



AEROSPACE INFORMATION REPORT

AIR5273™**REV. A**

Issued 2001-12
Reaffirmed 2007-01
Revised 2022-12

Superseding AIR5273

Aircraft Flight Control Actuation System Failure-Detection Methods

RATIONALE

This SAE Aerospace Information Report (AIR) is revised following a set of evolving requirements over the last 20 years since it has been originally published.

FOREWORD

This SAE Aerospace Information Report (AIR) is a sister document to AIR4094 and AIR4253. It provides only the failure detection method detail to accompany the more complete architecture and hardware descriptions contained in the referenced AIRs.

TABLE OF CONTENTS

1.	SCOPE.....	5
1.1	Purpose.....	5
1.2	Field of Application.....	5
2.	REFERENCES.....	5
2.1	Applicable Documents.....	5
2.1.1	SAE Publications.....	5
2.1.2	U.S. Government Publications.....	5
2.1.3	FAA Publications.....	5
2.1.4	EASA Publications.....	6
2.1.5	RTCA Publications.....	6
2.1.6	Books.....	6
2.2	Related Publications.....	6
2.2.1	SAE Publications.....	6
2.3	Acronyms and Abbreviations.....	6
3.	BACKGROUND.....	8
3.1	Evolution.....	8
3.2	Avoiding the "Nuisance-Disconnect".....	8
3.3	Architecture and Application.....	9
3.3.1	Cross-Channel versus In-Line Monitoring.....	9
3.4	Designing "By the Numbers".....	9
3.4.1	Probability of Failure.....	9
3.4.2	Fault Coverage.....	10
3.4.3	Commercial Aircraft Failure Criticality and Probability.....	10
3.4.4	Military Aircraft Failure Criticality and Probability.....	13

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 AIR5273A

For more information on this standard, visit
<https://www.sae.org/standards/content/AIR5273A/>

Documents

Document Sharing Hub

3.5	System Separation	13
3.6	Fighting Between Redundant Commands to a Surface	14
3.7	Electronic Rigging	14
3.7.1	Electronic Rigging Purpose	14
3.7.2	Rigging Definitions	15
3.7.3	Rigging and Failure Detection	15
3.8	Real-Time Monitoring, Continuous Built-in-Test, and Initiated Built-in-Test	15
4.	MONITORING TECHNIQUES	16
4.1	Failure Locations	16
4.2	Failure Types	16
4.2.1	Passive Failures	16
4.2.2	Active Failures	17
4.2.3	Latent Failures	17
4.2.4	Oscillatory Failures	17
4.3	Failure Detection Approach	17
4.4	EHV Failure Detection	18
4.4.1	Passive Failures and the Use of Bias	19
4.4.2	Where to Detect Failure	19
4.5	Direct Drive Valve Failure Detection	20
4.6	Linear and Rotary Variable Transformer Failure Detection	21
4.7	Logic Valve Failure Detection	22
4.8	Solenoid Valve Failure Detection	22
4.9	Outer Loop Modeling	23
5.	SERVOACTUATOR FAILURE DETECTION DESCRIPTIONS	23
5.1	General Dynamics F-111	23
5.1.1	Series Augmentation Servoactuator Configuration	23
5.1.2	Actuation Architecture	24
5.1.3	Failure Detection	24
5.2	Panavia Tornado	24
5.2.1	Taileron Servoactuator Configuration	24
5.2.2	Actuation Architecture	25
5.2.3	Failure Detection	25
5.3	Space Shuttle Orbiter	26
5.3.1	Actuator Configuration	26
5.3.2	Actuation Architecture	26
5.3.3	Failure Detection	26
5.4	General Dynamics F-16	27
5.4.1	Actuator Configuration	27
5.4.2	Actuation Architecture	27
5.4.3	Failure Detection	28
5.5	McDonnell Douglas F/A -18 C/D	28
5.5.1	Actuator Configuration	28
5.5.2	Actuation Architecture	28
5.5.3	Failure Detection	29
5.6	IAI LAVI	30
5.6.1	Actuator Configuration	30
5.6.2	Actuation Architecture	30
5.6.3	Failure Detection	31
5.7	Grumman X-29A	31
5.7.1	Actuator Configuration	31
5.7.2	Actuation Architecture	31
5.7.3	Failure Detection	32
5.8	Bell Boeing V-22	32
5.8.1	Actuator Configuration	32
5.8.2	Actuation Architecture	32
5.8.3	Failure Detection	33
5.9	Airbus A319/A320/A321 - Airbus A330/A340	33

5.9.1	Actuator Configuration	33
5.9.2	Actuation Architecture	34
5.9.3	Failure Detection	34
5.10	Boeing C-17	35
5.10.1	Actuator Configuration	35
5.10.2	Actuation Architecture	35
5.10.3	Failure Detection	36
5.11	Boeing 777	36
5.11.1	Actuator Configuration	36
5.11.2	Actuation Architecture	36
5.11.3	Failure Detection	37
5.12	Saab 2000	37
5.12.1	Actuator Configuration	37
5.12.2	Actuation Architecture	38
5.12.3	Failure Detection	39
5.13	IPTN N-250	39
5.13.1	Actuator Configuration	39
5.13.2	Actuation Architecture	39
5.13.3	Failure Detection	39
5.14	Boeing-Sikorsky RAH-66	41
5.14.1	Servoactuator Configuration	41
5.14.2	Actuation Architecture	41
5.14.3	Failure Detection	41
5.15	Light Combat Aircraft (LCA)	42
5.15.1	Actuator Configuration	42
5.15.2	Actuation Architecture	42
5.15.3	Failure Detection	42
6.	NOTES	44
6.1	Revision Indicator	44
Figure 1	The FBW servoactuator and its interactions	8
Figure 2	The FBW primary flight control actuator	16
Figure 3	The EHV	18
Figure 4	Biased servovalve operation	19
Figure 5	Typical DDV	20
Figure 6	DDV jam detection logic	21
Figure 7	LVDT failure detection	21
Figure 8	Logic valve failure detection	22
Figure 9	Outer loop modeling	23
Figure 10	General Dynamics F-111 EHV failure detection	24
Figure 11	Panavia Tornado Taileron actuator FBW control architecture	25
Figure 12	Space Shuttle EHV failure detection	27
Figure 13	General Dynamics F-16 EHV failure detection	28
Figure 14	McDonnell Douglas F/A-18 C/D servovalve failure detection	30
Figure 15	IAI LAVI servovalve failure detection	31
Figure 16	Grumman X-29 EHV failure detection mechanism	32
Figure 17	Bell Boeing V-22 EHV failure detection by modeling second stage position	33
Figure 18	Boeing C-17 integrated flight control module schematic	35
Figure 19	Boeing 777 servoactuator schematic	36
Figure 20	Saab 2000 control architecture	38
Figure 21	IPTN N-250 servovalve failure detection	40
Figure 22	IPTN N-250 runaway monitor	40
Figure 23	IPTN N-250 actuator jam monitor	40
Figure 24	LCA cross-channel monitoring algorithm	42
Figure 25	LCA Servoamplifier Inline Monitor	43
Figure 26	LCA stuck valve monitor	43
Figure 27	LCA main control valve inline monitor	44
Figure 28	LCA LES inline rate monitor	44

Table 1	FAA and EASA failure criticality and probability definitions.....	12
Table 2	Military usage severity category.....	13
Table 3	Military usage probability levels	13
Table 4	Servoactuator failures covered by real-time monitoring or BIT.....	18
Table 5	Servoactuator failures typically covered by inspection or prevented by design	18

1. SCOPE

This SAE Aerospace Information Report (AIR) provides descriptions of aircraft flight control actuation system failure-detection methods. The fault-detection methods are those used for ground and in-flight detection of failures in electrohydraulic actuation systems for primary flight controls.

1.1 Purpose

This AIR has been produced to aid the designers of the systems of the future by showing what has succeeded in the past.

1.2 Field of Application

This AIR generally concentrates on full fly-by-wire flight control actuation systems, but it includes one augmented-control system. The actuation system comprises the actuator, control valves, sensors, and related failure detection and monitoring elements.

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 International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

AIR4094 Aircraft Flight Control Systems Descriptions

AIR4253 Description of Actuation Systems for Aircraft with Fly-by-Wire Flight Control Systems

AS94900 Vehicle Managemetn Systems - Flight Control Function, Design, Installation, and Test of Piloted Military Aircraft, General Specification for

Harschburger, H., "Development of Redundant Flight Control Actuation Systems for the F/A-18 Strike Fighter," SAE Technical Paper 831484, 1983, <https://doi.org/10.4271/831484>.

2.1.2 U.S. Government Publications

Copies of these documents are available online at <https://quicksearch.dla.mil/>.

MIL-STD-882 System Safety Program Requirements.

2.1.3 FAA Publications

Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591, Tel: 866-835-5322, www.faa.gov.

AC 25.1309-1A FAA Advisory Circular, System Design Analysis (1988, June)

2.1.4 EASA Publications

Available from European Union Aviation Safety Agency, Konrad-Adenauer-Ufer 3, D-50668 Cologne, Germany, Tel: +49 221 8999 000, www.easa.europa.eu.

AMC 25.1309 System Design Analysis (2021, December)

CS-25, App. K Interaction of Systems and Structure (2021, December)

NPA 25C-199 JAA Notice of Proposed Rule Making, Interaction of Systems and Structure (1996, April).

2.1.5 RTCA Publications

Available from RTCA, Inc., 1150 18th Street, NW, Suite 910, Washington, DC 20036, Tel: 202-833-9339, www.rtca.org.

RTCA DO-178 Software Considerations in Airborne Systems and Equipment Certification

2.1.6 Books

Raymond, E.T. and Chenoweth, C.C., "Aircraft Flight Control Actuation System Design" (Warrendale, PA, Society of Automotive Engineers, Inc), ISBN 978-1-5609-1376-4, 1993.

2.2 Related Publications

The following publications are provided for information purposes only and are not a required part of this SAE Technical Report.

2.2.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

R-225 Fly-by-Wire: A Historical and Design Perspective

2.3 Acronyms and Abbreviations

BIT	Built-in-Test
CBIT	Continuous Built-in-Test
CCDL	Cross Channel Data Link
CCM	Cross-Channel Monitoring
CMM	Common Mode Monitor
CRM	Command Response Monitor
CSAS	Command and Stability Augmentation System
DDV	Direct Drive Valve
DFCC	Digital Flight Control Computer
EASA	European Aviation Safety Agency
ECU	Electronic Control Unit

EHV	Electrohydraulic Servovalve
EICAS	Engine Indicating and Crew Alerting System
FAA	Federal Aviation Administration
FBW	Fly-by-Wire
FCC	Flight Control Computer
FHA	Functional Hazard Analysis
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes and Effects Criticality Analysis
FO/FS	Fail-Operate/Fail-Safe
FO ² /FS	Double-Fail-Operate/Fail-Safe
FS	Fail-Safe
IBIT	Initiated Built-in-Test
IFCM	Integrated Flight Control Module
ILM	In-Line Monitoring
JAA	Joint Aviation Authorities
LCA	Light Combat Aircraft
LES	Leading Edge Slat
LRU	Line Replaceable Unit
LVDT	Linear Variable Differential Transformer
MBIT	Maintenance Built-in-Test
MCV	Main Control Valve
MMC	Mechanical Mode Coupler
MTBF	Mean Time Between Failures
NPRM	New Proposed Rule Making
NVM	Non-Volatile Memory
PBIT	Pre-Flight Built-in-Test
PLOC	Probability of Loss of Control
PLOF	Probability of Loss of Function
RLS	Reservoir-Level-Switching

RVDT	Rotary Variable Differential Transformer
RVT	Rotary Variable Transducer (sometimes used - RVDT with only four wires)
SVM	Servo Valve Monitor
WRA	Weapon Removable Assembly

3. BACKGROUND

The background to the subject is discussed in terms of the impact that factors such as the system architecture have on the detection methods chosen for the flight control system.

This section discusses some of the aspects of the design of flight control actuation systems. It attempts to discuss their impact on failure detection design only and to avoid a more general discussion of control system design.

3.1 Evolution

Primary flight control actuation systems have evolved through three generations since the general adoption of full-time powered actuation. Analog FBW replaced the electronic augmentation of mechanical commands and has in its turn been replaced by digital FBW. Meanwhile, the servoactuators have also changed significantly. The hydromechanical complication and relatively simple electrical interfaces marked the earlier FBW actuation concepts found in the Space Shuttle and the General Dynamics F-16. The current generation, typified by the Airbus A380, and the Boeing 787, employs significantly simpler hydromechanical logic and depends much more upon electronic failure detection and the associated electronic equipment.

The reasons for this are:

- Increased confidence in integrated electronics and digital processing, because of the increased competence and reliability of the hardware, allows taking advantage of the weight and initial cost savings made possible by the use of electrical logic instead of hydromechanical logic.
- Decentralization of the associated electronics makes the cable weight penalty for a more complex electrical interface less severe, a factor of increasing importance, as actuation systems become less centralized.

3.2 Avoiding the “Nuisance-Disconnect”

The flight control and actuation systems used in FBW aircraft employ redundancy for safety and incorporate many elements (see [Figure 1](#)) that interact in a closed loop manner.

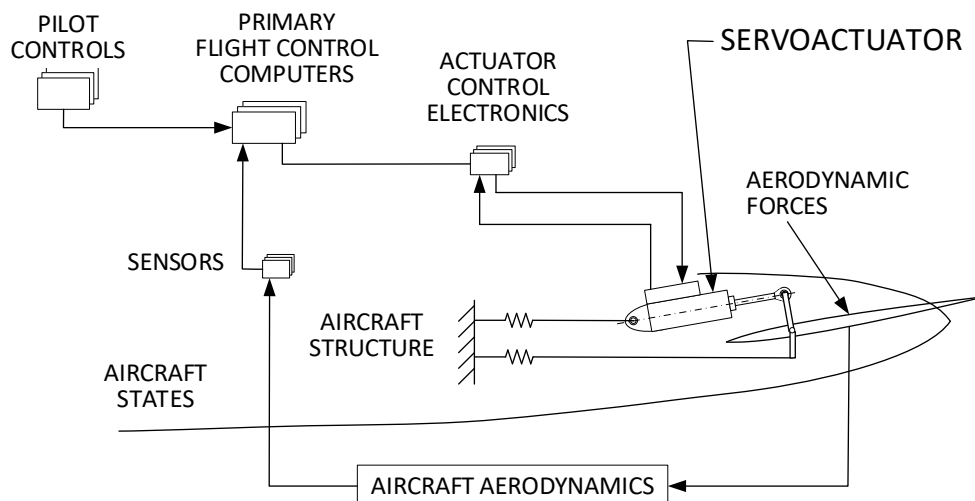


Figure 1 - The FBW servoactuator and its interactions

Because of the interactions and because the precise states of many of the elements cannot be known, it is often difficult to diagnose servomotor failures as quickly as the aircraft requires. To one degree or another, all of the satisfactory methods developed to date filter out transient events and require persistence of indication before a failure will be declared. The design of a diagnostic method always requires a balance to be drawn between satisfactory performance and an acceptable risk of the "nuisance-disconnect." This is defined as the declaration of a failure when none exists and the consequent mistaken attempt to provide protection by disconnecting correctly operating system components.

3.3 Architecture and Application

The primary flight control servomotors flying today use many different diagnostic techniques. These differences are a function of the year in which they were designed, the differing performance they must provide, and the various system architectures in which they are employed. There is no universally applicable, "best" architectural approach. The architecture chosen for each new aircraft will be determined by its mission and by the component and subsystem technology available to the design team. This available technology will change for each new generation of aircraft and this will force a re-evaluation for each new aircraft.

3.3.1 Cross-Channel versus In-Line Monitoring

The architectures proposed for the first generation of FBW aircraft were frequently differentiated by their approach to monitoring. Four-channel architectures featuring cross-channel comparison for failure detection competed with triplex architectures employing "in-line" monitoring.

Cross-channel comparison between four channels typically allows the detection and isolation of the first and second failures but not the third since a one-on-one comparison provides no basis for distinguishing the bad channel from the good. With this type of architecture, care must be taken to avoid the potential for single failures that will result in an even number of channels being compared since there is no way to distinguish the bad from the good. Two dual transducers, for example, provide no protection against disconnect of a single load path to the two probes of one paired transducer.

In-line monitoring provides "self-monitoring" of each channel and therefore can be designed to provide sustained operation with only one remaining channel. A triplex in-line monitored approach, therefore, provides the same degree of fault protection as a quadruplex cross-compared architecture, though each channel of the triplex architecture contains appreciably more hardware than each channel of the quadruplex architecture. In-line monitoring allows a greater degree of system separation, a desirable feature for flight critical applications, and of great assistance to the certification of commercial aircraft. Present-day FBW architectures almost invariably use combinations of in-line and cross-channel monitoring, protected for system safety, as described in the system separation discussion (see [3.5](#)).

3.4 Designing "By the Numbers"

3.4.1 Probability of Failure

Actuation systems were once designed to operate following a selected combination of failures such as "any hydromechanical failure plus loss of any two electrical systems." It is now customary to design an actuation system and each line-replaceable unit (LRU) to achieve allocated probabilities of loss of function and loss of control. Loss of function means that the system can no longer perform its intended function. In general, it will have reverted to a fail-safe (FS) mode of operation that allows continued safe flight and landing. This loss of function may or may not allow completion of a mission and mission reliability is one way in which military actuation systems are specified. Loss of control, by contrast, means loss of control of the aircraft.

Some military actuation systems have an FS mode that does not allow safe landing. Such a mode may allow continued flight for a time sufficient only to allow engine restart or safe ejection.

In the military aircraft field, the terms probability of loss of function (PLOF) and probability of loss of control (PLOC) are customarily used. During the preliminary phase of a military air vehicle design, the prime contractor and the procuring agency must agree on the vehicle mission reliability, its PLOC, and the associated safety hazard categories, see [3.4.3](#) and [3.4.4](#).

Each possible failure must be considered for its probability and its consequences using failure modes and effects analysis (FMEA) or failure modes and effects criticality analysis (FMECA), fault tree analysis, and functional hazard analysis techniques, see [3.4.3](#). The design of the failure-detection methods and the “coverage” they achieve is a vital part of this process.

Accessing historical data covering the failure rates and failure modes of actuation system components is also of prime importance. Refer to SAE publication “Aircraft Flight Control Actuation System Design,” section 12.1.9, for a list of potential sources.

3.4.2 Fault Coverage

Fault coverage is the number of failures that will be detected expressed as a percentage of all failures that could occur. It is a direct result of a system’s overall architectural design together with the detailed design of its hardware and software. Fault coverage is a vital system aspect because it is often true that certain undetected failures can result in loss of control. In this case, the product of the probability of these failures and their “lack of coverage” will increase the PLOC for the system.

An FMEA is conducted early in a system design to allow the failures to be separated into safety-critical, mission-critical, and non-critical categories and hence to determine which faults contribute to the PLOC and which to the PLOF. This categorization is mission-dependent. For example, trailing edge flap failures might be neither safety nor mission critical for a land-based aircraft but safety-critical for a carrier-based aircraft. The failure categorization allows a more realistic assessment to be made of the fault coverage required since failures that are not critical can be monitored with a relatively low coverage without impact on PLOF or PLOC. The results of the FMEA are used to develop algorithms to detect critical failures or to iterate the design to remove failure modes.

In a voting triplex or quadruplex redundant FBW actuation system, the issue of fault coverage is not so critical for first failures upstream of the last voting plane. This plane could be a digital voter or an averaging mechanism such as a magnetic flux summing point within a servovalve or a mechanical force sum point within or downstream of an actuator. The ability of such a voting plane to absorb the effects of an undetected failure allows the coverage of the upstream failures to be relatively low. This is because their contributions to the PLOF and PLOC are measured by combined probabilities and the calculation of series additive events suppresses the impact of the undetected failures on the overall failure rate.

For example, for a triplex system, the calculation might be as follows. The PLOC for upstream failures would be the product of the probability of the first failure, its lack of coverage, and the probability of the second failure. It should be noted that the precise form of these calculations is dependent on the type of monitoring used.

Failures within a specific channel or lane upstream of a voter can be grouped by their effects and isolated as a group. All of these failures must be addressed correctly to allow the PLOC allocations to be met. The PLOC is likely to be driven, however, by failures downstream of the voter. These must be sufficiently remote and monitored with sufficient coverage to yield an acceptable PLOC. Overall fault coverage during real-time computations is typically 90 to 95%. Achieving a higher percentage of coverage typically causes penalties in the mean time between failures (MTBF), cost, weight, and volume because of the additional circuitry and software required.

3.4.3 Commercial Aircraft Failure Criticality and Probability

The safety analysis of an aircraft flight control system starts with a functional hazard analysis (FHA). The FHA identifies the hazards associated with the failure modes of the system for that aircraft. These hazards are categorized with respect to their effect on the aircraft, the ability of the crew to deal with the failure condition, and the safety of the occupants.

Commercial aircraft airworthiness requirements define the various effect categories in terms that vary from “minor” to “catastrophic.” They define the criticality of the loss or degradation of function caused by the failure in terms that range from “non-essential” to “critical.” They define the allowable probability of occurrence of each category in quantitative terms ranging from “Probable” to “Extremely Improbable.” Finally, they dictate the quantitative range of the allowable probability of occurrence in failures per flight-hour terms. [Table 1](#) illustrates these relationships with information extracted from the FAA Advisory Circular AC 25.1309-1A. It also shows the differences in definition between the Federal Aviation Administration (FAA) of the United States and the European Aviation Safety Agency (EASA), the equivalent certification authority for Europe. The table shows that the certification authorities allow differing software levels to be associated with the different effect categories. This allows design approaches that segregate the detection of non-safety-critical failures to a separate lane of processing and a lower level of software. Similarly, different design criteria for the robustness of the detection with respect to component tolerancing could be adopted.

These requirements must be satisfied by the architecture chosen for the aircraft. The design of the failure detection plays an important part in the choice of architecture and design of the elements of the architecture. Correct detection and reconfiguration minimize the hazard that results from a failure; failure to correctly detect a failure can create an immediate hazard or set the system for a later catastrophic effect from a second failure as discussed below (see [4.2.3](#)). ARP4754 provides guidance in system development.

Analysis of the effects of each failure mode for a servoactuator allows differing approaches to be adopted for the different failure modes. More hazardous effects demand full-time, continuous monitoring. Less serious effects can be addressed by background monitoring. See [3.8](#) for a discussion of the different categories of testing. In the commercial aircraft field, failures with less serious effects and with low probabilities are tested for during scheduled testing every few hundred flight hours.

Table 1 - FAA and EASA failure criticality and probability definitions

Effects on aircraft and occupants of the identified failure condition per 14 CFR Part 25, AC 25.1309-1A definition.	No significant degradation of aircraft capability, crew actions well within their capabilities. Minor failure conditions may include, for example: • A slight reduction in safety margins or functional capabilities. • A slight increase in crew workload, such as routine flight plan changes, or some inconvenience to occupants.		Reduction of the airplane capability or of the crew ability to cope with adverse operating conditions to the extent that there would be: • A significant reduction in safety margins or functional capabilities. • A significant increase in crew workload or in conditions impairing crew efficiency. • Some discomfort to occupants. or in more <u>severe</u> cases: • A large reduction in safety margins or functional capabilities. • Higher workload or physical distress such that the crew could not be relied on to perform its tasks accurately or completely. • Adverse effects on occupants.		Prevention of continued safe flight and landing of the airplane.
Effect category per 14 CFR Part 25, AC 25.1309-1A.	Minor.		Major.		Catastrophic.
14 CFR Part 25, AC 25.1309-1A qualitative probability terms.	Probable. Occurrence anticipated one or more times during the entire operational life of each airplane.		Improbable. Occurrence not anticipated during the entire operational life of a single random airplane. However, failure conditions may occur occasionally during the entire operational life of all airplanes of one type.		Extremely improbable. Occurrence not anticipated during the entire operational life of all airplanes of one type.
Effects on aircraft, occupants and flight crew of the identified failure condition per AMC of CS 25.1309 definition.	No effect on safety or operational capability, no increase of crew workload, inconvenience for occupants possible.	No significant reduction of aeroplane safety, crew action well within their capabilities, e.g., • Slight reduction in safety margins or functional capabilities. • Slight increase in crew workload (e.g., routine changes in flight plan). • Physical discomfort to passengers or cabin crews.	Reduction of the capability of the aeroplane or of the ability of the crew to cope with adverse operating conditions to the extent that there would be, e.g., • Significant reduction in safety margins or functional capabilities. • Significant increase in crew workload or physical discomfort for flight crew. • Physical distress to passengers or cabin crew, possibly including injuries.	Reduction of the capability of the aeroplane or of the ability of the crew to cope with adverse operating conditions to the extent that there would be: • Large reduction in safety margins or functional capabilities. • Physical distress or excessive workload impairs the ability to perform tasks. • Serious or fatal injury to a small number of passengers or cabin crew.	Multiple fatalities, usually with the loss of the aeroplane.
Effect category CS 25.1309 and Eurocae ED-12A.	No safety effect.	Minor.	Major.	Hazardous.	Catastrophic.
EASA-CS qualitative probability terms.	No probability requirement.	Probable Occurrence one or more times during the entire operational life of each aeroplane.	Remote Unlikely to occur to each aeroplane during its total life, may occur several times considering the total operational life of a number of aeroplanes of the type.	Extremely Remote Unlikely to occur to each aeroplane during its total life, may occur a few times considering the total operational life of a number of aeroplanes of the type.	Extremely Improbable Not anticipated to occur during the entire operational life of all aeroplanes of one type.
14 CFR Part 25 and EASA-CS quantitative probability ranges.	No probability requirement.	$\leq 10^{-3}$ only reference.	$\leq 10^{-5}$	$\leq 10^{-7}$	$\leq 10^{-9}$
Criticality category RTCA DO-178A for system functions.	Non-essential		Essential		Critical
DO-178A Software Levels.	Level 3		Level 2		Level 1
DO-178B/C Software Levels.	Level E	Level D	Level C	Level B	Level A

The effect category also determines the subsequent action taken by the system. Failures that impact safety must lead to immediate and automatic reconfiguration. Failures that reduce the robustness of the system to subsequent failures may be annunciated to the pilot and used to prevent subsequent flight dispatches until corrected. More benign failures and degradations may be collected by a maintenance system for correction at a scheduled time and location. An assessment of the effects and probabilities of all of the possible latent failures must be performed to justify the scheduled maintenance time intervals.

3.4.4 Military Aircraft Failure Criticality and Probability

Almost all of the content of the previous subsection applies equally to actuation systems designed for military aircraft. Similar hazard definitions are established for military aircraft, though there is less consistency in the categories and their allowed probability of occurrence. The hazard categories are adjusted and their accompanying quantitative requirements are assigned on a program-by-program basis using AS94900 as a guide. A single-engine fighter requires different treatment from a multi-engine transport.

[Tables 2](#) and [3](#) contain information extracted from MIL-STD-882 providing guiding definitions for severity categories and probability levels, respectively.

Table 2 - Military usage severity category

Description	Severity Category	Mishap Result Criteria
Catastrophic	1	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding \$10M.
Critical	2	Could result in one or more of the following: permanent partial disability, injuries, or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding \$1M but less than \$10M. Severe injury, severe occupational illness, major system or environmental damage.
Marginal	3	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding \$100K but less than \$1M.
Negligible	4	Could result in one or more of the following: injury or occupational illness not resulting in a lost workday, minimal environmental impact, or monetary loss less than \$100K.

Table 3 - Military usage probability levels

Description	Level	Specific Individual Item	Fleet or Inventory
Frequent	A	Likely to occur often in the life of an item.	Continuously experienced.
Probable	B	Will occur several times in the life of an item.	Will occur frequently.
Occasional	C	Likely to occur sometime in the life of an item.	Will occur several times.
Remote	D	Unlikely, but possible to occur in the life of an item.	Unlikely but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced in the life of an item.	Unlikely to occur, but possible.
Eliminated	F	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated.	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated.

3.5 System Separation

Some applications demand a “brick wall” between the redundant electrical control channels. This design approach forbids the use of electrical cross-channel interaction to avoid the corruption of one channel by a neighbor. The issue of hydraulic and electrical system separation is similar. Hydraulic system switching is sometimes seen in military aircraft, usually protected to prevent loss of multiple systems through a single leak path, but very rarely used in commercial aircraft. Electrical bus switching is used in both military and commercial aircraft, accompanied by dedicated uninterruptible backup power for flight critical systems.

For commercial aircraft, brick wall separation greatly assists the certification process because of the elimination of some common-mode failures that could disable more than one electrical channel. A brick wall compels the use of “in-line” monitoring, that is, monitoring contained within the channel being monitored. The Space Shuttle monitoring description (see [5.3](#)) provides one example of this approach.

High-performance military aircraft typically operate at flight conditions that demand such close control of failure transients that the differences between channels must be minimal and divergence from the ideal state must be detected immediately. This situation has been addressed with the use of cross-channel equalization or voting and cross-channel comparison for failure detection

Brick-wall requirements have become less absolute. Design techniques and technology have been developed to provide safe means of cross-channel information handling through “buffering,” the use of data buses, and optical coupling. Data buses now carry multiple commands generated by parallel channels. DC buses that power each channel are themselves derived from redundant DC power supplies. Logic states of an actuation system can be signaled from one channel to another as hydraulic pressure. This pressure is often provided with a “fuse” to protect against loss of two systems from a single-point failure.

There is program cost associated with many of these means of protection, for example, the additional verification and validation required for Cross-Channel-Data-Link (CCDL) hardware. Despite their use, any data transfer between channels carries risk and in some situations remains prohibited. Where it is adopted care must be taken to limit cross-channel corruption by the use of, for example, authority limiting and particular care used to prevent a failed channel from turning off a healthy channel.

3.6 Fighting Between Redundant Commands to a Surface

When multiple command channels are summed to position a common surface in a majority-vote or “active-active” manner, the commands will tend to fight one another. The summation may be within the position control loop, or velocity control loop of a single servoactuator, or within the structure of a single surface driven by multiple servoactuators. It may take the form of a fight between electrically induced magnetic fluxes, a fight between summed flows, a force fight at the level of the forces required to drive a control valve, or a force fight at the level of the full output force capability of the servoactuator. The fighting is caused by small differences between the loops closed around the servoactuator. These differences are dominated by the tolerances of the elements of the loops, drifts, or biases, exaggerated by their high gain.

This fighting can degrade the performance of the servoactuator and, in the worst case, could damage the structure of the aircraft. In addition, successful failure detection within a system architecture that did not address force fight would be jeopardized because of the resultant effects on the measured indicators typically used in failure detection. Servovalve output pressure, for example, could be strongly biased or even hardover due to force fight, even though no failure had occurred.

The Space Shuttle servoactuators, see [5.3](#), employ an architecture that diminishes the effect of the fighting, places the fighting in a location where it cannot harm the life or performance of the actuator, and provides good failure detection despite a complete brick-wall. The actuation hardware is very complex hydromechanically, however. Simpler actuation schemes with better positioning accuracy are practicable if electronic rigging is adopted.

3.7 Electronic Rigging

3.7.1 Electronic Rigging Purpose

In some digital fly-by-wire flight control systems electronic rigging functions have been developed to reduce maintenance costs by eliminating the manual adjustments of actuator length normally required to accommodate manufacturing tolerance in the air vehicle structure. These functions have a secondary benefit in that they can compensate for the effects that cause the force fighting between redundant channels described above, see [3.6](#).

The critical end result of a rigging process is the correct alignment of the trim positions for the surfaces since this affects the aircraft range performance, and this part of the rigging process always requires some manual input. The accuracy over stroke, by contrast, the part of rigging which can be automated, may be very important for the flight control system but is much less important for the aircraft. This is because, in FBW aircraft, the pilot commands aircraft rates and accelerations and the control laws automatically adjust the control surface positions to meet the commands. The actuators are normally provided with sufficient stroke to allow the rate and acceleration requirements to be met with worst-case tolerances and structural deflection.