Transport Canada Transports Canada

Advisory Circular

Subject: **Aircraft Level Integration Testing to address loss of function, malfunction and fault propagation effects**

Issuing Office:	Civil Aviation, Standards	Document No.:	AC 525-022
File Classification No.:	Z 5000-34	Issue No.:	01
RDIMS No.:	14467866-V11	Effective Date:	2026-07-24

Table of contents

1.0 Introduction

(1) This Advisory Circular (AC) is provided for information and guidance purposes. It describes an example of an acceptable means, but not the only means, of demonstrating compliance with regulations and standards. This AC on its own does not change, create, amend or permit deviations from regulatory requirements, nor does it establish minimum standards.

1.1 Purpose

(1) The purpose of this document is to describe acceptable means of showing compliance with Airworthiness Manual (AWM) 525.1309 for integration testing to address loss of function, malfunction, fault propagation effects and unintended behaviour.

(2) Aircraft designs are becoming increasingly complex and highly integrated. Additional effort beyond traditional requirements-based testing is required to assess the loss of function, malfunction, fault propagation effects and the unintended behaviour in demonstrating compliance to AWM 525.1301 [Equipment - Function and Installation] and AWM 525.1309 [Equipment - Equipment, Systems, and Installations].

(3) The testing methodology for unintended effects was previously addressed by the use of project specific Issue Papers and Certification Memoranda (CM). The contents of this AC is the result of subsequent harmonization activities between Certification Authorities. It should be noted that SAE International Aerospace Recommended Practice (SAE ARP) 4754B also includes guidance on addressing unintended behaviours.

1.2 Objectives

(1) The applicant will be requested to develop an aircraft-level systems integration plan that outlines a structured and systematic approach to identifying the functions to be assessed and the relevant test cases to be conducted. The scope of testing and evaluations conducted will be directed towards ensuring any potential hazards or unwanted interactions are understood, identified and corrected. The complexity and associated interdependencies of these integrated systems introduce the need for a rigorous approach to characterize and understand the behaviours, both normal and abnormal, of these integrated systems at the Aircraft level. This advisory circular provides one means of evaluating the capacity of systems to protect against unintended behaviours.

(2) Normally, systems integration begins with item-by-item integration and progresses to complete system integration. The difficulty of fully anticipating or modeling the aircraft environment at any particular stage in design development dictates that integration activities may need to be performed at various phases of implementation (i.e. intra-system, inter-system, aircraft-level). While the confidence of on-the-aircraft integration testing can be high, meaningful or cost-effective results can also be achieved in laboratory or simulation environments. Specific procedures for systems integration will vary depending on the capabilities of test facilities, the functional interactions being represented and the interdependencies between functions/systems being assessed. A strategy or methods should be developed to investigate the potential for unintended behaviours, describing behaviour the level of testing to be performed (e.g. aircraft level, system-to-system integration level, intra-system level) and the types of testing to be performed (e.g. scenario based testing, targeted testing, subject matter opportunistic testing, etc.).

1.3 Applicability

(1) This document applies to all Transport Canada Civil Aviation (TCCA) employees, to individuals and organizations when they are exercising privileges granted to them under an External

Ministerial Delegation of Authority. This information is also available to the aviation industry for information purposes.

1.4 Description of changes

(1) Not applicable.

2.0 References and requirements

2.1 Reference documents

(1) It is intended that the following reference materials be used in conjunction with this document:

(a) *Aeronautics Act* (R.S.C., 1985, c. A-2)

(b) Part V, Subpart 21 of the *Canadian Aviation Regulations* (CARs) — Approval of the Type Design or a Change to the Type Design of an Aeronautical Product;

(c) Chapter 525 of the Airworthiness Manual (AWM) — Transport Category Aeroplanes;

(d) Chapter 529 of the Airworthiness Manual (AWM) — Transport Category Rotorcraft;

(e) SAE ARP 4754B Guidelines for Development of Civil Aircraft and Systems;

(f) SAE ARP 4761A Guideline for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment; and

(g) EASA CS 25.1309, Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes, CS 25 Amendment 28.

2.2 Cancelled documents

(1) Not applicable.

(2) By default, it is understood that the publication of a new issue of a document automatically renders any earlier issues of the same document null and void.

2.3 Definitions and abbreviations

(1) The following **abbreviations** are used in this document:

(a) **AC:** Advisory Circular

(b) **AFHA:** Aircraft level Functional Hazard Assessment

(c) **ARP:** Aerospace Recommended Practice

(d) **AWM:** Airworthiness Manual

(e) **CAR:** *Canadian Aviation Regulations*

(f) **CAS:** Crew Alerting System

(g) **CM:** Certification Memorandum

(h) **DAL:** Design Assurance Level

(i) **EICAS:** Engine Indicating and Crew Alerting System

(j) **PASA:** Preliminary Aircraft Safety Assessment

(k) **OEM:** Original Equipment Manufacturer

(l) **SAE:** SAE International (formerly “Society of Automotive Engineers”)

(m) **SFHA:** System Functional Hazard Assessment; and

(n) **TCCA:** Transport Canada Civil Aviation.

3.0 Background

(1) Aircraft/System integration is the task of ensuring all the aircraft systems operate correctly individually and together as installed on the aircraft. In addition to verifying intended functionality, this activity provides an opportunity to check for what has often been referred to as ‘unintended behaviour’.

(2) Many new aircraft designs are introducing a number of new and novel aircraft systems and features that employ a significant degree of systems integration. The complexity and associated interdependencies of these integrated systems introduce the need for a rigorous and systematic approach to characterize and understand the behaviours, during normal and abnormal conditions, of these integrated systems at the aircraft level. This AC focuses on the need for a systematic means of identifying, assessing and testing for the aircraft level effects associated with the loss of individual functions and systems and potential abnormal behaviour as a result of systems malfunction or unintended behaviour (Note: This does not refer to inappropriate crew actions). Assessment of individual systems behaviour in this manner should also investigate the potential for fault propagation and cascading failure effects impacting other functions, systems or aircraft common resources.

(3) While the assessment of loss of function can be readily carried out using traditional methods, it is recognized that additional effort will be required to more thoroughly identify and assess potential failure modes associated with systems malfunction or unintended behaviours. Past experiences, lessons learned, reported incident data and closer scrutiny to the interaction and interdependencies of aircraft systems should all be employed to aid in the determination of relevant test cases.

4.0 Aircraft integration test plan

(1) The Methodology for assessing robustness and integrity of critical aircraft functions, associated systems and components should be outlined in an aircraft-level systems integration plan that spans across all systems and takes into account the interactions and interdependencies of individual functions in both normal and abnormal operations of systems (i.e. loss of function, malfunction and unintended behaviour), and should include the potential for cascading/fault propagation effects. Verification coverage should be planned and conducted to provide confirmation of effective failure containment on all the failure paths leading to catastrophic and hazardous failure effects at the aircraft level. An aircraft-level systems integration plan and corresponding verification summary that addresses these aspects is typically required to demonstrate compliance with AWM 525.1301 and AWM 525.1309.

(2) The aircraft-level systems integration plan should outline a systematic and structured approach for identifying the systems test cases that span across system boundaries, highlighting the testing and evaluations to be conducted to ensure potential hazards are adequately understood, identified and corrected. While the assessment of loss of function can usually be carried out using traditional methods, it is recognized that additional effort will be required to more thoroughly identify and assess potential failure modes associated with systems malfunction or unintended behaviours, and their aircraft level effects. Past experiences, lessons learned, reported incident data and closer scrutiny of the interaction and interdependencies between aircraft systems should all be employed to aid in the determination of relevant test cases. Dedicated integration testing (rig and aircraft), supported as appropriate by systems-level integrated testing, should be utilized

to thoroughly understand and assess design robustness and integrity at the aircraft level, considering the following :

(a) Emphasis on functions and individual systems with failure conditions identified in the Aircraft level Functional Hazard Assessment (AFHA) / Preliminary Aircraft Safety Assessment (PASA) / System Functional Hazard Assessment (SFHA) as hazardous or catastrophic;

(b) Foreseeable aircraft configurations, operational conditions, environmental conditions and scenarios expected to be encountered:

(c) Expected system behaviours under both normal and abnormal (i.e. induced failures) conditions;

(d) Interfaces and interrelationships/interdependencies associated with the critical systems identified;

(e) Equipment where common mode errors could simultaneously affect multiple system level and/or aircraft level functions and their associated failures cases;

(f) Potential for fault propagation or cascading effects;

(g) Awareness/indications provided to the flight crew for failure conditions affecting multiple functions, especially those which potentially increase the overall hazard effects and pilot workload; and

(h) Effectiveness of system or aircraft level mitigations (architectural or otherwise).

(3) The Aircraft Integration plan should also clearly identify the roles and responsibilities of the various groups/specialists (e.g. safety, integration, delegates, etc.) involved in the various stages described below.

5.0 Testing and assessment

5.1 Testing methodology

(1) To address the above considerations for demonstration of design integrity and robustness, especially in the areas of malfunction and unintended behaviour, a systematic means of defining the sets of test cases (section 5.2) and test conditions (section 5.3) required should be applied, and the assessment results should be documented. The following considerations are not exhaustive but have been taken from observations on past certification programs, aircraft incident databases, etc., and should be taken into account when developing a plan to understand and address both the known and potential cases that could be identified based on the level of complexity and integration of the aircraft.

5.2 Test Cases

(1) The systematic means of defining test cases should consider the following as a minimum:

(a) Loss of function includes both permanent and temporary loss. Degraded system performance should also be assessed including during interrupts such as power interruptions, equipment resets or communication interruptions, and the consequences of any resets evaluated during flight;

(b) Malfunctions will be dependent upon the system/interface being assessed and could vary considerably system-to-system (e.g., signal/data interrupts, oscillating signals, transients, system producing data within normal range but not the anticipated/expected values, over/under voltage or pressure);

(c) Normal and abnormal operating modes including mode transitions (e.g., ground-to-air transition, primary-to-alternate);

(d) The potential for interference or adverse characteristics resulting from critical functions interacting with unrelated functions that share a common platform or resources (e.g., multiple functions including non-flight control functions embedded within flight control computers, lower Design Assurance Level (DAL) functions sharing a common computing platform with higher DAL functions);

(e) Systematic testing of the design/implementation provides good opportunities to uncover potential unintended effects or functionality in the design but may not be sufficient to address unintended behaviour. More thorough testing is required to uncover the effects of unintended behaviour of systems as defined in ARP 4754B section 5.5.5.4 which states “Testing to provide confidence that the implemented system does not perform unintended functions (i.e., not consciously part of the design) that impact safety. Ad hoc testing, and special vigilance during normal testing, may be used to identify unintended system or item operation or side-effects”; and

(f) Checklists and procedures associated with the aircraft-level systems integration plan should be developed to aid the various design groups to perform assessments in a consistent and structured manner when defining test cases and evaluating the impact of failures.

5.3 Test conditions

(1) Integration testing affords the opportunity to discover and eliminate undesired behaviours. Such behaviours can arise from issues such as requirements gaps or unanticipated interaction between functional elements. Particular attention should be directed during integration testing towards conducting dedicated testing of features implemented in the design to mitigate or eliminate potential unsafe operating conditions such as monitors, fault isolation means, partitioning, etc. and any related or relevant system interfaces.

(2) Tests may be derived from consideration of the following elements (examples only - not a checklist of cases):

(a) Testing and/or simulation of failure conditions developed to challenge architectural protective features (including outside of the operational envelope, as necessary);

(b) Operation of pilot inputs single and in combination over a wide range of input ranges and rates;

(c) Signals out of range, invalid inputs, etc.;

(d) Normal and abnormal power up sequences (electric and hydraulic);

(e) Power (electric and hydraulic) transients, failures, and abnormal levels;

(f) Failure conditions including sequential failures;

(g) External signal abnormal ranges and/or failure conditions;

(h) Databus disturbances, internal and external;

(i) Monitor focused specific tests to expose nuisance susceptibility.

5.4 Assessment

(1) The methodology for assessment during testing may be derived from consideration of the following aspects (examples only – not an exhaustive list of possible means):

(a) For each system and/or component identified, introduce or simulate failure conditions (i.e. misleading signal, corrupted data, loss of input, etc.), and assess whether the desired output has been achieved;

(b) Assess the system protection measures (e.g. monitors) to determine whether they behave as expected in the presence of faults or failures, and maintain the system/functions affected within their established limits;

(c) Verify that system channel independence (including independence through associated monitors or other protective mechanisms), where applicable, is maintained in the presence of failure conditions;

(d) Verify the independence of the failed component(s) (i.e. no further fault propagation);

(e) Ensure adequate fault codes/indications allowing the identification of the source/cause of failure;

(f) Ensure that system data buses failures do not create unsafe conditions;

(g) Ensure that fault clearance and protection coordination are adequately designed in order to isolate the fault and maintain smooth and stable operation of the systems affected;

(h) Through dedicated fault insertion testing, verify that erroneous/misleading signals, especially those that are common to multiple systems, can be adequately detected by systems and/or recognized and addressed by the crew;

(i) Human factors assessment of pilot workload should be conducted throughout the integration testing exercises, including the assessment of the initial failure condition and any subsequent cascading effects on aircraft systems and/or flight deck, pilot actions required and the overall hazard classification. Included in this assessment would be:

  (i) Engine Indicating and Crew Alerting System (EICAS) / Crew Alerting system (CAS) messages and synoptic indications are properly displayed (correct functions and alert levels) as per system design;

  (ii) Crew ability to deal with failures that result in multiple flight deck effects;

  (iii) EICAS/CAS messages and procedures validated by pilot reviews;

  (iv) Intersystem failures and their cascading effects observed and their impact on flight deck indications and pilot procedures;

(j) Cascading effects should be analyzed until there are no further effects on systems or aircraft level functions; and

(k) Verify the effectiveness of partitioning, fault isolation schemes, etc. to protect against any hazardous fault propagation.

6.0 Results

(1) All identified deficiencies or anomalies should be referred back to the appropriate development activity (e.g., requirements capture, allocation or validation; implementation; verification, configuration management) for resolution and the process iterated until concluded.

(2) When all iterations are concluded, the output of this activity is a verified integrated system, along with the data demonstrating that the system/aircraft satisfies all functional and safety requirements.

(3) Although the complete absence of undesired behaviours can never be established by test, the monitoring for unintended behaviours during development (e.g., requirements based testing, flight

operations, maintenance), in conjunction with the objectives outlined in this AC provides the means to show that intersystem requirements, taken as a group, have been satisfied.

(4) A summary of testing results obtained should be documented accordingly.

7.0 Information management

(1) Not applicable.

8.0 Document history

(1) Not applicable.

9.0 Contact us

(1) For more information, please contact:

Aircraft Certification Standards Division (AARTC) via the following e-mail address:
E-mail: TC.AARTCDAircraftDesignStandards-NormesdeconceptiondesaeronefsAARTCD.TC@tc.gc.ca

Suggestions for amendment to this document are invited, and should be submitted via:
E-mail: AARTDocServices-ServicesdocAART@tc.gc.ca

Original signed by

Jamie-Lee MacDermid,
Executive director, Standards branch (AART)
Civil Aviation,
Transport Canada