Certification Authorities for Large Transport Aircraft (CATA)

CATA Worklist Item TCCA-004 –Aircraft Level Integration Testing and Assessment of Unintended Functions

Date Raised:	Sept. 27/2016	Updated: N/A	Status: **CLOSED**
Date Revised	December 20, 2017, March 5, 2018		
Raised By:	[redacted]		
Contributors:	[redacted]		

Subject: **Aircraft Level Integration Testing**

Related Issue(s): None
(Identify Discussion Paper number, if any)

Description of Issue(s):

(Give a brief background of issue(s)

Aircraft designs are becoming increasingly complex and highly integrated to the point where additional effort beyond traditional requirements based testing is required to assess potential failures and/or malfunctions associated with unintended effects. The testing methodology for unintended effects is currently not harmonized between authorities but the need for harmonization has been established through the continued use of Issue Papers and Certification Memorada by some authorities.

TCCA expectation is that harmonized guidance be developed to address this issue.

Background:

Aircraft system designs are constantly evolving to provide increased efficiencies and reduced costs. This has resulted in systems incorporating capabilities/functionality of many previously federated systems onto common platforms such as Integrated Modular Avionics (IMA) or Common Computing Core, for example. This integration has increased the complexity of design and increased the potential for failures and malfunctions (e.g. common mode failures) where unintended function and wider ranging consequences are possible compared to a federated environment.

The complexity and associated interdependencies of integrated systems introduces the need for a rigorous and systematic approach to characterize and understand the behaviors, both normal and abnormal, of these complex and integrated systems at the aeroplane and systems levels. Investigation is required to develop a harmonized, systematic means for identifying cascading failures, common mode failures, and fault propagation effects through increased vigilance towards the identification of potential malfunctions and the prevention of unintended functions.

AC 25.1309 Arsenal draft and AMC 25.1309 mentions the consideration of malfunctions but mostly in terms of the impact on hazard classification. No specific mention of evaluating unintended functions is made. ARP 4754A states the need to investigate and eliminate undesired unintended functions but provides little to no specific guidance. This has been recognized and efforts are being made to provide some expansion in this area by an SAE S18 sub-group for ARP 4754 Rev B currently in work but it may still be insufficient. The optimum approach envisioned is to develop testing protocols/procedures to specifically address testing for unintended effects, which becomes an integral part of normal system robustness testing protocols.

This is not requirements driven testing and is not considered successful solely on the basis of "no anomalies found" during normal requirements based testing. The main objective is to uncover unintended effects by challenging protections (e.g. monitors, partitions, fault isolation, etc.) with operational scenarios or failure cases that attempt to "break" these or similar fault mitigation schemes.

Certification Authorities for Large Transport Aircraft (CATA)

CATA Worklist Item TCCA-004 –Aircraft Level Integration Testing and Assessment of Unintended Functions

Authority representatives presented a "harmonized" recommendation on this topic to the SAE S-18 Committee meeting Oct 2016 in Ft. Lauderdale, FL (attached below).

Plan for Unintended functio

Proposed Prioritization:

(Per CATA Technical Issues List Prioritization schema)

Question	Answer
1. Is there an active working group related to this issue?	Yes – SAE S18 WG and Sub working group under S18
2. In which documents are there deviations amongst the authorities?	Deviations in certification memoranda for specific projects.
3. Was this issue raised by or at the CMT?	No.
4. What is the level of impact on projects in the future (i.e. minor, major, critical)?	Major; historical issues with domestic certifications and foreign validations have taken up significant time and effort.
5. How many authorities does the issue impact?	Issue impacts all 4 authorities
6. What is the approximate technical complexity of the issue (i.e. low, medium, high)?	Highly complex.

Recommendation:

CATA to create a technical task group made up of specialists from all authorities to determine common advisory/guidance material with respect to this topic.

CATA Decision:

(Using CATA criteria for determination of technical issues)

CATA decision to action this issue. Authorities' SMEs consensus that topic deserved CATA attention.

SME Discussions:

(Indicate Source: Meeting, Telecon or E-mail)

Action	Status

Background included in presentation made by Jim Marko (TCCA) at the Sept. 27/28 CATA meeting. Presentation and meeting/discussion minutes can be found with the meeting materials on the CATA Sharepoint here:

https://avssp.faa.gov/avs/airtad/TSS/CATA/Authorities/SitePages/Home.aspx

Subsequently the SAE S18 WG formed a sub WG to develop guidance for such a harmonized approach, for incorporation in ARP4754 at revision B. While it is expected that this guidance will be sufficiently mature by end of 2017, revision to ARP4754 at Rev B will not be ready for publication until a much later date (2-3

years from now).

ARP4754 Rev B constitutes harmonized guidance to address this issue.

However, there is a time gap between the output of the Sub WG of S18 and ARP4754 Rev B. To address this time gap, the ANAC, EASA, FAA and TCCA will review the mature version of the guidelines developed by the Sub WG of S18 on this subject for consideration as guidance material.

This mature version of the guidance has now been developed by the Sub WG of S18. It is developed by means of revising the existing section 4.6.4 of ARP4754A. As a result, there is no need to use the SAE document AIR6218 DAPIS to convey the agreed guidance.

This guidance is now available (see attached PDF file) and will be incorporated into APR4754B.

SME Recommendation:

(Recommendations from SME Working Group; may contain links and/or embedded documents)

CATA to review the attached guidance.

To close this CWI, CATA is requested to provide its position that it will constitute the agreed guidance to be used by the ANAC, EASA, FAA and TCCA while waiting for ARP4754B to be published.

Final CATA Position:

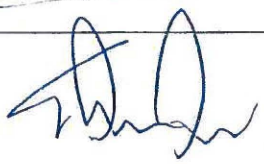
(Explain agreement, dissent or conclusion on this IP)

This CWI is closed on the basis that there is agreed guidance attached herein, which should be incorporated in ARP4754B later. In the meantime, the ANAC, EASA, FAA and TCCA, as Certification Authority, will provide this agreed guidance to its applicants as an acceptable means of compliance when new designs or changes to the approved designs requiring compliance with RBHA/CS/CFR/AWM (5)25.1309.

If the CA and its applicant agree to deviate from the guidance attached to this CWI, then the CA must inform the other CMT authorities.

If the applicant accepts the guidance, then the other CMT authorities will do so as well

Closure of CWI:

CATA Representative	Name	Signature	Date
ANAC	Marcelo Leite		03-08-2018
EASA	Ludovic Aron		03.08.2018
FAA	Tom Groves		3-8-2018
TCCA	Canh Nham		08.03.2018

CATA Worklist Item TCCA-004 –Aircraft Level Integration Testing and Assessment of Unintended Functions

Appendix A – Generic [redacted] Certification Memorandum Example

[redacted]

Project:	XXXX	**CM:**	
		Edition:	
File Number:		**Target:**	
RDIMS:		**Status:**	
NAPA:		**Date:**	
Discipline(s):			
Subject:	Aircraft Level Integration Testing to Address Loss of Function, Malfunction and Fault Propagation Effects		
Reference(s):			

Background/Discussion

The XXXX Aerospace (XX) Aircraft models design introduces a number of new and novel Aircraft systems and features with a significant degree of systems integration. The complexity and associated interdependencies of these integrated systems introduces the need for a rigorous and systematic approach to characterize and understand the behaviors, both normal and abnormal, of these integrated systems at the Aircraft level. This Certification Memorandum (CM) 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/systems and potential abnormal behavior as a result of systems malfunction or unintended behavior (Note: This does not refer to inappropriate crew actions). Assessment of individual systems behavior in this manner should also investigate the potential for fault propagation and cascading failure effects impacting other functions/systems or common resources.

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 behaviors. 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.

[redacted] Position

1. Aircraft-Level Systems Integration Plan

Individual XX Project Work Packages associated with critical systems such as Flight Control, Avionics, etc. will be conducting system-level testing to assess the acceptable performance/characteristics of their associated functions while also evaluating failure cases and fault propagation based on existing requirements, Transport Canada Issue Papers (IP), CM, or any

additional robustness requirements. 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 behavior), and should include the potential for cascading/fault propagation effects. Verification coverage should be 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 that addresses these aspects is required to demonstrate compliance to AWM 525.1301and AWM 525.1309

The Aircraft-Level Systems Integration Plan should outline a systematic and structured approach for identifying the systems test cases that span across system/Work Package boundaries, highlighting the testing and evaluations to be conducted to ensure potential hazards are understood, identified and corrected. In this manner, it is expected that the assessment of loss of function could be readily carried out using traditional methods while also recognizing that additional effort will be required to more thoroughly identify and assess potential failure modes associated with systems malfunction or unintended behaviors. 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. Dedicated integration testing (rig and Aircraft), supported by systems-level integrated testing, as appropriate, 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 AFHA/PASA/SFHA as hazardous or catastrophic;
b) Foreseeable Aircraft configurations expected to be encountered as well as the expected system behaviors under both normal and abnormal (i.e. induced failures) conditions;
c) Interfaces and interrelationships/interdependencies associated with the critical systems identified;
d) The identification of equipment where common mode errors could simultaneously affect multiple system level functions that lead to Aircraft level functions being affected. From the sources of failures discovered, a list of associated failure cases can then be identified;
e) The potential for fault propagation or cascading effects;
f) 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
g) Effectiveness of system or Aircraft level mitigations (architectural or otherwise).

2. Methodology

To address the above considerations for demonstration of design integrity and robustness, especially in the areas of malfunction and unintended behavior, a systematic means of defining the sets of test cases and test conditions required, and documenting the assessment results should

be devised. The following considerations are not exhaustive but have been taken from observations on past certification programs, Aircraft incident databases, etc., and should be considered in developing a plan to understand and address both the known and potential cases taking into account the level of complexity and integration of the Aircraft models.

Definition of test cases

i. Considerations for loss of function includes both permanent and temporary loss. Degraded system performance should be assessed including during interrupts such as power interruptions, equipment resets or communication interruptions, and the consequences of any resets evaluated during flight;
ii. Considerations for 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, etc.);
iii. Consider both normal and abnormal operating modes including mode transitions (e.g. ground-to-air transition);
iv. Identify 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 embedded within Flight Control Computers, lower Design Assurance Level (DAL) functions on same partition with higher DAL functions);
v. Systematic testing of the design/implementation provides good opportunities to uncover potential unintended effects or functionality in the design, but may not be sufficient enough to address unintended behavior. More thorough testing is required to uncover the effects of unintended behavior of systems as defined in ARP 4754 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
vi. Checklists and procedures associated with the Aircraft-Level Systems Integration Plan should be developed to aid the design groups (or Work Packages) perform assessments in a consistent and structured manner when defining test cases and evaluating the impact of failures.

a) Testing and Assessment

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

iv. Verify the independence of the failed component(s) (i.e. no further fault propagation);
v. Ensure adequate fault codes/indications allowing the identification of the source/cause of failure;
vi. Ensure that system data buses failures do not create unsafe conditions;
vii. 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;
viii. 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;
ix. 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:
    - CAS messages and synoptic indications are properly displayed (correct functions and alert levels) as per system design;
    - Crew ability to deal with failures that result in multiple flight deck effects;
    - EICAS messages and procedures validated by pilot reviews;
    - Intersystem failures and their cascading effects observed and their impact on flight deck indications and pilot procedures;
x. Cascading effects should analyzed until there are no further effects on systems or Aircraft level functions; and
xi. Verify the effectiveness of partitioning, fault isolation schemes, etc. to protect against any hazardous fault propagation.

XX is requested to address systems integration at the Aircraft level following an acceptable methodology. An Aircraft-Level Systems Integration Plan that addressed this is required to demonstrate compliance to [redacted]25.1301 and [redacted]25.1309

Applicant Position

[redacted]

Enhancing ARP4754B Guidance for the assessment of Unintended Functions

Background

- ARP 4754 & 4754A identify as the main process objectives the importance of "*examination of requirements to ensure they are both necessary and sufficient is a key aspect of validation. A further objective of the validation process is to limit the potential for unintended functions in the system or for unintended functions to be induced in interfacing systems.*"
- ARP4754A Table 7, Verification methods identifies the need to address unintended function through test. But no guidance beyond a statement of ad hoc testing or targeted analyses is provided to guide the scope of testing to be performed to "*discover and eliminating undesirable, unintended functions.*"
- ARP4754A and Arsenal AC 25.1309 define Failure as 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). Errors can cause malfunctions.
- Unintended function from a 25.1309 and Arsenal AC 25.1309 perspective is understood to be synonymous with a malfunction.

Recommendation - Authorities Represented at S18 (TCCA/FAA/EASA/ANAC)

- Address unintended function as hidden malfunctions (i.e. they are already present and discovery of them through formal requirements based testing may not be complete)
- The absence of unintended function during requirements based testing, or the rectification of anomalies discovered during requirements based testing, is insufficient to ensure that potential errors have been mitigated to the extent practicable.
- It is well understood that a number of OEM's and suppliers conduct informal testing in an attempt to "*discover and eliminating undesirable, unintended function*" but these details are not formally reported/documented. Documentation of the processes and the extent of testing conducted by OEM's and suppliers to discover these hidden malfunctions are needed to provide confidence that the potential for errors has been mitigated to the extent practicable.
- The scope of the assessment for discovering hidden malfunctions can be bounded by targeted testing to fully understand the performance limitations of the safety features (e.g. monitors) that have been put in place to mitigate aircraft/system failure conditions, or testing to fully understand the dynamics of interrelated systems (e.g. inadvertent control surface motions due to re-instatement of invalid/failed sensor data.)
- ARP4754A requires expansion of the verification content to provide additional guidance for identifying protocols/techniques for test cases/scenario's that can be used to provide confidence that the potential for errors has been mitigated to the extent practicable.
- ARP4754B expanded guidance could include OEM/Supplier methodology that has been used to date on recent programs. The authorities can also provide inputs based on certification documents (e.g. Issue Papers, Certification Memorandums, etc.) and experience acquired on certification programs.

Authorities Representatives Present

Current Section 4.6.4

4.6.4 Aircraft/System Integration

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 may dictate that some integration activities be performed on the aircraft. While the validity of on-the-aircraft integration is generally assumed to be high, more meaningful or cost-effective results often can be achieved in laboratory or simulation environments. Specific procedures for system integration vary widely across the industry.

During the integration process, identified deficiencies should be referred back to the appropriate development or integral activity (requirements capture, allocation or validation; implementation; verification, etc.) for resolution and the process iterated. When all iterations are concluded, the output of this activity is a verified integrated system, along with the data demonstrating that the system satisfies all functional and safety requirements.

Aircraft/System integration is the task of ensuring all the aircraft systems operate correctly individually and together as installed on the aircraft. This provides the means to show that intersystem requirements, taken as a group, have been satisfied. It also provides an opportunity to discover and eliminate undesired unintended functions.

Proposed Section 4.6.4

4.6.4 Aircraft/System Integration

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 functions'. However, it is a misnomer, and has led to confusion when trying to describe what is meant by the term, therefore the better descriptive term, 'unintended behavior' is used throughout.

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 ~~may~~ dictates that ~~some~~ integration activities may need to be performed ~~on the aircraft~~at various phases of implementation (i.e. intra-system, inter-system, aircraft-level). While the ~~validity~~ confidence of on-the-aircraft integration testing ~~is generally assumed to~~can be high, more meaningful or cost-effective results often can be achieved in laboratory or simulation environments. Specific procedures for systems integration will vary ~~widely~~ depending on the capabilities~~across the industry~~ of test facilities, the functional interactions being represented and the interdependencies between functions/systems being assessed. ~~.~~ A strategy/methods could be developed to investigate for unintended behaviors~~effects~~, citing 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.).

~~During the integration process, identified deficiencies should be referred back to the appropriate development or integral activity (requirements capture, allocation or validation; implementation; verification, etc.) for resolution and the process iterated. When all iterations are concluded, the output of this activity is a verified integrated system, along with the data demonstrating that the system satisfies all functional and safety requirements.~~

~~Aircraft/System integration is the task of ensuring all the aircraft systems operate correctly individually and together as installed on the aircraft.~~ ~~This provides the means to show that intersystem requirements, taken as a group, have been satisfied. It also~~Integration testing ~~provides confidence that the implemented system does not perform unintended functions and~~ affords the~~ provides an~~ opportunity to discover and eliminate undesired ~~unintended functions~~behaviors. Such behaviors can arise from issues such as requirements gaps or unanticipated interaction between functional elements ~~defined by requirements~~. ~~Special~~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. Such tests may be derived from consideration of the following elements (examples only - not ~~an inclusive~~a checklist of cases~~ listing~~):

- Testing and/or simulation of failure conditions developed to challenge architectural protective features (including outside of the operational envelope, as necessary)
- Operation of pilot inputs single and in combination over a wide range of input ranges and rates.
- Signals out of range, invalid inputs, etc.
- Normal and abnormal power up sequences (electric and hydraulic)
- Power (electric and hydraulic) transients, failures, and abnormal levels
- Failure conditions including sequential failures
- External signal abnormal ranges and/or failure conditions
- Databus disturbances, internal and external
- Monitor focused specific tests to expose nuisance susceptibility

During the integration process, identified deficiencies should be referred back to the appropriate development or integral activity (requirements capture, allocation or validation; implementation; verification, etc.) for resolution and the process iterated. When all iterations are concluded, the output of this activity is a verified integrated system, along with the data demonstrating that the system satisfies all functional and safety requirements. Although the complete absence of undesired behaviors can never be established by test, the monitoring for ~~anomalou~~unintended~~s~~ behaviors during requirements based testing, in conjunction with the objectives outlined in this section provides the means to show that intersystem requirements, taken as a group, have been satisfied. A summary of testing results obtained should be documented accordingly.

~~It should be noted that complete absence of undesired behaviors can never be established by test.~~

Current Section 5.4.1

5.4.1 Process Objectives

Ensuring correctness and completeness of requirements are the objectives of the requirements validation process (i.e. Are we building the right aircraft?).

Examination of requirements to ensure they are both necessary and sufficient is a key aspect of validation. A further objective of the validation process is to limit the potential for unintended functions in the system or for unintended functions to be induced in interfacing systems.

Propose Section 5.4.1

5.4.1 Process Objectives

Ensuring correctness and completeness of requirements are the objectives of the requirements validation process (i.e. Are we building the right aircraft?).

Examination of requirements to ensure they are both necessary and sufficient is a key aspect of validation. A further objective of the validation process is to limit the potential for ~~unintended functions~~~~anomalou~~unintendeds behavior in the system or for ~~unintended functions~~ ~~anomalous~~unintended behavior to be induced in interfacing systems.

Current Section 5.4.6

5.4.6 Validation Methods

Several methods may be needed to support validation. These methods include: traceability, analysis, modeling, test, similarity, and engineering review. Validation should consider both intended and unintended functions. Intended function requirements validation involves evaluation against objective pass/fail criteria. Vigilance during all analysis and testing can be used to identify unintended system/item operations or side-effects. While the absence of unintended functions can not be validated directly, ad hoc testing and targeted analyses can be used to reduce the probability of their presence.

Proposed Section 5.4.6

5.4.6 Validation Methods

Several methods may be needed to support validation. These methods include: traceability, analysis, modeling, test, similarity, and engineering review. Validation should consider both intended ~~and unintended~~ functions and undesired behaviors. Intended function requirements validation involves evaluation against objective pass/fail criteria. Vigilance during all analysis and testing can be used to identify ~~unintended~~ ~~anomalous~~unintended system/item operations or side-effects.~~.~~ It should be noted that complete absence of ~~anomalous~~unintended behavior can never be established by test or analysis.~~While the absence of unintended functions can not be validated directly, ad hoc testing and targeted analyses can be used to reduce the probability of their presence.~~

Current Section 5.5.2

5.5.2 Verification Process Model

Figure 13 shows an overview of a generic process model for verification at each level of system implementation.

The verification process is composed of three distinct elements described as follows:

a. Planning: Includes planning for the resources required, the sequence of activities, the data to be produced, collation of required information, selection of specific activities and assessment criteria, and generation of verification-specific hardware or software (see paragraph 5.5.3).

b. Methods: Includes the activity in which the verification methods are employed (see paragraph 5.5.5).

c. Data: Includes evidence of the results developed in the process (see paragraph 5.5.6).

Level of verification is determined by the FDAL and IDAL (see paragraph 5.5.3).

The inputs to the verification process include the set of documented requirements for the implemented aircraft, system or item and a complete description of the system or item to be verified.

More than one verification method may be necessary to substantiate compliance with the requirements. For example, an analysis may be required in conjunction with a physical test to assure that worst case issues have been covered.

During the process of verifying intended functions, any anomalies recognized (such as an unintended function or incorrect performance) should be reported so that they can be reviewed and dispositioned. Checking the verification process, design implementation process or requirement definition process may be warranted to identify the source of the anomaly.

Proposed Section 5.5.2

5.5.2 Verification Process Model

Figure 13 shows an overview of a generic process model for verification at each level of system implementation.

The verification process is composed of three distinct elements described as follows:

a. Planning: Includes planning for the resources required, the sequence of activities, the data to be produced, collation of required information, selection of specific activities and assessment criteria, and generation of verification-specific hardware or software (see paragraph 5.5.3).

b. Methods: Includes the activity in which the verification methods are employed (see paragraph 5.5.5).

c. Data: Includes evidence of the results developed in the process (see paragraph 5.5.6).

Level of verification is determined by the FDAL and IDAL (see paragraph 5.5.3).

The inputs to the verification process include the set of documented requirements for the implemented aircraft, system or item and a complete description of the system or item to be verified.

More than one verification method may be necessary to substantiate compliance with the requirements. For example, an analysis may be required in conjunction with a physical test to assure that worst case issues have been covered.

During the process of verifying intended functions, any anomalies recognized (such as an ~~unintended anomalous~~unintended ~~function~~ behavior or incorrect performance) should be reported so that they can be reviewed and dispositioned. Checking the verification process, design implementation process or requirement definition process may be warranted to identify the source of the anomaly.

Current Section 5.5.5.4

5.5.5.4 Testing or Demonstration

Testing provides repeatable evidence of correctness by exercising a system or item to verify that the requirements are satisfied. Test readiness reviews establish the applicability of the test cases to system or item requirements. Testing has the following two objectives:

a. To demonstrate that the system or item implementation performs its intended functions. Testing an intended function involves evaluation against objective pass/fail criteria established by the requirements.

b. 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. It should be noted that complete absence of unintended function can never be established by test.

Tests are performed on all or part of the physical system or item or an appropriate validated model using procedures documented in sufficient detail so that a second party could reproduce the test results. Problems uncovered during testing should be reported, corrective action tracked, and the modified system(s) and/or item(s) retested.

For each test or group of tests, the following should be specified:

a. Required input variability should be considered in setting the test criteria.

b. Actions required and action order if time dependent.

c. The purpose or rationale for the test(s).

d. The requirements covered by the test(s).

e. Expected results and the tolerances associated with those results.

Test result data should contain the following:

a. The version of the test specification used.

b. The version of the system or item being tested.

c. The version or reference standard for tools and equipment used, together with applicable calibration data.

d. The results of each test including a PASS or FAIL declaration.

e. The discrepancy between expected and actual results.

f. A statement of success or failure of the testing process including its relationship to the verification program.

5.5.5.4.1 Test Facilities

Functionality may be provided in a system test facility which will improve the probability of detecting incorrect or unintended functions.

Proposed Section 5.5.5.4

Testing provides repeatable evidence of correctness by exercising a system or item to verify that the requirements are satisfied. Test readiness reviews establish the applicability of the test cases to system or item requirements. Testing has the following two objectives:

a. To demonstrate that the system or item implementation performs its intended functions. Testing an intended function involves evaluation against objective pass/fail criteria established by the requirements.

b. To provide confidence that the implemented system does not ~~perform unintended functions~~exhibit ~~anomalous~~unintended behavior (i.e., not consciously part of the design) that impacts safety. ~~Ad hoc testing, and s~~Special vigilance during normal testing~~, may be used~~ should be applied to identify ~~unintended anomalous~~unintended system or item operation or side-effects. This is accomplished by monitoring all system behavior during testing as opposed to only the expected behavior documented in the test. It should be noted that complete absence of ~~unintended function~~anomalousunintended behavior can never be established by test.

Tests are performed on all or part of the physical system or item or an appropriate validated model using procedures documented in sufficient detail so that a second party could reproduce the test results. Problems uncovered during testing should be reported, corrective action tracked, and the modified system(s) and/or item(s) retested.

For each test or group of tests, the following should be specified:

a. Required input variability should be considered in setting the test criteria.

b. Actions required and action order if time dependent.

c. The purpose or rationale for the test(s).

d. The requirements covered by the test(s).

e. Expected results and the tolerances associated with those results.

Test result data should contain the following:

a. The version of the test specification used.

b. The version of the system or item being tested.

c. The version or reference standard for tools and equipment used, together with applicable calibration data.

d. The results of each test including a PASS or FAIL declaration.

e. The discrepancy between expected and actual results.

f. A statement of success or failure of the testing process including its relationship to the verification program.

5.5.5.4.1 Test Facilities

Functionality may be provided in a system test facility which will improve the probability of detecting incorrect or ~~unintended anomalous~~unintended ~~functions~~behavior.

Current Table A-1

2.7	Appropriate item, system and aircraft integrations are performed.	4.6.3 4.6.4	R	R	R	A	N	Verification Summary	②	②	②
5.2	Verification demonstrates intended function and confidence of no unintended function impacts to safety.	5.5.1 5.5.5.3	R*	R	R	A	N	Verification Procedures	①	①	②
		5.5.5.2	R*	R	R	A	N	Verification Results	②	②	②
5.3	Product implementation complies with aircraft, and system requirements.	5.5.1 5.5.2	R*	R	R	A	N	Verification Procedures	①	①	②
			R*	R	R	A	N	Verification Results	②	②	②

Proposed Table A-1

2.7	Appropriate item, system and aircraft integrations are performed.	4.6.3 4.6.4	R	R	R	A	N	Verification Summary	②	②	②
5.2	Verification demonstrates ~~intended function~~that product implementation complies with aircraft, and system requirements. ~~and confidence of no unintended function impacts to safety.~~	5.5.1 5.5.2 5.5.5.3	R*	R	R	A	N	Verification Procedures	①	①	②
		5.5.5.2	R*	R	R	A	N	Verification Results	②	②	②
~~5.3~~	~~Product implementation complies with aircraft, and system requirements.~~	~~5.5.1~~ ~~5.5.2~~	~~R*~~	~~R~~	~~R~~	~~A~~	~~N~~	~~Verification Procedures~~	~~①~~	~~①~~	~~②~~
			~~R*~~	~~R~~	~~R~~	~~A~~	~~N~~	~~Verification Results~~	~~②~~	~~②~~	~~②~~