ANSI/AIAA
S-102.2.18-2009

Standard

Performance-Based Fault Tree Analysis Requirements

Approved American National Standard

ANSI

AIAA

ANSI/AIAA
S-102.2.18-2009

American National Standard

Performance-Based Fault Tree Analysis Requirements

Sponsored by

American Institute of Aeronautics and Astronautics

Approved 17 November 2008

American National Standards Institute

Abstract

This standard provides the basis for developing the performance-based fault tree analysis (FTA) to review and analytically examine a system or equipment in such a way as to emphasize the lower-level fault occurrences that directly or indirectly contribute to the system-level fault or undesired event. The requirements for contractors, planning and reporting needs, and analytical tools are established. The linkage of this standard to the other standards in the new family of performance-based reliability and maintainability (R&M) standards is described, and a large number of keyword data element descriptions (DED) for use in automating the FTA process are provided.

Library of Congress cataloging-in-publication data on file

Published by
American Institute of Aeronautics and Astronautics
1801 Alexander Bell Drive, Reston, VA 20191

Printed in the United States of America

Contents

Tables

Foreword

Although the terms quality and reliability are often used interchangeably, they have different meanings. *Quality* as used in this standard, is the ability of a product to meet the workmanship criteria established by an organization. A different, but often used, definition of quality: Quality is the set of all desired attributes that can be put in a product. In this sense, quality cannot be achieved without achieving the desired reliability. *Reliability* is the ability of a product or system to perform its intended function(s) for a specified time or operating cycles. A high-quality product may not be a high-reliability product even though it conforms to stringent workmanship specifications. The ISO 9000 series standards that establish the ability of an organization to consistently produce high-quality products do not necessarily establish that same organization's ability to consistently deliver high-reliability products. Consequently, the ISO 9000 series certification process, which serves as the main international reference for quality program requirements in business-to-business dealings, is not the appropriate reference for international or domestic reliability program requirements. A more suitable reference is the suite of AIAA S-102 performance-based reliability and maintainability (R&M) standards, which provide a framework for quantifying and improving the performance of R&M practices.

As Annex A shows, there are 35 standards in the AIAA S-102 performance-based R&M standards document tree. These standards provide criteria for rating the capability of R&M practices and they represent proven approaches for planning and implementing the product life cycle R&M program. The S-102 R&M capability-rating criteria allow organizations to:

— specify a level of R&M program performance.

— plan the activities to achieve a level of R&M program performance.

— appraise the performance of an R&M program or individual practice.

— identify the activities necessary to improve the performance of an R&M program or individual practice.

The S-102 R&M capability-rating criteria (Annex B in all S-102 standards) are intended to aid organizations in ensuring their R&M programs are a "value-added" contribution to the product development effort. *There is no intent to prescribe a universal methodology for quantifying the evaluation or improvement of R&M programs or individual practices.* The S-102 R&M capability-rating criteria reflect the collective body of knowledge of the S-102 Working Group, which was chartered by the AIAA Standards Executive Council to develop and approve the S-102 standards. The S-102 Working Group is composed of R&M experts that represent the government and industry sectors affected by the S-102 standards.

This standard establishes uniform requirements and criteria for a performance-based fault tree analysis (FTA). The principles of the FTA as promoted in a performance-based approach can be learned from this document alone, but its proper use requires careful planning, for which the prerequisite is understanding associated S-102 documents and identifying the desired R&M data products in the systems engineering process. What distinguishes this standard from all past and present FTA standards are the following.

— It provides consistent criteria for rating the "capability" of the FTA process.

— It provides consistent criteria for rating the "maturity" of the FTA data products.

— It calls for the use of knowledge-based approaches to identify, analyze, and manage test anomalies that pose unacceptable risk.

— For a Capability Level 3 or above FTA process, it calls for the collection and review of existing lessons learned, and the generation and formal approval of new lessons learned.

— For a Capability Level 4 or above FTA process, it calls for the use of predefined R&M data parameters to facilitate the exchange of FTA data products among computer-aided analysis tools and other project databases.

At the time of approval, the members of the AIAA Performance-Based Reliability & Maintainability Standards Working Group were:

Tyrone Jackson (Chair)	SRS Technologies
Lily Lau	The Aerospace Corporation
David Oberhettinger	NASA Jet Propulsion Laboratory
Walt Willing	Northrop Grumman Electronic Systems
Steve Harbater	Northrop Grumman Integrated Systems
Alazel Jackson	Raytheon Space and Airborne Systems
Jan Swider	Pratt & Whitney Rocketdyne, Inc.
Dev Raheja	Design for Competitiveness
Jeff Merrick	Merrick Consulting
Ken Gibson	Boeing Space and Intelligence Systems
James French	RMS Partnership
Dawson Coblin	Lockheed Martin Space Systems Company
Ari Jain	Reliability Consultant
Terry Hardy	Federal Aviation Administration

The above consensus body approved this document in June 2006.

The AIAA Standards Executive Council (Mr. Amr ElSawy, Chairman) accepted the document for publication in July 2008.

The AIAA Standards Procedures dictate that all approved Standards, Recommended Practices, and Guides are advisory only. Their use by anyone engaged in industry or trade is entirely voluntary. There is no agreement to adhere to any AIAA standards publication and no commitment to conform to or be guided by standards reports. In formulating, revising, and approving standards publications, the committees on standards will not consider patents that may apply to the subject matter. Prospective users of the publications are responsible for protecting themselves against liability for infringement of patents or copyright or both.

1 Scope

This standard establishes uniform requirements and criteria for a performance-based fault tree analysis (FTA), including the modeling components, symbols, and analytical objectives. The performance-based aspect of this standard requires that the organization's FTA capability be rated according to predetermined criteria for process capability and data maturity. Although it is a common industry practice for FTA to be performed using computerized tools, this standard does not mandate that any particular computerized methodology be used.

1.1 Purpose

The primary purpose of FTA is to examine systematically a potential system failure and create a graphical representation of the system logic. The fault tree represents system relationships and fault paths and provides a means for qualitative or quantitative system evaluation. Fault tree analysis is a deductive, top-down method used to determine how a given system failure can occur. A system top undesired event is either identified or postulated and the analysis attempts to find out what contributes to this undesirable event. The FTA begins with a top event, establishes the component-level to which each system-level fault is examined, and determines the immediate causes for each fault at progressively lower levels until a component-level fault is reached. The FTA determines the various ways in which a particular type of top event or failure could occur. All of the possible system contributing factors and their relationships shall be established and, if possible, a top probability of occurrence calculated.

The primary output of FTA is the fault tree structure, which allows for qualitative or quantitative evaluation of a system failure. FTA is particularly useful in the examination of functional paths of high complexity, in which the outcome of one or more combinations of non-critical basic events may produce an undesirable system failure. Typical candidates for FTA are functional paths or interfaces that could have impact on flight safety, munitions handling safety, safety of operating and maintenance personnel, and probability of error-free command in automated systems in which a multiplicity of redundant and overlapping outputs may be involved. Fault tree is an analysis tool that provides a way to combine all contributing failures, events, and conditions that can lead to the occurrence of an undesired top event.

1.2 Application

This standard applies to acquisitions for the design, development, fabrication, test, and operation of commercial, civil, and military systems, equipment, and associated computer programs. Annex B of this standard provides capability-rating criteria that are intended to categorize the capability of sets of activities commonly found in FTA processes. The capability level criteria provide the logical order of activities for improving the effectiveness of an existing FTA process in stages. Therefore, an existing FTA process may be improved by using the FTA capability-level criteria to develop a list of minimally acceptable activities and then compare that list to the activities of the existing process. This comparison identifies the activities that need to be added to the existing FTA process.

This standard also applies to the integration of the FTA database with the product failure mode, effects, and criticality analysis (FMECA) database, event tree analysis database, and the project R&M database system. However, specification of this standard should not require the contractor to use a specific computerized tool, such as a commercial computer-aided design (CAD) system. Rather, the FTA database should be implemented using the computerized tools of the contractor's choosing given that those tools are validated to process input data and generate output data that are compatible with the data definitions in this standard.