1996

NASA/ASEE SUMMER FACULTY FELLOWSHIP PROGRAM

MARSHALL SPACE FLIGHT CENTER
THE UNIVERSITY OF ALABAMA

AN INDEPENDENT EVALUATION OF THE FMEA/CIL HAZARD ANALYSIS ALTERNATIVE STUDY

Prepared By:	Paul S. Ray, Ph.D
Academic Rank:	Associate Professor
Institution and Department:	The University of Alabama Industrial Engineering Department Tuscaloosa
NASA/MSFC:	
Office:	System Safety and Reliability Office
Division:	Safety and Mission Assurance
MSFC Colleague	Edward H. Kiessling William C. Smith Gordon B. Hoskins-SAIC

INTRODUCTION

The present instruments of safety and reliability risk control for a majority of the National Aeronautics and Space Administration (NASA) programs/projects consist of Failure Mode and Effects Analysis (FMEA), Hazard Analysis (HA), Critical Items List (CIL), and Hazard Report (HR). This extensive analytical approach was introduce in the early 1970's and was implemented for the Space Shuttle Program by NHB 5300.4 (1D-2. Since the Challenger accident in 1986, the process has been expanded considerably and resulted in introduction of similar and/or duplicated activities in the safety/reliability risk analysis. A study initiated in 1995, to search for an alternative to the current FMEA/CIL Hazard Analysis methodology generated a proposed method on April 30, 1996. The objective of this Summer Faculty Study was to participate in and conduct an independent evaluation of the proposed alternative to simplify the present safety and reliability risk control procedure.

SAFETY/RELIABILITY RISK CONTROL METHODS

Present Method: The present method uses analysis and reporting in two phases. The analysis for hardware failures are documented in FMEA and critical items based on FMEA is reported in CIL. The analysis for hazards are documented in HA. The Hazard Report is prepared on the basis of HA and CIL report.

Proposed Method: The proposed method integrates all analysis in a single phase documenting in Risk Analysis and a single report for all potential critical failures and other hazards in Risk Management Report (RMR). The method fosters a comprehensive analysis rather than the present compartmentalized one.

APPROACH OF THE STUDY

The evaluation approach has been to review the four basic risk control documents - FMEA, CIL, HA and HR for their functions, data elements contained in them, analytical process required to develop these, document user friendliness, and the effects of project characteristics.

ANALYTICAL PROCEDURE

Functions of the basic document: FMEA and HA are both analytical documents. The FMEA contains information on failure modes/causes excluding some environmental and human factor causes while HA deals with all hazards including critical failures, environmental and human factor causes. Both these two have a number of common data and are suitable for integration to eliminate duplication and/or compartmentalization of thought process. Similarity CIL and HR are both reports based on analysis done in developing FMEA and HA. These are suitable for integration to eliminate duplication of common data elements, and cross referencing between CIL and HR.

Data Elements of the basic document: The documents FMEA/HA, CIL/HR vary significantly depending on the project size, complexity and nature. The contents of the documents are of the following types:

- Introductory/identification
- Analytical
- Analysis support
- Review and approval

Integration of the analysis and reports is expected to reduce number common/similar data in integrated documents by about 20 to 3o percent as shown in table 1 and 2.

Table 1

Number of Data Elements in Analysis Document(s)

	Present Method			Proposed Method
	FMEA	HA	Total	RA Total
Introductory	4	4	8	4
Analytical	9	8	17	13
Support Data	5	4	9	7
Review/Approval	1	1	2	1
Total			36	25

Data elements reduced from 36 to 25 (30.6%)

Table 2

Number of Data Elements in Report(s)

	Present Method			Proposed Method
	CIL	HR	Total	RMR Total
Introductory	4	4	8	6
Analytical	8	8	16	13
Support Data	4	1	5	4
Review/Approval	2	2	4	2
Total			33	25

Data elements reduced from 33 to 25 (24.4%)

Analytical Process: The present method of separating failure mode effect analysis (FMEA) and hazard analysis (HA) introduces duplication and compartmentalization in the thought process. There is a possibility of incomplete analysis due to responsibility of partial analysis assigned to different groups. To complete the hazard analysis, the safety group has to obtain hardware failure mode/cause data from the FMEA group requiring coordination and/or occasional duplication of analysis due to scheduled milestones. In addition, the proposed method

of documentation has scope of simplification resulting in faster comphehension at less effort. For example, key information can be summarized in a tabular format for a hypothetical case of "Premature Release Bolt Failure" that is currently contained in three separate CILs and a Hazard Report which contains four additional hazards. The key information would include the critical failures/hazards, critical items identification, number of items required, critical/hazard effect, failure/hazard causes, single and redundant failure identification, criticality categories, severity levels, likelihood of occurrence, and hazard classification. This would provide the user key information about a critical event without having to search four different reports. User activities like planning test/inspection points, verifying redundancy, certification of flight readiness, life extension of hardware etc. at various phases of a project life. The improved presentation, reduction of cross-referencing, reduction of number of documents to deal with will result in less user effort for higher productivity for the project as a whole.

User friendliness/cross referencing: The purposed integration of analysis and reports will reduce the need of cross referencing to a significant extent. Two cases of Space Shuttle Program studied, indicated that the FMEA and/or CIL are referenced on an average of twenty-two times for each CIL or five times for each failure cause. The need of so much cross referencing between the CIL
and HR, imposing a significant amount of time and effort on analyst, will be eliminated in the integrated system.

Document Retention, Storage, and Retrieval: The proposed integrated system will reduce the number of documents to retain, store, and retrieve and as such reduce the time required for assessment of safety and reliability risks in a program/project.

Effect of Project characteristics: The nature of size of a project will effect the risk management process significantly . A large and complex project will require extensive analysis while a small and simpler project may require only environmental/human error type hazards and no critical failure type hazards. This difference will result in substantially more savings for a larger project. However the integrated approach will result in some savings in all cases.

MERITS OF THE PROPOSED METHOD

The proposed method appears to have several advantages over the current procedure as listed below:

- Focus on a single and integrated analysis process instead of the present compartmentalized system is likely to produce more comprehensive safety/reliability risk analysis. The integration will eliminate the possibility of critical situations being left out of analysis due to partial work done by each group.
- Integrated risk analysis and reporting process will greatly reduce the coordination required now between two groups FMEA/CIL and HA/HR.

- Duplication of common data elements will be eliminated in the analysis as well as in the reporting documents. This will reduce the volume of reports and result in a reduction in the effort required to review and comprehend the safety/reliability risk status.
- The possibility of occasional duplication of analysis due to different time constraints for different groups will also be eliminated.
- All safety/reliability risk data will be submitted simultaneously for review and approval to appropriate authorities. This will eliminate duplication of review/approval process.
- A more effective documentation method (e.g. tabular format, etc.), will improve comprehension of the status at a glance and reduce the frequent referencing to pages of multiple documents.
- Recording, storing, and maintaining a significantly lower volume of documents during the life time of a program will result in a considerably large savings in manpower and cost.

RECOMMENDATIONS

In view of the substantial merits of the proposed integrated system over the present FMEA/HA and CIL/HR, the following recommendations are made:

- Develop the final formats for:
    - Risk Analysis Worksheet, and
    - Risk Management Report
- Continue to develop requirements and guidelines detailing method to follow with clear definitions of limits for analysis and reporting.
- Continue the independent and concurrent evaluation, as continuation of the Summer Research Program (1996) of The University of Alabama during the development of the proposed risk management system.
- Conduct a test run and/or parallel run of the proposed method, preferably for an in-house project.
- Debug the weak points from the system, on the basis of the test/parallel run.
- Arrange for orientation of the analysts in the proposed integrated process.
- Implement the proved-in integrated system of safety/reliability risk analysis for the future programs/projects.

COMMENTS

The present evaluation study covered only the basic thought process and the development of documentation required to support the system. The proposed system does not exclude any analytical technique e.g. checklists, fault trees, but propose to use these as required in a cost effective way. The indication of savings at this stage (20 to 40 %) is approximate but savings will result from integrated thought process, improvement in documentation format, reduction of volume and number of documentation, and reduced effort for users at various phases of a project life.

ACKNOWLEDGMENT

It is to acknowledge the extensive help I received from Mr. Gordon B. Hoskins of Science Applications International Corporation (SAIC) in studying the Safety/Risk Analysis process at MSFC/NASA. It would have been impossible to complete this study without his help within a few weeks of the Summer Fellowship Program (1996).

REFERENCES

1. Department of Defense. Military Standard-System Safety Program Requirements. MIL-STD-882C. Department of Defense, January 19, 1993.

2. JSC-NASA. Methodology for Conduct of Space Shuttle Program Hazard Analysis. NSTS-22254, Revision B, Change 4. JSC-NASA, December 30, 1993.

3. JSC-NASA. Requirements for Preparation and Approval of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL). NSTS-22206, Revision D, Change 24. JSC-NASA, July 13, 1995.

4. Reliability and Quality Assurance Publication-NASA. Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program. NHB 5300.4 (1D-2). Reliability and Quality Assurance Publication-NASA, October, 1979.

5. Space Station Freedom Program Office-NASA. Safety Analysis and Risk Assessment Requirements. SSP 30309, Revision D. Space Station Freedom Program Office-NASA, June 1993.

6. Science Applications International Corporation. Failure Mode and Effects Analysis (FMEA), Critical Items List (CIL) and Hazard Analysis Alternative Study Including A Proposed Risk Assessment Method. Interim Report, SAIC, February 26, 1996

7. Science Applications International Corporation. Failure Mode and Effects Analysis (FMEA), Critical Items List (CIL) and Hazard Analysis Alternative Study Including A Proposed Risk Assessment Method. Final Report, SAIC, April 30, 1996

8. Science Applications International Corporation. Risk Assessment Requirements Document. (Draft) Interim Report, SAIC, June 3, 1996

9. United Technologies USBI. Critical Items List for Space Shuttle Solid Rocket Booster And Range Safety Command Destruct System. USBI-RA-21, Item Code 60-03-12. United Technologies USBI, March 1, 1994.

10. United Technologies USBI. SRB Flight Systems Hazard Analysis Report, Boost Phase, B-60-05 Thermal Curtain Failure. USBI-49220-RA-22-B-60-05, Item Code 60-03-12. United Technologies USBI, March 1, 1994.