

Standard

Performance-Based Sneak Circuit Analysis (SCA) Requirements

AIAA standards are copyrighted by the American Institute of Aeronautics and Astronautics (AIAA), 1801 Alexander Bell Drive, Reston, VA 20191-4344 USA. All rights reserved.

AIAA grants you a license as follows: The right to download an electronic file of this AIAA standard for storage on one computer for purposes of viewing, and/or printing one copy of the AIAA standard for individual use. Neither the electronic file nor the hard copy print may be reproduced in any way. In addition, the electronic file may not be distributed elsewhere over computer networks or otherwise. The hard copy print may only be distributed to other employees for their internal use within your organization.

Performance-Based Sneak Circuit Analysis (SCA) Requirements

Sponsored by

American Institute of Aeronautics and Astronautics

Approved 17 November 2008

Abstract

This standard provides the basis for developing the analysis of sneak conditions. The sneak conditions may consist of hardware, software, operator actions, or combinations of these elements. 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 standards is described, and all of the keywords for use in automating the SCA 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

Copyright © 2009 American Institute of Aeronautics and
Astronautics
All rights reserved

No part of this publication may be reproduced in any form, in an electronic retrieval system
or otherwise, without prior written permission of the publisher.

Printed in the United States of America

Contents

Foreword	v
1 Scope	1
1.1 Purpose	1
1.2 Application	2
2 Applicable Documents	2
2.1 Normative References	2
2.2 Relationship To Other S-102 Standards	3
3 Vocabulary	4
3.1 Acronyms and Abbreviated Terms	4
3.2 Terms and Definitions	4
4 General Requirements	7
4.1 Contractor Responsibility	7
4.2 Planning	7
4.3 SCA Report	8
5 Detailed Requirements	8
5.1 Establish SCA Requirements and Define Analytical Ground Rules	8
5.2 Establish SCA Technical Performance Metrics	9
5.3 Collect System Design Data	9
5.4 Perform the Analysis	9
5.5 Sneak Condition Disposition	17
5.6 SCA Database	18
5.7 Data Exchange Between SCA Process And Other Project Functions	19
5.8 SCA Process Performance Evaluation	19
5.9 Lessons Learned	21
5.10 Structured Review	21
Annex A AIAA S-102 Document Tree (normative)	24
Annex B AIAA S-102 SCA Capability Level Requirements (normative)	25
Annex C AIAA S-102 SCA Keyword Data Element Descriptions (normative)	28
Figures	
Figure 1 — S-102 Standardized Set of Functional Operators	12
Figure 2 — Five Basic Sneak Circuit Analysis Topographs	13
Figure 3 — Sneak Condition Dataset Evaluation	22
Figure 4 — Sneak Condition Disposition Evaluation	23
Tables	
Table 1 — Sample Sneak Circuit Analysis Topological Clue List	14

Table 2 — AIAA S-102 Failure Severity Classification Criteria 16

Table 3 — Sneak Condition Dataset Maturity Rating Criteria 20

Table 4 — Sneak Condition Disposition Maturity Rating Criteria 20

Downloaded by Siavash Sohrab on April 21, 2015 | http://arc.aiaa.org | DOI: 10.2514/4.867163

Foreword

A performance-based Sneak Circuit Analysis (SCA) standard has been developed to aid organizations in assuring that their SCA tasking presents a “value-added” contribution to the product-development effort. The need for such a standard arises from the absence of an accepted methodology for assessing the capability of reliability and maintainability (R&M) programs. The ISO 9000 series standards presently guide organizations in establishing practices for consistently producing superior products, but only within the discipline of quality assurance. The ISO 9000 series of standards does not define processes and practices for achieving high-reliability products. Because the criteria for quality and reliability differ, an organization that conforms to stringent workmanship specifications and produces high-quality products through participation in the ISO 9000 certification process may still lack the capability to consistently deliver high-reliability products. Hence, this SCA standard was developed as part of a suite of AIAA S-102 performance-based R&M standards for quantifying the results of, and improving the performance of, R&M programs.

The AIAA S-102 performance-based R&M standards document tree (Annex A) includes 35 standards that provide criteria for rating the capability of R&M practices. 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 necessary to achieve a level of R&M program performance;
- appraise the performance of an R&M program or individual practice; and
- 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 assuring 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 comprises R&M experts that represent the government and industry sectors affected by the S-102 standards.

This standard establishes uniform requirements for a performance-based SCA. The principles of the SCA as promoted in a performance-based approach can be learned from this standard 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 SCA standards is the following.

- It provides consistent criteria for rating the capability of the SCA process.
- It provides consistent criteria for rating the maturity of the SCA data.
- It calls for the use of knowledge-based approaches to identify, analyze, and manage sneak conditions that pose unacceptable risk.
- For a Capability Level 3 or above SCA 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 SCA process, it calls for the use of predefined R&M data parameters to facilitate the exchange of SCA data among computer-aided analysis tools and other project databases.

This standard includes three annexes, all of which are normative.

At the time of approval the members of the AIAA Performance-Based Reliability and 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
Ari Jain	Reliability Consultant
Dawson Coblin	Lockheed Martin Space Systems
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 sneak circuit analysis (SCA). This performance-based aspect of this standard requires that the organization's SCA capability be rated according to predetermined criteria for process capability and data maturity. Although it is a common industry practice for SCA to be performed using computerized tools, this standard does not mandate that any particular computerized methodology be used.

1.1 Purpose

Sneak circuit analysis may be performed on high-criticality systems to uncover inherent design flaws that may cause occurrence of an unwanted function or the inhibition of a desired function. The primary purpose of the SCA process is to identify and eliminate or control all sneak conditions that may lead to such unplanned modes of operation. In this regard, SCA is an important analysis technique because it uncovers latent system faults that otherwise may have gone undetected. SCA should be considered for application on high criticality systems, where undetected design flaws may cause catastrophic events such as loss of life, critical system failure, or loss of mission. To assure maximum analysis benefit while controlling cost, the SCA effort should be scoped to those specific high-criticality areas where sneak conditions are most likely to occur. The early identification and control of such conditions improves system safety and reliability, while enabling design changes to be made in a more cost-effective manner.

The defining cause and effect characteristics of a sneak condition are as follows:

- It is caused by an unintended system path (e.g., wiring, tubing, software interfaces, operator actions, instrumentation, mechanical interlocks, or some combination thereof) or condition (e.g., timing incompatibility) that was inadvertently introduced into the system.
- It leads to unintended system effects that range from an intermittent nuisance to complete system loss or loss of life.

Regardless of whether the SCA is performed using manual, semi-automated, or automated methods, a prerequisite is the collection, processing, and evaluation of detailed system design information. The SCA results may be used to support the activities of a variety of Systems Engineering functions, but its most important use is to aid in the improvement of design reliability prior to product manufacture and test. For this standard, there are four types of sneak conditions:

- sneak paths - Unexpected paths along which current, energy, or logical sequence flows in an unintended direction;
- sneak timing - Events occurring in an unexpected or conflicting sequence;
- sneak indications - Ambiguous or false displays of system operating conditions that may cause the system or operator to take an undesired action¹;
- sneak labels - Incorrect or imprecise labeling of system functions (e.g., system inputs, controls, displays, and buses) that may cause an operator to apply an incorrect stimulus to the system.

The SCA process assures that the likelihood of unwanted functions or inhibition of desired functions is minimized for all designed-for operating modes. In this context, an unwanted function is a system response that violates a design requirement, and designed-for operating modes include all known states of system success.

The analysis of sneak conditions can be considered static in nature because it does not involve stepping through all the possible combinations of inputs and system states. Instead, the analysis applies a rule

¹ An example of a potential sneak indication is when two identical failure indications (i.e., fault signatures) can be generated by different system functions.

base (i.e., sneak clues) to topological or functional models of the system to uncover potential sneak conditions. The models contain all possible connectivity paths; e.g., electrical current flow and data/signal flow. Because of its static nature, SCA is a good complement for simulation and testing, which are more dynamic in nature, but may be prone to overlook latent problems that occur only during unexpected operating modes.

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. This standard provides criteria for rating the capability of an acquisition project's SCA practices and assigning the practice to one of five predetermined levels of performance capability. The capability criteria provide the logical sequence of activities for improving the effectiveness of an existing SCA practice by advancing in stages. Organizations may evaluate their existing SCA practices against these minimum acceptable criteria to identify the features that need to be added to improve their existing SCA practices.

This standard also applies to the integration of the SCA database with a project R&M database system. However, specification of this standard shall not be construed as a requirement for the contractor to use a particular computer-aided design (CAD) system. Rather, contractors may use the computerized tools of their choosing, given that those tools are validated to process input data and generate output data in formats that are compatible with the data definitions in this standard.

2 Applicable Documents

2.1 Normative References

The following reference documents of the issue in effect on the date of invitation for bid or request for proposal, form a part of this standard to the extent specified:

- | | |
|-----------------------------|---|
| 1) AIAA S-102 (Draft) | Performance-Based R&M Program General Requirements |
| AIAA S-102.1 | Performance-Based R&M Management |
| 2) AIAA S-102.1.1 (Draft) | R&M Program Planning Requirements |
| 3) AIAA S-102.1.6 (Draft) | R&M Risk Management Requirements |
| 4) AIAA S-102.1.7 (Draft) | Project R&M Database System Requirements |
| AIAA S-102.2 | Performance-Based R&M Engineering and Analysis |
| 5) AIAA S-102.2.1 (Draft) | Functional Dependency and Architectural Modeling Requirements |
| 6) AIAA S-102.2.2 | System Reliability Modeling Requirements |
| 7) AIAA S-102.2.3 (Draft) | Component Reliability Predictions Requirements |
| 8) AIAA S-102.2.4 | Failure Mode, Effects and Criticality Analysis Requirements |
| 9) AIAA S-102.2.6 (Draft) | Design Concern and Drawing Error Analysis Requirements |
| 10) AIAA S-102.2.7 (Draft) | Parts Stress Derating Analysis Requirements |
| 11) AIAA S-102.2.8 (Draft) | Worst Case Analysis Requirements |
| 12) AIAA S-102.2.9 (Draft) | Human Error Predictions Requirements |
| 13) AIAA S-102.2.11 | Anomaly Detection and Response Analysis Requirements |
| 14) AIAA S-102.2.12 (Draft) | Maintainability Predictions Requirements |

- 15) AIAA S-102.2.13 (Draft) Operational Dependability and Availability Modeling Requirements
- 16) AIAA S-102.2.14 (Draft) Hazard Analysis Requirements
- 17) AIAA S-102.2.15 (Draft) Software Reliability Predictions Requirements
- 18) AIAA S-102.2.16 (Draft) Process Failure Mode, Effects and Criticality Analysis Requirements
- 19) AIAA S-102.2.20 (Draft) R&M Similarity and Allocations Analysis Requirements
- 20) AIAA S-102.2.21 (Draft) Parts Engineering and Analysis Requirements
- 21) AIAA S-102.2.22 (Draft) Stress and Damage Simulation Analysis Requirements

AIAA S-102 Performance-Based R&M Testing

- 22) AIAA S-102.3.2 (Draft) Reliability Development Growth Testing Requirements
- 23) AIAA S-102.3.5 (Draft) Design of Experiments Requirements

AIAA S-102 Performance-Based R&M Guidance

- 24) AIAA S-102-Annex B.5 (Draft) Sneak Circuit Analysis Guide
- 25) AIAA S-102-Annex B.6 (Draft) Design Concern and Drawing Error Analysis Guide

2.2 Relationship To Other S-102 Standards

This standard is one of 35 standards in the AIAA S-102 standards document tree. The S-102 standards define rated sets of activities that aid the identification, assessment,² and management of R&M risks for high unit-value systems. For S-102 standards, the performance-based R&M program is defined as the set of activities that address product R&M risk factors at one or more predetermined capability levels.

In the schema for the S-102 performance-based R&M program (See AIAA S-102.1.1 (Draft)), the SCA process supports several R&M practices. Accordingly, this standard identifies the SCA data products that are inputs for performance-based R&M practices defined by the following S-102 standards:

AIAA S-102.1.7 (Draft)	AIAA S-102.2.7 (Draft)	AIAA S-102.2.13 (Draft)
AIAA S-102.2.1 (Draft)	AIAA S-102.2.8 (Draft)	AIAA S-102.2.14 (Draft)
AIAA S-102.2.2	AIAA S-102.2.9 (Draft)	AIAA S-102.2.16 (Draft)
AIAA S-102.2.4	AIAA S-102.2.11	AIAA S-102.2.20 (Draft)
AIAA S-102.2.6 (Draft)	AIAA S-102.2.12 (Draft)	AIAA S-102.2.21 (Draft)

Also, this standard identifies the SCA inputs that are data products of performance-based R&M practices defined by the following S-102 standards:

AIAA S-102.1.6 (Draft)	AIAA S-102.2.22 (Draft)
AIAA S-102.2.3 (Draft)	AIAA S-102.3.2 (Draft)
AIAA S-102.2.15 (Draft)	AIAA S-102.3.5 (Draft)

² Assessment as used here includes qualification and quantification and also numerical evaluation and ranking of R&M risks.

3 Vocabulary

3.1 Acronyms and Abbreviated Terms

CA	Criticality Analysis
CN	Criticality Number
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
HW	Hardware
LLAA	Lessons Learned Approval Authority
QA	Quality Assurance
R&M	Reliability and Maintainability
SCA	Sneak Circuit Analysis
SPFM	Single Point Failure Mode
SW	Software

3.2 Terms and Definitions

acquisition activity

activity (government, contractor, or subcontractor) that levies SCA requirements on another activity through a contract or other document

ambiguity group

set of components that, if considered potentially faulty, does not give a unique solution in fault location

baseline practice

minimum set of activities that constitute an AIAA S-102 Capability Level 1 R&M practice

capability level

measure of the ability of an R&M practice, as specified by a set of activities, to address the pertinent R&M needs of a high unit-value systems engineering process

capability level growth

improvement in the ability of a task to support the systems engineering objectives due to an increase in resources, engineering data processed, or number of other tasks supported

credible failure mode

failure mode with a probability of occurrence greater than $1.0E-6$, 0.000001, or one in a million

data reduction / pathfinding

process of reducing a large, complex system composed of numerous hardware elements and interfaces into a series of simplified, functionally equivalent representations.

design concern

a poor design practice, design weakness, or misapplication of an electronic component that may cause reduced reliability or degraded operation

digital sneak condition

an unwanted operating mode, timing race, logical error, or similar deficiency in digital hardware

NOTE: Depending on system complexity, the identification of digital sneak conditions may involve the use of sneak path analysis techniques, manual or graphical analysis, computerized logic simulators, or computer aided design (CAD) circuit analysis.

failure

termination of the ability of a unit to perform its required function

NOTE: A fault may cause a failure.

failure mode

consequence of the mechanism through which a failure occurs, or the manner by which a failure is observed

fault³

(1) [Software Reliability] a manifestation of an error in software; (2) [Hardware Reliability] any undesired state of a component or system; (3) [Components] a defect or flaw in a hardware or software component,

NOTE: (1) An accident may cause a fault.

NOTE (2) A fault may cause a failure.

NOTE (3) A fault does not necessarily require failure.

maturity level

measure of the degree of accuracy of a data product, as developed using a specified set of input data, in relation to what is considered the best achievable results

mission assurance

project-wide identification, evaluation, and mitigation or control of all existing and potential deficiencies that pose a threat to mission success, throughout the product life cycle

NOTE Deficiencies include damage-threatening hazards, mission-impacting failures, and system performance anomalies that result from unverified requirements, optimistic assumptions, unplanned activities, ambiguous procedures, undesired environmental conditions, latent physical faults, inappropriate corrective actions, and operator errors.

network forest

a higher-order network diagram depicting the interrelationships among the numerous network trees

network tree

a functional, topologically oriented circuit segment that is analyzed for the existence of sneak circuits and conditions.

NOTE Numerous network trees are generated to describe the system under analysis.

partitioning

subdivision of functions at the circuit or device level into separate, cross-referenced functions, to aid in the data reduction / pathfinding process, as well as to facilitate the generation of topological network trees

performance-based R&M program

a set of activities that address product R&M risk factors at one or more predetermined capability levels

process-based lesson learned

important information created, documented, and retrieved according to a process or procedure descriptor

³ Definition source: IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms*.

product-based lesson learned

important information created, documented, and retrieved according to a system or device life-cycle-specific functional or physical descriptor

prognostics

identifying conditions or clues that indicate imminent failure prior to its occurrence

SCA dataset

set of data that describes a specific sneak condition, its effects, severity classification, and compensation method

sneak clue

a specific question that is applied to a particular topograph to uncover the existence of a sneak circuit or condition

NOTE: Table 1 provides the list of sneak clues appropriate to each topograph.

sneak condition

any one of four types of system conditions that may cause unwanted functions to occur or inhibit desired functions

sneak indication

ambiguous or false displays of system operating conditions that may cause the system or operator to take an undesired action

sneak label

incorrect or imprecise labeling of system functions

EXAMPLE System inputs, controls, displays, and buses may cause an operator to apply an incorrect stimulus to the system.

sneak path

an unexpected path along which current, energy, or logical sequence flows in an unintended direction

NOTE Sneak paths are also called sneak circuits, and are found in hardware systems, primarily power distribution, control, switching networks, and analog circuits. The technique is based on known topological similarities of sneak circuits in these types of hardware systems.

sneak timing

events occurring in an unexpected or conflicting sequence

software sneak path

a computer software logical flow that possesses topologies similar to those with known sneak path conditions in them

tailoring

process by which the individual requirements of a standard are evaluated to determine the extent to which each requirement is most suited for a specific system acquisition and the modification of these requirements, where necessary, to ensure that each tailored document invokes only the minimum needs of the customer

EXAMPLE Tasks, sections, paragraphs, words, phrases, or sentences are elements that may be subject to this process.

timely

performance of a task, subtask, or effort when planning and execution results in the output being provided with sufficient time for management, if need be, to identify and implement cost-effective action

EXAMPLE action that avoids or minimizes schedule delays and cost increases for achieving, preserving, or verifying system R&M requirements

topograph

a graphical, structured representation corresponding to a basic circuit function that is used as a building block in network tree construction

NOTE Sneak clues are applied to each topograph to uncover sneak circuits and conditions. Figure 2 provides the five basic sneak circuit analysis topographs.

validation

the act of determining that a product or process, as constituted, will fulfill its desired purpose

verification

the process of assuring that a product or process, as constituted, complies with the requirements specified for it

4 General Requirements

4.1 Contractor Responsibility

The contractor and his subcontractors shall provide the necessary training and tools to allow the SCA process to be cost-effectively planned and implemented as needed in a project. The SCA shall evaluate all possible functional paths for all system modes within the defined scope of the SCA, and the method of detection for all undesired sneak conditions. Verifiable failure compensation methods⁴ shall be identified for each sneak condition that poses unacceptable risk or rationale provided for taking no action. The timing of the analysis shall allow needed reliability improvements to be identified and implemented in a timely manner. The SCA data and results shall be accessible to all major stakeholders. If the contractor intends to use an already existing model, procedure, or computerized methodology to perform the SCA, then a description of how those resources will be employed to meet the requirements shall be provided for acquisition activity review and approval. If a Capability Level 3 SCA process is required, the SCA process shall support the efforts of the Lessons Learned Approval Authority (e.g., Lessons Learned Committee), which is chartered to document lessons learned associated with designed-in sneak conditions and shall assist in infusing the lessons learned recommendations throughout the project. If a Capability Level 4 or above SCA process is required, the SCA data products shall be prefaced with one or more of the keyword data element descriptions (DED) listed in Annex C.

4.2 Planning

The contractor's SCA process plan shall be developed, documented, and flowed down, as appropriate, as an integral part of the R&M program plan. The contractor shall document the approved methods for implementing the SCA process and reference the applicable document number(s) in the plan. The SCA plan shall establish a project policy that delineates the contractor's commitment to the application of SCA as needed to meet the R&M requirements of the contract. The SCA plan shall define:

- a) responsibilities for the SCA planning and performance throughout design, test, inspection, and operations;
- b) the SCA requirements as needed to support the project, including milestones for developing fault trees, or modifying existing fault trees;
- c) scope and ground rules of the SCA;

⁴ Failure compensation methods may include special design features, analyses, inspections, tests, controls, instructions, or operational corrective actions, such as replacement, reconfiguration, repair, or preventive maintenance.