



AEROSPACE RECOMMENDED PRACTICE

ARP6539™

Issued 2017-11
Reaffirmed 2022-08

Validation and Verification Process Steps for Monitors Development in Complex Flight Control and Related Systems

RATIONALE

There is a need for a document that provides a process for the development and approval of monitoring algorithms for highly integrated and complex aircraft flight control and related systems. This document satisfies this need.

ARP6539 has been reaffirmed to comply with the SAE Five-Year Review policy.

FORWARD

A monitor is a mechanism in place to detect failures at the component or system level. The monitor functionality includes input signal sampling, a detection scheme and a corrective action. Poorly designed monitors can result in an inability of the monitor to detect or react to the failure condition in a time frame appropriate to the failure threat, or in nuisance trips affecting system availability.

The inability to detect a failure in a timely fashion can have a negative impact on:

- Aircraft safety
- The pilots' ability to cope with a developing problem
- Aircraft safety margins

Nuisance trips can have a negative impact on:

- Baseline safety due to reductions in redundancy following system re-configuration, or reduced system availability
- Degradation of the importance attached to warnings due to complacency resulting from frequency of occurrence
- Development program cost and schedule increases if the issues are only discovered at the aircraft integration rigs, or during flight test
- Dispatch interruption rate increases and unplanned diversions for fleets if the problems emerge, or persist into revenue service of the aircraft
- Increase in no fault found rates following unscheduled maintenance removals

SAE Executive Standards Committee 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 revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2022 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE ARP6539

For more information on this standard, visit
<https://www.sae.org/standards/content/ARP6539/>

Documents
Document Sharing Hub

This recommended practice provides program level guidance to validate and verify the need for, and robustness of monitoring functions for highly integrated aircraft systems.

As a general note, the Supplier described in this document is a system, sub-system, or equipment supplier. In some cases though, the monitor(s), or monitoring scheme, may be developed by the OEM, or consist of some combination of OEM and Supplier derived monitors. The process steps for this type of development work are the same and are aimed at the level at which the monitor requirements are specified. The OEM monitors development team can be assigned the role of the Supplier in the context of this process.

TABLE OF CONTENTS

1.	SCOPE.....	2
1.1	Field of Application.....	2
2.	APPLICABLE DOCUMENTS.....	3
2.1	Definitions.....	3
2.2	Abbreviations.....	4
3.	MONITORS DESIGN PROCESS STEPS.....	5
3.1	Monitors Development Plan.....	5
3.1.1	Critical Monitors.....	6
3.2	Validation, Definition and Review of Monitors.....	6
3.2.1	Completeness Check.....	7
3.2.2	Correctness Check.....	7
3.2.3	Peer Communities.....	7
3.2.4	Monitor Performance.....	8
3.3	Verification of Monitors.....	9
3.3.1	Safety of Flight.....	10
3.3.2	Type Certification and Entry into Service.....	11
3.3.3	Post Entry into Service.....	11
3.4	Monitors V&V Design Data.....	11
4.	NOTES.....	12
4.1	Revision Indicator.....	12
Figure 1	Monitors development V&V cycle.....	5
Figure 2	Example of a monitor performance analysis.....	9
Figure 3	V&V deliverables mapping.....	12

1. SCOPE

This SAE Aerospace Recommended Practice (ARP) provides a process for the verification and validation of monitors used in highly-integrated and complex aircraft flight control and related systems.

1.1 Field of Application

Although this ARP is primarily intended to be used for complex flight control and related systems, it can be also used for utility control systems. This document refers to commercial aircraft design and approval practices; however, it can also be used for military aircraft applications.

2. APPLICABLE DOCUMENTS

There are no applicable documents.

2.1 Definitions

ANALYSIS: An evaluation based on decomposition into simple elements.

ASSESSMENT: An evaluation based upon engineering judgment.

ASSUMPTIONS: Statements, principles, and/or premises offered without proof.

AVAILABILITY: Qualitative or quantitative attribute that a system or item is in a functioning state at a given point in time. It is sometimes expressed in terms of the probability of the system or item not providing its output(s).

COMMON CAUSE ANALYSIS: Generic term encompassing zonal safety analysis, particular risk analysis, and common mode analysis.

COMMON MODE ANALYSIS: An analysis performed to verify that failure events identified in the ASA/SSA are independent in the actual implementation.

DERIVED REQUIREMENTS: Additional requirements resulting from design or implementation decisions during the development process which are not directly traceable to higher-level requirements.

ERROR: An omitted or incorrect action by a crewmember or maintenance person, or a mistake in requirements, design, or implementation.

FAILURE: An occurrence which affects the operation of a component, part or element such that it can no longer function as intended. This includes both loss of function and malfunction. Note: errors may cause failures, but are not considered to be failures.

FAILURE CONDITION: A condition having an effect on the aircraft and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions or external events.

FAILURE EFFECT: A description of the operation of a system or item as the result of a failure; i.e., the consequence(s) a failure mode has on the operation, function or status of a system or an item.

FAULT: A manifestation of an error in an item or system that may lead to a failure.

FUNCTIONAL HAZARD ASSESSMENT: A systematic, comprehensive examination of functions to identify and classify Failure Conditions of those functions according to their severity.

HAZARD: A condition resulting from failures, external events, errors, or combinations thereof where safety is affected.

ITEM: A hardware or software element having bounded and well-defined interfaces.

MONITOR: A monitor is a mechanism in place to detect failures at the component or system level.

ORIGINAL EQUIPMENT MANUFACTURER: Airframe manufacturer, typically responsible for structural and systems requirements specification and aircraft level integration.

PRELIMINARY SYSTEM SAFETY ASSESSMENT: A systematic evaluation of a proposed system architecture and its implementation, based on the Functional Hazard Assessment and Failure Condition classification, to determine safety requirements for systems and items.

SYSTEM: A combination of inter-related items arranged to perform a specific function(s).

SYSTEM SAFETY ASSESSMENT: A systematic, comprehensive evaluation of the implemented system to show that the relevant safety requirements are met.

TRACEABILITY: The recorded relationship established between two or more elements of the development process. For example, between a requirement and its source or between a verification method and its requirement.

VALIDATION: The determination that the requirements for a product are correct and complete. i.e. Are we building the right aircraft/ system/ function/ item?

VERIFICATION: The evaluation of an implementation of requirements to determine that they have been met. i.e. Did we build the aircraft/ system/ function/ item right?

2.2 Abbreviations

AFHA	Aircraft Functional Hazard Assessment
ARP	Aerospace Recommended Practice
ASA	Aircraft Safety Assessment
CAS	Crew Alerting Systems
CCA	Common Cause Analysis
CDR	Critical Design Review
CMA	Common Mode Analysis
DCS	Designated Certification Specialist (EASA)
DER	Designated Engineering Representative (FAA)
EASA	European Aviation Safety Agency
EIS	Entry into Service
FAA	Federal Aviation Administration
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effect Analysis
OEM	Original Equipment Manufacturer
PASA	Preliminary Aircraft Safety Assessment
PDR	Preliminary Design Review
PSSA	Preliminary System Safety Assessment
SFHA	Systems Functional Hazard Assessment
SoF	Safety of Flight
SSA	System Safety Assessment
V&V	Validation and Verification