

AEROSPACE INFORMATION REPORT

Submitted for recognition as an American National Standard

Issued 1996-07

RELIABILITY AND SAFETY PROCESS INTEGRATION

TABLE OF CONTENTS

1.	SCOPE.....	3
2.	REFERENCES.....	3
2.1	Applicable Documents.....	3
2.1.1	SAE Publications.....	3
2.1.2	U.S. Government Publications.....	3
2.2	List of Acronyms.....	4
3.	TECHNICAL REQUIREMENTS.....	5
3.1	Overview	5
3.2	Statement of Need	7
3.3	Introduction to the Concept	7
3.4	Discussion of Each Analysis as Currently Performed	7
3.4.1	Introduction	7
3.4.2	Failure Mode, Effects, and Criticality Analysis (FMECA).....	7
3.4.3	Reliability Allocation.....	9
3.4.4	Reliability Prediction	9
3.4.5	Hazard Analysis.....	9
3.4.6	Fault Tree Analysis.....	9
3.4.7	Testing and FRACAS	9
3.5	Details of Reliability and Safety Interrelationships	9
3.5.1	Reliability Prediction ----> FMECA	10
3.5.2	FMECA ----> MODE FAILURE RATE ----> FAULT TREE ANALYSIS	10
3.5.3	FRACAS ----> FMECA.....	10
3.5.4	HAZARD ANALYSIS ----> FAULT TREE ANALYSIS.....	10
3.5.5	FMECA ----> DETECTION METHOD/COMPENSATING PROVISIONS ----> FAULT TREE ANALYSIS	11
3.5.6	FRACAS ----> FAULT TREE ANALYSIS	11
3.5.7	Coordination and Control.....	11

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be reaffirmed, revised, or cancelled. SAE invites your written comments and suggestions.

Copyright 1996 Society of Automotive Engineers, Inc.
All rights reserved.



Documents
Printed in U.S.A.
Document Sharing Hub

TABLE OF CONTENTS (CONTINUED)

3.6	Example of R&S Processes: Turbine Engine Overspeed Control	12
3.6.1	Description of Turbine Engine Overspeed Control.....	12
3.6.2	Reliability and Safety Analysis Tasks for Overspeed Control Example System	13
3.6.3	Conclusion of Example	23
3.7	Discussion and Recommendations.....	23
FIGURE 1	Integrated Reliability and Safety Analyses Process Flow Diagram.....	6
FIGURE 2	Reliability and Safety Program Relationships.....	8
FIGURE 3	Overspeed Control System - Primary Speed Sensor FMECA.....	14
FIGURE 4	FTA: Overspeed Control System	17
FIGURE 5	FRACAS: Overspeed Control System - Primary Speed Sensor	22
TABLE 1	Reliability Prediction: O/S Control System	15

SAE AIR5022

1. SCOPE:

This SAE Aerospace Information Report (AIR) describes several of the commonly performed Reliability and Safety (R&S) analysis tasks, with emphasis on their inter-relationships and common data elements. This document also describes how the R&S process can be integrated, reducing duplicate work effort and providing more accurate, comprehensive, and standardized analysis results.

To illustrate how this integration can be accomplished, several specific reliability and safety tasks are performed on a subsystem of an example product.

2. REFERENCES:

2.1 Applicable Documents:

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1 SAE Publications: Available from SAE, 400 Commonwealth Drive, Warrendale, PA 15096-0001.

AIR4276 Survey Results - Computerization of Reliability, Maintainability and Supportability (RM&S) in Design

AIR4845 The FMECA Process in the Concurrent Engineering (CE) Environment

AIR4896 Recommended RMS Terms and Parameters

2.1.2 U.S. Government Publications: Available from DODSSP, Subscription Services Desk, Building 4D, 700 Robbins Avenue, Philadelphia, PA 19111-5094.

Reliability Program for Systems and Equipment Development and Production (Reference MIL-STD-785B). By Department of Defense.

Military Standard System Safety Program Requirements (Reference MIL-STD-882B). By Department of Defense.

Procedures for Performing a Failure Mode, Effects and Criticality Analysis (Reference MIL-STD-1629A). By Department of Defense.

Electronic Reliability Design Handbook (Reference MIL-HDBK-338). By Department of Defense.

Electronic Reliability Prediction (Reference MIL-HDBK-217). By Department of Defense.

SAE AIR5022

2.2 List of Acronyms:

AIR	Aerospace Information Report
BIT	Built-in Test
CAA	Civil Aviation Authority
CALS	Continuous Acquisition and Life-cycle Support
CCA	Cause Consequence Analysis
CCDL	Cross Channel data Link
CE	Concurrent Engineering
DoD	Department of Defense (U.S.)
ETA	Event Tree Analysis
FADEC	Full Authority Digital Electronic Control
FHA	Functional Hazard Analysis
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
FRACAS	Failure Reporting and Corrective Analysis System
FTA	Fault Tree Analysis
G-11	SAE RMS Committee
G-11AT	SAE G-11 Automation and Tools Subcommittee
G-11CR	SAE G-11 Computerization of RMS Subcommittee
G-11PT	SAE G-11 Processes and Tools Subcommittee
IEC	International Electro Chemical
ILS	Integrated Logistics Support
IPD	Integrated Product Development
LCC	Life Cycle Cost
LSA	Logistic Support Analysis
LVDT	Linear Variable Differential Transformer
M	Maintainability
MIL-HDBK	U.S. Military Handbook
MIL-STD	U.S. Military Standard
MTBF	Mean Time between Failures
O&SHA	Operating and Support Hazard Analysis
NASA	National Aerospace and Space Administration
PHA	Preliminary Hazard Analysis
R	Reliability
R&S	Reliability and Safety
RBD	Reliability Block Diagram
RMS	Reliability, Maintainability and Supportability
S	Safety
SAE	Society of Automotive Engineers
SCA	Sneak Circuit Analysis
SDS	System Design Solution
SHA	System Hazard Analysis
SSHA	Subsystem Hazard Analysis
SIM	System Integrity Monitoring
US	United States

3. TECHNICAL REQUIREMENTS:

3.1 Overview:

A number of DoD initiatives such as Concurrent Engineering (CE), Integrated Product Development (IPD), and Continuous Acquisition and Life Cycle Support (CALS) have emphasized the importance of integrating all technical disciplines during the life cycle phases of a program to produce an improved product at lower acquisition and life cycle cost. Surveys have been conducted that indicate most companies have automated various engineering and logistic processes but have not integrated them to achieve the level of improved performance and lower costs expected. The survey conducted by the SAE G-11CR (Computerization of RM&S) subcommittee and documented in AIR4276 shows that 30 to 40% of the aerospace companies surveyed have automated their RMS tasks but only 5% have integrated them together.

AIR4276 also indicates that survey respondents feel that the Failure Mode, Effects and Criticality Analysis (FMECA) has the highest priority for automation since it is labor intensive and has a large number of users of the output data. The G-11AT (Automation and Tools Subcommittee) examined the FMECA in detail and made recommendations on which elements of the current process could be automated and how this could be accomplished. A set of recommendations was given for integrating FMECA automation into the concurrent engineering process. This is documented in AIR4845.

As a follow-on to the above two projects the G-11PT (Processes and Tools) Subcommittee decided that there is benefit to examining the integration of various reliability analyses with safety analyses to create a more effective reliability and safety assessment environment. The G-11PT Subcommittee has developed an integrated reliability and safety process which is described in this document (see Figure 1). An example is provided, to illustrate how an integrated R&S process can be accomplished, and the resulting benefits. This document is limited to reliability and safety analysis techniques and only peripherally addresses maintainability and supportability. The specific reliability and safety analyses being discussed in this document are:

- a. Reliability Allocations
- b. Reliability Predictions
- c. FMECA
- d. Hazards Analysis
- e. Fault Tree Analysis

Paragraph 3.2 examines the need for integrating the reliability and safety tools and analyses to produce a complete, consistent, and cost effective product. Specific needs are described along with the benefits of integration. Paragraph 3.3 provides an overview of overlaps between analyses. Paragraph 3.4 describes each analysis as it is presently performed and paragraph 3.5 provides a description of the dependencies and interrelationships between the various tools and analyses. Paragraph 3.6 uses a turbine engine overspeed control as an example to show how the analyses can be integrated. Paragraph 3.7 concludes the document and adds recommendations for future action.

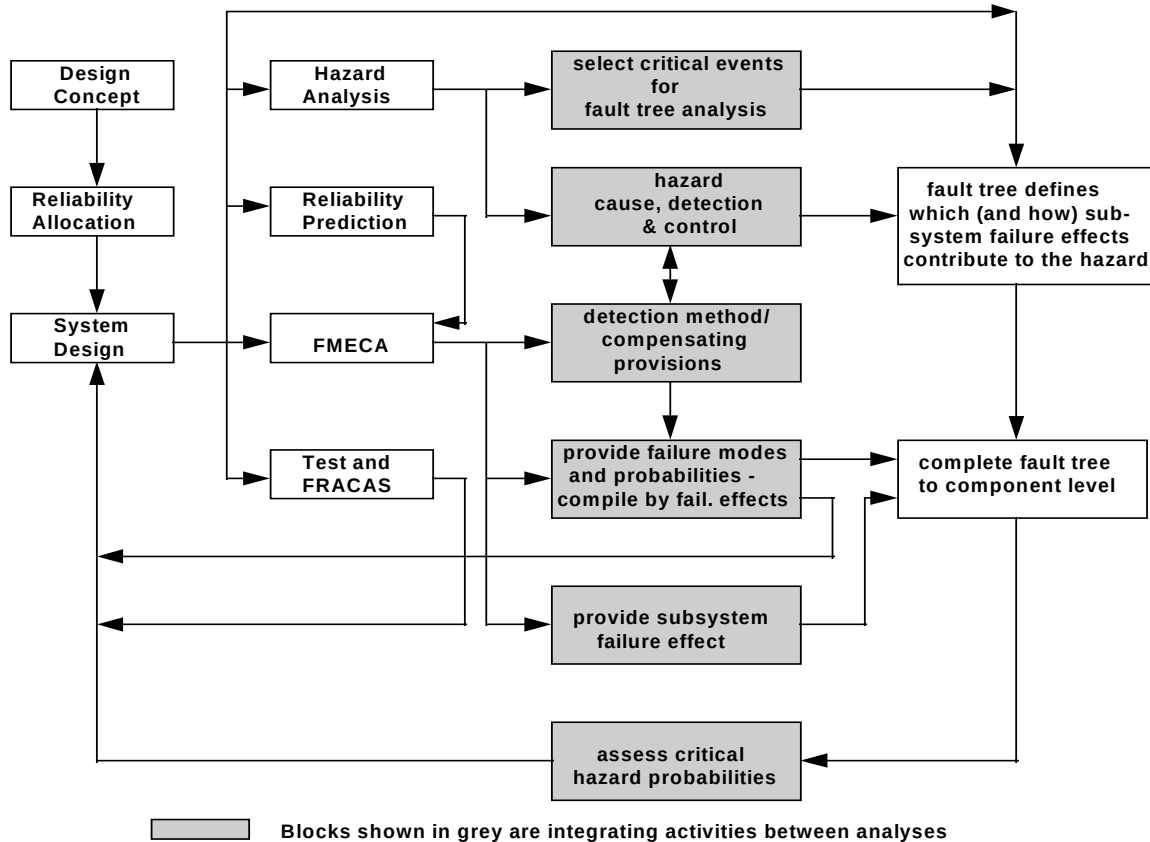


FIGURE 1 - Integrated Reliability and Safety Analyses Process Flow Diagram

3.2 Statement of Need:

Various reliability and safety analysis tasks are available to help ensure that a product design will meet reliability and safety requirements. By integrating these tasks in an efficient and effective manner, duplicate work effort can often be eliminated. Even more important, integrating these tasks will provide more accurate and consistent analysis results, by ensuring that common ground rules, assumptions, and input data are used throughout. Many companies will find that in integrating the R&S process, the tasks themselves will become more structured and clearly defined. This will facilitate more effective control and management of the process, including schedules, personnel assignments, and training needs.

3.3 Introduction to the Concept:

Figure 2 is an overview of the interaction of R&S tasks necessary to produce a complete, consistent, and cost-effective product. The overlaps and interactions between R&S are illustrated. The increasing complexity of systems compounded by commercial pressure and skill limitations are factors that make more urgent the integration and automation of most of these processes. In order to generate data for the various R&S analyses shown in Figure 2 it becomes apparent that several of these analyses share the same or very similar data elements.

The end result of defining the common elements in the various R&S analyses will be a more cost-effective and streamlined program with less duplication among the disciplines. The benefit to the customer is lower cost analyses and the benefit to the equipment developer is the need for less resources to generate the necessary data. Other major benefits will be better awareness of the various analysts of the other analyses and better and more consistent quality. The long-term benefit, if managed correctly, will be the development of greater skills flexibility and the capability of performing a variety of different types of analysis. This is particularly important as defense and military budgets shrink and less personnel are available after company downsizings.

3.4 Discussion of Each Analysis as Currently Performed:

- 3.4.1 Introduction: R&S analyses and their design influence are iterative processes. R&S engineers are continuously assessing the design and evaluating its reliability and safety characteristics. They feed the results of these assessments with recommendations for improvements to the rest of the design team. The following sections describe some of the major analyses.
- 3.4.2 Failure Mode, Effects, and Criticality Analysis (FMECA): The Failure Mode, Effects, and Criticality Analysis (FMECA) is a systematic analysis to determine the various ways an item may fail (the failure modes); the effect of each failure mode on other items (the failure effects); and a measure of effects of each failure mode on the performance of the entire system (the criticality). FMECA is performed for each system function or each system component/piece part. Each potential failure mode is ranked by the severity of its effects to help prioritize corrective actions that may be taken to eliminate or control the high risk items. FMECA is used in maintainability analysis, safety analysis, survivability and vulnerability analysis, LSA, maintenance plan analysis, and testability analysis.