

(R) Guidelines for Development of Civil Aircraft and Systems

RATIONALE

This document provides updated and expanded guidelines for the processes used to develop civil aircraft and systems.

TABLE OF CONTENTS

1.	SCOPE.....	5
1.1	Purpose.....	6
1.2	Document Background:	7
2.	REFERENCES.....	8
2.1	Applicable Documents	8
2.1.1	SAE Publications.....	8
2.1.2	FAA Publications.....	8
2.1.3	EASA Publications	9
2.1.4	RTCA Publications.....	9
2.1.5	EUROCAE Publications.....	9
2.2	Definitions	10
2.3	Abbreviations and Acronyms	14
3.	DEVELOPMENT PLANNING	16
3.1	Planning Process	16
3.2	Transition Criteria.....	17
3.2.1	Deviations from Plans	19
4.	AIRCRAFT AND SYSTEM DEVELOPMENT PROCESS.....	19
4.1	Conceptual Aircraft/System Development Process.....	20
4.1.1	Development Assurance.....	22
4.1.2	Introduction to Development Assurance Process.....	22
4.1.3	Introduction to Hierarchical Safety Requirements Generated from Safety Analyses.....	23
4.1.4	Identification of Aircraft-Level Functions, Function Requirements and Function Interfaces	25
4.1.5	Allocation of Aircraft Functions to Systems	25
4.1.6	Development of System Architecture	25
4.1.7	Allocation of System Requirements to Items	25
4.1.8	System Implementation	25
4.2	Aircraft Function Development.....	25
4.3	Allocation of Aircraft Functions to Systems	28
4.4	Development of System Architecture:	28
4.5	Allocation of System Requirements to Items	28
4.6	System Implementation	29
4.6.1	Information Flow - System Process To & From Item Process(es)	29
4.6.2	Hardware and Software Design/Build.....	30

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 © 2010 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
SAE WEB ADDRESS: http://www.sae.org

SAE values your input. To provide feedback on this Technical Report, please visit
<http://www.sae.org/technical/standards/ARP4754A>

4.6.3	Electronic Hardware/Software Integration	31
4.6.4	Aircraft/System Integration.....	31
5.	INTEGRAL PROCESSES.....	31
5.1	Safety Assessment	31
5.1.1	Functional Hazard Assessments	34
5.1.2	Preliminary Aircraft / System Safety Assessment.....	34
5.1.3	Aircraft / System Safety Assessment.....	34
5.1.4	Common Cause Analysis.....	35
5.1.5	Safety Program Plan	36
5.1.6	Safety-Related Flight Operations or Maintenance Tasks	37
5.1.7	Relationship with In-Service Safety	37
5.2	Development Assurance Level Assignment	37
5.2.1	General Principles – Introduction to Development Assurance Level Assignment	38
5.2.2	FDAL and IDAL	39
5.2.3	Detailed FDAL and IDAL Assignment Guidelines	39
5.2.4	FDAL Assignment Taking Credit for External Events	50
5.3	Requirements Capture	51
5.3.1	Types of Requirements	52
5.3.2	Deriving Safety-related Requirements from the Safety Analyses.....	54
5.3.3	Capturing Maintenance Requirements for In-service Use.....	54
5.4	Requirements Validation	54
5.4.1	Process Objectives	55
5.4.2	Validation Process Model	56
5.4.3	Correctness Checks.....	59
5.4.4	Completeness Checks	60
5.4.5	Validation Rigor.....	62
5.4.6	Validation Methods.....	62
5.4.7	Validation Data.....	64
5.5	Implementation Verification.....	65
5.5.1	Verification Process Objectives	65
5.5.2	Verification Process Model	66
5.5.3	Verification Rigor.....	67
5.5.4	Verification Planning	67
5.5.5	Verification Methods	68
5.5.6	Verification Data.....	70
5.6	Configuration Management.....	72
5.6.1	Configuration Management Process Objectives	72
5.6.2	Configuration Management Process Activities:	73
5.7	Process Assurance	75
5.7.1	Process Objectives	75
5.7.2	Process Assurance Plan.....	76
5.7.3	Project Plan Reviews	76
5.7.4	Evidence of Process Assurance	76
5.8	Certification and Regulatory Authority Coordination.....	76
5.8.1	Certification Planning	77
5.8.2	Agreement on the Proposed Means of Compliance.....	77
5.8.3	Compliance Substantiation	77
5.8.4	Certification Data.....	77
6.	MODIFICATIONS TO AIRCRAFT OR SYSTEMS.....	80
6.1	Modification Process Overview.....	80
6.2	Modification Management Process.....	81
6.3	Modification Impact Analysis.....	81
6.4	Modification Categorization and Administration.....	82
6.5	Evidence for Acceptability of a Modification:	82
6.5.1	Use of Service History	83
6.6	Considerations for Modifications.....	83
6.6.1	Introducing a New Aircraft-Level Function.....	83

6.6.2	Replacing Item or System With Another on an Existing Aircraft.....	84
6.6.3	Adapting Existing Item or System to a Different Aircraft Type.....	85
6.6.4	Modification to Item or System Without Adding a Function:.....	86
6.6.5	STC Production Introduction.....	87
7	NOTES.....	87
APPENDIX A	PROCESS OBJECTIVES DATA	88
APPENDIX B	SAFETY PROGRAM PLAN	97
APPENDIX C	FDAL/IDAL ASSIGNMENT PROCESS EXAMPLE	110
APPENDIX D	DELETED.....	115
FIGURE 1	GUIDELINE DOCUMENTS COVERING DEVELOPMENT AND IN-SERVICE/OPERATIONAL PHASES	6
FIGURE 2	PLANNING PROCESS	18
FIGURE 3	DEVELOPMENT LIFE CYCLE	20
FIGURE 4	AIRCRAFT OR SYSTEM DEVELOPMENT PROCESS MODEL.....	21
FIGURE 5	INTERACTION BETWEEN SAFETY AND DEVELOPMENT PROCESSES	24
FIGURE 6	AIRCRAFT FUNCTION IMPLEMENTATION PROCESS	27
FIGURE 7	SAFETY ASSESSMENT PROCESS MODEL	33
FIGURE 8	FDAL/IDAL ASSIGNMENT PROCESS	39
FIGURE 9	FUNCTION INDEPENDENCE AND ITEM DEVELOPMENT INDEPENDENCE	45
FIGURE 10	DEVELOPMENT DEPENDENCY OF MULTIPLE FUNCTIONS IN THE SAME FC.....	48
FIGURE 11	PROTECTION FUNCTION FDAL ASSIGNMENT AS A FUNCTION OF PROBABILITY OF AN EXTERNAL EVENT	51
FIGURE 12	VALIDATION PROCESS MODEL	56
FIGURE 13	VERIFICATION PROCESS MODEL	67
FIGURE 14	CONFIGURATION MANAGEMENT PROCESS MODEL	73
TABLE 1	DEVELOPMENT PLANNING ELEMENTS.....	19
TABLE 2	TOP-LEVEL FUNCTION FDAL ASSIGNMENT	40
TABLE 3	DEVELOPMENT ASSURANCE LEVEL ASSIGNMENT TO MEMBERS OF A FUNCTIONAL FAILURE SET	44
TABLE 4	EXAMPLE ASSURANCE ASSIGNMENT FOR DESIGN DEPENDENCY OF MULTIPLE FUNCTIONS SAME FC	46
TABLE 5	EXAMPLE ASSURANCE ASSIGNMENT FOR DESIGN DEPENDENCY OF MULTIPLE FUNCTIONS SAME FC	49
TABLE 6	REQUIREMENTS VALIDATION METHODS AND DATA	64
TABLE 7	VERIFICATION METHODS AND DATA	70
TABLE 8	CM ACTIVITIES TO CONTROL CATEGORY MAPPING	75
TABLE 9	CERTIFICATION DATA CROSS REFERENCE.....	78