elements of systems engineering had been applied before, the Air Force -375 (1) series of manuals in 1964 focused attention to combining these elements into an engineering discipline. This series has now evolved into MIL-STD-499 (2), "System Engineering Management," which is taken as the baseline description of the systems engineering process for the purpose of this paper.

The government objectives in MIL-STD-499 are: a) the efficient engineering definition of a complete system; and b) the efficient planning and control of the technical program for the design, development, test, and evaluation of the system. Contractors must provide a logical sequence of activities and decisions leading to the definition of the configuration, usage and support of the system and technical program for acquiring a system. The definitions established by systems engineering provide the basis for the subfunctions to conduct their analyses and establish their requirements on the system. This is an iterative process starting with the conceptual phase and extending through the life of the program. The subfunctions include but are not limited to the following: Design, Test, System Safety, Reliability, Logistics, Maintainability, Quality, Human Engineering, Configuration Control, Security Engineering, and Value Engineering. Other subfunctions may be added for specific programs.

THE SYSTEMS ENGINEERING PROCESS

The basic elements of the systems engineering process are given in Figure 1. Detailed discussion of each of the systems engineering elements are included in MIL-STD-499 and will not be covered here. This paper will address itself to the information that system safety requires from systems engineering, and the information that system safety provides to other subfunctions of systems engineering.

MIL-STD-499 requires and defines the preparation of the systems engineering plan. It is recognized that this is essential to the proper planning and control of the systems engineering program. MIL-STD-882 (3) places a great emphasis on the system safety plan. It requires that one be prepared for each Department of Defense Program. NASA NHB 1700.1 - Vol. III (5) also specified that a system safety plan be prepared for each project or program.

The proper preparation and integration of these two plans is of utmost importance. After they are approved by management they become the controlling documents for systems engineering and system safety. It is in the

system safety plan that the necessarily general requirements of a specification or program guide are merged with the specific needs of a particular program to define tasks and responsibilities to make a safety program live and breathe.

SYSTEM SAFETY PROGRAM

System safety has gone through many of the same growing pains as systems engineering. The need for improved product safety was recognized and the only way to assure it was to consider the entire system. The problems of definition, purpose, scope, and charter of system safety were pounded into shape until there is now general acceptance of the system safety discipline. MIL-S-38130 was published and later revised to MIL-STD-882. That, combined with the NASA SPD-1 (4) and NHB 1700.1 series, provides all of the baseline and direction necessary for a system safety program. Vern Grose offers a definition for system safety (6) that illustrates its pervasiveness with the systems engineering process (see Figure 2).

The successful and cost effective implementation of the safety program requires information to be available or developed. The results of the safety analyses and other efforts must flow to other organizations to become useful. Figures 3-8 show a simplified flow of a typical system safety program. The sections that follow will discuss this flow of information, how it is used by system safety and how the rest of the systems engineering subfunctions are affected.

The basic tasks of any system safety program can be grouped into four basic headings: 1) the assembly of information and data; 2) the analysis of that information and data to determine the hazards to the system and the probability of the hazards resulting in accidents; 3) the establishment of preventive measures through requirements and standards; and 4) a follow-up activity that assures the requirements and standards are included in the design and operation of the system and that they are adequate. Ideally, the tasks should be started at the conceptual phase and upgraded throughout the life cycle, through an iterative process, improving the system as more information becomes available.

Information and Data (See Figure 9)

It is obvious that no work can start until there is some kind of system description. This is the start of the systems engineering process and one of the most important elements. The description must be as complete as the program phase allows; it must be published to all functional elements; it must be revised as necessary and all subfunctions must be kept aware of the revisions. This description must include the hardware, its intended use and the environment in which it is intended to operate.

The initial system description allows system safety engineers to start to assemble experience retention information and data to prepare for the analyses and trade studies that may be needed. Information from past and current programs can provide the basis for the initial safety criteria and guidelines that should be provided to the systems engineers and designers. Range safety documents, government standards and codes and documents such as the Air Force System Command Handbook DH 1-6 (7) are sources for much of the initial information needed. The experience retention data accumulated by other subfunctions should also be made available in a data center to avoid duplication of materials. Reliability, maintainability and human factors experience data must also be considered by system safety.

Preliminary system safety requirements can be established from this initial data. For example, ordnance design requirements are well established and can often be taken directly from past programs. The use of fuels and propellants may require ignition proofing or explosion proof equipments. Nuclear power sources require special shielding and handling. These and many other obvious requirements are provided to systems engineering to be included in the systems requirements. It is also advisable to start a system safety requirements document that can be used as a checklist during design reviews, flight readiness reviews and audits.

System Safety Analyses (See Figure 10)

The systems engineering inputs given on Figure 9 must be available to allow a complete and effective safety analysis. The system description, functional flows and time line analysis must be current and controlled by configuration control to assure that all subfunctions of systems engineering are considering the same system.

The system safety analyses must: a) identify the hazardous elements, hazardous conditions and potential accidents that could occur; b) determine their potential effects on the system; c) determine the probability of their occurrence (qualitative or quantitative); and d) provide adequate detail to direct the corrective action necessary to control the hazards to an acceptable level.

Mission goals and objectives must be considered in the emphasis given to system safety. A much higher risk may have to be taken in a weapons system with a high priority for early use than would be acceptable on a manned space station. The system safety function, along with others in the systems engineering process, must identify levels associated with trades against cost, weight, functional capabilities, and other system constraints.

The system requirements of other subfunctions must be known to system safety engineers so they can be considered in the safety analyses. More will be said of requirements later. The reliability, maintainability, logistics, and functional design requirements may conflict with the safety requirements. The safety analyses must show any conflict and provide enough detail to enable corrective action to be taken.

System safety has been critized for a great proliferation of analyses. As many as thirty-five different analyses have been listed. Some effort has been expended in attempts to standardize on several specified analyses with little success. Standardization of an analysis method is not the proper approach at this time. Specification of an output resulting from a credible analysis is appropriate. Some outputs of system safety analyses are shown on Figure 10. The main inputs supplied to the systems engineering process are the safety requirements that must be imposed on the system to make it safe enough.

The system description, functional flows and time line analyses provide the basis for the system safety analyst to identify the hazardous elements and conditions inherent in the system. The information may be analyzed, using a tabular format such as the Preliminary Hazard Analysis or the logic network format of the fault tree analysis. If the output required is qualitative, which is usually the case in early program phases, the time line data, functional flows and hardware descriptions are adequate. If a complete risk evaluation is to be made and a numerical requirement for safety is imposed in the system, more definitive design data is required. This information often is provided by reliability specialists. The failure mode and effect analysis contains most of the information needed. Care must be taken to consider the Failure Modes and Effects Analysis (FMEA) results from a safety viewpoint which can have a different criticality than the effect on reliability.

Hazard Identification

Experience retention, in the form of data taken from previous programs and personal experience of qualified system safety personnel, provides the basis for the initial identification of hazardous elements and conditions. High energy levels, hazardous environments, toxic gases, and structural problems are some of the first considerations. The type of fuel to be used dictates the ignition proofing requirements that must be imposed. The use of explosives requires many well established requirements to be imposed.

The environment the system is intended to operate in dictates requirements for adequate oxygen, thermal protection, shock or acceleration limits, etc. Safety factors for pressure vessels and basic structures must be established with proper consideration for the functional use of the equipment. For instance, the safety factors for pressure vessels on unmanned systems can be much less than for manned systems. However, care must be taken to be sure that such tanks are not pressurized when personnel are maintaining

the system or checking it out for launch. The identification of hazards continues throughout the entire safety program. As more is learned about the system, additional hazards become apparent. All hazardous elements and conditions should be recorded and action taken to control them to prevent accidents.

Hazard Potential Effect

The emphasis given to the control of hazardous elements is dependent on the potential effect or accident that could occur if control of the hazardous element is lost. This part of the analysis looks at all possible ways an accident could occur. The probability of the event occurring will be considered later. There are two ways this part of the analysis may be conducted. The analysis may start at the part level and continue through the subsystem and consider the system as a whole. The analysis can also start as a top down analysis, such as the fault tree analysis, which starts with an undesired event, and then goes down through all series of events that could occur to yield the undesired event. Single thread failure analyses are helpful but multiple failures must be considered to make the analyses complete. A fuel leak may increase the hazard level but a catastrophic event may not occur without an ignition source. In the case of hypergolic fuels, two leaks may be necessary.

The potential effect may be categorized as catastrophic, critical, marginal, or negligible as is required by MIL-STD-882 and NASA NHB 1700.1. This grouping enables increased emphasis to be given to the worst category. However, all of the hazards and their potential effect should be listed and provided to systems engineering. This data is essential and must be considered during trade-off studies. Also, each of the items listed should be closed out to show what preventive actions have been taken to prevent an accident from occurring. The hazard analysis format established in D2-113072-1, (8) "System Safety Analytical Technology - Preliminary Hazard Analysis," provides for the tabulation and recording of the identification of the hazard, subsystems involved, the potential effect, the category, and the recommended preventive measure to control the hazard.

Probability of Occurrence

The amount of resources that will be applied in preventive measures depends not only on the potential effect, but also on its probability of occurrence. An excellent example of this is the potential of meteorite damage to spacecraft. The effect of a meteorite hit would be catastrophic. However, the probability of significant hits is so small that resources have been diverted from meteorite protection to more effective areas in the spacecraft.

There are two methods of determining the probability of occurrence of accidents. The qualitative approach such as probable, possible or improbable can be used. This approach is very subjective and must be based on empirical data, experience retention or just plain engineering judgment. It is used on most safety programs today. The quantitative approach uses the best failure and statistical data to determine more accurate probabilities of an event occurring. A method of using FMEA data in a Fault Hazard Analysis provides some degree of quantification. The most thorough method is the Fault Tree Analysis which is used on weapons systems such as Minuteman and the Short Range Attack Missile (SRAM) where the undesired event is so serious that a numerical limit is imposed by the customer. The Fault Tree Analyses may be used for either qualitative or quanitative analyses. It has been described in numerous papers (9, 10, 11) and is documented in D2-113072-2, (12) "System Safety Analytical Technology - Fault Tree Analysis."

Corrective Action

The output of system safety analyses is shown on Figure 10. Each of them are of importance to systems engineering. Some of them such as inputs to trade studies and critical systems lists can be used directly. The safety requirements that result from the analysis will be covered later. The systems

engineering approach provides the way for the system safety input to be integrated into the mainstream engineering effort and to cause the implementation of the corrective action that is necessary to assure a safe system.

Safety Requirements (See Figure 11)

The systems engineering process defines the system and then establishes the requirements for what must be included in the system design and operation. The system safety requirements initiated from experience retention data are upgraded as more information is obtained from the above analyses. As mentioned earlier, they also include appropriate standards and guidelines developed for other programs. When combined into a single document they are readily available to all levels of the contractor and customer organizations. The requirements document should be divided into design requirements and operational requirements. Design requirements include the systems requirements and more specific requirements for each of the subsystems components and parts. Operating requirements specify what must be included in procedures to enable the as-designed system to operate safely.

System Safety Assurance (See Figure 12)

System safety assurance is used by this writer to include all of the safety effort expended to assure that the design and operating safety requirements are included in the system and that they are adequate. Figure 12 lists the activities involved. The systems engineering process control of the technical program includes reviews, trade studies, change control, and audits. System safety must participate in these activities to assure that safety is included in the design and operation of the system.

Program and Design Reviews

The entire series of program and design reviews provide an excellent opportunity for system safety to follow-up on the safety program. The system safety design requirements document provides an excellent baseline for safety review. The design can easily be reviewed against the requirements and extra emphasis can be given to looking for weak points in the safety program. System safety sign-off should be required at all such reviews.

Drawing Reviews

System safety requirements should indicate which drawings require safety review and sign-off. In some programs all drawings must be signed off by safety. In less hazardous programs only those items that are termed critical to safety receive such sign-off. Again the control inherent in the systems engineering process provide the means for system safety to carry out its function.

Configuration Control

It is not enough to prove that the initial design is safe. As stated earlier, all subfunctions of systems engineering must be aware of all changes to the system. This is especially true of system safety. Some of the worst accidents in past programs have been caused by lack of safety considerations of changes to the system. This includes changes to operating procedures as well as design changes. System safety should have the same sign-off responsibility on changes as it does on design reviews. Here again the systems engineering change control provides the means for system safety to "work within the system" to carry out its functional responsibilities.

SUMMARY

The primary purpose of systems engineering is to assure the optimum allocation of resources to achieve mission objectives. Consequently, the entire system safety program is aimed at achieving the safest system possible within program constraints and to further assure that this safety level is adequate. A decision of a program manager that a system is safe enough is a difficult one at best. To

the extent that the system safety program can contribute toward that decision with meaningful data, effective program controls and credible measurements of results, system safety activities will be able to demonstrate their value and successfully compete for the limited resources that any program has.

REFERENCES

(1) AFSCM 375 series, "Air Force Systems Command Manual - Systems Management, "June 1964.

(2) MIL-STD-499 (USAF), "Military Standard - System Engineering Standard."

(3) MIL-STD-882, "Military Standard - System Safety Program for Systems and Associated Subsystems and Equipment: Requirements for."

(4) NASA Office of Manned Space Flight Safety Program Directive 1-A, "Safety Requirements for Manned Space Flight."

(5) NASA Safety Manual NHB 1700.1 (V-3), "System Safety," 6 March 1970.

(6) Grose, Vernon L., "System Safety in Rapid Rail Transit," Presented to the Rail Transit Conference, San Francisco, California, 13-16 April 1971, p. 2.

(7) Air Force Systems Command Handbook DH 1-6, "System Safety."

(8) Boeing Document D2-113072-1, "System Safety Analytical Technology - Preliminary Hazard Analysis." (Available from the the Defense Documentation Center.)

(9) Mearns, A. B., "Fault Tree Analysis, the Study of Unlikely Events in Complex Systems," System Safety Symposium, Seattle, Washington, 8-9 June 1965.

(10) Feutz, R. J. and Waldeck, T. A., "The Application of Fault Tree Analysis to Dynamic Systems, "System Safety Symposium, Seattle, Washington, 8-9 June 1965.

(11) Crosetti, P. A. and Bruce, R. A., "Commercial Application of Fault Tree Analysis, "Ninth Annual Reliability and Maintainability Conference, Detroit, Michigan, 20-22 July 1970.

(12) Boeing Document D2-113072-2, "System Safety Analytical Technology - Fault Tree Analysis." (Available from the Defense Documentation Center.)

SYSTEMS ENGINEERING

MISSION AND REQUIREMENTS ANALYSIS
FUNCTIONAL ANALYSIS
EXPERIENCE RETENTION
TRADE STUDIES
REQUIREMENTS ALLOCATION
DESIGN/OPTIMIZATION EFFECTIVENESS ANALYSIS
SYNTHESIS
TECHNICAL INTERFACE COMPATIBILITY
CHANGE AND CONFIGURATION CONTROL
DESIGN REVIEWS
ENGINEERING INTEGRATION
TEST INTEGRATION
PROGRAM REVIEWS
REPORTS AND EXPERIENCE RETENTION

FIGURE 1

SYSTEM SAFETY DEFINED

"THE OPTIMUM DEGREE OF HAZARD ELIMINATION AND/OR CONTROL WITHIN THE CONSTRAINTS OF OPERATIONAL EFFECTIVENESS, TIME AND COST, ATTAINED THROUGH THE SPECIFIC APPLICATION OF MANAGEMENT, SCIENTIFIC AND ENGINEERING PRINCIPLES THROUGHOUT ALL PHASES OF A SYSTEM LIFE CYCLE."

FIGURE 2

SIMPLIFIED SYSTEM SAFETY FLOW DIAGRAM

FIGURE 3

ESTABLISH SYSTEM BASELINE AND SAFETY GUIDELINES

FROM:

- o CUSTOMER REQUIREMENTS
  - o STATEMENT OF WORK
- o EXISTING GUIDELINES AND STANDARDS
  - o DH 1-6
  - o SFCM 8080
  - o FED CODES
- o EXPERIENCE RETENTION INFORMATION

FIGURE 4

IDENTIFY HAZARDOUS ELEMENTS AND HAZARDOUS CONDITIONS

- o PRELIMINARY HAZARD ANALYSIS
- o FAULT HAZARD ANALYSIS
- o FAULT TREE ANALYSIS
- o OPERATIONS HAZARD ANALYSIS

FOR

COMPONENTS
SUBSYSTEMS
SYSTEMS
INTERFACES
OPERATIONS

FIGURE 5

DETERMINE RISK INVOLVED

- o QUALITATIVE
  - o CATASTROPHIC
  - o CRITICAL
  - o MARGINAL
  - o NEGLIGIBLE
- o QUANTITATIVE
  - o STATISTICAL PROBABILITY
  - o PASSENGER MILES/FATALITY
  - o FATALITIES PER YEAR
- o COMPARE WITH COST AND DEGRADATION OF FUNCTION

FIGURE 6

ESTABLISH PREVENTIVE MEASURES

SAFETY REQUIREMENTS AND CRITERIA
- o DESIGN
- o OPERATIONAL
- o PERSONNEL

ORDER OF PRECEDENCE
- o SAFETY DEVICES
- o WARNING DEVICES
- o SPECIAL PROCEDURES

INTEGRATE WITH SYSTEMS ENGINEERING

FIGURE 7

SAFETY ASSURANCE (FOLLOW-UP)

- o DRAWING REVIEWS
- o DESIGN REVIEWS
- o FIRST ARTICLE INSPECTION
- o PROCEDURE REVIEWS
- o TESTING
- o LIAISON AND SURVEILLANCE
- o AUDITS

FIGURE 8

ESTABLISH AND MAINTAIN REQUIREMENTS AND STANDARDS (UTILIZING SAFETY ANALYSES)

INPUT REQUIRED

- PROGRAM REQUIREMENTS
- FUNCTIONAL REQUIREMENTS
- OPERATIONAL REQUIREMENTS
- EXPECTED ENVIRONMENTAL CONDITIONS
- EXISTING STANDARDS
- OTHER SUBFUNCTIONS RQMTS.
  - RELIABILITY
  - MAINTAINABILITY
  - HUMAN FACTORS
- ALLOCATE REQUIREMENTS

OUTPUT

- SPECIFIC SAFETY RQMTS. & STDS.
- INPUTS TO:
  - DESIGN & PROCEDURES
  - SAFETY DEVICES
  - WARNING DEVICES
  - TRAINING
  - PERSONNEL
- REQUIREMENTS FOR FURTHER ANALYSES, TRADE STUDIES & TESTING
- BASELINE FOR PROGRAM REVIEWS & AUDITS

FIGURE 11

ASSEMBLE BACKGROUND AND EXPERIENCE RETENTION INFORMATION

INPUT REQUIRED

- SYSTEM DESCRIPTION
- EXPER. RETENTION INFO.
- INFO. FROM SIMILAR CURRENT SYSTEMS
- HISTORICAL ENVIRONMENTAL DATA
- SUBFUNCTIONS EXPERIENCE RETENTION DATA
- RESEARCH

OUTPUT

- INITIAL SYSTEM SAFETY STDS.
- EXPERIENCE DATA FOR
  - QUALITATIVE ANALYSES
  - QUANTITATIVE ANALYSES

FIGURE 9

SAFETY ASSURANCE ACTIVITIES

- DESIGN REVIEWS
- TRADE STUDIES
- CHANGE CONTROL
- TEST
- DOCUMENTATION
- TRAINING
- PROGRAM CLOSEOUT

INPUT REQUIRED

- DESIGN CONFIGURATION
- TRADE CANDIDATES
- DESIGN CHANGE CONFIGURATION
- HISTORICAL

OUTPUT

- SAFETY ASSURANCE
- SAFETY OPTIMIZATION
- EXPER. RETENTION DATA
- INTEGRATED SAFETY PROGRAM

FIGURE 12

ANALYSES

- QUALITATIVE
- QUANTITATIVE

INPUT REQUIRED

- CURRENT SYSTEM DESCRIPTION
- FUNCTIONAL FLOWS
- TIME LINE ANALYSIS
- MISSION OBJECTIVES
- MISSION GOALS
- KEY MILESTONES
- REQMTS. OF OTHER SUBFUNCTIONS
  - RELIABILITY
  - MAINTAINABILITY
  - HUMAN FACTORS
  - QUALITY CONTROL
  - LOGISTICS
  - DESIGN
- SYSTEMS ENG. RQMTS.

OUTPUT

- IDENTIFY HAZARDOUS ELEMENTS & HAZARDOUS CONDITIONS
- IDENTIFY RISK
- INPUTS TO TRADE-STUDIES
- CRITICAL SYSTEM LIST
- CRITICAL OP. LIST
- CHANGE RECOMMENDATION
  - DESIGN
  - PROCEDURE
- SAFETY PREDICTIONS
- ALLOCATIONS
- INPUT TO SAFETY RQMTS.

FIGURE 10