View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Embry-Riddle Aeronautical University

The Space Congress® Proceedings

1989 (26th) Space - The New Generation

Apr 27th, 2:00 PM

Paper Session III-A - Space Station Freedom: Safety Program

John G. Griggs

III Chief, Safety Division, Space Station Freedom Program Office, National Aeronautics and Space Administration

Follow this and additional works at: https://commons.erau.edu/space-congress-proceedings

Scholarly Commons Citation

Griggs, John G., "Paper Session III-A - Space Station Freedom: Safety Program" (1989). *The Space Congress® Proceedings*. 12.
https://commons.erau.edu/space-congress-proceedings/proceedings-1989-26th/april-27-1989/12

This Event is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in The Space Congress® Proceedings by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE Aeronautical University™
SCHOLARLY COMMONS

SPACE STATION FREEDOM
SAFETY PROGRAM

John G. Griggs, III
Chief, Safety Division
Space Station Freedom Program Office
National Aeronautics and Space Administration

ABSTRACT

This paper begins with a renewed safety consciousness within NASA. There is focused management emphasis on the incorporation of firmly established safety design requirements and evolving new Safety analysis techniques, including the quantitative safety risk assessment methods. We as an Agency must do our very best to preclude another accident.

Further discussed is the framework for the Space Station Freedom Safety Program. This framework provides for integration of the partial safety analysis performed by the numerous NASA Centers and the International Partners into a Programmatic Safety Assessment for each of the launch increments as well as the complete Space Station Freedom on orbit.

INTRODUCTION

The Space Station Freedom is on a course to effect the agreements necessary to implement, early on, a program-wide safety program. The safety program includes carefully reviewed and tailored requirements for a) design, and b) safety analysis efforts which can then be integrated to develop the programmatic risk assessment for the Program Director. Internally, NASA has adopted new procedures for the traditional analyses efforts and incorporated new quantitative assessment methods on the Space Station Freedom Program. NASA is working with the International Partners to insure that their equivalent practice to our methodology, and the result, is acceptable and achievable.

The status of that work, and discussion of agreements still needed, are the focus of this report.

TEXT

History has documented that the NASA had fallen into the so-familiar pattern of "disregard of the situation" (just as you might with your power saw at home).

History has also shown that Reliability's Failure Modes And Effects Analysis (FMEA), as well as the various safety analyses which key from the FMEA as a starting point had become an historical record rather than analyses which drive design.

It is fair to say that over time the significance of the safety input to decisions concerning manned space flight diminished. This has been well documented in

the various commission reports. I judge this in part because of the quality of the safety input to the decisions diminished and in part because of the management attention to the safety program. Jointly, hand-in-hand, the management attention and the quality of the safety program eroded until the safety effort was "silent" and the management recognition was absent.

We are springing vigorously off of this renewed intensity in the development of the SRM&QA program for the Space Station Freedom Program. Not to diminish the efforts of those involved in the resumption of the manned space flight on the shuttle program, we on the Space Station Freedom have the opportunity (the obligation) to build a program which will not require revamping in the late 1990's.

We in the NASA have now taken steps to insure that the FMEA and the safety analysis will be in the correct time frame relative to the design milestones, and will impact that design.

For the NSTS program, the FMEA and safety analyses have been re-accomplished, and many design changes have resulted. Further, where a safety risk has been accepted, it has been done in a systematic manner, with the Program Director making knowledgeable decisions.

NASA has also revisited the techniques for performing these safety analyses, and has linked them in a manner which will improve the result in the future. The Preliminary Hazards Analyses fed into the detailed SubSystem Hazards Analyses, and these, with unresolved hazards, carry into the Operating Hazards Analyses which consider the operator and other environment factors.

The NASA is now incorporating a more rigorous analysis methodology. Quantitative analysis techniques developed in the chemical and nuclear industries are being evaluated and applied now to some efforts.

On the Space Station Freedom Program we are defining and implementing a safety program which will insure the safe launch, assembly, and 30 year operation of a manned base, and unmanned free flying platforms. The safety program includes requirements for a) design, and b) analysis of the evolving design for hazards. A part of the analysis is the identification of "hazard control requirements" which in the early program phases are derived design requirements.

We have in place today the initial set of safety design requirements, documented in the Program Definition and Requirements Document (PDRD). We further have defined an updated and workable process for performing the traditional qualitative safety analyses. The NASA level III Centers have agreed to use a common process and format for the analysis and the worksheet as well as the formal report.

We are now in the process of providing a program-wide electronic data base which will make the hazard data available to all who may be affected, and allows for feedback by the affected party. This assists in the severity categorization and development of hazard control requirements.

Within the NASA this data base will reside in the Technical and Management Information System (TMIS) which is a SSF program-wide host system for data bases.

The next advancement, now in work, will be to incorporate the Quantitative Risk Assessment (QRA) analysis process. The goal is to implement the QRA process in a manner which uses the FMEA and the qualitative hazards analyses as the input, and extends these WHERE REQUIRED into more in-depth analyses.

This is an advancement over the qualitative hazard analysis in several ways. First, it is more rigorous in the "What can go wrong?" portion of the qualitative analysis. This leads to a more complete hazard analysis, should the process be allowed to stop there.

The next step is to determine the likelihood of the occurrence. This is done in a detailed manner by the construction of a fault tree composed of the events which can lead up to the occurrence of the undesired event described in the scenario. The fault tree is first built in a qualitative manner, describing the combinations of events which could cause the Hazard.

The additional benefit is that the undesired events can now be attached with a likelihood of occurrence, which we did before (but now with the application of statistical confidence limits). The overall fault tree can then be "summed" giving the hazard scenario a likelihood of occurrence (with confidence limits) and a damage estimate ($).

The damage estimate is "simply" the estimated loss should the hazard occur in one of the manifestation modes which is possible. Since we seldom know that value, the application of statistical confidence limits is appropriate.

A risk function, be it a simple multiplication of the three factors, or some more complex function, can be used to establish a safety risk assessment.

Development of the criteria to determine when the additional, more rigorous analysis is required is under way and should be completed during the first quarter of 1989. It seems clear that at a minimum, any residual risk which is categorized as catastrophic requires this additional knowledge of causal factors, probability of occurrence, and definition of damage states.

As with the standard methodology for the qualitative safety hazards analyses, the QRA analytical method will be standard across the NASA portion of the Space Station Freedom program. This technique, too, will utilize the TMIS system for housing a master data base with the QRA models and fault tree analyses. The QRA model data base will link to the engineering data base for FMEA data, thereby insuring the accuracy of the data, and use of common data.

This brings the discussion to the International Partners and how they will interface with or use these processes.

The U.S. NASA commitment to the Space Station Freedom Program is to build the core station, and to perform the integration of the portions built by the International Partners. The NASA core station involves the efforts of six NASA

Centers, building the electrical power system, the habitant module and the U.S. laboratory module, as well as the truss assembly and the logistics module for servicing and crew re-supply.

These centers have agreed to use the safety analysis processes described above.

The three International Partners, each charged with building a significant element of the space station, currently have their own engineering and management systems. These include the European Space Agency, who builds the ESA attached laboratory module; the Japanese Space Agency, who also builds an experiment laboratory, an outside space exposure deck, and the remote manipulator arm to service the experiments; and Canada, who is responsible for the mobile servicing system. This system includes the remote manipulator capability designed to assemble the space station during the assembly stages.

Clearly, the International Partner elements are critical to the manned life support, and in the case of Canada, to the assembly of Space Station Freedom itself.

By Memorandum of Understanding (MOU), the International Partners agree to "meet or exceed" the requirements the NASA applies to the U.S. portion of the space station. In the safety arena, this is true of both the design requirements and the analysis requirements for identifying and mitigating hazards.

Below the level of the MOU, the actual workings of the safety program between all partners can only be insured by the use of common (or equivalent) design requirements and safety analysis processes. A positive spirit of cooperation is allowing the development of compatibility in these areas.

All of the effort to date within the NASA portion of the SSF program in standardizing the analysis methodology and the timing of the application has been shared with the International Partners. This is also true of the studies of the QRA, together with the criteria for its application.

Each of the three partners have likewise shared their proposed safety analyses methodologies with the other International Partners. We all recognize that control of hazards and their possible effects requires analysis efforts which cross the international interfaces. We can be sure that the hazard and the effects will not feel constrained by the international interfaces; therefore, we must insure that the analysis is not so constrained.

What has been outlined above is the first step in achieving this treaty requirement; that of developing good analysis requirements, and insuring, by exchange of process information, that the similar (if not identical) processes will produce equivalent results.

Further, the community of the NASA and the three International Partners, working through the exchange described above, are adopting data form and formats as similar as our differing systems will allow. As the ESA safety manager says: "That is not a requirement, but it certainly makes our job easier".

As the safety design requirements and the analysis process methods,

be they identical or similar, they must be documented in the Joint PDRD, which is a joint requirements document between each International Partner and the NASA. This document, too, is under configuration control by both partners.

Once the analysis tools and the basic set of safety requirements are agreed to and implemented, the safety data flow between the international partners and the NASA must be unimpeded. The electronic data bases of the partners must be compatible with that of the NASA TMIS. While we must remain mindful of the U.S. Dept of State requirement to oversee Technology Transfer, we MUST achieve unrestricted flow of the safety data to a) understand the hazards, and b) mitigate the hazards or the effects. The system described above will insure the daily hazards data interchange.

At major milestone reviews through the Critical Design Review (CDR), and then more often, the integrated safety assessment must be documented and reviewed by the safety community and then with program management.

That is not to say that a given issue must wait for the periodic review; a specific issue must be worked in its turn, and taken to program management with the engineering request for requirements change, deviation, or waiver; and the associated safety risk acceptance of residual risk.

Safety engineering can no longer accept the safety risk for the program; that risk, along with the germane program performance, schedule, and cost data, must be given to the program management for decisions on safety risk reduction or acceptance.
During the periodic reviews which document and review the safety risk model, a board, composed of all affected agencies, must review the risk elements and jointly recommend disposition to management. This is the only manner in which we can insure that the risk is truly understood.

At these periodic safety risk reviews, one parameter to be studied is the consistency of the safety data. The job jointly belongs to the safety community to insure that the thoroughness of the analyses is maintained, as we are all affected by the outcomes.

The additional check on the compliance with the agreed to design and analysis requirements is a process for "audit", or "survey" of the system to assess compliance. Any deviation or non-compliance must be identified and rectified.

Within the NASA, there are established processes for audits. The process details of how this activity can be accomplished across the interface and into the International partners' program have not been defined and agreed to as yet.

SUMMARY

Space Station Freedom is the largest international space endeavor undertaken since the beginning of space exploration. Building a diverse, distinctive and international Safety Program and Safety Community on the Space Station Freedom Program will be challenging. Within the safety community, the individual dedication is allowing the accomplishment of required goals and objectives.

Concurrently, painstaking examination to detail and careful documentation of the Space Station Freedom requirements are being implemented and are mandatory for success.

Communication in the safety program will utilize state-of-the-art software and computers, which will provide broad accessibility to safety information among the NASA and the International Partners. Safety information flow will be a key tool for integrating and achieving a safely designed Space Station Freedom and disseminating integrated safety assessment results.

There have been joint NASA projects with other nations, but the Space Station Freedom Program brings a new level of complexity and challenge for successful integration of the United States, Canada, Japan and the European Space Agency. This integration to ensure Space Station Freedom success will assuredly advance the science of safety engineering, human engineering and quantitative risk assessment in space.