DOT/FAA/TC-16/39

Federal Aviation Administration
William J. Hughes Technical Center
Aviation Research Division
Atlantic City International Airport
New Jersey 08405

Safety Issues and Shortcomings With Requirements Definition, Validation, and Verification Processes Final Report

December 2016

Final Report

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof. The U.S. Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report. The findings and conclusions in this report are those of the author(s) and do not necessarily represent the views of the funding agency. This document does not constitute FAA policy. Consult the FAA sponsoring organization listed on the Technical Documentation page as to its use.

This report is available at the Federal Aviation Administration William J. Hughes Technical Center's Full-Text Technical Reports page: actlibrary.tc.faa.gov in Adobe Acrobat portable document format (PDF).

Technical Report Documentation Page

1. Report No. DOT/FAA/TC-16/39	2. Government Accession No.	3. Recipient's Catalog No.

4. Title and Subtitle

SAFETY ISSUES AND SHORTCOMINGS WITH REQUIREMENTS DEFINITION, VALIDATION, AND VERIFICATION PROCESSES FINAL REPORT

5. Report Date

December 2016

6. Performing Organization Code

7. Author(s)

Peter DeSalvo and Daniel Fogarty

8. Performing Organization Report No.

9. Performing Organization Name and Address

Boeing Aerospace Operations, Inc.
6001 S Air Depot
Oklahoma City, OK 73135- 6601

10. Work Unit No. (TRAIS)

11. Contract or Grant No.

12. Sponsoring Agency Name and Address

FAA National Headquarters
950 L'Enfant Plaza N SW
950 L'Enfant Plaza
Washington, DC 20024

13. Type of Report and Period Covered

Phase 3 Final Report/DS #18

14. Sponsoring Agency Code

AIR-134

15. Supplementary Notes

This report addresses safety issues and shortcomings with requirements definition, validation, and verification processes. It was revised (Revision A) in response to FAA review and feedback. The FAA Aviation Research Division COR was John Zvanya.

16. Abstract

This document presents safety issues and shortcomings with requirements definition, validation, and verification processes.

System architectures and associated requirements for aerospace digital avionics systems have accelerated in complexity and integration over the last two decades. Initial generations of digital avionics automated individual functions were standalone or had limited integration with other airplane-level functions. However, today's complex avionics architectures can be highly integrated across complex systems. This research has been initiated to identify and address problems caused by, or that contributed to, incorrect or incomplete requirements.

This report builds on research completed in years 1 and 2 of this task order, which addressed safety issues with requirements definition, validation and verification processes and practices, and the root causes of requirements errors, omissions, or conflicts. Included is research based on input from subject matter experts, including recommendations to address the root causes.

17. Key Words

Requirements, Validation, Verification, safety, Development assurance, ARP4754A, ARP4761, DO-178B/C, DO-254, DO-297, Digital avionics systems, Systems integration, Cascading failure effects, Supplier oversight, Process assurance

18. Distribution Statement

This document is available to the U.S. public through the National Technical Information Service (NTIS), Springfield, Virginia 22161. This document is also available from the Federal Aviation Administration William J. Hughes Technical Center at actlibrary.tc.faa.gov.

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 161	22. Price

ACKNOWLEDGEMENTS

The authors would like to acknowledge the following FAA review team individuals for providing support to the project: Chakradhar Agava, Charles Kilgore, Srini Mandalapu, Robin Sova, and John Zvanya.

TABLE OF CONTENTS

APPENDICES

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

AC	Advisory Circular
AD	Airworthiness Directive
ADIRU	Air data inertial reference unit
AEH	Airborne electronic hardware
AFHA	Airplane functional hazard assessment
AIR	Aerospace Information Report
AR	Authorized Representative
ARP	Aerospace Recommended Practice
ATC	Air Traffic Control
AVSI	Aerospace Vehicle System Institute
BCA	Boeing Commercial Airplanes
BITE	Built-in Test Equipment
BQN	Borinquen International Airport
CAS	Caution Advisory System
CCA	Common cause analysis
CIA	Change impact analysis
CMA	Common mode analysis
DA	Development assurance
DAL	Development assurance level
ECL	Electronic checklist
EICAS	Engine instrument and crew alerting system
FHA	Functional hazard assessment
FMEA	Failure modes and effects analysis
FTA	Fault tree analysis
IMA	Integrated modular avionics
IP	Issue paper
LRM	Line replaceable module
LRU	Line replaceable unit
MBD	Model-based design
MBSE	Model-based systems engineering
MIA	Modification Impact Analysis
MIT	Massachusetts Institute of Technology
NTSB	National Transportation Safety Board
NextGen	Next Generation Air Transportation System
OEM	Original equipment manufacturer
PA	Process assurance
PR	Problem report
S&MF	Single and multiple failure
SAVI	System Architecture Virtual Integration
SCD	Specification control drawing
SEE	Single event effects
SFHA	System functional hazard assessment
SME	Subject matter expert
SOS	System of systems
SSA	System safety assessment

T&E	Test and evaluation
TC	Type certification
UTC	Universal Coordinated Time
V&V	Validation and verification

EXECUTIVE SUMMARY

System architectures and associated requirements for aerospace digital avionics systems have accelerated in complexity and integration over the last two decades. Though initial generations of digital avionics automated individual functions were often standalone or limited with respect to integration with other airplane-level functions, today's complex avionics architectures can be highly integrated across complex systems.

Task Order 22 was issued by the FAA to examine possible relationships between requirements development and validation and verification (V&V) processes; identify the root causes of requirements errors, omissions, or conflicts; and to offer recommendations pertaining to potential solutions to the root causes.

This final report consolidates research completed on this task order to date, including findings and recommendations with requirements definition and V&V processes. Included in section 6 are recommendations pertaining to possible solutions to the root causes identified during the research.

The researchers solicited input from subject matter experts (SMEs) and evaluated eight scenarios for possible causes that might have contributed to requirements errors, omissions, and conflicts. The research also included reviewing industry guidance for possible gaps in requirements formulation and V&V for complex avionics architectures.

Findings from this research were summarized into four major root causes that suggest potential improvements and additions to industry guidance related to:

1. Incomplete, incorrect, or missing requirements
2. Incorrect implementation of otherwise correct requirements
3. Incomplete, inadequate change impact analysis
4. Incomplete, incorrect programmatic and technical planning

All four major root causes are discussed in detail in section 5.1.2. These categories served as the basis for a questionnaire issued to The Boeing Company and other industry SMEs to solicit recommendations on possible solutions to the root causes of the requirements errors, omissions, or conflicts. These recommendations are discussed in detail in section 6.3.

This report also includes, in section 8.2, recommendations for future research.

1. INTRODUCTION

During the last two decades, the complexity and integration of system architectures and associated requirements for aerospace digital avionics systems have increased. Though initial generations of digital avionics automated individual functions were often standalone or limited with respect to integration with other functions, today's complex avionics architectures are highly integrated across complex systems. Furthermore, emerging next-generation air traffic management systems are further integrating platform-level complex systems into a broader system of systems (SOS), where data are shared across aircraft and air traffic management resources without pilot/controller intervention. This evolution of increased complexity and integration has been noted by the FAA and industry alike. The purpose of this research effort was to examine possible relationships between requirements development; validation and verification (V&V) processes; identifying the root causes of requirements errors, omissions, or conflicts; and to offer recommendations on possible solutions to the root causes.

1.1 TASK BACKGROUND

Integrating complex systems has resulted in increased systems interdependence and integration.

Compelling questions before both industry and regulators include:

- What are commonly accepted industry guidelines and practices used in requirements capture, definition, refinement, and V&V processes?
- What does the trend of accelerated growth of systems' complexity mean to design and V&V practices?
- What changes are required in the approaches to address this trend?

The realization of this trend was one of the key drivers for the creation of the new Aerospace Recommended Practice (ARP) 4754 Revision A [1]. ARP4754 Revision New was originally developed in response to a request from the FAA to SAE International to define an acceptable development assurance (DA) process for highly integrated and complex avionics systems [2].

The issuance of ARP4754 Revision A provides industry with a framework that addresses the growth of increased integration and complexity. In addition, industry and regulators are considering further steps. This research highlights that ARP4754 Revision A can be improved with respect to the increased integration and complexity (section 5.1.2, table 1 in section 6.2, and section 6.3.2).

1.2 RESEARCH SCOPE

The scope of the research required answers to the questions listed in section 1.1 and involved reviewing real-world scenarios that focused on specific situations that actually occurred and issuing two questionnaires to subject matter experts (SMEs) on requirements and V&V issues.

In addition to analyzing these sources of information (real-world scenarios and questionnaires), analysis was conducted on the current state of industry process documents and practices to identify possible shortcomings and consider potential recommendations. Analysis was also conducted on the basis of the lessons learned that were gained from applying ARP4754 Revision New and ARP4754 Revision A on one type of certificate airplane program and four amended type certificate airplane programs; this included both original equipment manufacturer (OEM) and supplier perspectives.

Consideration for potential applicability of this research toward emerging next generation air traffic management systems is discussed in section 7.

1.3 RESEARCH APPROACH, ACTIVITIES, AND PRINCIPAL RESULTS

The research approach for this study was divided into three phases:

1. The Phase 1 research identified issues and shortcomings that contributed to incorrect or incomplete requirements definition and V&V processes and practices. Phase 1 research was documented in three white papers:

    a. White Paper 1 to identify adverse events in which requirements definition and V&V may have been, at a minimum, a contributing factor, as necessary to identify instances of requirements errors, omissions, or conflicts from commercial aviation (extracts located in section 3 and appendix A).
    b. White Paper 2 to identify and document requirements definition, V&V processes, and interfaces among the processes (extracts located in section 3 and appendix B).
    c. White Paper 3 to study the identified requirements definition, V&V processes, and interfaces to highlight the issues and shortcomings (extracts located in section 3 and appendix C).

2. The Phase 2 research classified and categorized Phase 1 issues and shortcomings along with root causes. Phase 2 research was documented in two additional white papers:

    a. White Paper 4 to classify and categorize issues and shortcomings identified in prior white papers (extracts located in section 4 and appendix).
    b. White Paper 5 to identify the root causes of the requirements errors, omissions, or conflicts (extracts located in sections 4 and 5 and appendices E and F).

3. The Phase 3 research identified recommendations and solutions to the root causes identified in Phase 2 [3]. Phase 3 content can be reviewed in sections 5, 6, and 8 and appendices G and H.

Phase 1 activities included a review of potential process issues and shortcomings via review of the following industry process documents:

- SAE International ARP4754A/EUROCAE ED-79A, “Guidelines for Development of Civil Aircraft and Systems,” December 21, 2010, covering DA processes [1].
- SAE International ARP4754/EUROCAE ED-79, “Certification Considerations for Highly Integrated or Complex Aircraft Systems,” 1996, covering DA processes [2].

- SAE International ARP 4761, “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems,” 1996, describing safety assessment processes [4].
- Document-178B/C (DO-178B/C), “Software Considerations in Airborne Systems and Equipment Certification,” RTCA, Inc., Washington, DC, 2001, covering software design assurance processes [5].
- DO-254, “Design Assurance Guidance for Airborne Electronic Hardware,” RTCA, Inc., Washington, DC, April 19, 2000, covering airborne electronic hardware design assurance processes [6].
- DO-297, “Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations,” RTCA, Inc., Washington, DC, November 8, 2005, covering integrated modular avionics [7].

In addition to the industry process documents reviewed above, Phase 1 research also included a review of available industry literature and related aircraft and safety information databases and requirements data discussions and industry committee participation. The selected sources of information were:

- Review of Boeing Commercial Airplanes (BCA) in-service data fleet service bulletins.
- Review of BCA product development flight squawks.
- Review of FAA Airworthiness Directives (ADs).
- Internal airplane safety events and information databases.
- Safety lessons learned.
- Discussions/meetings with BCA safety and requirements SME.
- SAE International S-18 committee participation, providing a valuable conduit for direct communication with industry and understanding the direction of these guidelines.

The principal results of the Phase 1 research identified the need to (1) clarify roles and responsibilities between OEM and suppliers, (2) work to a complete and correct set of requirements, (3) potentially identify and address process gaps in industry V&V guidance material, and (4) improve the V&V processes.

Phase 2 research included a questionnaire that was given to The Boeing Company SMEs to further broaden the research base completed in Phase 1. As outlined in sections 5.1–5.1.2 and appendix E, high-level questions were posed to obtain a broad basis of input across programs and suppliers. The principal results of Phase 2 research led to the identification of root cause categories:

- Incomplete, incorrect, or missing requirements
- Incorrect implementation of otherwise correct requirements
- Incomplete, inadequate change impact analysis
- Incomplete, incorrect programmatic and technical planning

Phase 3 research included a questionnaire that was given to Boeing and industry SMEs to solicit recommendations and solutions to the root causes identified in Phase 2. Additional information regarding the Phase 3 questionnaire is provided in sections 5.2–5.2.2 and appendix G.

The principal results of Phase 3 research led to solutions to the root cause categories listed above, including recommendations to improve:

- Understanding of the OEM and supplier interrelationships and roles and responsibilities with respect to DA.
- Cross-functional systems integration activities, which would help identify decomposed and derived integration requirements.
- Single and multiple failure (S&MF) analyses guidance.
- Change impact analysis.
- Technical planning, particularly related to process assurance (PA) reviews.
- Supplier risk assessments.
- Usage and extension of model-based systems engineering (MBSE).

Throughout all three phases, the research team used a multi-sourced/integrated approach to develop and identify findings.

2. AVIONICS EVOLUTION IMPACT ON REQUIREMENTS ISSUES AND VERIFICATION AND VALIDATION

Minimizing developmental errors and ensuring integration of highly integrated, safety-critical systems has become more challenging on several fronts—namely due to increasing system integration and increasing data-management complexity. There is generally universal recognition that systems are becoming more complex. In addition, integrating these complex systems with other complex systems results in increased interdependence and integration. As airplane systems have become more complex and interdependent, the challenge of building well-behaved systems becomes more difficult. Throughout most industries, system architectures have evolved to combine functionality from previously separate systems into integrated, software-intensive systems.

Examining the evolution of communications technologies provides informative comparisons regarding the evolution of complex digital aviation systems. Early versions of telegraph systems provided a seminal link to long distance communications over wire. Early wireless systems provided the ability to communicate by one-way transmitters/receivers (radios) and two-way transceivers. These systems evolved and later supported voice communication (telephone) and video communication (television). Early cellular technology provided a mobile telephone to those who could afford their cost. However, these technologies remained separate and were not integrated. Presently, single digital devices are available that combine all of these capabilities, and more, into a single smartphone that provides voice and text communications; on-screen video playback and recording; Global Positioning System services; and access to the Internet, all at a price that is well below that of early cell phones.

There has been a trend across most industries to combine functionality from previously separate physical systems into integrated systems. Though this is the case with the aviation industry, systems architecture evolution may not be as immediately obvious to the flying public. The Boeing 767 and 787 both serve the same middle market; both aircraft have a similar external appearance. However, the differences in their digital avionics architecture are as significant as the difference between early cell phones and today's smartphones.

The fundamental course of study for requirements definition and V&V addresses this dilemma by seeking to identify potential gaps in the current requirements formulation and V&V process for complex, digital systems.

To highlight the implications of architecture changes on the requirements process, aircraft such as the piston-engine Boeing 377 had systems that were functionally and physically separate. The 1949 flight deck of a Boeing 377 Stratocruiser represents a federated architecture. It was relatively easy for a single designer to define the interfaces. The integration effort was correspondingly simple. There were very limited cross-functional cascading effects, making failure behavior easier to understand. From an individual designer's perspective, it was relatively easy to design, validate, integrate, and test.

However, there were also some disadvantages to this design. It required significant effort for the crew to process the displayed information while maintaining situational awareness. The workload was so great that a third person was required to perform the navigation function so the pilots could focus on basic flight activities.

Modern aircraft that use complex digital systems, such as the Boeing 787, have increased functionality, performance, and integration. The 787 Dreamliner is an example of the latest flight deck evolution. It incorporates an IMA architecture and a distributed electrical power system architecture. Migrating to an IMA architecture and introducing more electrically powered systems helped improve performance and reduced overall airplane weight, but these design decisions also increased the importance of managing system interfaces. For the IMA architecture, airplane functions traditionally supported in a federated manner were now integrated on a common platform. The electrical system moved from a traditional centralized bus design to a remote distribution design. There are numerous advantages to this type of architecture, primarily in the increased functionality and performance of the aircraft. In this flight deck, it is much easier for the crew to maintain situational awareness. Examples of some of the integrated systems that allow for improved situational awareness and help create an easy-to-manage flight deck include:

- Weather radar
- Terrain collision avoidance
- Thrust management system
- Flight management system
- Heads-up displays

However, this integrated architecture drives a corresponding increase in complexity and cross-functional allocation. Interfaces tend to be defined by many inputs and outputs, resulting in increased integration efforts. Failure behavior can be more opaque, so the effort to understand cascading effects becomes very important. As shown in figure 1, airplanes with highly IMA architectures have measureable increases in complexity and integration, as is apparent by the number of interfaces or software lines of code. These data are for illustrative purposes only and do not represent actual aircraft.

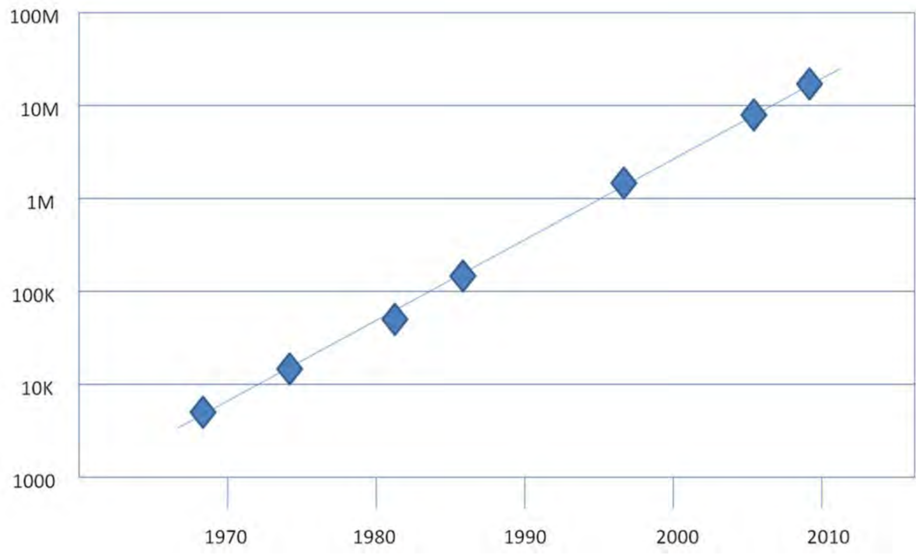


Figure 1. Notional large commercial passenger transport airborne software development (software lines of code by decade)

The requirements process for functionally and physically separated systems of federated airplanes may no longer apply to complex integrated airplanes. As system architectures have evolved to become more complex, integrated, and distributed, an increased focus on requirements development and V&V processes is suggested.

The increased integration, data traffic, and network intricacy associated with integrated avionics and distributed electrical power systems have costs related to complications in understanding the operational availability of system services and data flows. System behavior, particularly during system disturbances and failures, for federated architectures may be transparent and easily understood, but system behavior is not as apparent for complex, integrated systems. In a federated architecture, the failure of a component may result in isolated effects that rarely touch more than one or two systems. With highly integrated architectures, the failure of a single component can propagate to numerous systems and result in diverse failure effects. This increases the challenge of designing well-integrated systems and fully validating that safety is maintained throughout the operational environment.

A key part of understanding the requirements process for complex, integrated airplanes is to evaluate cross-functional interfaces and cascading failure effects. A failure in one system could result in some undesirable effects in another system, which, in turn, can lead to some undesirable effects in its integrated systems.

As aircraft architectures have evolved to IMA, many airplane functions that had been historically supported with federated (i.e., non-integrated) systems are now interrelated and highly integrated. Therefore, many system functions, which typically had been separated with limited interdependence, now are interrelated and highly integrated. The possibility exists that certain failure modes, which in a federated system may have had limited effect on other systems, may now have a cascading effect on other systems. There is a need to validate that failures do not have unintended, unacceptable cascading effects.

In addition to understanding the cascading effects and ensuring that an acceptable level of safety is maintained during degraded performance, how information is presented to the flight crew to ensure that they can take appropriate actions must be considered.

The FAA's Transport Airplane Issues List (TAIL) for "Unique Flight Deck Failure Modes and Effects" states, "Many system functions that were typically separated with limited interdependence are now very interrelated and highly integrated. Certain failure modes having a limited effect in federated systems may now have a cascading effect on other systems" [8]. This includes hypothetical instances of:

- Partial or complete failure of an IMA system causing significant cascading failure effects on numerous aircraft functions. Hypothetically, this could result in numerous, confusing, and at times unrelated Caution Advisory System (CAS) messages. There is a potential need for additional crew training to help recognize and deal with multiple failure indications and CAS messages because critical cascading failure indications, such as cabin depressurization (which requires prompt crew attention) may sometimes be buried among other failure indications.
- Loss of all displays due to an anomalous IMA process.
- Partial failure on two IMA systems (one channel of each unit), which could cause all primary flight deck displays to revert to a non-functional display presentation, forcing pilots to go to the standby flight displays.
- Uncommanded and inappropriate display reversions.
- Instances of simple failures (generator or engine loss), which could have a significant failure effect: disruption of power to a portion of the IMA architecture and loss of all displays on one side of the cockpit.
- Complete loss of CAS capability under certain failure scenarios.
- Complete loss of electronic checklist (ECL) capability under certain failure scenarios.
- ECL not robust enough to deal with certain complex, multiple-system cascading failure scenarios.
- Generation of unnecessary checklists in the ECL system during cascading failure scenarios, which could add to crew workload; often, each unnecessary ECL had to be either individually worked or individually overridden.
- Degraded braking performance during landing or a rejected takeoff because of how inertial deceleration data were handled by the IMA during certain failure scenarios.
- Failure of single elements of the electrical power distribution architecture potentially causing wholesale loss of sensor or system information and the removal of such information from the systems synoptic. In these hypothetical cases, certain aircraft systems may continue to operate, but any information pertaining to the health and performance of such systems was unavailable to the aircrew. In addition, in some hypothetical cases, secondary systems (e.g., aircraft pressurization) could be negatively affected, requiring the aircrew to take precautionary measures (e.g., descent to a safe altitude for pressurization).

3. SAFETY ISSUES WITH REQUIREMENTS DEFINITION, V&V PROCESSES

Phase 1 of this research study involved research of adverse events, V&V processes, and issues with requirements definition and V&V processes and involved the preparation of three white paper extracts, which can be found in appendices A, B, and C.

3.1 SUMMARY OF PHASE 1 WHITE PAPERS 1–3

White Paper 1 researched various information sources to identify adverse events in which the requirements definition and V&V may have been contributing factors. A number of potential candidates were evaluated and rejected because they did not meet specific criteria. Following this process, the research team recommended that the 2005 Malaysian Airlines 777 incident be used for further research.

White Paper 2 examined requirements, V&V processes, and interfaces among the processes. The findings from the research showed there are potential improvements in industry guidance related to the roles and responsibilities of the OEM and supplier related to requirements validation. In addition, there are potential process improvements to address cross-functional/systems architecture analyses from a highly integrated, distributed systems perspective. Furthermore, there is a potential need to improve industry guidance for both single system-level requirements and functional-level requirements.

White Paper 3 examined issues and shortcomings related to requirements definition, V&V processes, and interfaces especially in scenarios in which requirements were not properly validated or verified or requirements did not exist at all. The findings showed there may be room for process improvement in industry V&V guidelines related to horizontal and vertical integration at the airplane, intersystem, intrasystem, and component levels.

3.2 SUMMARY OF PHASE 1 FINDINGS

The following are the findings of Phase 1 of this research study:

- The 2005 Malaysian Airlines 777 incident has elements of cascading effects across multiple integrated systems that make it an excellent event for further research (White Paper 1 finding).
- Review of industry guidelines showed the importance of clearly establishing the DA roles and responsibilities between the OEM and the suppliers, particularly those related to requirements validation, to ensure a complete, correct set of requirements exists before beginning hardware and software design-assurance activities (White Paper 2 finding).
- It is possible that existing DA processes may not adequately address the cross-functional/systems architecture integration. Industry guidance potentially needs to be improved for the integration of distributed systems to address potential gaps in validation processes and identify missing requirements for highly integrated, distributed systems (White Paper 2 finding).

- Processes to validate single system-level and functional-level requirements are generally acceptable, but potential improvement is needed for pilot evaluation of the aircraft-level operation for single system-level and functional-level requirements (White Paper 2 finding).
- Potential improvement is needed in the industry process guidance for the validation of intersystem/cross-functional requirements at the subsystem-to-subsystem level, component-to-component level, and message-to-message level (White Paper 2 finding).
- The V&V processes at the component, intrasystem, intersystem, and airplane level may require improvements for horizontal and vertical integration (White Paper 3 finding).
- Existing processes to facilitate requirements validation for the modification of existing systems may have gaps (White Paper 3 finding).
- Existing processes may not address cumulative effects of otherwise acceptable individual systems-level cascading effects (White Paper 3 finding).

3.3 SUMMARY OF PHASE 1 RECOMMENDATIONS

The research conducted in Phase 1 led to the following recommendations:

1. The research team recommended that the Malaysian Airline 777 pitch-up incident (summarized in White Paper 1) be used for further review, along with the additional scenarios evaluated as part of White Paper 3.
2. Investigate processes to help identify missing requirements during the requirements validation phase (summarized in White Paper 2).
3. Examine processes to ensure that OEMs and suppliers are working toward a complete and correct set of requirements to the greatest practical extent (summarized in White Paper 2).
4. Consider the potential need to clarify roles and responsibilities between OEMs and suppliers regarding the transition from DA activities to design assurance activities (summarized in White Paper 2; Note: It is recognized that this clarification will vary based on the different business models).
5. Identify potential gaps that may exist with processes to validate requirements for both single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation (summarized in White Paper 2).
6. Consider establishment of an approach to validate and verify intrasystem functionality to determine whether proper function, content, and performance exist. Include consideration of aircraft-level failure modes and effects (summarized in White Paper 2).
7. Investigate the potential need to improve horizontal and vertical integration for V&V processes at the component, intrasystem, intersystem, and airplane level (summarized in White Paper 3).
8. Investigate potential process improvements to facilitate requirements validation for the modification of existing systems (summarized in White Paper 3).
9. Consider potential process improvements to address cumulative effects of otherwise acceptable individual systems-level cascading effects (summarized in White Paper 3).

4. PROBLEMS, ISSUES, SHORTCOMINGS, AND ROOT CAUSE DETERMINATION

This section summarizes root causes derived from Phase 2 research addressing requirements issues and shortcomings found on Phase 1. Phase 2 results were originally documented in White Papers 4 and 5, extracts of which can be found in appendices D, E, and. Also, a portion of White Paper 5 addressed information solicited from Boeing SMEs via a questionnaire; this information is addressed in sections 5.1–5.1.2 and appendix E.

4.1 SUMMARY OF WHITE PAPERS 4 AND 5

White Paper 4 classified and categorized identified issues and shortcomings from work completed in Phase 1. This research developed detailed research findings for each of the eight scenarios reported on in White Paper 3. Additionally, a matrix of each scenario tabulated against possibilities—complexity, organization, planning, publications, schedules, experience, V&V, and integration—that could have contributed to shortcomings was developed.

White Paper 5 determined root causes of requirements errors, omissions, or conflicts to requirements issues and shortcomings. Four major root cause categories were identified, as listed in section 4.2.

4.2 SUMMARY OF PHASE 2 FINDINGS

The research involved two approaches: (1) input from Boeing SMEs was solicited and the eight scenarios outlined in Phase 1 were evaluated for possible causes that might contribute to requirements errors, omissions, and conflicts; and (2) the research approach also included reviewing industry guidance for possible gaps in requirements formulation and V&V for complex avionics architectures. From this research, four major categories were identified as root causes:

1. Incomplete, incorrect, or missing requirements.
2. Incorrect implementation of otherwise correct requirements.
3. Incomplete, inadequate change impact analysis.
4. Incomplete, incorrect programmatic and technical planning.

Additional information regarding these root causes is provided in section 5.1..

The principal findings of Phase 2 research emphasized the importance of having validated, complete, and correct requirements and recognizing the iterative nature of requirements V&V.

4.3 SUMMARY OF PHASE 2 RECOMMENDATIONS

The Phase 2 report also identified the following candidate areas for improvement of requirements issues in Phase 3.

1. Analyze existing industry processes and issue a questionnaire to industry committee members responsible for guidelines associated with V&V of highly integrated, complex digital systems:

    a. Identify existing industry guidelines for requirements definition, V&V processes, systems integration, and change impact analysis.
    b. Identify potential shortcomings in current processes, particularly related to Section 4.6.4 (Aircraft/System Integration) and Section 6 (Modifications to Aircraft or Systems) of ARP 4754A.
    c. Identify integral systems integration process gaps related to safety that are not currently part of ARP4754/ARP4754A and ARP4761.
    d. Identify common errors that occur in the interrelationships between process steps in ARP4754A, DO-178, DO-RTCA/DO-331 [9], DO-254, DO-297, and Aerospace Vehicle System Institute (AVSI) report Authorization for Expenditure 75 [10], particularly those that could result in incomplete and incorrect requirements/systems integration issues. AVSI's System Architecture Virtual Integration (SAVI) project may also provide source material.

2. Conduct analysis on process execution problems:

    a. Issue a questionnaire to Boeing's SMEs, including those who have work experiences as Authorized Representative (AR) advisors and ARs. The SMEs will have experiences across multiple programs, multiple design disciplines, and multiple suppliers.
    b. Identify potential gaps in the development/design assurance processes.
    c. Analyze integration-related problem reports (PRs) and determine root causes.
    d. Investigate how a model-based design (MBD) approach could mitigate integration and safety issues for process execution problems:

        i. Identify how MBSE can help force early and continuous integration of requirements through the architecture selection and system design to the left of the systems engineering V.
        ii. Recognizing that simulations that model a system may not be accurate in every situation and function that it contains; identify how accurate the modeling has to be and how its accuracy can and should be determined.

3. Analyze and identify how change impact analyses need to be modified as systems transition from federated to highly integrated, distributed systems:

   a. Analyze PRs where change impact analysis may have allowed for gaps that became apparent in subsequent V&V efforts. Conduct root cause analysis and determine whether improvements are required for guideline standards.
   b. Evaluate potential safety implications if change impact analysis is not thoroughly conducted for complex, highly integrated digital systems.
   c. Investigate how an MBD approach could mitigate integration and safety issues for change impacts:

      i. Identify how MBSE models should be formulated and maintained to ensure they change to achieve the required fidelity, change as the system changes to maintain this fidelity, and provide insight into both successes and failures of the system to meet requirements, help refine requirements, or identify missing requirements.

4. Analyze evolution of OEM-supplier relationship over multiple programs:

   a. Review whether level of supplier oversight changed over time or level of supplier oversight remained the same but integration/complexity increased.
   b. Analyze how required supplier DA activities are documented, communicated, and audited by the OEM.
   c. Analyze and identify characteristics that can be used to determine supplier and vendor expertise.
   d. Analyze validity of assumption that requirements allocated to the software and airborne electronic hardware (AEH) items are correct and complete, which makes it very important to ensure that both the OEM and the supplier understand their DA roles and responsibilities, particularly those related to requirements validation.
   e. Analyze risk assessment for outsourcing.
   f. Investigate how an MBD approach could mitigate integration and safety issues for OEM/supplier relationships.

5. QUESTIONNAIRES

Research for Phase 2 addressed classification and categorization of identified issues and shortcomings from Phase 1 and addressed determination of associated root causes of the requirements issues and shortcomings. These results are included in appendices D and E. To broaden the results obtained in Phase 1, additional research was conducted through questionnaire input from SMEs to identify potential problems with current requirements development and V&V processes. Results of this questionnaire are provided in sections 5.1–5.1.2 and appendix E.

Taken together, these two basic research approaches have distinct differences:

1. The real-world scenario evaluation was focused on specific situations that actually occurred, which made it less definitive for basing additional work on mitigations. The approach of starting with major accidents and incidents and tracing back to the cause in requirements does not identify all requirements issues and shortcomings, nor does it necessarily identify useful solutions to these issues and shortcomings.
2. To gather a broader basis for analysis, the research team issued two questionnaires to SMEs: the first (issued in Phase 2) solicited input on potential problems with current requirements development and V&V processes; the second (issued in Phase 3) solicited input on recommendations for possible solutions to the root causes of the requirements errors, omissions, or conflicts.

As opposed to specific situations, the SME solicitation approach is based on broad experiences across multiple programs and design disciplines, making it more definitive for basing additional work on mitigations. It is of significant value that highly experienced avionics systems engineers evaluated real-world occurrences of operational aircraft/system impacts that may be based on requirements issues and also provided concepts for improving future requirements engineering and V&V tools, techniques, and processes to be considered for future aircraft/systems development, certification, operation, and maintenance.

The research approach for Phase 3 was to use a second questionnaire that solicited SME recommendations to address root causes and additional or improved standards/guidance needed. Results of this questionnaire are provided in sections 5.2–5.2.2, and appendix G.

5.1 QUESTIONNAIRE USED IN PHASE 2

5.1.1 Approach

The Phase 2 questionnaire solicited input from ten Boeing SMEs, each possessing decades of experience, to identify:

- Where current requirements development and V&V processes are breaking down.
- What possibilities might cause or contribute to requirements errors, omissions, and conflicts.
- Why problems with digital systems requirements for aircraft continue to occur.

Additional information for analysis was provided by the SMEs in the areas of:

- Software (those with experience as ARs).
- AEH (those with experience as ARs).
- Boeing enterprise designated experts in requirements management.
- Flight tests.

All of the people who received the questionnaire have more than 20 years of experience in the aviation industry working on multiple programs. The people were selected based on their experiences working with flight-critical systems (flight controls, IMA, etc.) and their knowledge of typical problems encountered related to requirements V&V. Each SME has experience across multiple programs and suppliers.

Based on decades of experience from SMEs, multiple PRs from different programs with differing system architectures were considered to inform their responses to the questionnaire. The information is summarized to reflect trends, similarities, or commonalities among the SME responses.

The questionnaire included several questions leading to the identification of possible root causes for requirements errors, omissions, and conflicts. Appendix E shows the questionnaire sent to SMEs for this exercise.

5.1.2 Root Causes Identified for Recommendation

Four major categories were identified as root causes, which are primarily driven by the complexity associated with highly integrated architectures. Overall, this suggested a potential area for improvement with regard to additional industry guidance related to helping ensure a complete and correct set of requirements:

1. Incomplete, incorrect, or missing requirements. A problem area with digital systems design and development are requirements that are incomplete (requirement is not fully specified for nominal and off-nominal conditions), incorrect (requirement is not specified correctly), or missing (requirement does not exist). Examples for each of these were discussed in this report (discussion of these scenarios is provided in appendices C and D):

   a. Incomplete requirement: Scenario #5 addressed a requirement that was correct for normal operation, but did not completely consider related failure conditions.
   b. Incorrect requirement: Scenario #1 addressed an incorrect requirement for transition time for a handshake between two systems.
   c. Missing requirement: Scenario #3 addressed a missing requirement for required initialization of latches, counters, and inputs that were not specified for an in-flight power-up process.

   The following were identified as potential improvements to address root causes contributing to incomplete, incorrect, or missing requirements:

   a. Improved understanding of the integration of new technologies, particularly with respect to timing (e.g., latency and jitter).
   b. Improved clarification of the process handoffs between ARP4754A DA activities and DO178B/C and DO254 activities, particularly the roles and responsibilities between the OEM and supplier. This includes single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.
   c. Improved understanding of requirements in light of potential failure conditions/unexpected pilot actions.

d. Improved systems integration focus leading to prevention of requirements conflict between systems/subsystems boundaries.
e. Improved systems integration focus leading to cumulative effects of otherwise acceptable individual systems-level cascading effects.
f. Improved validation of interfaces between systems commensurate with the inevitable evolutionary nature of this complex problem.
g. Improved validation of the assumptions concerning the environment. As necessary, assumptions are included as part of the requirements definition. In addition, key safety assumptions can be documented in the respective systems' safety analyses and as requirements. In addition, it can be helpful to include an "assumption/rationale" field to facilitate assumptions documentation when required.
h. Improved process training to help validate requirements completeness and correctness.

2. Incorrect implementation of otherwise correct requirements. Another problem area with digital systems design and development are requirements that are not correctly implemented. One example is when a software developer incorrectly implements a requirement in their code. Scenario #2 addressed an incorrect translation of a correct requirement for an incorrect implementation of a (+/-) sign—a convention for a control-law summing junction.

   The following were identified as potential improvements to address root causes contributing to incorrect implementation of otherwise correct requirements:

   a. Improved process to detect software implementation bugs. (Note: This does not address incorrect requirements; it addresses incorrect implementation of correct requirements. The existing processes are robust at identifying software bugs, but there is always room for improvement.)
   b. Improved implementation of the software and AEH development guidance contained in DO-178/DO-254.

3. Incomplete, inadequate change impact analysis. A third problem area with digital systems design and development deals with interface considerations for changes made to a system that integrates to other systems. Scenario #8 addressed an inadequate analysis of impacts of one system's change on other interfacing systems.

   The following was identified as a potential improvement to address root causes contributing to incomplete, inadequate change impact analysis:

   a. Improved consideration of integration aspects when developing a problem solution, particularly for new, novel, and/or complex systems and new environments.
   b. Improved industry guidance to facilitate requirements V&V for the modification of existing systems. This research highlights that ARP4754A can be improved with regard to the increased integration and complexity.

4. Incomplete, incorrect programmatic and technical planning. A fourth problem area addresses incomplete or incorrect programmatic and technical planning with respect to the V&V of digital systems design and development. One important example is thorough test planning, in which the test team ensures that adequate fidelity and detail exists to fully test both nominal and off-nominal conditions. Examples of ways to help mitigate incomplete, incorrect planning include:

   a. Programmatic and contractual plans that address the roles, responsibilities, and accountabilities at OEM and supplier levels.
   b. Systems engineering plans that set forth the approach for managing systems engineering activities, which can include requirements management; design processes and reviews; and requirements V&V activities.
   c. Requirements V&V plans that address processes and approaches to (1) validating that requirements are complete and correct and (2) verifying that the design meets the validated requirement. For example, the verification plans often include a requirements matrix that identifies what method(s) of verification will be used (e.g., inspection, review, analysis, similarity, demonstration, and test).
   d. Test plans that address required tests at the software, subsystem, system, and vehicle level. These typically include both lab and flight test plans and specifying objectives, initial/final conditions, procedures, and pass/fail criteria.

   The following were identified as potential improvements to address root causes contributing to planning:

   a. Recognizing the inherently iterative nature of development, including schedule provisions for planning refinement, development, design changes, and V&V refinement for complex, integrated systems.
   b. Optimizing level of detail for development of plans in a disciplined fashion.
   c. Optimizing level of technical oversight to ensure plans are executed in a disciplined fashion.
   d. Developing optimum level of fidelity in highly integrated lab testing equipment and test procedure completeness to accelerate learning and reduce cost of problem discovery on the aircraft.
   e. Providing a uniform definition and training approach regarding what constitutes validation and what the expectations are at each phase of the design. Without having this in place, it is possible for varying levels of coverage and rigor during reviews, analysis, and testing. In light of the growth of complexity and integration, there is a need to migrate to an integrated solution.
   f. Looking to the future, as designs grow in complexity, consider prototyping to help with validating the completeness and correctness of requirements against preliminary system architectures. The prototyping process can augment the peer review process, which will remain necessary. Prototype tools can include MBD, simulation, and simulated distributed tests, particularly for integrating across multiple systems.

g. Having a systems integration organization that will proactively coordinate and validate that there is an integrated solution. Additionally, this system integration organization would lead efforts to ensure technical adequacy of requirements definition/validation, architecture refinement, interface control specification revision, and requirements verification plans as they are revised during the course of iterative development.

5.2 QUESTIONNAIRE USED IN PHASE 3

5.2.1 Approach

To gather data that addressed root causes and additional or improved standards/guidance, a follow-on questionnaire was issued to experienced Boeing and industry avionics systems SMEs. The industry SMEs are members of the SAE International S-18 safety committee and have practical experiences applying ARP4754A. Seven Boeing SMEs and three industry SMEs responded. This questionnaire was organized via the four major root-cause categories identified in Phase 2:

1. Incomplete, incorrect, or missing requirements.
2. Incorrect implementation of otherwise correct requirements.
3. Incomplete, inadequate change impact analysis.
4. Incomplete, incorrect programmatic and technical planning.

The questionnaire included several questions leading toward the identification of possible root causes for requirements errors, omissions, and conflicts.

Appendix G provides the questionnaire sent to SMEs for this exercise and the tabulated results.

5.2.2 Recommendations to Address Root Causes

The findings and results identified four different areas for potential improvement in industry guidelines:

1. Improving the cross-functional systems integration activities, which would help identify decomposed and derived integration requirements.
2. Improving S&MF analyses guidance.
3. Improving change impact analysis.
4. Improving technical planning, particularly related to PA reviews.

6. RESEARCH TO DETERMINE RECOMMENDATIONS TO ROOT CAUSES

During Phase 3 of this research, recommendations to address possible issues and shortcomings with the commercial aviation industry’s processes for digital system requirements definition and V&V were identified.

6.1 APPROACH

In addition to the recommendations obtained from the Phase 3 questionnaire, the research results were informed from the lessons learned from practical experiences of applying ARP4754 Rev New and ARP4754A on one type of certificate program and four amended types of certificate airplane programs.

The following resources were leveraged during this research:

- Communication with over 70 ARs (system, software, and AEH).
- Communication with safety and system engineering SMEs implementing DA on multiple programs.
- Communication with suppliers on required DA aspects (particularly related to requirements).

Phase 3 research was conducted along the recommended steps identified at the conclusion of Phase 2 (Section 4.3):

1. Analyze existing industry processes and issue a questionnaire to industry committee members responsible for guidelines associated with V&V of highly integrated, complex digital systems.
2. Conduct analysis on process execution problems.
3. Analyze and identify how change impact analyses need to be modified as systems transition from federated to highly integrated, distributed systems.
4. Analyze evolution of OEM-supplier relationship over multiple programs.

6.2 FINDINGS AND RESULTS

The findings and results identified seven areas in industry guidelines, with the potential to improve:

1. Understanding of the OEM and supplier interrelationships and roles and responsibilities with regard to DA.
2. Cross-functional systems integration activities, which would help identify decomposed and derived integration requirements.
3. S&MF failure analyses guidance.
4. Change impact analysis.
5. Technical planning, particularly related to PA reviews.
6. Supplier risk assessments.
7. Usage and extension of MBSE.

Table 1 contains a mapping of the root causes to the seven findings listed above. Specific recommendations to address the findings are contained in section 6.3.

Table 1. Phase 3 root causes to findings

	OEM and Supplier Development Assurance Responsibilities	Cross-Functional Systems Integration	Single and Multiple Failures	Change Impact Analysis	Technical Planning–Process Assurance Reviews	Supplier Risk Assessment	Model-Based Systems Engineering
Incomplete, Incorrect, or Missing Requirements							
Improved understanding of the integration of new technologies, particularly with respect to timing (e.g., latency and jitter).		X		X			X
Improved clarification of the process handoffs between ARP4754A DA activities and DO178 and DO254 activities, particularly the roles and responsibilities between the OEM and supplier. This includes single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.	X				X		X

Table 1. Phase 3 root causes to findings (continued)

	OEM and Supplier Development Assurance Responsibilities	Cross-Functional Systems Integration	Single and Multiple Failures	Change Impact Analysis	Technical Planning–Process Assurance Reviews	Supplier Risk Assessment	Model-Based Systems Engineering
Incomplete, Incorrect, or Missing Requirements (continued)							
Improved understanding of requirements in light of potential failure conditions/unexpected pilot actions.			X				X
Improved systems integration focus, leading to prevention of requirements conflict between systems/subsystems boundaries.		X		X			X
Improved systems integration focus, leading to cumulative effects of otherwise acceptable individual systems-level cascading effects.	X	X	X	X			X

Table 1. Phase 3 root causes to findings (continued)

	OEM and Supplier Development Assurance Responsibilities	Cross-Functional Systems Integration	Single and Multiple Failures	Change Impact Analysis	Technical Planning–Process Assurance Reviews	Supplier Risk Assessment	Model-Based Systems Engineering
Incomplete, Incorrect, or Missing Requirements (continued)							
Improved validation of interfaces between systems commensurate with the inevitable evolutionary nature of this complex problem.		X					X
Improved validation of the assumptions concerning the environment.				X			X

Table 1. Phase 3 root causes to findings (continued)

	OEM and Supplier Development Assurance Responsibilities	Cross-Functional Systems Integration	Single and Multiple Failures	Change Impact Analysis	Technical Planning–Process Assurance Reviews	Supplier Risk Assessment	Model-Based Systems Engineering
Incomplete, Incorrect, or Missing Requirements (continued)							
Improved training to help validate requirements completeness and correctness.	X	X	X	X	X	X	X
Incorrect Implementation of Otherwise Correct Requirements							
Improved process to detect software implementation bugs. Note: This does not address incorrect requirements; it addresses incorrect implementation of correct requirements. The existing processes are robust at identifying software bugs, but there is always room for improvement.	Further research determined this not to be a DO-178 factor.						

Table 1. Phase 3 root causes to findings (continued)

	OEM and Supplier Development Assurance Responsibilities	Cross-Functional Systems Integration	Single and Multiple Failures	Change Impact Analysis	Technical Planning–Process Assurance Reviews	Supplier Risk Assessment	Model-Based Systems Engineering
Incorrect Implementation of Otherwise Correct Requirements (continued)							
Improved understanding and implementation of the software and AEH development guidance contained in DO-178/DO-254.	X Note: This only covers the handoff to DO-178/ DO-254.				X Note: This only covers the handoff to DO-178/ DO-254.		
Incomplete, Inadequate Change Impact Analysis							
Improved consideration of integration aspects when developing a problem solution, particularly for new, novel, and/or complex systems and new environments.				X			X

Table 1. Phase 3 root causes to findings (continued)

	OEM and Supplier Development Assurance Responsibilities	Cross-Functional Systems Integration	Single and Multiple Failures	Change Impact Analysis	Technical Planning–Process Assurance Reviews	Supplier Risk Assessment	Model-Based Systems Engineering
Incomplete, Inadequate Change Impact Analysis (continued)							
Improved industry guidance to facilitate requirements V&V for the modification of existing systems. This research highlights that ARP4754A can be improved with respect to the increased integration and complexity.				X			
Incomplete, Incorrect Programmatic and Technical Planning							
Recognizing the inherently iterative nature of development, including schedule provisions for planning refinement, development, design changes, and V&V refinement for complex, integrated systems.					X		X

Table 1. Phase 3 root causes to findings (continued)

	OEM and Supplier Development Assurance Responsibilities	Cross-Functional Systems Integration	Single and Multiple Failures	Change Impact Analysis	Technical Planning–Process Assurance Reviews	Supplier Risk Assessment	Model-Based Systems Engineering
Incomplete, Incorrect Programmatic and Technical Planning (continued)							
Optimizing level of detail for development of plans in a disciplined fashion.					X		
Providing a uniform definition and training approach pertaining to what constitutes validation and what the expectations are at each phase of the design. Without having this in place, it is possible for varying levels of coverage and rigor during reviews, analysis, and test. In light of the growth of complexity and integration, there is a need to iterate to an integrated solution.					X		

Table 1. Phase 3 root causes to findings (continued)

	OEM and Supplier Development Assurance Responsibilities	Cross-Functional Systems Integration	Single and Multiple Failures	Change Impact Analysis	Technical Planning–Process Assurance Reviews	Supplier Risk Assessment	Model-Based Systems Engineering
Incomplete, Incorrect Programmatic and Technical Planning (continued)							
Looking to the future as designs grow in complexity, consider modeling to help with validating the completeness and correctness of requirements against preliminary design architectures. The prototyping process can augment the peer review process, which will remain necessary. Tools can include MBD/system engineering, simulation, and simulated distributed tests, particularly for integrating across multiple systems.[1]							X

[1] MBSE is already being used in a way that does not require new guidance. The need for new guidance should be evaluated based on future emerging MBSE developments. This new guidance may subsume the improvements made to existing guidance to handle integration concerns.

6.3 RECOMMENDATIONS ON SPECIFIC CHANGES TO ADDRESS AND MITIGATE IDENTIFIED ROOT CAUSES FOR REQUIREMENTS ISSUES AND SHORTCOMINGS

This section provides recommendations on how to address the root causes for requirements issues and shortcomings.

6.3.1 Establishing OEM and Supplier DA Roles and Responsibilities

Existing industry guidelines address requirements definition, validation, and verification. Figure 2 illustrates the flow of data between safety assessment processes covered by ARP4761, DA processes covered by ARP4754, and design assurance processes covered by DO-178, DO-254, and DO-297 when an IMA architecture is included in the design.

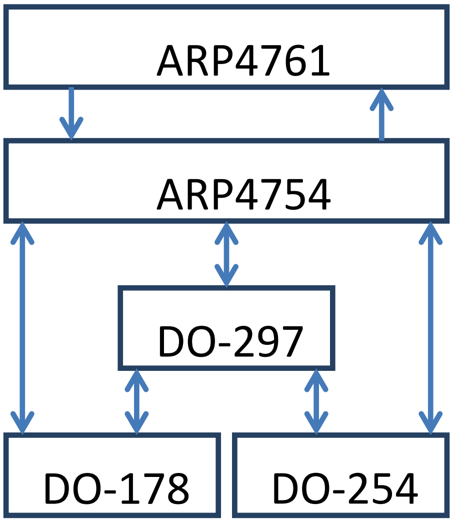


Figure 2. Interrelationships among processes

In addition, the FAA has issued four Advisory Circulars (AC) that define industry guidelines as acceptable means of compliance to the policies (see table 2).

Table 2. Advisory circulars and industry guidelines

Advisory circular	Industry guideline
AC20-174	ARP4754A
AC20-170	DO-297
AC20-115C	DO-178C
AC20-152	DO-254

However, based on lessons learned, it is important to clearly establish the required DA work between the OEM and the supplier; it should not automatically be assumed that a supplier has no DA work statement.

Figure 3 provides a method designed to determine whether a supplier has a DA work statement.

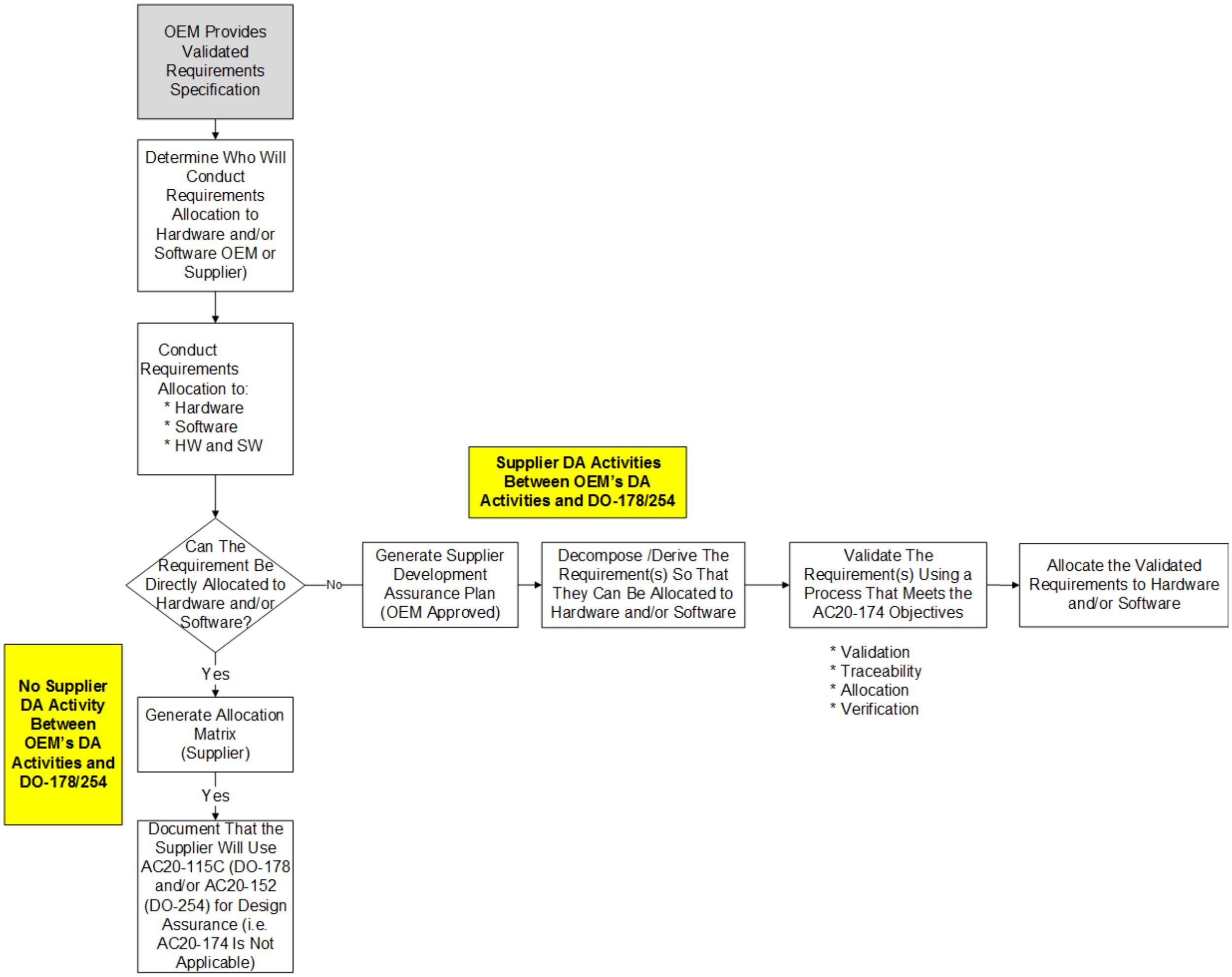

OEM Provides Validated Requirements Specification
Determine Who Will Conduct Requirements Allocation to Hardware and/or Software OEM or Supplier)
Conduct Requirements Allocation to:
* Hardware
* Software
* HW and SW
Can The Requirement Be Directly Allocated to Hardware and/or Software?
No
Yes
Supplier DA Activities Between OEM's DA Activities and DO-178/254
Generate Supplier Development Assurance Plan (OEM Approved)
Decompose /Derive The Requirement(s) So That They Can Be Allocated to Hardware and/or Software
Validate The Requirement(s) Using a Process That Meets the AC20-174 Objectives
* Validation
* Traceability
* Allocation
* Verification
Allocate the Validated Requirements to Hardware and/or Software
No Supplier DA Activity Between OEM's DA Activities and DO-178/254
Generate Allocation Matrix (Supplier)
Yes
Document That the Supplier Will Use AC20-115C (DO-178 and/or AC20-152 (DO-254) for Design Assurance (i.e. AC20-174 Is Not Applicable)

Figure 3. Supplier DA determination

It is common for a supplier to define one or more hierarchical levels of allocated requirements to provide the decomposition or derivation of OEM-provided requirements into (1) software requirements that are appropriate inputs to DO-178 software development and (2) hardware requirements that are appropriate inputs to DO-254 hardware design. If the supplier is required to perform further requirement decompositions/derivations from the OEM-provided specification control drawing (SCD) requirements to allocate to hardware and software, then the supplier is working between the OEM's DA activities and DO-178/254.

As shown in figure 3, the OEM and supplier should decide who will review the OEM-provided requirements specification and, as required, allocate the requirements to hardware and software. If the requirements can be directly allocated to hardware/software, then there is no additional supplier DA activity between the OEM's DA activities and DO-178/254 activities. An artifact that captures the requirements allocation should be created.

If the OEM-provided specification requirements need to be decomposed or derived prior to being allocated to DO-178 Software Development and DO-254 Airborne Electronic Hardware design, there is supplier DA activity within the scope of AC 20-174. In this case, the supplier should develop necessary plans and processes to meet DA process objectives defined in ARP4754A. These plans and processes, and the artifacts from the processes, should be available to the OEM for review and oversight.

Supplier activities that are within the scope of DA should have processes that meet ARP4754A objectives. It is recommended that the supplier provide a matrix to map their processes to the objectives listed in table A-1 of ARP4754A. This mapping should be part of the planning document.

Listed below are the processes the supplier should provide to show they are meeting the ARP4754A objectives:

- Requirements management process, including traceability and allocation processes
- Requirements validation process
- Requirements verification process
- Safety analysis process
- Configuration control processes (for DA data)
- Change management process (covering change impact and regression analysis)
- Problem reporting process
- PA (audit/assessment process to verify adherence to the processes)

A list of DA data that is typically used to show that the ARP4754A objectives are met is provided below. The list is provided as guidance only; suppliers should work with the OEM to tailor this list considering the scope of the project. The data list is derived from ARP4754A table A-1. To meet ARP4754A objectives and show compliance with certifications requirements, this data should be available for review by the OEM, as applicable. The purpose of the OEM review is to confirm that an adequate DA process is used by the supplier and ensure that the allocated functions and associated requirements are completely and correctly implemented:

- System development planning documents
- Supplier system requirements documents or database
- Supplier system description document
- Requirements traceability data (parent-child relationship between requirements)
- Requirements allocation matrix
- Safety analysis
- Requirements validation evidence including validation matrix
- Requirements verification procedure
- Requirements verification results, including verification matrix
- PRs
- Configuration management records (including change impact and regression analysis)
- Evidence of PA
- Accomplishment summary

6.3.2 Cross-Functional Systems Integration

ARP4761 describes the required safety analyses, which comprise an important source of derived safety requirements. The following can result in incorrect, incomplete, or missing safety derived requirements:

- Required safety analysis not completed.
- Safety analysis incorrectly completed.
- Safety analysis correctly completed, but derived safety requirements not captured and communicated to design team.

As airplane systems architectures become more integrated, it becomes increasingly important to validate that the integration requirements are correct and complete. However, ARP4754A Section 4.6.4, “Aircraft/Systems Integration,” does not adequately cover the required systems integration activities, particularly the analyses required to ensure that systems are truly integrated. As a result, this increases the likelihood that integration requirements may not be captured. When these higher-level integration requirements are either incomplete or incorrect, they can sometimes manifest themselves as what originally appear to be software or AEH problems.

As shown in figure 4, the systems integration analyses should occur at multiple levels:

- Airplane level−Address integrated behavior and performance for selected airplane functions or scenarios involving multiple airplane functions. The functions and scenarios may be assessed in routine states. These airplane-level analyses address significant airplane functions that span multiple line replaceable units (LRUs) and subsystems (e.g., power up).
- Intersystem−Address system-to-system interfaces in the nominal and failure scenarios.
- Intrasystem−Address how each system meets all of its interfaces, performance, and functional requirements. The intrasystem analyses examine the interfaces between LRUs in the same system to ensure proper systems operation.

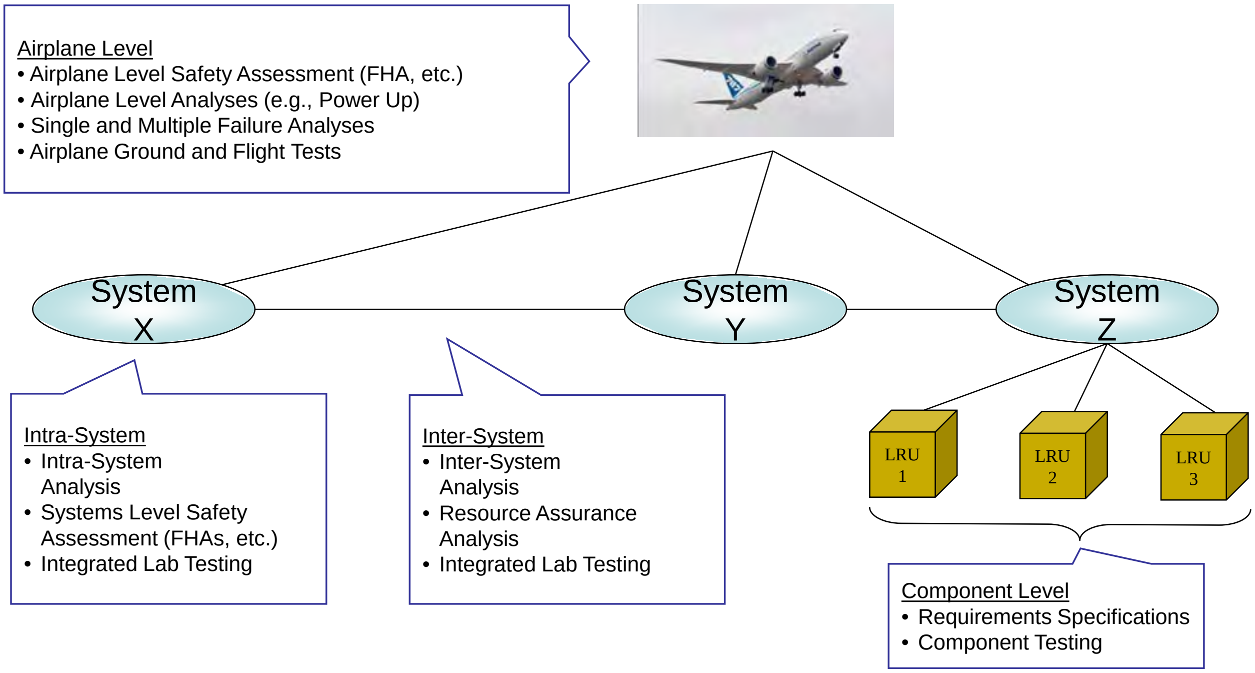

Airplane Level
• Airplane Level Safety Assessment (FHA, etc.)
• Airplane Level Analyses (e.g., Power Up)
• Single and Multiple Failure Analyses
• Airplane Ground and Flight Tests
System X
System Y
System Z
Intra-System
• Intra-System Analysis
• Systems Level Safety Assessment (FHAs, etc.)
• Integrated Lab Testing
Inter-System
• Inter-System Analysis
• Resource Assurance Analysis
• Integrated Lab Testing
LRU 1
LRU 2
LRU 3
Component Level
• Requirements Specifications
• Component Testing

Figure 4. Systems integration analysis

The systems integration analysis helps fill in the "missing middle" of the standard V&V chart, as shown in figure 5. The left side of the "V" chart deals with requirements development and validation. Validation is the process for ensuring the requirements are complete and correct. The right side of the "V" chart deals with integration and verification. Verification is the process for ensuring the design meets the requirements.

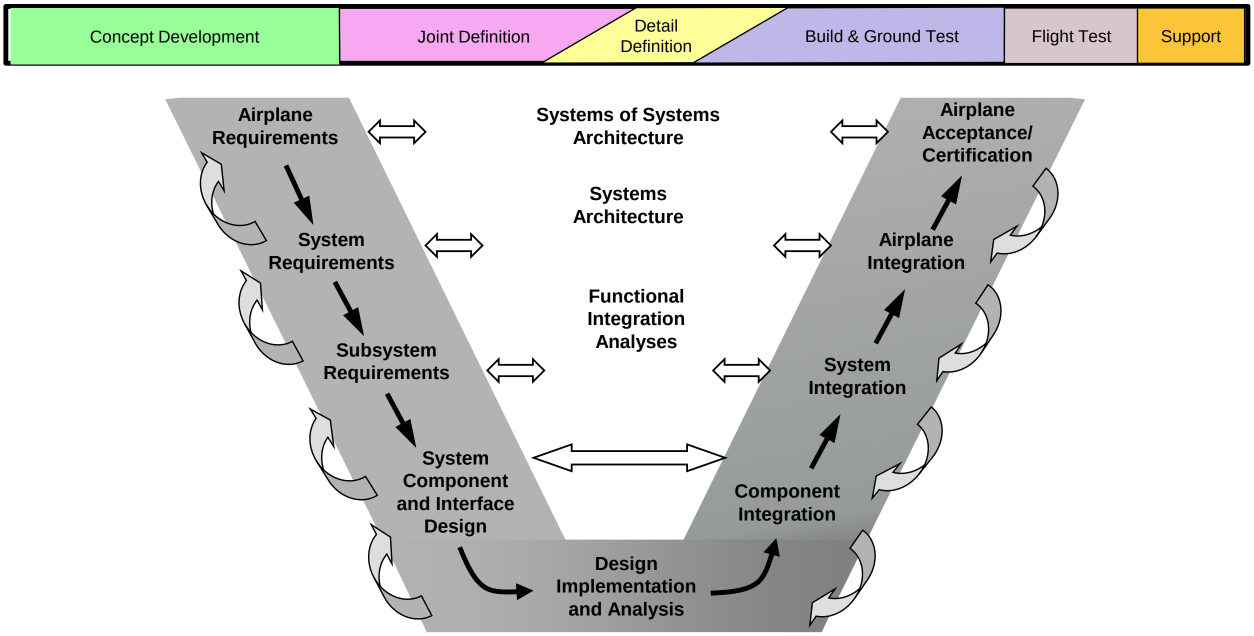


Figure 5. V&V

The high-level requirements are decomposed and allocated in a top-down manner and validated at successively lower levels of detail. For example, airplane-level requirements, such as payloads and range, are decomposed into lower-level system requirements, which are decomposed further into subsystem and component requirements. Parent or child traceability is established between each level of the requirements. The requirements are eventually decomposed to a level that drives system component and interface design. This is a recursive, iterative process. In addition to the “top-down” decomposition, there is a corresponding “bottom-up” validation.

Requirements, in and of themselves, are not the end goal. The end goal is to ensure that the delivered product is going to meet or exceed the customer, safety, and certification requirements. This is achieved by ensuring that the functions that have to be implemented (functional requirements), how well they have to perform (performance requirements), under what constraints—such as design specifications or allowable material (design requirements)—and how the equipment is supposed to interface with other equipment (interface requirements) are known.

The verification side is accomplished in a “bottom-up” manner, as shown on the right side of figure 5, starting with item-level component verification. The components are verified to individually meet their requirements. The next step is to verify that the components perform as expected within the given system, followed by verification that the item-level components perform as expected across the system. The final step is to ensure that the airplane performs as expected and meets the airplane-level requirements.

Conducting the intrasystem, intersystem, and airplane-level analyses help ensure that the airplane meets its requirements, performs its intended function, and works with no anomalous behavior.

As shown in figure 6, the relationships between the “phase” analyses are as follows:

- Airplane–Reviews the systems involved with implementing airplane-level (and decomposed system/subsystem level) functions.
- Intersystem–Focuses on the interfaces required for the systems to be able to implement required functionality.
- Intrasystem–Focuses on the internal interfaces and required intrasystem functionality.

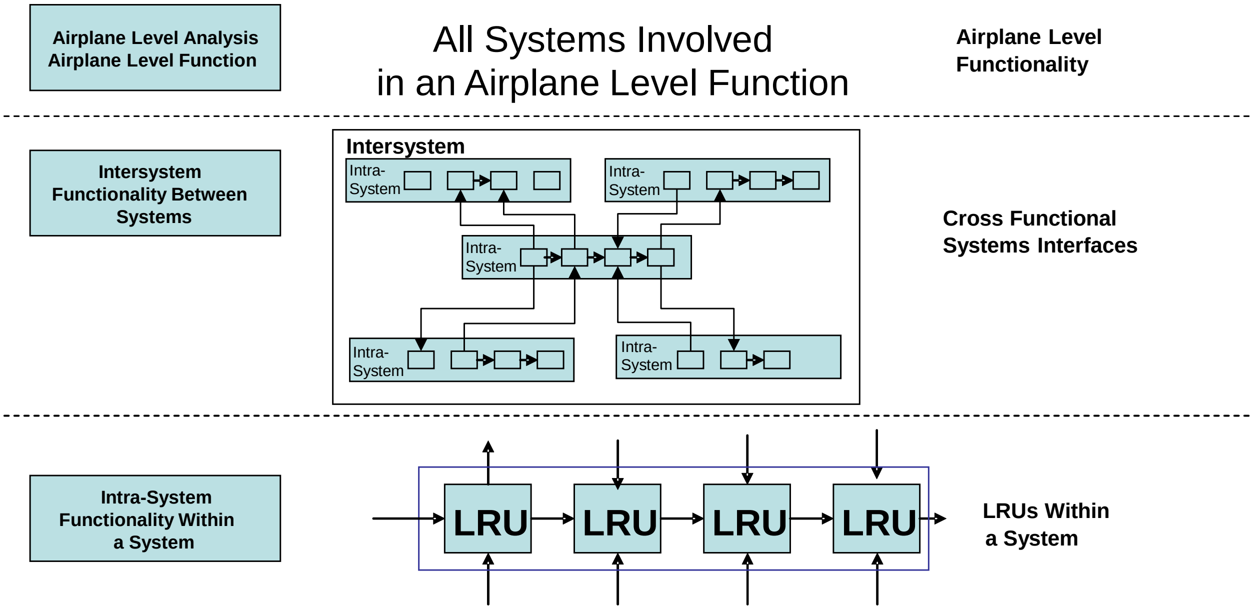


Figure 6. Integration analyses relationships

Figure 7 shows an alternate perspective of these relationships:

- Airplane-level functions are identified and understood (airplane functional hazard assessment [AFHA]).
- Subfunctions of airplane-level functions and systems implementing subfunctions are identified and understood (airplane-level analysis/airplane safety assessment).
- Interfaces between systems required to implement subfunctions (including end-to-end message timing analysis) are identified, negotiated, and resolved (intersystem analysis).
- External function that a system performs by defining the behaviors that it exhibits in doing that function addressed (intrasystem analysis).

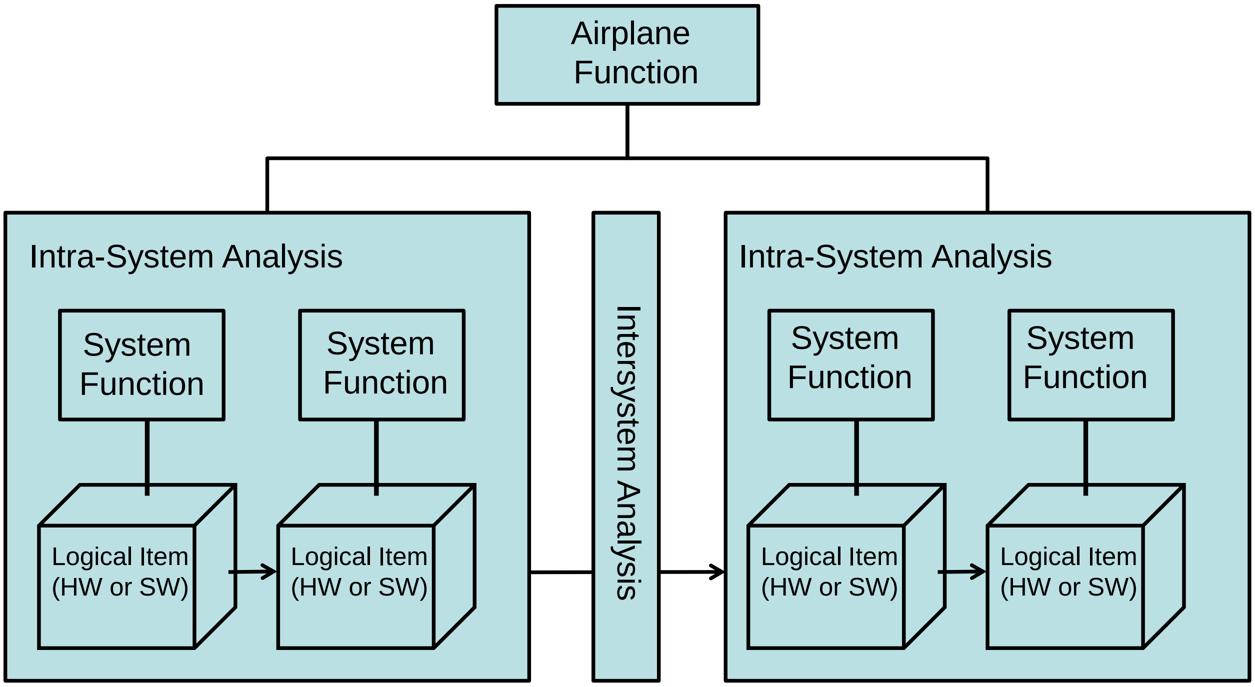


Figure 7. Airplane, intersystem, and intrasystem integration

One of the primary goals of the functional integration analyses was to ensure that the interfaces were correctly and completely defined at both ends and at each hierarchical level. These analyses are basically structured reviews at different hierarchical levels that were designed to ensure that the interfaces were defined correctly and completely (see figure 8). The different analyses result in both a top-down and bottom-up validation. In addition, the analyses should be integrated with each other to ensure:

- Total effect of the components working together achieves the desired airplane-level performance and behavior (bottom-up).
- Airplane-level performance and behavior defined so that requirements and interfaces for components could be derived and designed (top-down).

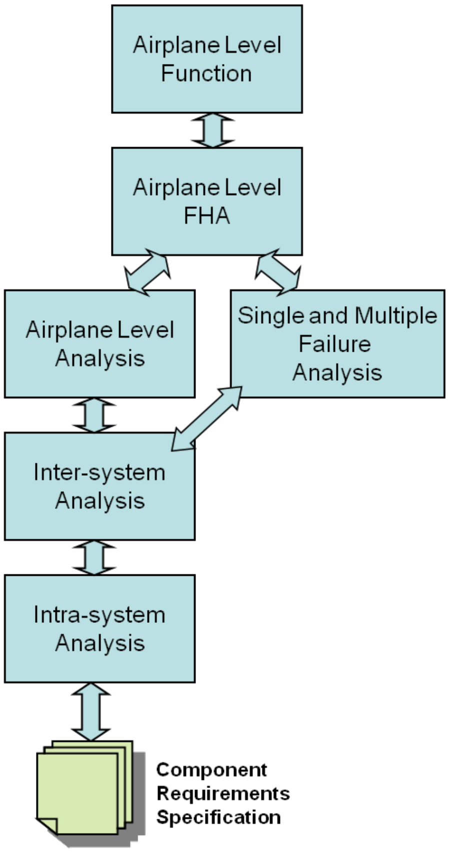


Figure 8. Functional integration analyses interrelationships

The intrasystem analyses should convey to interfacing systems the behavior of outputs for a given system (see figure 9). Information conveyed should cover items that are important for users (i.e., subscribers) to know to correctly use the system's data—and for publishers to check for the function's correct interpretation of input characterization.

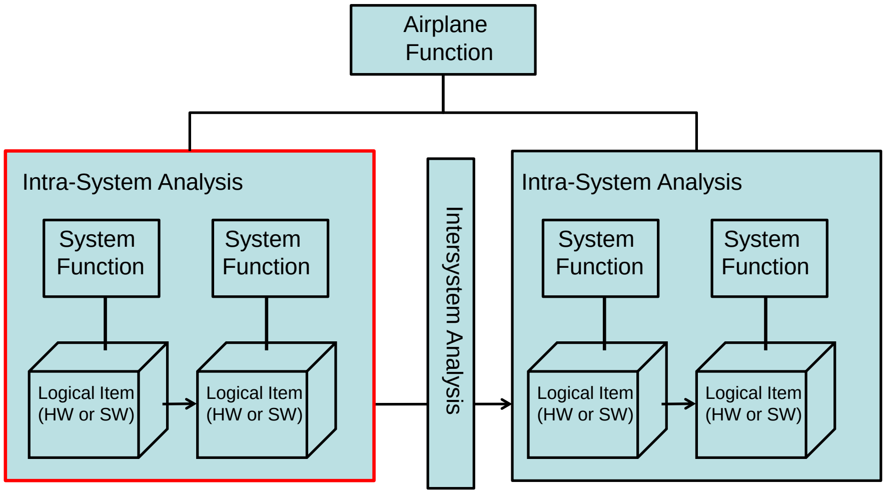


Figure 9. Intrasystem analysis

In the intrasystem analyses, it should be assumed that the other systems will provide the required inputs needed to implement the functionality; these assumptions will be validated during the subsequent intersystem analysis activities.

The intersystem analyses should validate the interaction of an equipment item with all of its interfacing equipment (see figure 10). Assumptions from intrasystem analyses concerning the meaning, accuracy, or content of a signal received from other equipment, and failure modes of the senders and receivers, should be verified.

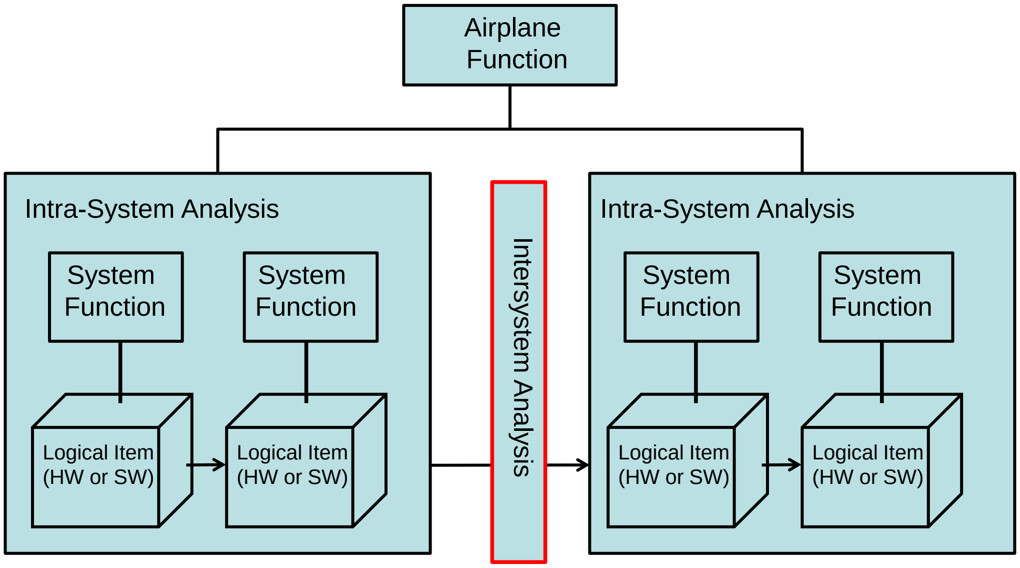


Figure 10. Intersystem analysis

The three main elements of the intersystem analyses should be:

- Validation of system architecture, including LRUs, software, and mechanical elements.
- Validation that data exchanged between systems are sufficient, complete, and agreed upon.
- System-to-platform analysis (including platform interfaces, redundancy, and source preference indicators).

For a system to perform its intended function, inputs are required to produce the required outputs (see figure 11). The intended functions should be identified as part of the requirements and functional architecture development. This should be an iterative process that is repeated at the subsystem and LRU levels.

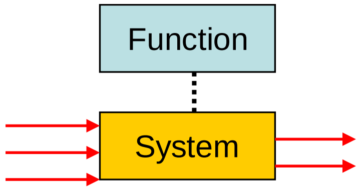


Figure 11. Interfaces required for functionality

As a result of this iterative process, the required interfaces should be identified for the systems to achieve their intended functions (and for the systems to cumulatively achieve the airplane-level functions), as shown in figure 12.

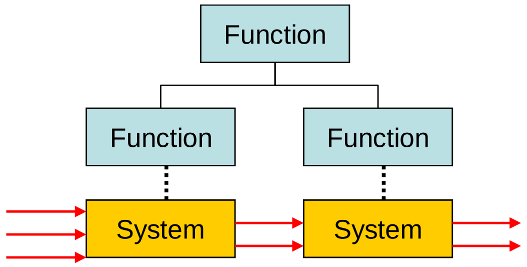


Figure 12. Simplified interfaces required to implement functionality

The interfaces required to implement the required functionality should be analyzed and validated at the system/subsystem, LRU, message, and parameter levels. This helps minimize incorrect or incomplete requirements.

The purpose of the system-to-system interface analyses should be to:

- Validate each system is receiving inputs from required systems (i.e., subscribed to correct publishers).
- Validate other systems are subscribing to the outputs.
- Validate the number of parameters.
- Identify and resolve:
  - Under subscription
  - Over subscription
  - Incorrect subscription
- Ensure subscribing system is receiving necessary inputs from external systems.

The system-to-system interface analyses should be completed at different levels of detail. They should also be conducted from both a publisher and subscriber perspective. With many parameters, it is easy to lose the overarching perspective if unable to look at the data at different levels.

As shown in figure 13, the “horizontal” and “vertical” interface integration occurs at multiple levels.

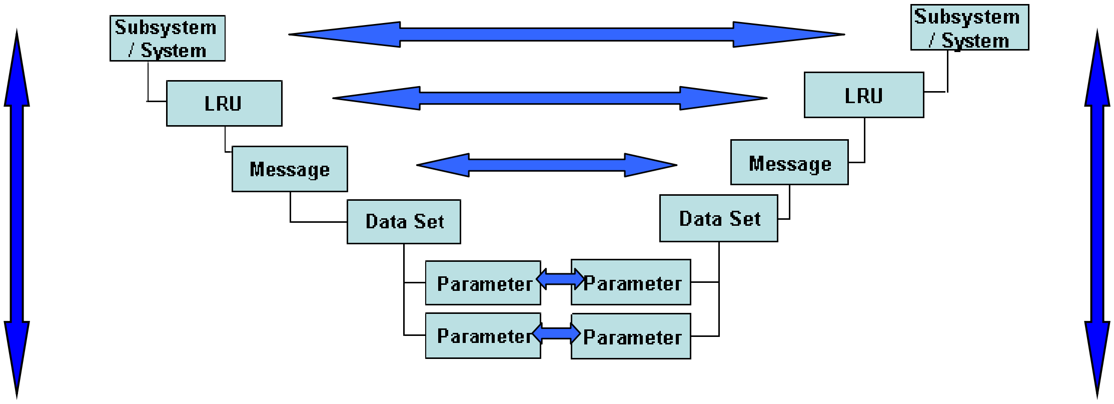


Figure 13. Multiple levels of interface integration

The interfaces required to implement the required functionality are analyzed at detailed levels.

Conducting these intersystem analyses should allow for the following:

- Validation of system architecture, including LRUs, software, and mechanical elements (including hydraulics, electrical, etc.).
- Validation that data exchanged between systems are sufficient, complete, and agreed upon.
- System-to-platform analysis (including platform interfaces, redundancy, and source preference indicators).
- End-to-end message timing analysis.

6.3.3 S&MF Analyses

The S&MF analyses provide an airplane-level assessment of equipment failures. The S&MF analyses include intersystem failures and their cascading effects, flight deck indications, and pilot procedures. The S&MF analyses help validate system functional hazard assessment (SFHA) and development assurance level (DAL) assertions.

The S&MF analyses can also help to identify any missing, incorrect, or incomplete requirements.

As shown in figure 14, first order failure effects are analyzed and downstream impacts are identified (e.g., second order, third order, and additional cascading order effects are described as required by the design teams). The analyses should not stop at a pre-ordained level of cascading effects. Cascading effects should be evaluated until there are no further effects on systems or airplane-level functions. This process includes identification of flight deck effects, including engine instrument and crew alerting system (EICAS) messages.

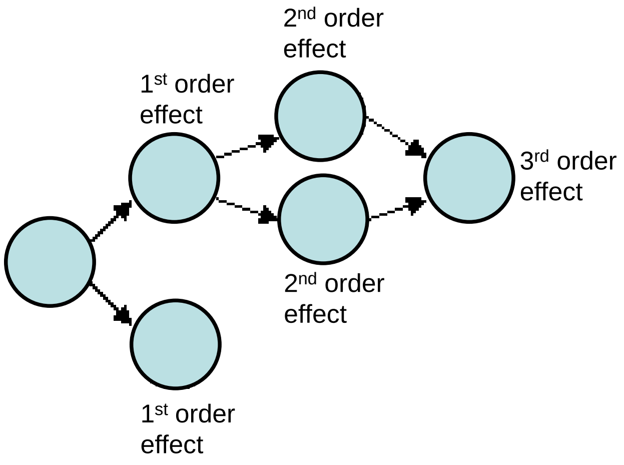
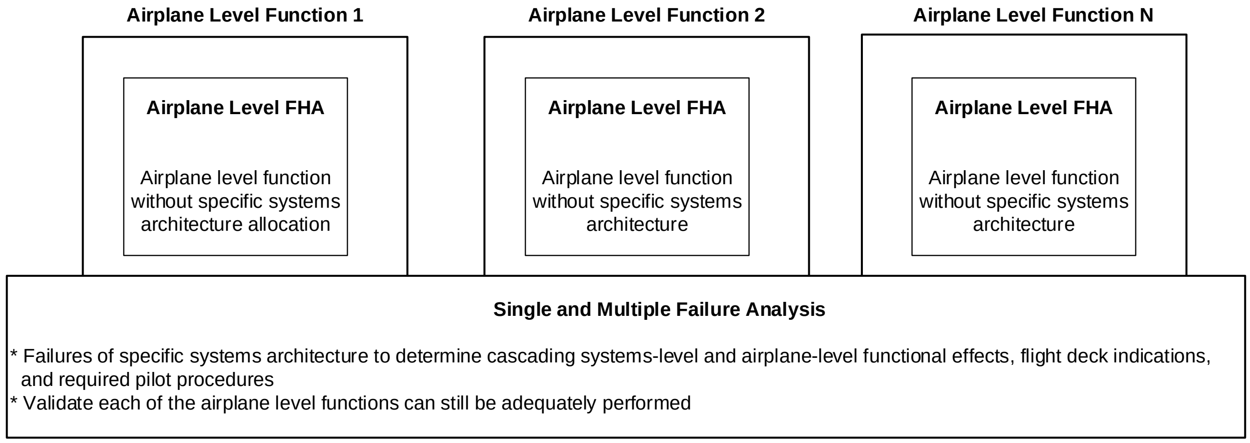


Figure 14. Example of cascading effects for a single failure

The S&MF analyses should:

- Identify and analyze cascading effects based on single or multiple failures.
- Identify and analyze system-level effects from failure and cascading effects on each of the airplane-level functions.
- Identify and analyze the cumulative cross-functional impact of degradations to the airplane-level functions from failures and the cascading effects.

The S&MF analyses provide a more detailed and comprehensive view of the airplane-level functional effects, as shown in figure 15. As airplane-level analyses, the S&MF analyses consider the functional impact of the failure and the cascading effects on each of the eight airplane-level functions and validate whether each of the eight airplane-level functions could still be adequately performed. The S&MF analyses evaluate the stack-up of degradation in each of the eight airplane-level functions to determine the overall airplane-level hazard categorization.


Airplane Level Function 1
Airplane Level FHA
Airplane level function without specific systems architecture allocation
Airplane Level Function 2
Airplane Level FHA
Airplane level function without specific systems architecture
Airplane Level Function N
Airplane Level FHA
Airplane level function without specific systems architecture
Single and Multiple Failure Analysis

* Failures of specific systems architecture to determine cascading systems-level and airplane-level functional effects, flight deck indications, and required pilot procedures
* Validate each of the airplane level functions can still be adequately performed

Figure 15. S&MF analyses–multi-airplane-level function assessment

The hazard categorizations should be based on the cumulative assessment of:

- Functional effect on airplane
- Effect on flight crew
- Effect on occupants (excluding flight crew)

The S&MF analyses should use the systems architecture and interfaces that were validated as part of the systems architecture and interface integration activities (captured as part of the intersystem analyses). This process begins with the identification and selection of cases on which S&MF analyses will be performed, continues with a system-level assessment of failure effects, and concludes with an airplane-level review of all cascading system-level effects. This process is akin to failure modes and effects analysis (FMEA), though with a distinct difference: FMEA is performed at the individual system-level, whereas S&MF analysis is performed at the airplane-level.

The S&MF analyses help validate that the airplane-level hazards are acceptable based on failure probability and that no single failure results in a catastrophic condition. These analyses help support validation that the systems architecture integrated on the airplane meet the airplane's safety requirements.

Reviews should be conducted to make an integrated airplane-level evaluation. The airplane-level assessment of equipment failures includes:

- Primary failure effect on system.
- Cascaded failure effects on other systems.
- Flight-deck effects.
- Crew actions.
- Validating each of the airplane-level functions can still be performed.
- Validating airplane-level hazard categorizations are acceptable based on failure probability (25.1309 compliance).

The reviews should determine the cumulative hazard categorization and airplane acceptability.

The results of the top-down FHA and bottom-up S&MF analyses should be validated. This activity validates that the airplane-level functions can still be adequately performed.

Individual ARs should assess failure effects from the context of their system (system safety assessment [SSA] and FHA). Simply because it is acceptable for each individual system AR does not mean it is acceptable at the airplane level. Functional integration analyses can be used to determine the acceptability of multi-system failure modes and effects analysis.

6.3.4 Change Impact Analysis

If change impact analysis is not done correctly, it can lead to incomplete or inadequate requirements. As shown in figure 16, change impact analysis needs to occur at three different levels:

1. Evaluating impact of changes internal to component/system.
2. Evaluating impact of changes external to component/system.
3. Evaluating cumulative airplane-level effect of the different system-level effects.

Change impact analysis focuses on identifying those parts of a system that are (potentially) affected by modification requests. Change impact assessment should evaluate both internal and external impacts.

It is helpful to have a standardized checklist to ensure that all affected groups are identified. In addition, this helps to ensure a level of process consistency.

Change impact analysis is also the basis for regression analysis and testing, allowing for identification of tests that have to be retested after a modification is performed (see figure 16).

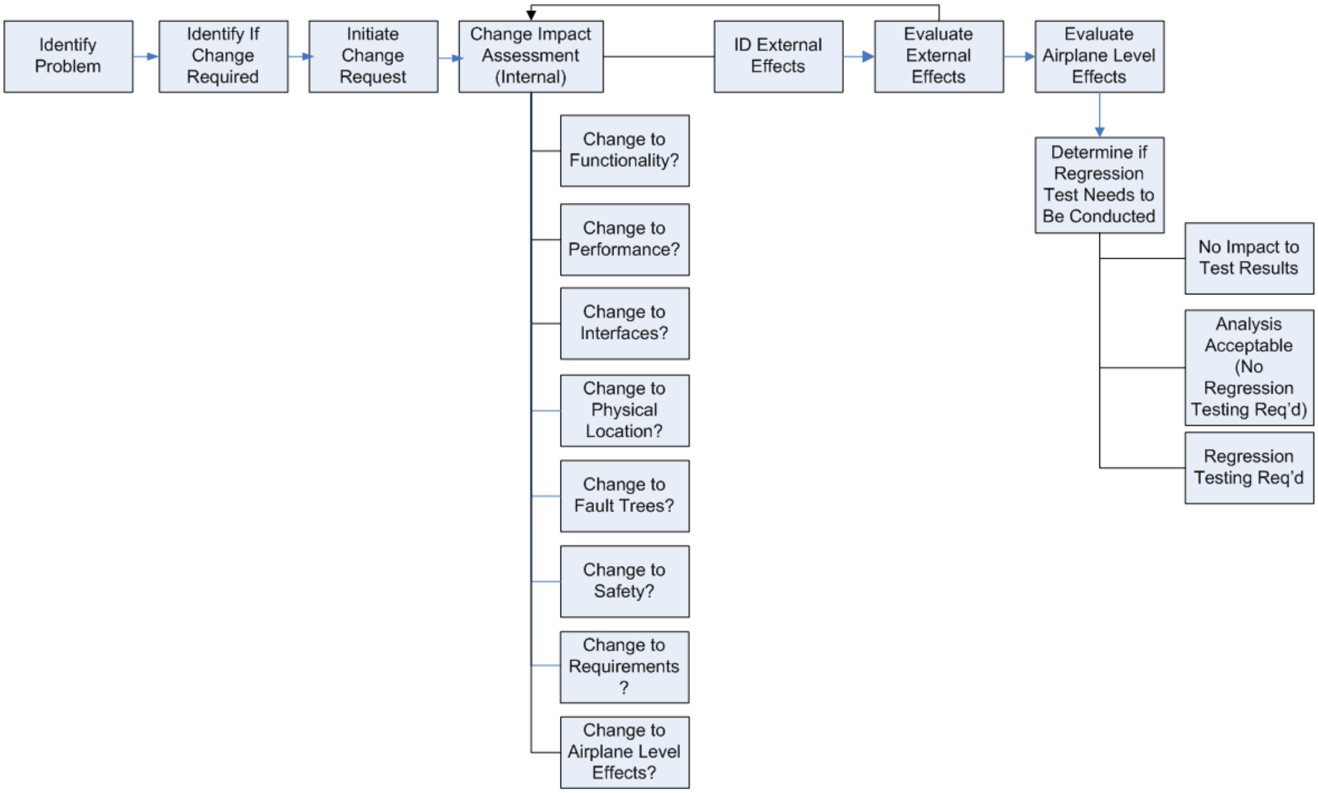

Identify Problem
Identify If Change Required
Initiate Change Request
Change Impact Assessment (Internal)
ID External Effects
Evaluate External Effects
Evaluate Airplane Level Effects
Change to Functionality?
Change to Performance?
Change to Interfaces?
Change to Physical Location?
Change to Fault Trees?
Change to Safety?
Change to Requirements ?
Change to Airplane Level Effects?
Determine if Regression Test Needs to Be Conducted
No Impact to Test Results
Analysis Acceptable (No Regression Testing Req'd)
Regression Testing Req'd

Figure 16. System- and airplane-level change impact analysis

As show in figure 17, it is important to evaluate whether there are any cross-functional impacts as part of the change impact assessment. Also shown in figure 17, the first evaluation is to determine the change impact internally to the component/system that is initiating the change.

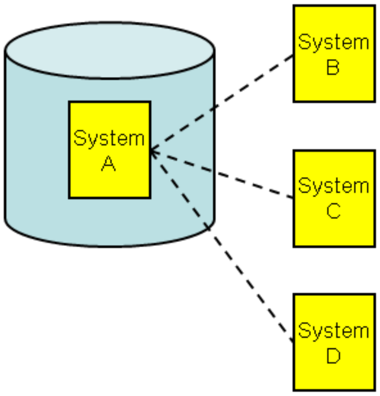


Figure 17. Evaluating intersystem effects

Table 3 lists questions that can be considered when attempting to do this evaluation. The next step is to evaluate whether there are any cross-functional impacts. Examples that could have cross-functional impacts include impacted performance, impacted logical interfaces, impacted power interfaces, or changes in functionality. Systems that are affected can then use the same questions in table 3 to evaluate whether they have any impacts on other systems. This should be repeated, as necessary, to ensure that all cross-functional interfaces are clearly understood.

Table 3. Component-/system-level change impact considerations

Does the change impact any requirements validation activities?
Does the change impact any requirements verification activities (analysis, test, etc.)?
Does the change impact functionality?
- Does the change modify functionality?
- Does the change reduce or degrade functionality?
Does the change impact performance?
- Does the change result in performance outside of existing tolerance ranges?
Does the change impact the interfaces?
- Does the change impact any external logical interfaces?
- Does the change impact any external physical interfaces (e.g., structural, transport element, wiring)?
- Does the change impact any power interfaces (electrical, hydraulic, etc.)?
Does the change impact other functional disciplines (flight deck, electrical subsystems, hydraulics, flight controls, etc.)?
Does the change impact the physical location?
Does change impact safety?

It is important to evaluate the cumulative airplane effects. As system architectures become more integrated, it is possible for the cumulative effects of acceptable, individual systems-level effects to be unacceptable at the airplane level.

Table 4 contains a list of cumulative airplane-level effects that should be considered during a change impact analysis.

Table 4. Cumulative airplane-level effect considerations

Do the cumulative system impacts affect airplane-level function?
Do the cumulative system impacts affect airplane-level performance (range, stopping capability, etc.)?
Do the cumulative system impacts affect airplane-level safety?

It is critical to have knowledgeable people participate in the change impact analysis to ensure that the cross-functional and cumulative airplane-level effects are clearly understood. This is particularly true for assessing safety impact.

The following objective statement is from ARP4754A, Section 5.3.1.1, Safety Requirements:

> "Requirements that are defined to prevent failure conditions or to provide safety related functions should be uniquely identified and traceable through the levels of development. This will ensure visibility of the safety requirements at the software and electronic hardware design level."

However, in discussions with dozens of software ARs, AEH ARs, and suppliers, it became evident that there was not a clear, consistent understanding of when a requirement should be identified as related to "safety." The practices associated with the identification and management of safety-related requirements can vary widely if there are no consistent definitions. This topic crosses both systems and software processes; it is not something that can be addressed exclusively within the software domain. This increases the likelihood that a change could be made at the software or AEH level while not fully understanding the safety impact. Safety requirements are used during DO-178/254 activities.

With system changes occurring over the life of the system, tagging helps facilitate the change impact assessment by highlighting the potential impact on safety or safety analysis for design/requirements changes. Tagging safety requirements does not mitigate the need for the change impact assessment to be performed by a person who understands the system and the role the impacted requirements have in the system.

Any requirement that is derived from the safety analysis will be tagged "Yes" using this attribute. The term "safety analysis" in this report includes the following analyses: AFHA, SFHA, preliminary airplane safety assessment, preliminary systems safety assessment, zonal safety analysis, particular risk analysis (e.g., threat analysis), common mode analysis (CMA), S&MF, FMEA, and fault tree analysis (FTA).

To establish a consistent approach to tagging safety requirements, table 5 lists typical requirements types that are derived from the safety analyses and should be tagged as safety. This is not an exhaustive list and is provided here as guidance to help ensure consistency in identifying and tagging safety requirements.

Table 5. Criteria for safety requirement types

Requirements specifying probability limits (e.g., 1E-X) for system or equipment integrity and availability derived from the safety analysis (to meet 25.1309 criteria).
“No single failure” requirements for meeting Code of Federal Regulations /critical safety requirements.
Architecture requirements that define functional separation and independence derived from or required for safety analysis.
Physical separation and isolation requirements derived from the safety analysis that defines implementation separation and independence.
Requirements minimizing assembly or installation errors—for example, making design derived from or required by safety analysis physically impossible to assemble or install incorrectly.
Requirements for functional or implementation redundancy derived from safety analysis.
Requirements to protect from fault propagation, including temperature requirements for equipment in flammable leakage zones, requirements for fault currents, requirements for oscillatory structural loads, requirements for load alleviation, and flutter requirements. These requirements allow for the “no single failure” certification requirement and maintain independence between failure events.
Requirements that define fail-safe conditions or operation. These requirements generally allow system operation in the presence of failures. They drive redundancy, fault isolation, and dissimilarity, etc. These requirements allow for the “no single failure” certification requirement and use “And” gates between failure events on the FTA.
Requirements that define the DAL for a function development assurance level or item development assurance level.
Requirements that define airplane CMRs. These requirements include functions and performance requirements that implement the CMR and the pass/fail criteria used for the CMRs.
Requirements for ensuring continued airworthiness of high-intensity radiated fields/lightning protection features.
Requirements that ensure that master minimum equipment list conditions provide acceptable safety level for the flight.
Requirements that define fault detection; fault or error mitigation; and fault annunciation functions used to limit the latency of equipment and system failure effects in the equipment and airplane safety analyses. These requirements include built-in-test, system monitors, EICAS annunciation logic, and dissimilarity requirements.

CMR = certification maintenance requirement

There are also benefits in having a consistent, documented agreement. The following types of requirements in table 6 may be critical for operation of the system. However, these requirements are not derived from the safety analysis and will not be tagged as safety requirements.

Table 6. Non-safety requirements types

MTBF/mean time between unscheduled removal requirements to meet economic criteria, unless the MTBF is used as the failure rate in the safety analysis.
Requirements for monitors that limit failure ambiguity groups (i.e., monitors to help the ground crew with troubleshooting).
Requirements for normal operation and performance (e.g., rate, accuracy, range, loads, gains, hysteresis, interface, and quality requirements, etc.).
Requirements for equipment operating environment qualification.
Requirements for normal equipment maintenance in service, including general requirements for interchangeability, Occupational Safety and Health Administration requirements, or weight.
Requirements for equipment detail implementation features (for example, materials, finishes, or fastener types).
Requirements for transmission of data for airplane health management.
Requirements for development or production processes (statement of work requirements).

MTBF = mean time between failure

The safety tagging criteria listed in table 5 should be applied at each requirement level. This should be done to avoid two situations:

- Incorrectly not tagging a child requirements as safety, which loses the intent of safety requirements being identified for the software and AEH processes.
- Unnecessarily tagging a child requirement as safety solely based on the parent being tagged as safety.

6.3.5 Technical Planning–Process Assurance Reviews

For systems identified as having high DA risk, it is recommended that the following four DA assessment reviews be conducted:

1. Planning review
2. Validation review
3. Verification review
4. Final review

These structured reviews provide a "gated" methodology for decision making at specific phases of the development cycle of a program. The gated method is a decision-making process that helps drive development throughout the different stages. These structured reviews help identify the maturity a program or product should have before it moves to the next stage of its development while minimizing risk.

Conducting these reviews in a timely and structured manner can help identify incomplete, incorrect, or inadequate requirements. The high-level objectives of the reviews, which can be conducted at both the OEM and supplier level, are to verify that the program's DA processes (particularly those related to requirements V&V) are:

- Widely and consistently understood and correctly applied by the systems' developers.
- Capable of identifying and mitigating errors that may be present in safety requirements and in the implementation of those requirements.

It is recommended that the respective review dates should occur when the OEM/supplier is available to support the review criteria for the respective reviews. The reviews should not occur too early (when artifacts are not ready) or too late (when findings are difficult to address). In addition, it is acknowledged that it is possible to combine reviews.

Table 7 identifies recommended DA artifacts that should be reviewed during the respective PA reviews.

Table 7. Artifacts for process assessment reviews

	Process Assurance Reviews			
DA Artifact	Planning Review	Validation Review	Verification Review	Final Review
Program-specific DA Plan - Requirements Development, V&V - Safety - Configuration Management - Process Assurance	X	X	X	
Certification plan and relevant system certification plans (if applicable, technical standard order, etc.)	X			
SSA (e.g., SFHA, common cause analysis) - initial/final)	X	X	X	
Configuration and change records		X	X	
Planning review report		X		
Requirements (SCD and below)		X	X	
Validation artifacts (includes traceability, allocation, etc.)		X		
Evidence of SME review of supplier requirement validation		X		
Evidence of SME review of supplier requirement changes, change impact assessments, and regression analyses		X	X	
Evidence of SME review of supplier safety analyses		X	X	
Validation review report			X	
Verification artifacts			X	
Verification test procedures and reports			X	
PRs			X	
Requirement deviation records (OEM authorized and supplier approved)			X	
Evidence of SME review of supplier requirement verification			X	
Verification review report				X
Supplier system DA accomplishment summary–initial, final				X

Table 7 helps identify when the different artifacts should be reviewed. The purpose of this table is to help alleviate the level of subjectivity regarding PA reviews in ARP4754A. Reviews should be scheduled during the normal coarse of program development from planning, validation, verificaiton, and final PA reviews.

Appendix H contains detailed criteria for conducting these structured reviews.

6.3.6 Supplier Oversight−Assessing Supplier Risks

The ability to leverage industry knowledge and experience is very important, and suppliers play an integral part of ensuring the safety of the aviation industry. Because of their critical roles in the development of airplane programs, it is critical to be able to evaluate the suppliers' capabilities. An equally important part of this is ensuring that the roles and responsibilities are clearly understood.

Some of the key capabilities a supplier should be able to provide are:

- Identification of program risks and complementary mitigation plans through a closed-loop flow-down validation of requirements.
- Awareness of supplier responsibilities and accountability for sub-tier performance. The supplier should similarly have a gated design approach. The gated design approach should include supplier planning, performance, and reporting using measurable and appropriate performance criteria that include the scope and effectiveness of design reviews and other airplane lifecycle activities.
- Following industry standards for the training, qualification, and certification of supplier personnel performing OEM required (non-FAA) inspections.

Table 8 includes questions that can be considered in conducting a supplier risk assessment.

Table 8. Supplier risk assessment

Category	Risk Assessment Question
Requirements	Does supplier use and execute an effective requirements management process (including V&V)?
Requirements	Does supplier design/design methodology effectively address requirements (i.e., ensure design compliance to requirements)?
Requirements	Has supplier been using a process to ensure development of requirements with high quality and has supplier also flowed down requirements with high quality to sub-tier?
Requirements	Did supplier plan for and use an effective design verification/qualification process?
Requirements	Did supplier have a requirements verification procedure?
Technical Performance	What is the supplier’s past technical performance and related experience?
Allowable Development	Does supplier have appropriate experience (certification; safety; functional and spatial integration; test, in-service support; etc.)?
Allowable Development	Is the supplier familiar with required aerospace standards?
Data Management and Control	Has supplier demonstrated its ability to successfully manage and control engineering data?
Capability	Is the supplier’s technical staff and resources/infrastructure adequate to support contract requirements?
Capability	Does supplier have adequate facilities, equipment, tools, resources, and expertise to support development, build, and test similar products and complexity?
Capability	Does the supplier’s organizational structure reflect its product architecture and show clear lines of authority, roles, and responsibilities?
Capability	Is the supplier’s intended tool use compatible with the OEM requirements for project performance?
Readiness and Process Assurance Reviews Effectiveness	Does supplier demonstrate an appropriate readiness and process assurance review process?
Configuration and Change Management Implementation	Is supplier change and configuration management process executed to program requirements?

6.3.7 Model-Based Systems Engineering

As airplane systems have become more integrated, improved performance, system stability, weight reduction, improved maintainability, and other benefits have been realized. However, the increased integration has also resulted in attendant challenges, particularly to ensuring systems integration and safety. Table 9 indicates the impact of evolution of systems architectures.

Table 9. Evolution of systems architectures

System Architecture		Characteristics
Simple Components	Simple Interfaces	• Single designer can define the interfaces • Connectivity and context easily understood • Integration effort is correspondingly simple • High part and wires count
Simple Components	Complex Interfaces	• Interface defined by several designers • Design has to absorb and produce a large amount of data • Connectivity and context less easily understood • Increased integration efforts • Lower parts and wires count
Complex Components	Complex Interfaces	• Multiple interfaces to achieve functionality • High level of integration • Much lower parts and wires count

Figure 18 contains an example of how commercial airplane digital networks have evolved from having individual, federated LRUs to being integrated with centralized computing resources systems architectures. Both the legacy architecture and IMA architecture are achieving the same functionality: turn on a hydraulic pump with a switch in the flight deck and provide a positive indication that the pump is operating.

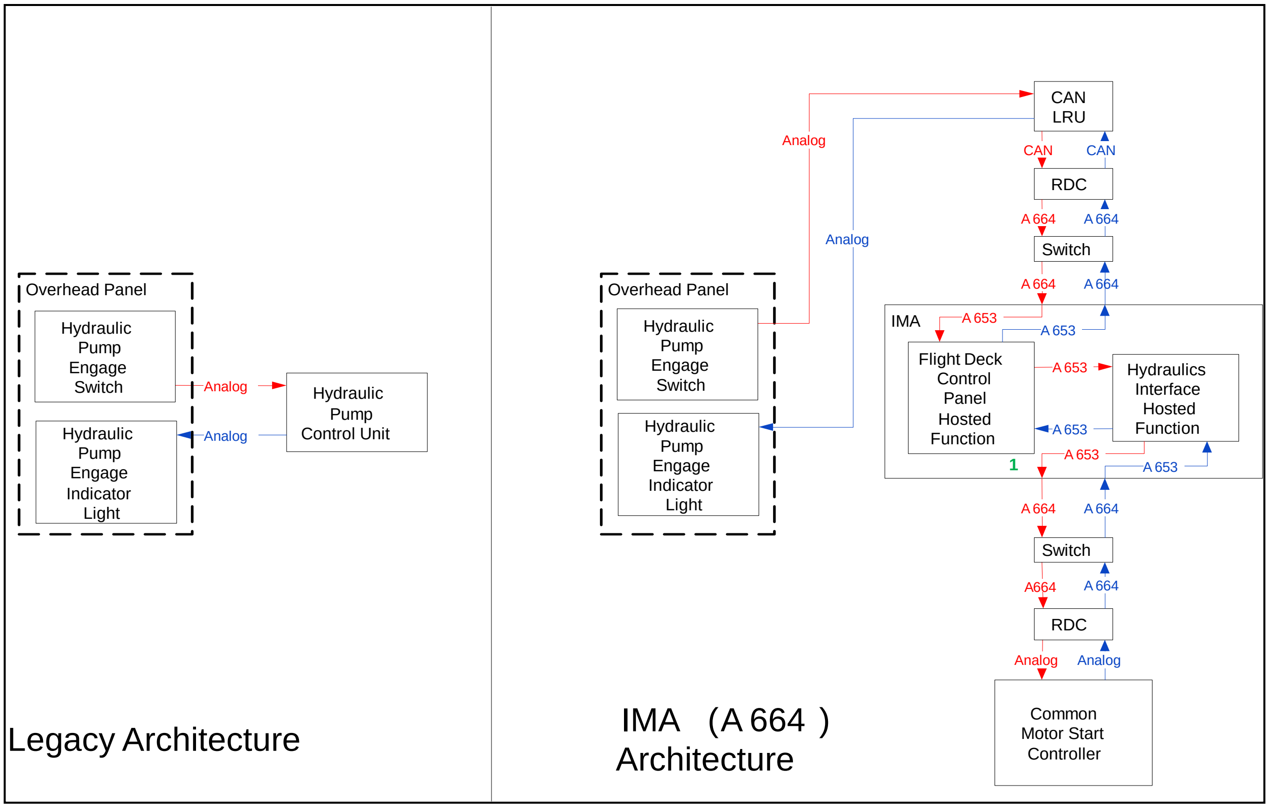

Overhead Panel
Hydraulic Pump Engage Switch
Analog
Hydraulic Pump Control Unit
Analog
Hydraulic Pump Engage Indicator Light
Legacy Architecture
Analog
Analog
CAN LRU
CAN
CAN
RDC
A 664
A 664
Switch
A 664
A 664
Overhead Panel
Hydraulic Pump Engage Switch
Hydraulic Pump Engage Indicator Light
IMA
A 653
A 653
Flight Deck Control Panel Hosted Function
A 653
Hydraulics Interface Hosted Function
A 653
1
A 653
A 653
A 664
A 664
Switch
A664
A 664
RDC
Analog
Analog
Common Motor Start Controller
IMA (A 664) Architecture

Figure 18. Commercial airplane digital network evolution

Most commercial airplanes are built with components procured from multiple suppliers. Having complete and correct requirements specifications is critical to minimizing errors, particularly those that could adversely affect safety. It is beneficial to be able to discover discrepancies prior to bench, system, or airplane-level testing. Models can help facilitate identifying and resolving reconciling requirements and interface discrepancies.

MBSE models and, specifically, system architecture models can help minimize errors during the systems development and design. MBSE provides the ability to engineer more complete modeled definitions of the lower-level requirements by linkage to architecture and design; by its ability to inject faults to examine failure mode performance; and by using model execution as an additional reference for verification beyond that of requirements. MBSE can improve the detection of unexpected aircraft and system characteristics and their inclusion in the systems integration analyses.

It has been shown that modeling can result in increased flight test stability on current commercial aircraft programs as compared to equivalent programs in the 1990s. As shown in figure 19, there was increased design stability during the flight test program even though there were increased interfaces. The resulting benefit realized from this additional modeling effort is an order of magnitude decrease in required interface control drawing changes during test on current programs compared to earlier programs.

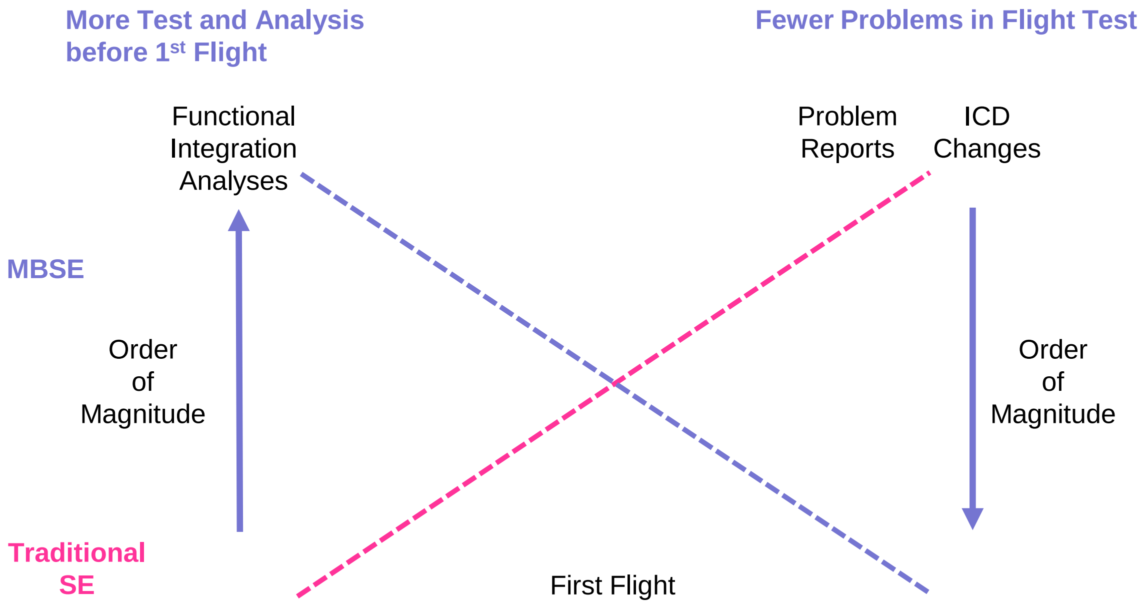

More Test and Analysis before 1st Flight
Fewer Problems in Flight Test
Functional Integration Analyses
Problem Reports
ICD Changes
MBSE
Order of Magnitude
Order of Magnitude
Traditional SE
First Flight

Figure 19. Model-based system engineering benefits

MBSE can support analyses of performance and failure modes, consistency checking, and error detection and correction.

In the area of digital network modeling, significant success has been achieved in addressing these challenges with large-scale system architecture models—allowing for early discovery of design data errors.

MBSE can help with change impact analysis (single truth determination and impact and use of modeled analyses and consistency checking to support and simplify change impact analyses).

It is recommended that MBSE continue to be explored as a method to help with improving requirements quality within the aviation industry; the new methods embedded in the use of MBSE may require changes or additions to existing standards and guidance.

7. NEXT GENERATION AIR TRANSPORTATION SYSTEM DISCUSSION

The trend for increasing system integration and data management complexity has considerations for the Next Generation Air Transportation System (NextGen). This research is linked with the development of NextGen, as stated in the FAA's Performance Work Statement:

> "This research work is directly related to NextGen. The NextGen architecture will be tightly integrated across airborne and ground-based components and, require end-to-end performance specification that includes a comprehensive system's development and assurance approach. The increased system complexity and integration, as well as the NextGen vision, will require system level standards that focus on system life cycle assurance in addition to [software and] electronic hardware design assurance. The results

> of this research would be used to provide input in the development of standards, guidance, and training for approval of aircraft products.” [3]

The focus of this research was on the airplane and its systems. In and of themselves, airplanes are becoming more integrated. The air traffic management system under NextGen is also becoming more integrated. These more highly integrated airplanes will be integrated into the more highly integrated air traffic management system. Therefore, it is recommended that further research be conducted to review safety considerations in system integration to include the evaluation of existing industry guidance, identification of gaps for development of new industry guidance, and recommendations for conducting the system integration process and the corresponding activities and assurance that this entails. Understanding the interrelationships between aircraft and the air traffic management system (particularly in the presence of failures) and understanding how systems’ changes can affect another system will be critical in maintaining safety in the growingly complex NextGen architecture.

AD 2005-19-19 is an example of the interrelationships that can occur:

> “The FAA is adopting a new Airworthiness Directive (AD) for certain Boeing Model 757-200 and -300 series airplanes and Model 767 series airplanes. This AD requires replacing the existing operational software of the Pegasus flight management computer (FMC) system with new, improved operational software. This AD results from reports of “old” or expired air traffic control (ATC) clearance messages being displayed on the control display unit (CDU) of the FMC system during subsequent flights. We are issuing this AD to prevent display of old or expired ATC clearance messages on the CDU of subsequent flights, which could result in the airplane entering unauthorized airspace or following a flight path that does not provide minimum separation requirements between aircraft, and a consequent near miss or a mid-air collision” [11].

8. FINDINGS, RESULTS, AND RECOMMENDATIONS (PHASES 1, 2, AND 3)

8.1 FINDINGS AND RESULTS

To address acceleration in complexity and integration of digital avionics systems, the TO-22 research team identified issues, shortcomings, and root causes of requirements errors, omissions, or conflicts.

The research involved two approaches: solicited input from Boeing SMEs and the evaluation of eight scenarios for possible causes that might contribute to requirements errors, omissions, and conflicts. The research approach also included reviewing industry guidance for possible gaps in requirements formulation and V&V for complex avionics architectures.

The principal finding of the Phase 1 research was to use the 2005 Malaysian Airlines 777 incident for further research.

The principal findings of the Phase 2 research emphasized the importance of having validated, complete, and correct requirements and recognizing the iterative nature of requirements V&V.

The principal findings of the Phase 3 research were to improve cross-functional systems integration, failure analysis guidance, change impact analysis, and technical planning.

8.2 RECOMMENDATIONS FOR FURTHER RESEARCH

Additional areas of potential improvements for post-Phase 3 research include the following topics:

1. Improved configuration management (both tools and processes).
2. Requirements developed in English (a language known for ambiguous, inaccurate semantic and syntactical content).
3. Improved process control in the decomposition, synthesis, restructuring, and analyses of requirements completeness during iterative integration of highly complex systems.
4. Improved languages and related tools to model highly integrated and complex systems accurately and maintain system fidelity across OEM-supplier boundaries throughout system development and maintenance.
5. Improved tools to simulate aircraft and system failures with high fidelity prior to implementation and during analyses of extensive trade studies.
6. Improved automated approaches to establish system and requirements integrity throughout the aircraft/system lifecycle.
7. Improved automated tools to perform hazard analyses and SSA.
8. Improved proposed content for ARP4754A that addresses increased integration and complexity.
9. Investigate possible benefits and use of MBD, virtualization, distributed test, and interoperability-based testing for improving V&V of complex integrated digital systems. Additional information regarding concepts for each of these tools is included in appendix I.
10. Another future task could be to harmonize SAVI efforts and analyses with other recommendations made in this report.

9. REFERENCES

1. SAE International ARP4754A/EUROCAE ED-79A. (December 21, 2010). Guidelines for Development of Civil Aircraft and Systems.

2. SAE International ARP4754/EUROCAE ED-79. (1996). Certification Considerations for Highly Integrated or Complex Aircraft Systems.

3. FAA. (April 11, 2015). *SE2020-TORP 1380-Task Order 0022-Modification 0001, Safety Issues with Requirements Definition, Validation, and Verification Processes and Practices* (FAA Publication No. DTFAWA-10-D-00019).

4. SAE International ARP 4761. (1996). Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems.

5. RTCA. (2001). DO-178B/C, Software Considerations in Airborne Systems and Equipment Certification. Washington, DC.

6. RTCA. (April 19, 2000). DO-254, Design Assurance Guidance for Airborne Electronic Hardware. Washington, DC.

7. RTCA. DO-297. (November 8, 2005). Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations. Washington, DC.

8. FAA. Transport Airplane Issues List. Retrieved from https://www.faa.gov/aircraft/air_cert/design_approvals/transport/media/rptTAIListForPublicWeb.PDF.

9. RTCA. DO-RTCA/DO-331. (December 13, 2011). Model-Based Development and Verification Supplement to DO-178C and DO-278A. Washington, DC.

10. FAA. (October 7, 2014). AFE 75 COTS AEH Issues and Emerging Solutions Final Report. Retrieved from https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/%20media/AFE75_COTS_AEH.pdf.

11. FAA. (September 12, 2005). *AD 2005-19-19*.

APPENDIX A—WHITE PAPER 1 EXTRACT, INCLUDING EVENTS NOT SELECTED FOR FURTHER RESEARCH WITHIN THIS TORP 1380 DELIVERY ORDER 0022

A.1 RESEARCH APPROACH

Internal and external database sources were reviewed to identify adverse events for which requirements definition and validation and verification (V&V) may have been, at a minimum, a contributing factor. Table A-1 identifies the initial input data sources that were used. The most productive sources were the discussions with Boeing Commercial Airplanes (BCA) safety and requirements subject matter experts (SMEs).

Table A-1. Initial data sources

FAA Recommended Resources [A1]	Initial Input Data Sources
Personal knowledge and direct experience of contractor	• Review of BCA in-service data fleet advisory directives, service bulletins, and flight squawks • Internal airplane safety events and information databases • Safety lessons learned • Discussions/meetings with BCA safety and requirements SMEs
Literature search	• Flight Safety Foundation • Aviation Safety Network • Skybrary • Engineering A Safer World: Systems Thinking Applied to Safety, Dr. Nancy Leveson (Massachusetts Institute of Technology [MIT])
Investigation of publicly available official reports involving commercial aviation accidents and safety-related incidents	• National Transportation Safety Board (NTSB) • FAA Lessons Learned • Transportation Safety Board Canada • Australian Transport Safety Bureau • Airworthiness Directives

Table A-1. Initial data sources (continued)

FAA Recommended Resources [A1]	Initial Input Data Sources
Questionnaires were originally planned to be sent to selected parties within the commercial aviation community	• Questionnaires were not sent out to selected parties because this was covered as part of: – Industry participation as a member of the SAE International S-18 committee, which is responsible for ARP4754A and ARP4761 – Access to BCA in-service fleet data – Access to BCA PRs – Access to BCA safety and requirements SMEs
Direct communication with selected parties within industry, academia, and government agencies (e.g., FAA, NASA, university faculty members known to be working in this field, coworkers, and ex-coworkers)	• SAE International S-18 committee participation, providing a valuable conduit for direct communication with industry and understanding the direction of these guidelines • Meeting/discussion with Dr. Nancy Leveson, MIT

ARP = Aerospace Recommended Practice; PR = problem report

The aviation industry has an enviable safety record. The number of accidents and incidents is relatively low. Any accident or incident provides an opportunity to identify potential requirements process improvements. However, because of the amount of potential data that could be reviewed, a method to select potential candidates was developed. As a result, a series of filters were applied, as shown in figure A-1.

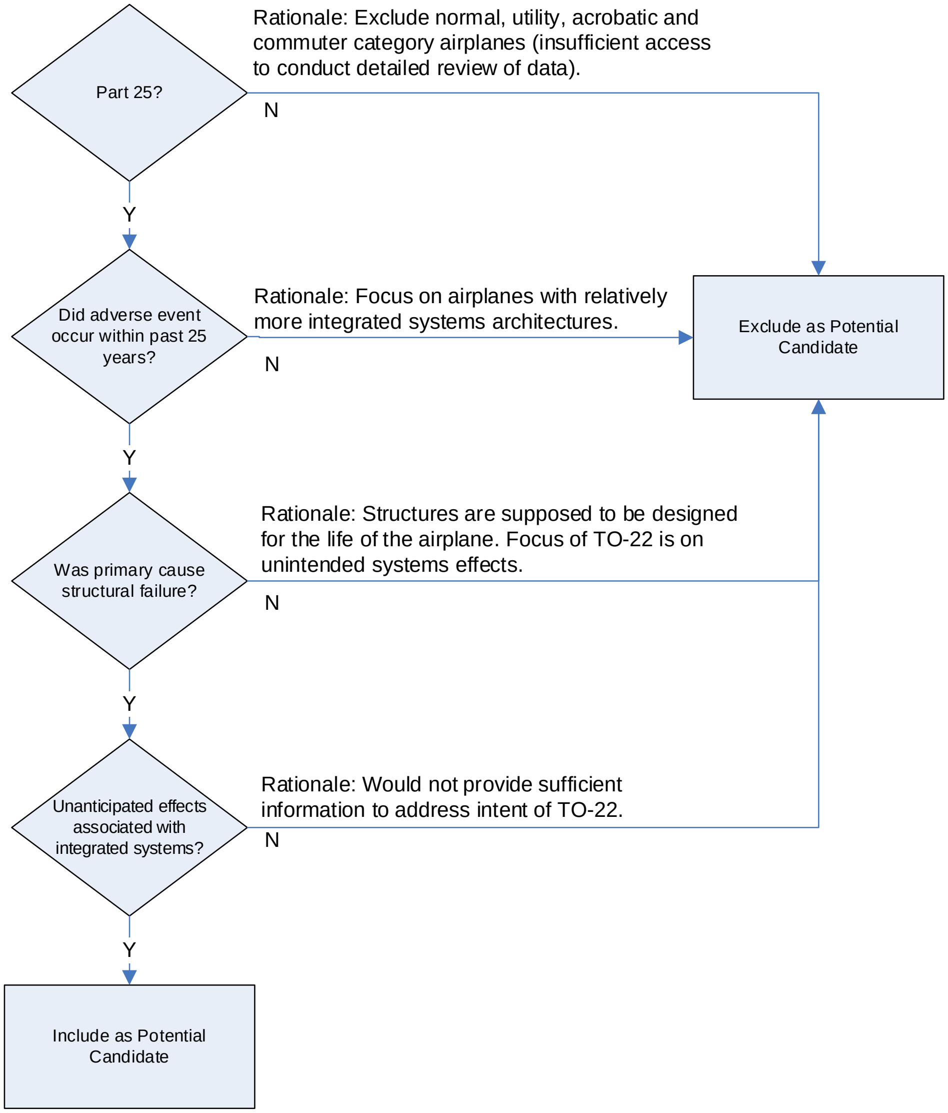

Part 25?
Rationale: Exclude normal, utility, acrobatic and commuter category airplanes (insufficient access to conduct detailed review of data).
N
Y
Did adverse event occur within past 25 years?
Rationale: Focus on airplanes with relatively more integrated systems architectures.
N
Exclude as Potential Candidate
Y
Was primary cause structural failure?
Rationale: Structures are supposed to be designed for the life of the airplane. Focus of TO-22 is on unintended systems effects.
N
Y
Unanticipated effects associated with integrated systems?
Rationale: Would not provide sufficient information to address intent of TO-22.
N
Y
Include as Potential Candidate

Figure A-1. Down-select method

The primary goal of the filters was to identify potential candidates for which requirements definition and V&V may have been a contributing factor [A1].

In addition, the filtering criteria were consistent with the guidance provided by the FAA [A1]:

- This research was limited to those aspects related to the specification of digital systems—that is, those systems that involve microprocessors, software, digital networks, and other such digitally based system elements.
- It did not investigate issues involving structural, mechanical, hydraulic, pneumatic, or electrical power systems unless those systems also involved control and monitoring by digital systems.
- The research used the FAA-recommended window of January 2000 to the present.

The primary data sources reviewed were the NTSB database, FAA lessons learned data, and the BCA safety databases. The first filter excluded utility, acrobatic, and commuter category airplanes. This was primarily done because of the potential difficulty in getting additional data. The next filter considered the time frame. The research period was extended to September 1998 to include the Swissair MD-11 event [A1]. The next filter eliminated cases that appeared to be mostly structurally related. Fatigue is important, but translating these insights to digital avionics systems would be difficult. The next filter considered whether the accident/incident was associated with unintended effects for highly integrated systems. As part of this review, candidates were removed that appeared to be operational in nature (e.g., an aircraft landing at the wrong airport).

Pilot evaluation of aircraft level operations [A1] was addressed through discussion with safety and requirements SMEs, who identified potential cases to review in further detail.

Throughout this exercise, special attention was paid to how the information could be used from a requirements definition and V&V process.

A.2 FINDINGS

Prior to any literature review or searching of internal and external databases, one candidate immediately stood out as a great candidate. However, the decision was made not to immediately select the case. Each step in this process allowed an evaluation for general trends in requirements definition and V&V. One of the key reasons that the potential candidates, listed in table A-2, were reviewed in further detail was to consider pilot evaluation of aircraft operation. It is for this reason that accidents such as the Swissair in-flight fire were included. It was not directly related to digital avionics systems, but it was an opportunity to consider this from an operational and wiring requirements perspective.

Table A-2. Potential candidates

Date	Airline/Flight Number	Aircraft Model	Location
9/2/1998	Swissair Flight SR 111	MD-11	Nova Scotia
1/31/2000	Alaska Airlines Flight 261	MD-83	Pacific Ocean near Anacapa Island, CA
8/20/2007	China Airlines Flight 120	737-800	Okinawa, Japan
6/1/2009	Air France 447	A330-200	Atlantic Ocean
11/4/2010	Qantas 32	A380-800	Singapore
11/9/2010	ZA002	787-8	Laredo, TX
8/1/2005	Malaysian Airlines 777	777-200	Perth, Australia

After evaluating each of these events for potential research applicability, all but the 2005 Malaysian Airlines 777 incident were rejected for reasons listed in section A.4 [A1].

The 2005 Malaysian Airlines 777 incident occurred on August 1, 2005, at 17:03 Western Standard Time, as a Boeing 777-200 operated by Malaysian Airline System experienced a pitch up approximately 30 minutes after takeoff from Perth, Australia, while climbing through 36,000 ft with autopilot on [A2].

During the pitch up, the aircraft climbed to 41,000 ft and the indicated airspeed dropped from 270 knots to 158 knots. The stick shaker and stall warning indicator activated during the event. The flight landed uneventfully back at Perth [A2].

On August 29, 2005, the FAA issued emergency Airworthiness Directive (AD) 2005-18-51 [A3] to install Air Data Inertial Reference Unit-03 (ADIRU-03) software, stating that faulty ADIRU data could cause anomalies in 777 primary flight controls, autopilot, pilot displays, autobrakes, and autothrottles.

A contributing safety factor was an anomaly that permitted inputs from a known faulty accelerometer to be processed by the ADIRU and used by other aircraft systems, including the primary flight computer and autopilot [A2].

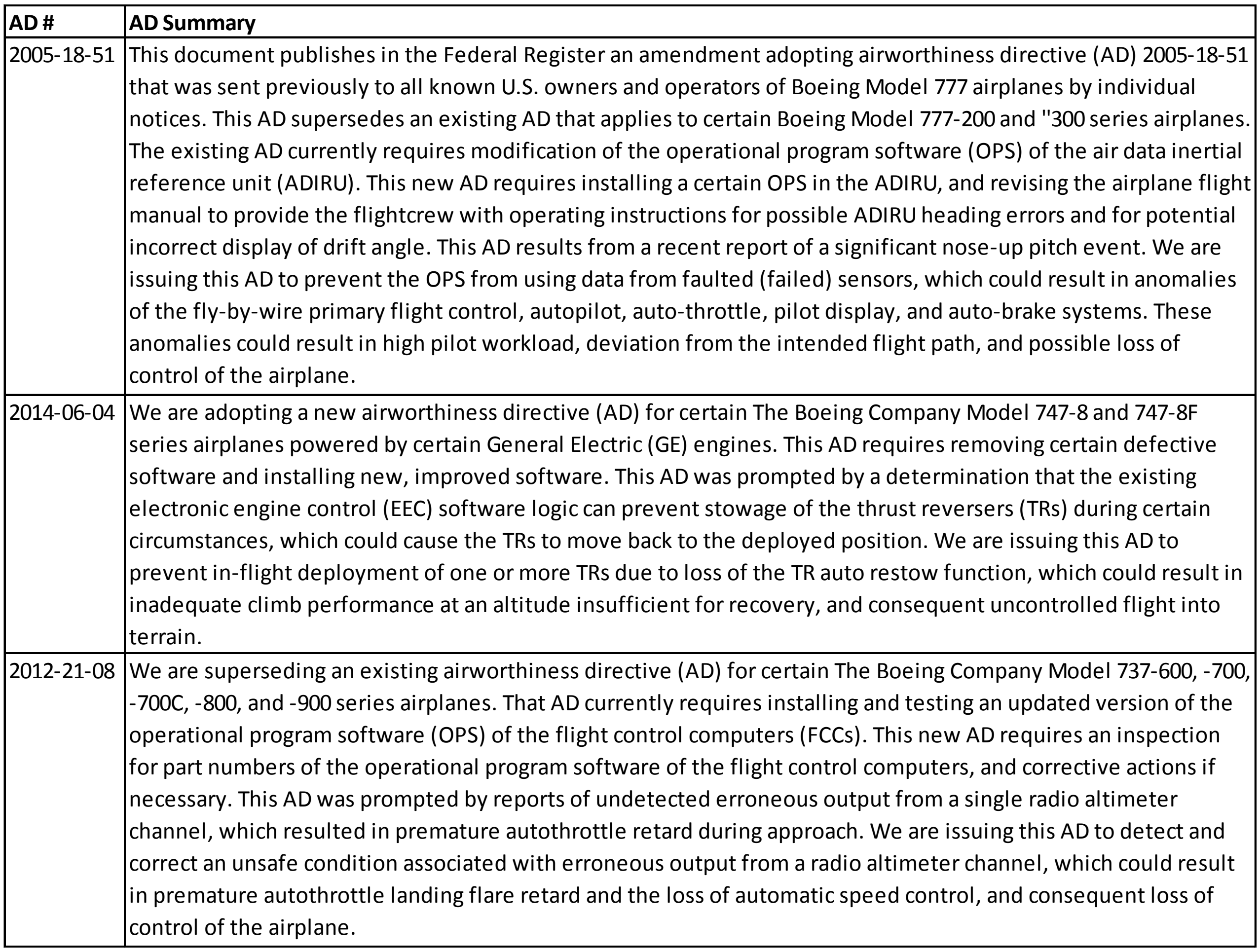
The potential research applicability included:

- Requirements definition and V&V (particularly related to fault-handling requirements)
- Cascading system failure effects and crew workload
- This case was selected because it would allow an in-depth review, particularly from a requirements definition and V&V perspective, of the integration between the different industry standards listed below:

    – ARP4761, “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems” [A4].
    – ARP4754A, “Guidelines for Development of Civil Aircraft and Systems” [A5].
    – Document-297 (DO-297), “Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations” [A6].
    – DO-178B/C, “Software Considerations in Airborne Systems and Equipment Certification” [A7].
    – DO-254, “Design Assurance Guidance for Airborne Electronic Hardware” [A8].

The research team also conducted a review of PRs (from pre-flight systems architecture analyses and flight-test squawks) of recent product development programs. Specifically, requirements changes, systems architecture changes, and software changes were reviewed.

To review possible linkages, the research team reviewed 46 ADs that addressed software involving Boeing aircraft. Three were selected for additional analysis, as shown in figure A-2.



AD #	AD Summary
2005-18-51	This document publishes in the Federal Register an amendment adopting airworthiness directive (AD) 2005-18-51 that was sent previously to all known U.S. owners and operators of Boeing Model 777 airplanes by individual notices. This AD supersedes an existing AD that applies to certain Boeing Model 777-200 and "300 series airplanes. The existing AD currently requires modification of the operational program software (OPS) of the air data inertial reference unit (ADIRU). This new AD requires installing a certain OPS in the ADIRU, and revising the airplane flight manual to provide the flightcrew with operating instructions for possible ADIRU heading errors and for potential incorrect display of drift angle. This AD results from a recent report of a significant nose-up pitch event. We are issuing this AD to prevent the OPS from using data from faulted (failed) sensors, which could result in anomalies of the fly-by-wire primary flight control, autopilot, auto-throttle, pilot display, and auto-brake systems. These anomalies could result in high pilot workload, deviation from the intended flight path, and possible loss of control of the airplane.
2014-06-04	We are adopting a new airworthiness directive (AD) for certain The Boeing Company Model 747-8 and 747-8F series airplanes powered by certain General Electric (GE) engines. This AD requires removing certain defective software and installing new, improved software. This AD was prompted by a determination that the existing electronic engine control (EEC) software logic can prevent stowage of the thrust reversers (TRs) during certain circumstances, which could cause the TRs to move back to the deployed position. We are issuing this AD to prevent in-flight deployment of one or more TRs due to loss of the TR auto restow function, which could result in inadequate climb performance at an altitude insufficient for recovery, and consequent uncontrolled flight into terrain.
2012-21-08	We are superseding an existing airworthiness directive (AD) for certain The Boeing Company Model 737-600, -700, -700C, -800, and -900 series airplanes. That AD currently requires installing and testing an updated version of the operational program software (OPS) of the flight control computers (FCCs). This new AD requires an inspection for part numbers of the operational program software of the flight control computers, and corrective actions if necessary. This AD was prompted by reports of undetected erroneous output from a single radio altimeter channel, which resulted in premature autothrottle retard during approach. We are issuing this AD to detect and correct an unsafe condition associated with erroneous output from a radio altimeter channel, which could result in premature autothrottle landing flare retard and the loss of automatic speed control, and consequent loss of control of the airplane.

Figure A-2. Airworthiness directives for additional analysis

AD 2005-18-51 [A3] stems from the Malaysian Airlines 777 pitch-up incident that occurred on August 1, 2005, as summarized above. AD 2014-06-04 [A9] and AD 012-21-08 [A10] were also considered for additional research but were later determined not to be required since additional scenarios for White Paper 3 were introduced to support the research.

A.3 RECOMMENDATION

Based on the findings in Section A.2, the research team recommended that the Malaysian Airline 777 pitch-up incident be utilized for further investigation. To ensure that an adequate quantity of cases was identified to complete the research, additional scenarios were evaluated as part of White Paper 3 (further information is contained in Appendix C/Scenario 3).

A.4 EVENTS NOT SELECTED FOR FURTHER RESEARCH

The following events were reviewed in light of the litmus filter questions documented in figure A-1 and not included for further research for the reasons indicated.

A.4.1 Swissair Flight SR 111

On September 2, 1998, Swissair Flight 111, a Boeing/McDonnell Douglas MD-11 departed from John F. Kennedy International Airport, in New York, at 2018 eastern daylight savings time (0018 Universal Coordinated Time [UTC]) on a flight to Geneva, Switzerland. The flight included 215 passengers and a crew of 2 pilots and 12 flight attendants. Approximately 1 hour into the flight, the pilots detected an unusual smell. Some 14 minutes later, the pilots declared an emergency. Six minutes after the declared emergency, Flight 111 impacted the ocean about five nautical miles southwest of Peggy's Cove, Nova Scotia, Canada. The aircraft was destroyed and there were no survivors [A11].

The key safety issues were:

- Metalized polyethylene terephthalate thermal/acoustic insulation, in certain installations, had significantly different flammability characteristics than had been demonstrated in compliance tests.
- The inability of the flight crew to easily remove electrical power from the in-flight entertainment network system (lack of a flight deck switch) [A11].

The potential research applicability included:

- Requirements definition, V&V processes.
- Unintended cascading effects of "non-essential" system on continued safe flight and landing.

This case was not selected because it would be difficult to extend the requirements V&V lessons learned to digital avionics systems. In addition, Advisory Circular 25.1701-1, "Certification of Electrical Wiring Interconnection Systems on Transport Category Airplanes," was released on December 4, 2007 and provides guidance for certification of electrical wiring interconnection systems [A12].

A.4.2 Alaska Airlines Flight 261

Alaska Airlines Flight 261, with 2 pilots, 3 cabin crew, and 83 passengers, departed Puerto Vallarta, Mexico to Seattle, with a scheduled stop in San Francisco [A11].

The airplane was functioning normally during the initial phase of flight, but the horizontal stabilizer stopped responding to autopilot and pilot commands after the airplane passed through 23,400 ft.

The pilots recognized the longitudinal trim system was not functioning but could not determine why. The safety board determined the probable cause of the accident was a loss of airplane pitch control resulting from in-flight failure of the horizontal stabilizer trim system jackscrew assembly's Acme nut threads. The thread failure was caused by excessive wear resulting from Alaska Airlines' insufficient lubrication of the jackscrew assembly.

The key safety issues were:

- Inadequate lubrication resulted in failure of the horizontal stabilizer jackscrew assembly Acme nut threads.
- Undetected, plugged grease fitting passage [A11].

The potential research applicability included:

- Requirements definition and V&V.
- Flight crew situational awareness.

This case, which was structural in nature, was not selected because it would be difficult to extend the requirements V&V lessons learned to digital avionics systems.

A.4.3 China Airlines Flight 120

On August 20, 2007, a Boeing 737-800 operated by China Airlines departed from Taiwan's Taoyuan International Airport on a regularly scheduled flight to Naha Airport, Okinawa, Japan. Following landing and leading edge slat retraction, a failed portion of the slat track assembly was pressed through the slat track housing and penetrated the right main fuel tank, causing a fuel leak. At approximately 10:33 local time, fuel that had been leaking from the right wing tank during taxi and parking was ignited by hot engine surfaces and/or hot brakes, resulting in the aircraft being engulfed in flames [A11].

There were 165 passengers and crew onboard, consisting of 8 crewmembers and 157 passengers (including 2 infants). Everyone onboard was evacuated from the aircraft with no casualties. The aircraft was destroyed by the fire, leaving only part of the airframe intact.

The key safety issue was:

- A fuel tank breach, caused by a failed downstop assembly being pushed through the No. 5 slat can, which led to a fuel leak and subsequent fire that destroyed the airplane [A11]

The potential research applicability included:

- Requirements definition and V&V (maintenance/service letters and bulletins)

This case was not selected because it would be difficult to extend the requirements V&V lessons learned to digital avionics systems.

A.4.4 Air France 447

On May 31, 2009, flight AF447 took off from Rio de Janeiro-Galeão International Airport bound for Paris Charles de Gaulle Airport. The airplane was in contact with Brazilian air traffic control at FL350. At approximately 2 hr 02 min, the captain left the cockpit. At approximately 2 hr 08 min, the crew made a course change of approximately 10 degrees to the left, probably to avoid echoes detected by the weather radar [A11].

At 2 hr 10 min 05 sec, likely following the obstruction of the pitot probes in an ice crystal environment, the speed indications became erroneous and the automatic systems disconnected. The airplane's flight path was not brought under control by the two copilots, who were rejoined shortly after by the Captain. The airplane went into a stall that lasted until the impact with the sea at 2 hr 14 min 28 sec.

The key safety issues were:

- Temporary inconsistency between the measured speeds, likely a result of the obstruction of the pitot tubes by ice crystals, causing autopilot disconnection and reconfiguration to alternate law.
- Inappropriate crew control inputs destabilized the flight path.
- Failure to follow appropriate procedures for loss of displayed airspeed information.
- Failure to recognize that the aircraft had stalled—the crew failed to recognize that the aircraft had stalled and consequently did not make inputs that would have made it possible to recover from the stall [A11].

The potential research applicability included:

- Crew situational awareness in the presence of systems failures/degradations.

This case was not selected because it would be difficult to extend the requirements V&V lessons learned to digital avionics systems. The obstruction of the pitot tubes had cascading failure effects. However, there was also operational error (inappropriate crew control inputs, failure to follow procedures, etc.).

A.4.5 Qantas 32

On November 4, 2010, at 01:57 UTC, an Airbus A380 aircraft, registered VH-OQA (OQA) and operated as Qantas flight 32, departed from runway 20 center (20C), at Changi Airport, Singapore, for Sydney, New South Wales. Onboard the aircraft were 5 flight crew, 24 cabin crew, and 440 passengers [A11].

Following a normal takeoff, the crew retracted the landing gear and flaps. The crew reported that, while maintaining 250 knots in the climb and passing 7000 ft above mean sea level, they heard two almost coincident abrupt loud noises followed shortly after by indications of a failure of the No. 2 engine.

A subsequent examination of the aircraft indicated that the No. 2 engine had sustained an uncontained failure of the intermediate pressure turbine disc. Sections of the liberated disc penetrated the left wing and left wing-to-fuselage fairing, resulting in structural and systems damage to the aircraft.

The key safety issues were:

- The investigation team has inspected the damaged engine and components and determined the sequence of events that led to the failure of the engine disc.
- The investigation is also examining the airframe and systems damage that resulted from the engine disc burst to understand its effect on those systems and the impact on flight safety. That includes their effect on the aircraft's handling and performance and on crew workload [A11].

A flight simulator program was used to conduct a number of tests in a certified A380 flight simulator. Analysis of the flight simulation test data is ongoing.

The potential research applicability included:

- Cascading system failure effects and crew workload.

The A380 has an IMA architecture. Though the initial failure source was an engine, there were cascading failure effects for multiple systems. This case was not selected because of the potential difficulties in obtaining the necessary data required to conduct an extensive analysis.

A.4.6 ZA002 Dreamliner

The 787-8 flight test airplane ZA002 experienced an onboard electrical fire during approach to Laredo, Texas on November 9, 2010.

The ZA002 lost primary electrical power as a result of an onboard electrical fire; backup systems, including the deployment of the Ram Air Turbine, functioned as expected and allowed the crew to complete a safe landing.

The team determined that a failure in the P100 panel led to a fire involving an insulation blanket, which self-extinguished once the fault in the panel cleared.

In response to the Laredo incident, Boeing developed minor design changes to power distribution panels on the 787 and updates to the systems software that manages and protects power distribution on the airplane.

Engineers have determined that the fault began as either a short circuit or an electrical arc in the P100 power distribution panel, most likely caused by the presence of foreign debris. The design changes improved the protection within the panel. Software changes were also implemented to further improve fault protection.

The contractor performed extensive analyses in support of the return to 787 flight-test activities. This case was not selected because, though there was a certain level of visibility with this event, it would not provide significant insight into requirements definition and V&V.

Table A-3 lists examples of candidates excluded because of incorrect maintenance/preflight checks of static ports (AeroPeru) and engine turbine hardware failure (Martinaire).

Table A-3. Excluded candidates

Date	Airline	Aircraft Model	Location	Investigation
11/2/1996	AeroPeru	757-23A	Lima, Peru	Preliminary investigation results showed that the aircraft's three static ports on the left side were obstructed by masking tape. The tape had been applied before washing and polishing of the aircraft prior to the accident.
08/30/2013	Martinaire Cargo	MD-11F	BQN International Airport, Aguadilla, Puerto Rico.	Experienced an uncontained LPT failure during takeoff roll from BQN International Airport, Aguadilla, Puerto Rico. No injuries were reported. The takeoff was aborted at 17 knots. Airport fire and rescue responded to the aircraft, but no fire was observed. The aircraft taxied back to the ramp under its own power. Post-event airplane inspection found multiple holes through the left and right sides of the No. 1 engine, aft core cowl, and numerous small airplane wing and main gear impacts/punctures. Inspection of the No. 1 engine, a Pratt & Whitney PW4462-3, serial number (S/N) 733827, found a partial LPT-to-turbine exhaust case flange separation.

BQN = Borinquen; LPT = low-pressure turbine

A.5 REFERENCES

A1. FAA. (April 11, 2014). *SE2020-TORP 1380-Task Order 0022-Modification 0001, Safety Issues with Requirements Definition, Validation, and Verification Processes and Practices* (FAA Publication No. DTFAWA-10-D-00019).

A2. Australian Transport Safety Bureau. (August 1, 2005). *Transport Safety Investigation Report, Aviation Occurrence Report* (ATSB Publication No. 200503722).

A3. FAA. (September 9, 2005). *AD 2005-18-51*.

A4. SAE International. (1996). SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems.

A5. SAE International. (2010). SAE ARP4754A/EUROCAE ED-79A, Guidelines for Development of Civil Aircraft and Systems.

A6. RTCA. (November 8, 2005). DO-297, Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations. Washington, DC.

A7. RTCA. (2001). DO-178B/C, Software Considerations in Airborne Systems and Equipment Certification. Washington, DC.

A8. RTCA. (April 19, 2000). DO-254, Design Assurance Guidance for Airborne Electronic Hardware. Washington, DC.

A9. FAA. (June 4, 2014). *AD 2014-06-04*.

A10. FAA. (November 27, 2012). *AD 2012-21-08*.

A11. FAA. *Lessons Learned From Transport Airplane Accidents*, Retrieved from http://lessonslearned.faa.gov/.

A12. FAA. (December 4, 2007). *AC25.1701-1, Certification of Electrical Wiring Interconnection Systems on Transport Category Airplanes*.

APPENDIX B—WHITE PAPER 2 EXTRACT

B.1 RESEARCH APPROACH

The following research approach was used for White Paper 2:

- Identified existing industry guidelines for requirements definition and validation and verification (V&V) processes.
- Identified shortcomings in current processes in Aerospace Recommended Practice (ARP) 4754A [B1].
- Identified additional processes that are currently not part of ARP4754 [B2]/ARP4754A [B1] or industry best practices. This included:
  - Identified existing industry guidelines for interfaces between:
    - Airplane
    - System/subsystem
    - Software
    - Airborne Electronic Hardware (AEH)
- Identified potential shortcomings in current process interfaces.
- Identified additional process interface clarifications (particularly transition to and from ARP4754A [B1] and Document-178 (DO-178) [B3]).

To identify potential shortcomings in industry guidelines, scenarios were considered in which following these industry guidelines perfectly could potentially fail to identify a potentially catastrophic condition.

Both nominal and failure modes were considered in the evaluation of potential requirements process deficiencies. Understanding the intrasystem and intersystem behavior and validating that an acceptable level of safety is maintained in the presence of cascading failure effects was an integral part of this evaluation.

B.2 PRELIMINARY FINDINGS

B.2.1 Overview of Existing Processes Related to Requirements Definition, Validation, and Verification

Existing industry guidelines were reviewed to identify possible issues and shortcomings with the current process used by the commercial aviation industry regarding requirements definition and V&V for aircraft digital system requirements.

Relevant industry processes related to requirements definition and V&V for avionics and electronic systems are listed in table B-1. Note that this table is provided to emphasize certain aspects of the listed documents and is not a comprehensive listing of all contents.

Table B-1. Existing industry processes

Industry Guideline	Purpose	Primary Applicable Level
ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment [B4]	Provides guidelines and methods for performing the safety assessment for civil aircraft, including (but not limited to) safety analyses such as functional hazard assessment, preliminary system safety assessment, and system safety assessment.	Airplane system/subsystem
ARP4754A, Guidelines for Development of Civil Aircraft and Systems [B1]	Provides guidelines for the DA process. This includes validation of requirements and verification of the design implementation for certification and product assurance. The development planning elements consist of: • Development • Safety program • Requirements management • Validation • Implementation verification • Configuration management • Process assurance (PA) • Certification • Software integration process • Software configuration management • Software quality assurance process • Certification liaison	Airplane system/subsystem

Table B-1. Existing industry processes (continued)

Industry Guideline	Purpose	Primary Applicable Level
DO-254, Design Assurance Guidance for Airborne Electronic Hardware [B5]	Provides design assurance guidance for the development of AEH. Key processes include: • Hardware safety assessment • Requirements capture process • Validation • Verification • Configuration management • PA • Certification liaison	AEH
DO-297, IMA Development Guidance and Certification Considerations [B6]	Provides guidance for IMA modules, applications, and systems. The integral processes consist of: • Safety assessment • System DA • Validation • Verification • Configuration management • Quality assurance • Certification liaison	Software AEH

DA = development assurance; PA = process assurance; IMA = Integrated Modular Avionics

B.2.2 Interrelationships Between Processes

The interrelationships between the processes are shown in figure B-1.

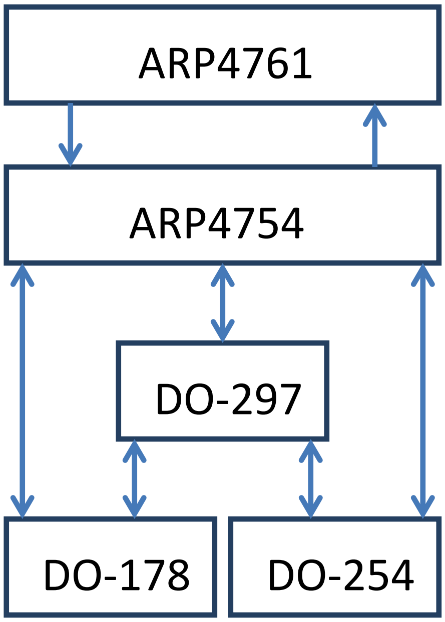


Figure B-1. Interrelationships between processes

Figure B-1 shows the flow between safety assessment processes covered by ARP4761 [B4], development assurance (DA) processes covered by ARP4754 [B2], and design assurance processes covered by DO-178 [B3] and DO-254 [B5]. For the purpose of this document, DO-178 and DO-254 are referred to as "design assurance activities."

Function, failure, and safety information (particularly, derived safety requirements) flow from the ARP4761 processes to the ARP4754A processes. System design information flows from the ARP4754A processes to the ARP4761 processes.

The transition from DA processes to software and hardware design assurance processes occurs when the requirements are allocated to hardware and software items. This is when the transition from ARP4754/ARP4754A to DO-178 and DO-254 occurs.

B.2.3 Information Flow From System DA Processes and Software and AEH Design Assurance Processes

Requirements are allocated to the following elements:

- Hardware
- Software
- DA levels and descriptions of failure conditions, if applicable
- Hardware allocated failure rates and exposure intervals
- System description
- Design constraints
- System verification activities
- Verification evidence

ARP4754A [B1] provides guidance in each of these areas.

B.2.4 Information Flow From Hardware/Software Processes to System DA Processes

The hardware and software processes pass the following information to the system DA process:

- Derived requirements
- Hardware/software/system architecture description
- Verification evidence
- Failure rates and fault detection
- Problem and change reports
- Deficiencies or limitations of intended functionality
- Installation drawings, schematics, part lists, etc.
- System level verification plans

ARP4754A [B1] provides guidance in each of these areas.

B.2.5 Information Flow Between Hardware and Software Processes

The following information is passed between software and hardware processes:

- Derived requirements
- Hardware and software verification
- Hardware and software incompatibilities

ARP4754A [B1] provides guidance in each of these areas.

B.2.6 Potential Errors in Information Flow

Any time there is an interface/information flow, the possibility exists for an error or omission to be introduced. This can occur in the information flow between:

- Airplane to system
- System to airplane
- System to software
- Software to system
- System to hardware
- Hardware to system
- Software to hardware (by way of the system process)
- Hardware to software (by way of the system process)

B.2.7 Clarifying Roles and Responsibilities for Different Information Flows

It is imperative to clearly understand the roles and responsibilities between the different information flows. There is sometimes, erroneously, an assumption that DA activities are the responsibility of the original equipment manufacturer (OEM) and that the supplier is responsible for software and hardware design assurance activities. The research team's experience has noted that this incorrect assumption can sometimes occur (validated by discussions with Boeing supplier management and direct discussions with suppliers).

The FAA has released the following Advisory Circulars (ACs) that state how industry standards/guidelines are an acceptable means of compliance:

- AC20-115C [B7], which recognizes DO-178C
- AC20-152 [B8], which recognizes DO-254
- AC20-174 [B9], which recognizes ARP4754A

The industry guidelines, understandably, do not specify which roles are completed by the OEMs as opposed to the suppliers.

As shown in figure B-2, the transition from AC20-174 DA activities and AC20-115C software design assurance activities, or AC20-152 hardware design assurance activities, occurs with the requirements allocation to hardware and software. The red box indicates the focus area for the requirements allocation process. This step is key to ensuring that hardware and software design assurance activities start with a complete and correct set of requirements.

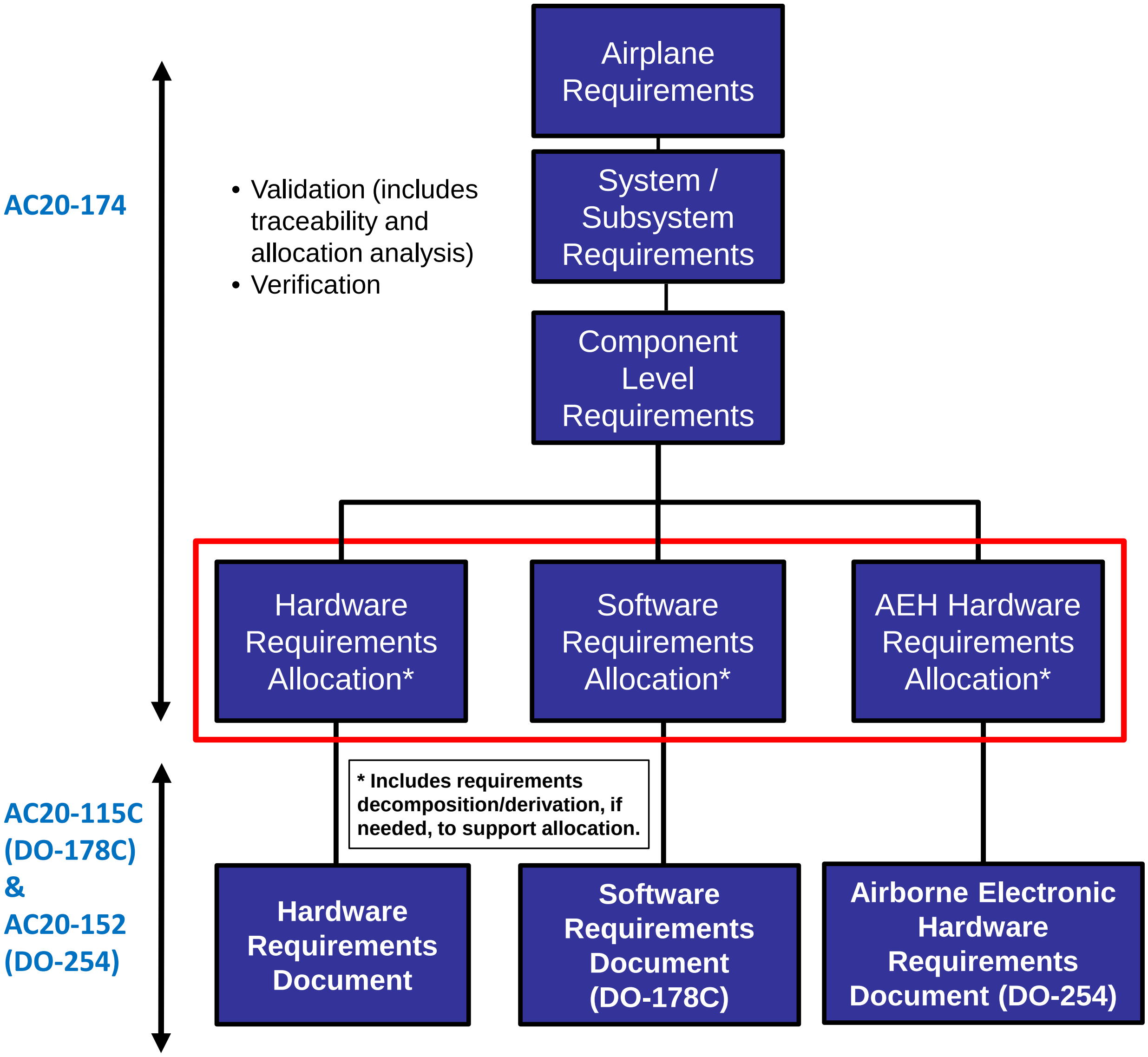

Airplane Requirements
System / Subsystem Requirements
Component Level Requirements
AC20-174
• Validation (includes traceability and allocation analysis)
• Verification
Hardware Requirements Allocation*
Software Requirements Allocation*
AEH Hardware Requirements Allocation*
* Includes requirements decomposition/derivation, if needed, to support allocation.
AC20-115C (DO-178C) & AC20-152 (DO-254)
Hardware Requirements Document
Software Requirements Document (DO-178C)
Airborne Electronic Hardware Requirements Document (DO-254)

Figure B-2. Relationship of ACs

The importance of clarifying the OEM and suppliers' roles and responsibilities was highlighted in different programs and suppliers. This becomes particularly true for business scenarios, as shown in figure B-3, in which the requirements allocation to software and AEH is done by the supplier. This is only one potential scenario. The following example is meant to highlight the importance of clearly understanding roles and responsibilities.

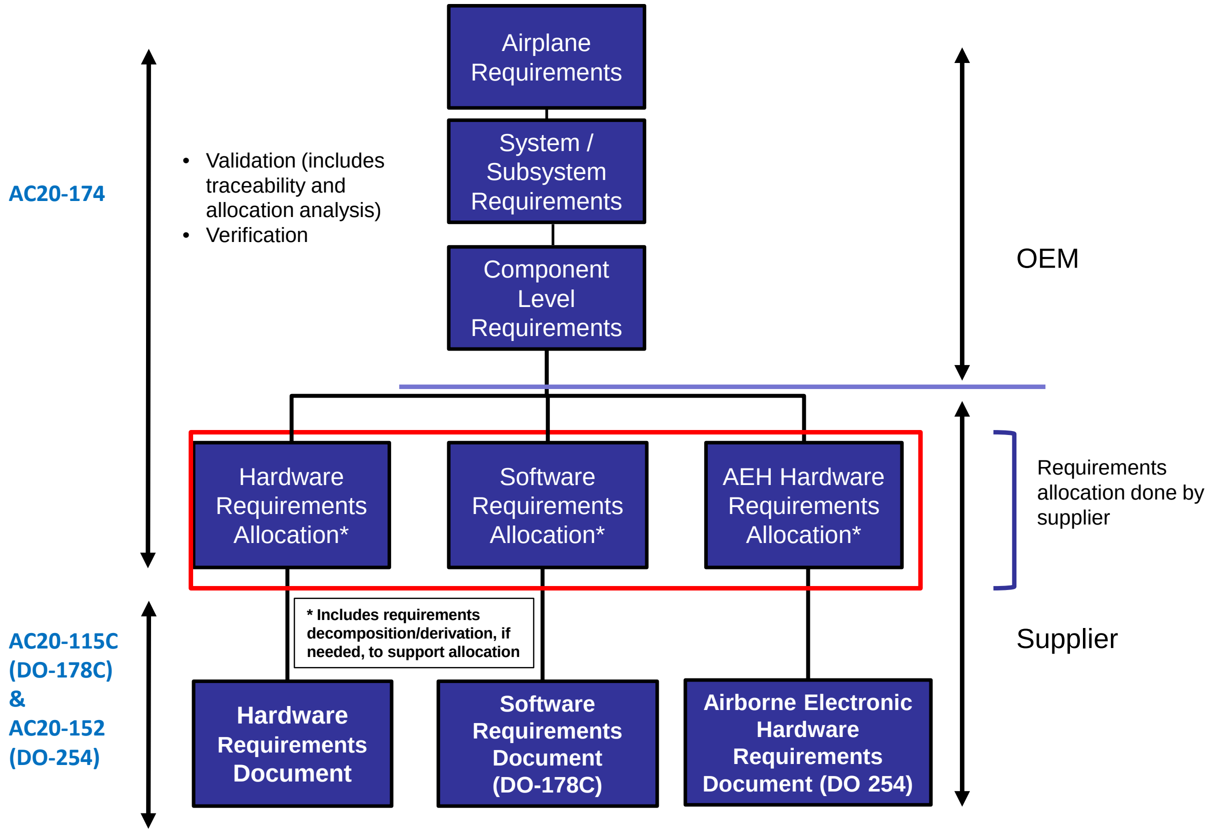

Airplane Requirements
System / Subsystem Requirements
Component Level Requirements
AC20-174
Validation (includes traceability and allocation analysis)
Verification
OEM
Hardware Requirements Allocation*
Software Requirements Allocation*
AEH Hardware Requirements Allocation*
Requirements allocation done by supplier
* Includes requirements decomposition/derivation, if needed, to support allocation
Supplier
AC20-115C (DO-178C) & AC20-152 (DO-254)
Hardware Requirements Document
Software Requirements Document (DO-178C)
Airborne Electronic Hardware Requirements Document (DO 254)

Figure B-3. Typical OEM versus supplier roles and responsibilities

In this scenario, the OEM is following ARP4754A for DA and decomposes and derives airplane-level, system-level, and component-level requirements. A component-level specification is provided to the supplier before requirements allocation to hardware and software. The requirements allocation is typically done by the supplier. To illustrate the importance of supplier requirements allocation, figure B-3 indicates the notional delineation of responsibility between OEM and supplier.

In figure B-3, this means that the supplier would have some DA activities. Figure B-4 shows this same concept from a slightly different perspective.

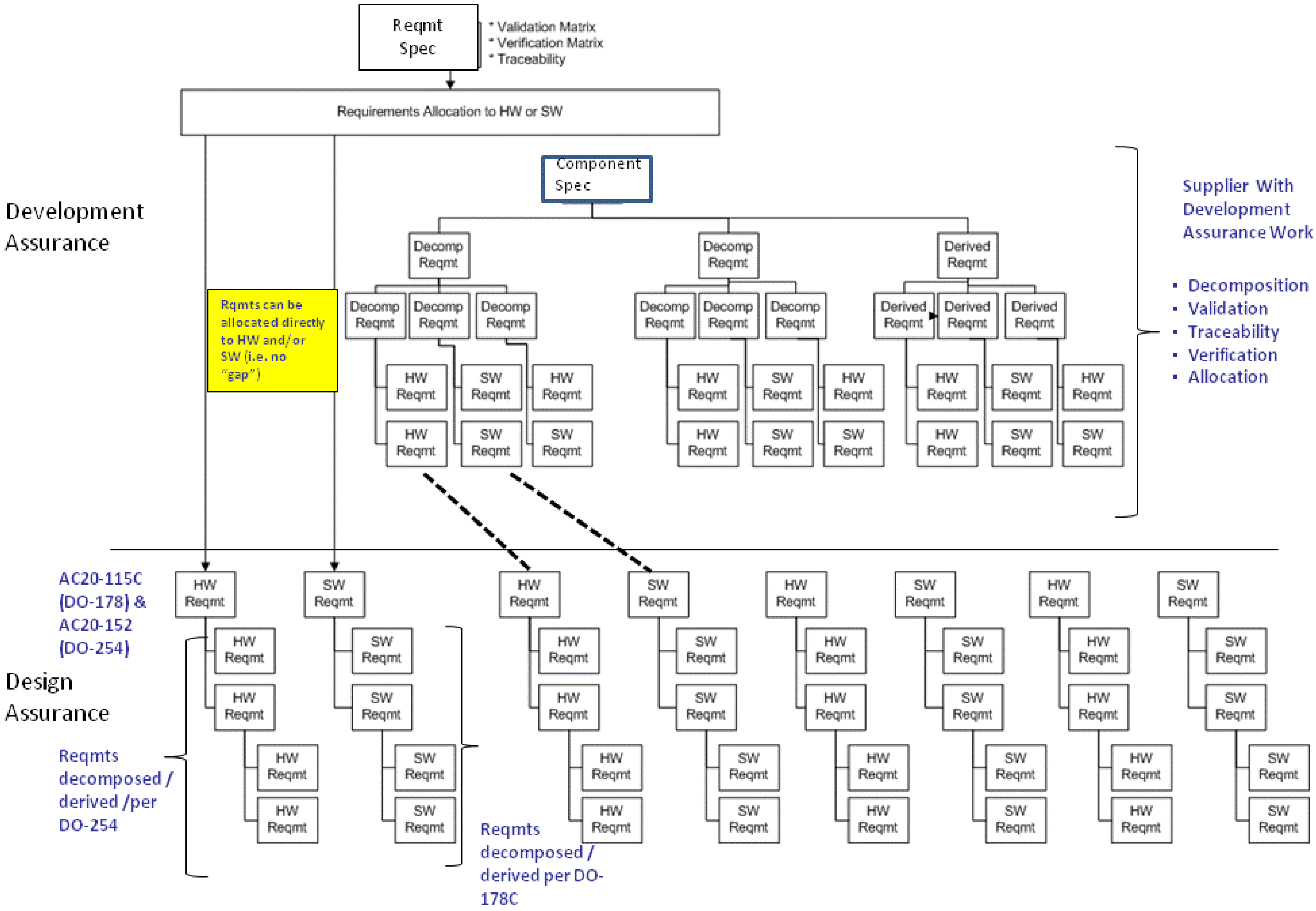

Reqmt Spec
* Validation Matrix
* Verification Matrix
* Traceability
Requirements Allocation to HW or SW
Component Spec
Development Assurance
Decomp Reqmt
Derived Reqmt
HW Reqmt
SW Reqmt
Rqmts can be allocated directly to HW and/or SW (i.e. no "gap")
Supplier With Development Assurance Work
▪ Decomposition
▪ Validation
▪ Traceability
▪ Verification
▪ Allocation
AC20-115C (DO-178) & AC20-152 (DO-254)
Design Assurance
Reqmts decomposed / derived /per DO-254
Reqmts decomposed / derived per DO-178C

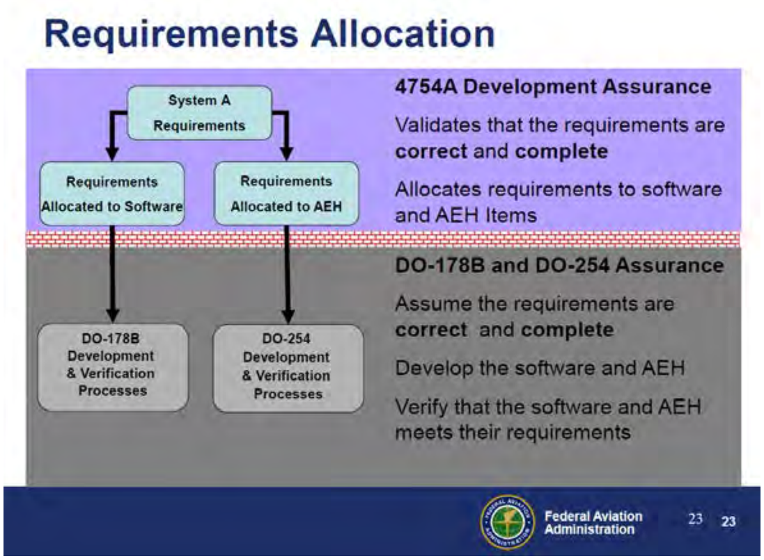
Figure B-4. Requirements decomposition/derivation required for allocation

If the requirements can be directly allocated to hardware/software (i.e., no further requirements decomposition or derivation is required to do the allocation), then the supplier can transition to DO-178 software design assurance processes or DO-254 hardware design assurance processes.

If the supplier is required to conduct requirements decomposition or derivation before the requirements can be allocated to hardware/software, then the supplier has DA activity. In particular, the supplier would need to validate that the decomposed requirements have been validated to be complete and correct.

Validating requirements as complete and correct is an important part of DA. Industry realizes the importance of requirements being verifiable and consistent with other requirements (e.g., that they are correct) and that requirements address the interests (e.g., that they are complete) of all users including operators, maintainers, regulatory agencies, and end customers.

As shown in figure B-5, the assumption is that the requirements allocated to the software and AEH items are correct and complete. As a result, it becomes very important to ensure that both the OEM and the supplier understand their DA roles and responsibilities, particularly those related to requirements validation.


System A Requirements
Requirements Allocated to Software
Requirements Allocated to AEH
DO-178B Development & Verification Processes
DO-254 Development & Verification Processes
Federal Aviation Administration
23
23

Requirements Allocation

4754A Development Assurance

Validates that the requirements are **correct** and **complete**

Allocates requirements to software and AEH Items

DO-178B and DO-254 Assurance

Assume the requirements are **correct** and **complete**

Develop the software and AEH

Verify that the software and AEH meets their requirements

Figure B-5. FAA training on ARP4754A relationship to DO-178/254 [B3, B5]

If the roles and responsibilities are not clearly understood, the chance increases that required DA activities (particularly requirements validation) will not be conducted properly. This can manifest itself in the following information flow problems:

- System to software
- Software to system
- System to hardware
- Hardware to system
- Software to hardware (by way of the system process)
- Hardware to software (by way of the system process)

Based on the research team's experiences, this transition to and from ARP4754A [B1] and DO-178 [B3]/DO-254 [B5] is an important clarification. Discussions with multiple organizations led to the conclusion that there is a certain amount of confusion regarding this topic. As shown in figure B-5, the handoff between DA activities (covered by ARP4754A) and the design assurance activities (covered by DO-178 and DO-254) occurs after the requirements allocation to hardware and software. It is important to clearly establish the DA roles and responsibilities between the OEM and the suppliers. It should not always be assumed that a supplier has no DA activities. As a broad generalization, it appears that this incorrect assumption sometimes occurs because it is assumed that the contractual work statement is directly aligned to the transition between DA and design assurance (i.e., the OEM will be responsible for all ARP4754A-type, DA-type activities, including requirements allocation to hardware and software).

Figures B-2,–B-4 are effective in clarifying the different roles and responsibilities. It should never be assumed that the OEM will be solely responsible for all DA activities and that the suppliers will only be responsible for DO-178 software design assurance processes and DO-254 hardware design assurance processes.

B.2.8 Classic Systems Engineering Validation and Verification

To a certain extent, the existing industry guidelines follow the classic systems engineering V&V model, shown in figure B-6.

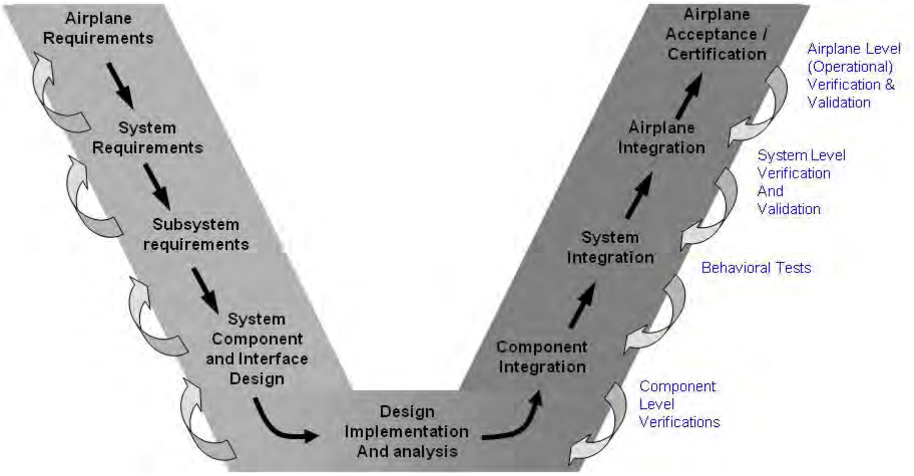

Airplane Requirements
System Requirements
Subsystem requirements
System Component and Interface Design
Design Implementation And analysis
Component Integration
System Integration
Airplane Integration
Airplane Acceptance / Certification
Airplane Level (Operational) Verification & Validation
System Level Verification And Validation
Behavioral Tests
Component Level Verifications

Figure B-6. Systems engineering "V" model

Starting with ARP4754A on the left side of the V, aircraft functions and requirements are developed and derived. There is the further decomposition or derivation of requirements at subsequently lower levels. From an ARP4754A perspective, a large part of the left side of the V is the validation of the requirements. The right side of the V involves the implementation verification of requirements at progressively higher levels.

Similarly, ARP4761 follows a systems engineering V model, as shown in figure B-7.

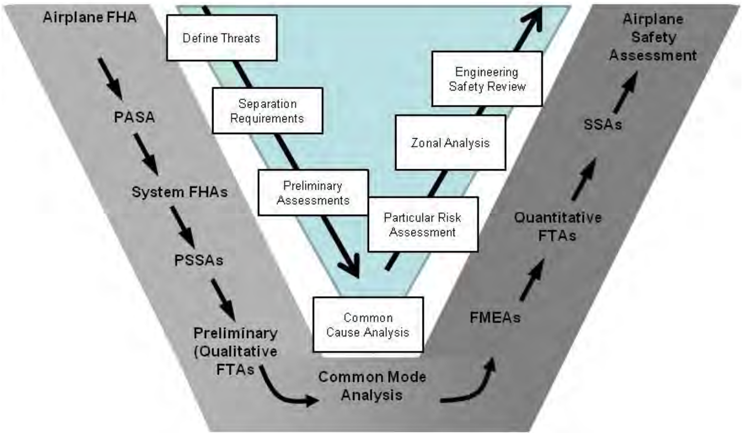


Figure B-7. Safety V model

The left leg of the V represents a top-down requirement development and validation process. This includes the airplane’s functional hazard assessment (FHA), the preliminary aircraft safety assessment, the system FHAs, the preliminary system safety assessment (SSA), and the preliminary (qualitative) fault tree analysis (FTA). The inner V of figure B-7 represents the common-cause analyses steps used to validate that no common threats or failure modes violate the redundancy designed into the systems.

The right leg represents a bottom-up verification process. It includes the failure modes and effects analyses; quantitative FTAs, SSAs; and airplane safety assessment.

In and of itself, there is nothing incorrect with the V model (as modeled in either ARP4754A or ARP4761); however, it is not adequate, particularly when systems move from being federated to highly integrated.

For highly integrated systems, it is important that the “missing middle” of the classic system’s engineering V model be filled in as shown in figure B-8.

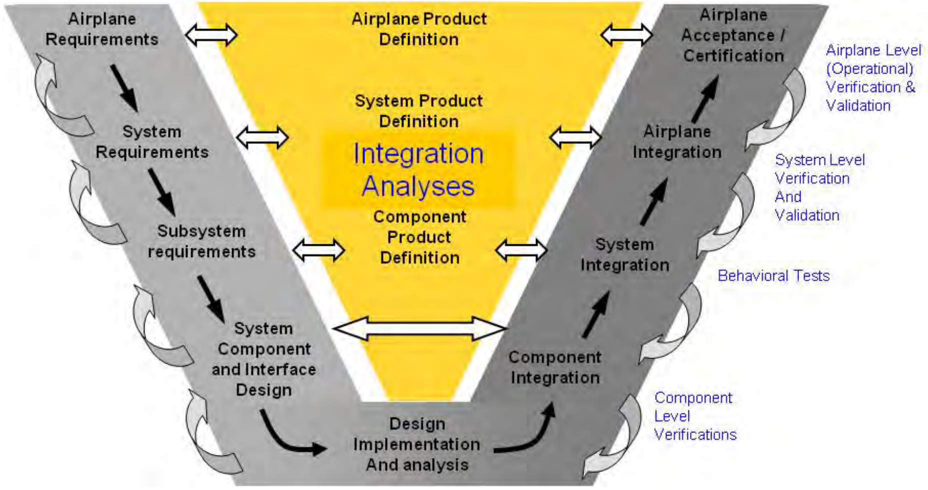

Airplane Requirements
System Requirements
Subsystem requirements
System Component and Interface Design
Design Implementation And analysis
Component Integration
System Integration
Airplane Integration
Airplane Acceptance / Certification
Airplane Product Definition
System Product Definition
Integration Analyses
Component Product Definition
Airplane Level (Operational) Verification & Validation
System Level Verification And Validation
Behavioral Tests
Component Level Verifications

Figure B-8. Systems engineering V model's missing middle

ARP4754A has a very requirements-centric perspective. The requirements are validated to be complete and correct on the left side of the V model. On the right side, the implementation of the requirements is verified; however, the existing DA processes potentially do not adequately address the cross-functional/systems architecture analyses. Validating the requirements on the left side of the V ignores the challenge of addressing emergent behavior and implementation analyses of interactions between system elements that can be partially seen through modeling on the left but only fully seen after implementation on the right side of the V.

In addition, ARP4754A and ARP4761 processes are largely written from a federated (not a highly integrated) perspective.

As shown in figure B-9, for a federated system, it is generally easy for a single designer (or small team) to define the interfaces. By the very nature of a federated system, there are limited cross-functional interfaces. In addition, the failure behavior is more "visible."

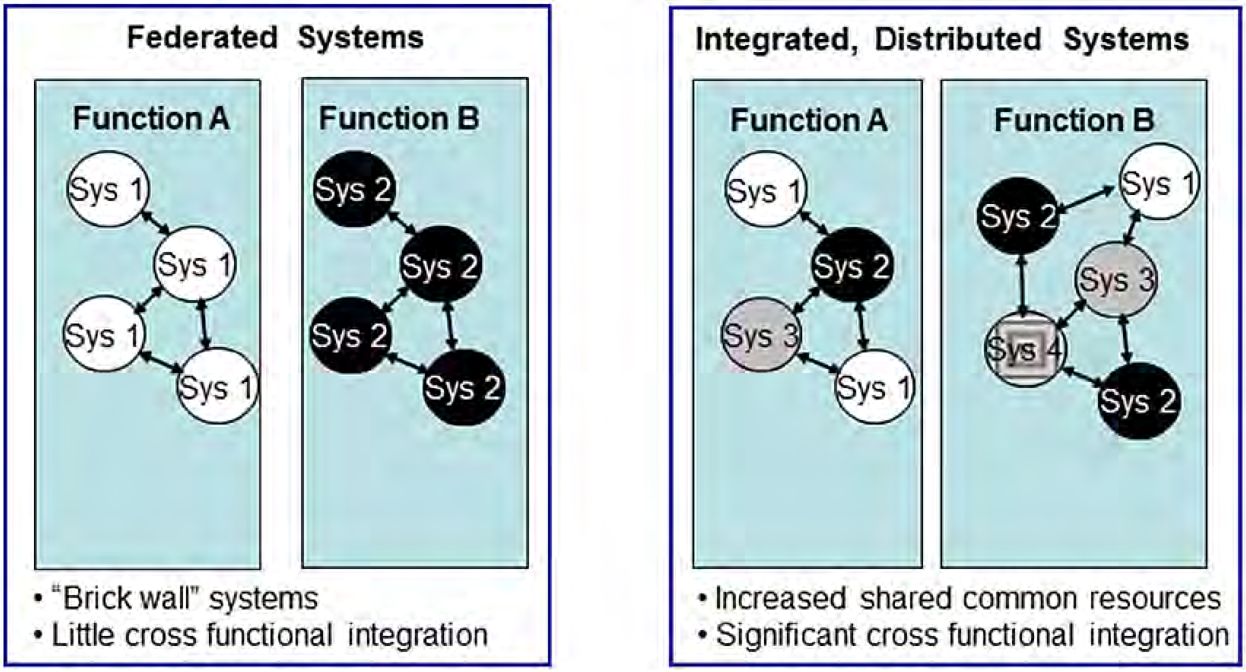


Figure B-9. Federated versus integrated, distributed systems

For an integrated, distributed system, the interfaces need to be defined by many designers. By the very nature of an integrated, distributed system, there are increased cross-functional interfaces.

Industry guidance is not as robust for the integration of distributed systems. The potential gaps in the existing processes include both nominal and failure modes. Table B-2 lists integral processes and industry guidance for their acceptability.

Table B-2. Industry guidance acceptability for integral processes

Integral Process	Industry Guidance Acceptability for Highly Integrated, Distributed Systems
The processes currently used for initial definition of aircraft system-/function-level requirements.	Generally acceptable.
The processes currently used for assigning aircraft system-/function-level requirements into implementation requirements, such as those needed for software and AEH.	Generally acceptable (particularly if OEM/supplier roles and responsibilities are clarified).
The processes currently used for validating single system-/function-level requirements, including pilot evaluation of aircraft-level operation.	Improvement needed to address critical gaps (reference section B.2.9).
The processes currently used for validating intersystem/cross-function requirements, including pilot evaluation of aircraft-level operation.	Improvement needed to address critical gaps (reference section B.2.10).
The processes currently used for identifying missing requirements.	Improvement needed to address critical gaps (reference section B.2.11).
The processes of using requirements-based testing for verification that the system/function operation is correct and complete.	Generally acceptable.

B.2.9 Processes for Validating Single System-/Function-Level Requirements, Including Pilot Evaluation of Aircraft-Level Operation

In general, the processes for validating single system-/function-level requirements are acceptable (from an individual system perspective). However, improvement is needed for the pilot evaluation of the aircraft-level operation for single system-/function-level requirements. This is particularly true for resource systems in which the system's architecture is now very interrelated and highly integrated. The possibility exists that certain failure modes, which in a federated system may have had a limited effect on other systems, may now have a cascading effect on other systems. The resulting cascading effects affect the ability of the flight crew to cope with the situation and provide for safe operation of the airplane.

The following generic example shown in figure B-10 illustrates this process gap. This potentially catastrophic situation would not be found if the existing industry guidelines were followed (particularly ARP4754A [B1] and ARP4761 [B4]).

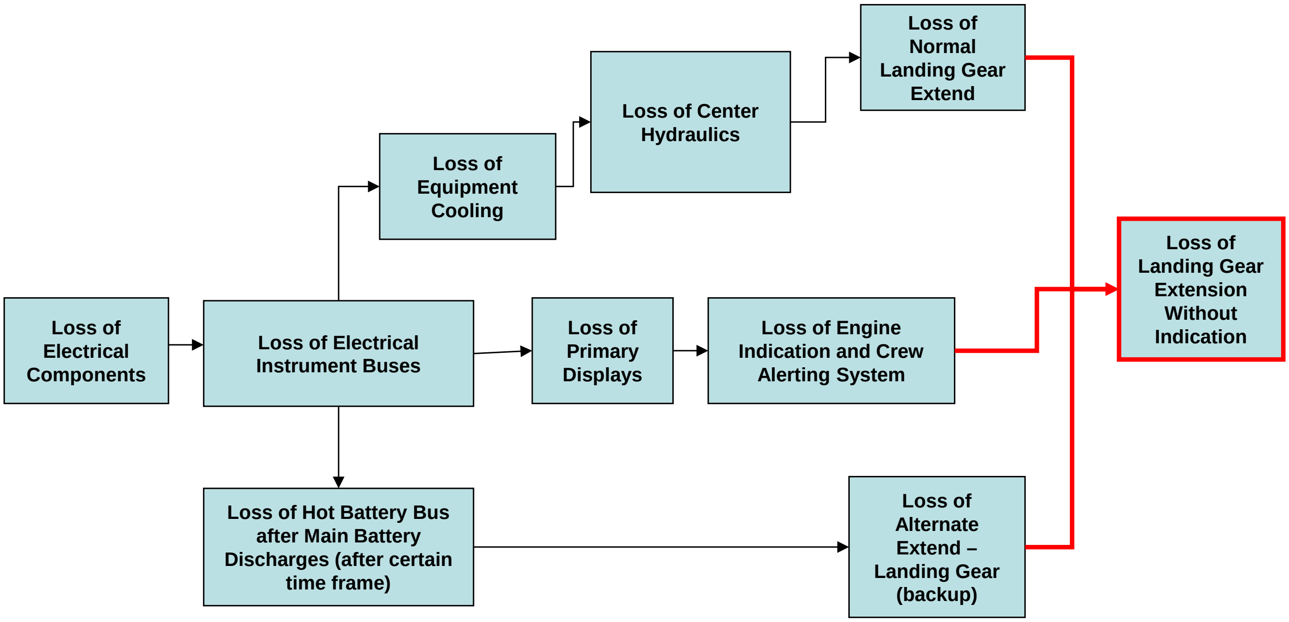

Loss of Normal Landing Gear Extend
Loss of Center Hydraulics
Loss of Equipment Cooling
Loss of Landing Gear Extension Without Indication
Loss of Electrical Components
Loss of Electrical Instrument Buses
Loss of Primary Displays
Loss of Engine Indication and Crew Alerting System
Loss of Hot Battery Bus after Main Battery Discharges (after certain time frame)
Loss of Alternate Extend – Landing Gear (backup)

Figure B-10. Unacceptable, cumulative cascading failure effects

The simplified diagram above shows the results of the cascading failure effects of electrical component failures. The purpose is to illustrate how the stack up of the cumulative system-level effects needs to be understood to ensure that an adequate level of safety is maintained in the presence of failures. At each point, all of the failures are acceptable from a systems perspective (acceptable loss of redundancy). However, the cumulative effect of acceptable systems-level effects is catastrophic at the airplane level. Note that this is for illustrative purposes only; aircraft systems would not be designed and certified in this manner.

B.2.10 Processes Currently Used for Validating Intersystem/Cross-Function Requirements, Including Pilot Evaluation of Aircraft-Level Operation

There is room for improvement in the industry process guidance for the validation of intersystem/cross-function requirements. This occurs at multiple levels:

- Subsystem-to-subsystem
- Component-to-component
- Message-to-message

Figure B-11 shows the braking system for a more federated system. As expected, there are very few cross-functional interfaces. The basic elements include the spoiler handle, brake system control unit, and autobrake solenoid valve.

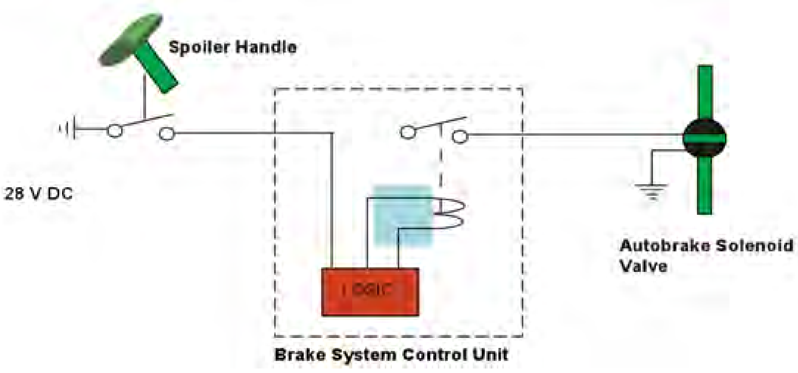


Figure B-11. More federated system

Figure B-12 shows the same system's functionality, as implemented on a more integrated system. The same basic elements exist: spoiler handle, brake system control unit, and autobrake solenoid valve. However, there are significantly more cross-functional interfaces, for which better industry process guidance would be helpful.

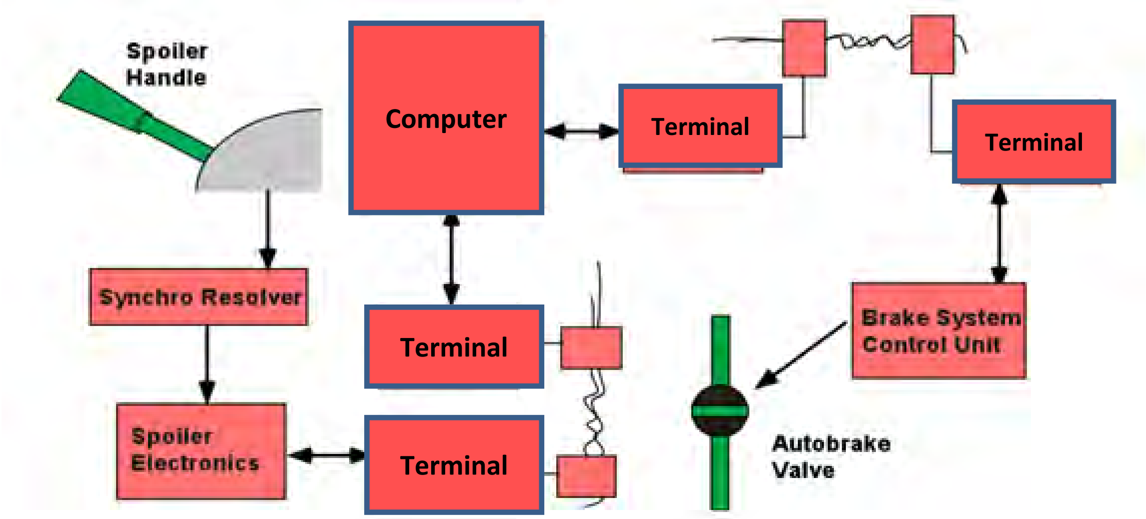


Figure B-12. More integrated system

Another process gap is that there tends to be an assumption that if all of the airplane-level FHAs are acceptable, than the cumulative airplane-level effects of cascading effects will be acceptable. However, this is not a valid assumption for highly integrated systems.

B.2.11 Process for Validating Missing Requirements

The process for validating missing requirements can be improved by:

- Establishing an approach to validate and verify the intrasystem functionality to determine that functions perform as required:
  - System functions within its boundaries using known definitions of its interfaces/boundaries
  - Describe system behavior to interfacing systems
- Establishing an approach for verification of the intersystem functionality to determine proper content and performance:
  - System functions properly in relation to associated functionality provided by interfacing/interacting systems
  - Validation of assumptions made at the intrasystem level
  - V&V of end-to-end functionality and end-to-end signal timing
- Identifying aircraft-level failure modes and effects considerations:
  - Identify single and combination failure conditions to analyze, targeting key integration components/functions to determine that the impacts of failures are as expected and acceptable
  - Include resource systems:
    - Power sources, power distribution systems (engine, electric, hydraulic, pneumatic), and data networks
    - Systems/control signals that affect multiple aircraft functions

B.2.12 Process Gaps Versus Implementation Escapes

It is not possible to have consistent, perpetual flawless execution of any process. The objectives of DA processes are to minimize safety errors that could adversely affect safety. However, no DA process can guarantee that there will be no DA errors.

Errors can occur for different reasons:

- Process gaps do not indicate necessary work statement, increasing the chance for developmental errors (which was the focus of this white paper).
- Implementation escape in executing documented processes.

B.2.13 Summary of Preliminary Findings for White Paper 2

During the examination of requirements, V&V process, and interfaces among the processes, the team noted several potential gaps in industry guidance. A summary of the preliminary findings for White Paper 2 is listed below.

- Review of industry guidelines showed the importance of clearly establishing the DA roles and responsibilities between the OEM and the suppliers—particularly those related to requirements validation, to ensure a complete, correct set of requirements—exists before beginning hardware and software design assurance activities.
- It is possible that existing DA processes may not adequately address the cross-functional/systems architecture analyses. Industry guidance potentially needs to be improved for the integration of distributed systems, to address potential gaps in validation processes, and to identify missing requirements for highly integrated, distributed systems.
- Processes to validate single system- and functional-level requirements are generally acceptable, but potential improvement is needed for pilot evaluation of the aircraft-level operation for single system-/functional-level requirements.
- Potential improvement is needed in the industry process guidance for the validation of intersystem/cross-functional requirements at the subsystem-to-subsystem level, component-to-component level, and message-to-message level.

B.2.14 Preliminary Recommendations

The following preliminary recommendations are suggested for follow-on efforts in Phases 2 and 3 of this TO:

- Investigate processes to help identify missing requirements during the requirements validation phase.
- Examine processes to ensure that OEMs and suppliers are working toward a complete and correct set of requirements to the greatest practical extent.
- Consider the potential need to clarify roles and responsibilities between OEMs and suppliers' potential regarding the transition from DA activities to design assurance activities. Note that it is recognized that this will vary based on the different business models.
- Identify potential gaps that may exist with processes to validate requirements for both single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.
- Consider establishment of an approach to validate and verify intrasystem and intersystem functionality to determine that proper function, content, and performance exist. Include consideration of aircraft-level failure modes and effects.

B.3 REFERENCES

B1. SAE International. (December 21, 2010). SAE ARP4754A/EUROCAE ED-79A, Guidelines for Development of Civil Aircraft and Systems.

B2. SAE International. (1996). SAE ARP4754/EUROCAE ED-79, Certification Considerations for Highly Integrated or Complex Aircraft Systems.

B3. RTCA. (2001). DO-178B/C, Software Considerations in Airborne Systems and Equipment Certification. Washington, DC.

B4. SAE International. (1996). SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems.

B5. RTCA. (April 19, 2000). DO-254, Design Assurance Guidance for Airborne Electronic Hardware. Washington, DC.

B6. RTCA. (November 8, 2005). DO-297, Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations. Washington, DC.

B7. FAA. *Lessons Learned From Transport Airplane Accidents*. Retrieved from http://lessonslearned.faa.gov.

B8. FAA. (December 4, 2007). *AC 25.1701-1, Certification of Electrical Wiring Interconnection Systems on Transport Category Airplanes*.

B9. FAA. (July 19, 2013). *AC20-115C, Airborne Software Assurance*.

APPENDIX C—WHITE PAPER 3 EXTRACT

White Paper 3 examined issues and shortcomings related to requirements definition; validation and verification (V&V) processes; and interfaces, especially in scenarios in which requirements were not properly validated or verified or requirements did not exist at all. Eight real-world scenarios were selected for review.

C.1 SCENARIO #1

In Scenario #1, the system-level requirement was initially specified incorrectly and implemented according to that requirement. The error was not discovered during the validation process or, alternatively, the validation requirements at that level did not occur. This would be an example of a requirements error and an error in the validation of that requirement.

An example is the transition time for the handshake between two systems. The requirement was reviewed by subject matter experts (SME). They were knowledgeable and believed the requirement to be correct. However, during testing, it was determined that the handshake time between the two systems was too long and, accordingly, was adjusted.

C.2 SCENARIO #2

Scenario #2 involved incorrect translation of a correct system-level requirement when assigning that requirement to a specific implementation. For example, a “+” input into a control-law summing junction was incorrectly implemented as a “–” input. This would be an example of a requirement error and an error in the verification of that requirement. This differs from Scenario #1 in that an error in the translation or transcription of requirements occurred. The initially defined requirement was correct.

A bug was introduced by way of a coding error when a data field was used without initialization. The data field was associated with the number of flights between operational tests. The data field is typically initialized when a system test is performed, but not otherwise. When a new software data load is performed to update the equipment, the field is not initialized. The coding error was in using an uninitialized space. Errors like this are typically discovered during peer reviews and testing. Consistency checking and automated removal of the problem without the possibility of human error in peer reviews is also a possible approach.

C.3 SCENARIO #3

In Scenario #3, a requirement that would have addressed an anomalous system operation was never specified. For example, the power-up process while the aircraft was in the air did not specify certain latches, counters, and inputs that were to be initialized.

On August 1, 2005, at 17:03 Western Standard Time, a Boeing 777-200 operated by Malaysian Airline System experienced a pitch up approximately 30 minutes after takeoff from Perth, Australia, while climbing through 36,000 ft with autopilot on.

During the pitch up, the aircraft climbed to 41,000 ft and the indicated airspeed dropped from 270 knots to 158 knots. The stick shaker and stall warning indicator activated during the event. The flight landed uneventfully back at Perth.

In June of 2001, accelerometer #5 failed, with erroneous high output values. The air data inertial reference unit (ADIRU) disregarded the accelerometer output values. The power cycle on the ADIRU occurred on each occasion the aircraft’s electrical system was shut down and restarted. In August 2005, accelerometer #6 failed. The latent software anomaly allows use of the previously failed accelerometer #5 output. The result is the in-flight upset.

On August 29, 2005, the FAA issued emergency Airworthiness Directive (AD) 2005-18-51 [C1] to install ADIRU-03 software, stating that faulty ADIRU data could cause anomalies in 777 primary flight controls, autopilot, pilot displays, autobrakes, and autothrottles.

A contributing safety factor was an anomaly that permitted inputs from a known faulty accelerometer to be processed by the ADIRU and used by other aircraft systems, including the primary flight computer and autopilot [C2].

C.4 SCENARIO #4

Scenario #4 involved requirements that were correctly specified for normal operation but not correctly specified for unexpected operation or for failure conditions (either single or multiple). This could include the situation in which the system response to the unexpected operation or failure condition was specified but that response turned out to be undesirable or the situation in which the failure condition was not anticipated and, therefore, the system response was undefined. This could be an example of a requirements error/omission and an error in requirements validation.

An example is pump reservoir rise/fall due to a dip in pump speed resulting from long power interrupts. Long power interrupts lead to dips in pump speed that cause a momentary rise/fall of the pump reservoir, with corresponding dips in pump current and loop pressure. The falling edge of the transient in the reservoir position is quick enough to initiate the leak detection/isolation logic, leading to nuisance leak indications.

C.5 SCENARIO #5

Scenario #5 involved requirements that were correct for operations for an individual system or systems, but the operation of the two or more interfacing systems—during normal operations or during failure conditions—were incompatible with each other. This would be an example of a requirements conflict between two systems.

This scenario covers cases in which the requirements are correct from a federated systems perspective but not from an integration perspective. This scenario can cause problems for interfacing systems (particularly in the presence of failures) and usually occurs during design changes. For example, if a system makes a design change to its voting algorithm, its effects would need to be understood and clearly communicated to other systems.

C.6 SCENARIO #6

Scenario #6 involved cascading failure conditions through multiple aircraft systems or functions due to an initial failure or set of failures not correctly identified. This would be an example of the requirements for multiple systems not having been adequately validated or, possibly, a requirements conflict between two or more aircraft systems.

As systems architectures become more integrated, many systems functions that were typically separated with limited interdependence are now interrelated and highly integrated. The possibility exists that certain failure modes, which in a federated system may have limited effect on other systems, may now have cascading effects on other systems. It is important to validate that the flight crew will be able to cope with failures that result in multiple flight-deck effects. Integration analyses and testing are necessary to validate the acceptability of failure modes, which may result in the following flight deck effects:

- Highly integrated (e.g., integrated modular avionics system, electrical system, and others) unit failures that cause multiple, confusing, or cascading effects, alerts, unusable electronic checklists. For existing related regulations, reference Title 14 Code of Federal Regulations Parts 25.1302 and 25.1322, which address precedence of warning, cautions, advisories, and applicable crew actions for each.
- Burying time-sensitive alerts.
- Display loss or inappropriate reversions.
- Cascading effects from “simple” single failures (e.g., generator).
- Loss of crew alerting.
- Inability of crew to find correct checklist.

Boeing developed processes to address gaps in existing industry guidelines. The cascading failure analyses support validation that the systems architecture integration on the airplane meets the airplane-level safety requirements. The implementation of Boeing’s processes identified requirements changes, design changes (including software changes), wiring changes, crew procedure changes, and test changes. Boeing does not believe that it would have identified these required changes if it had simply followed Aerospace Recommended Practice (ARP) 4754A and ARP4761.

From the March 2011 issue of Boeing’s *Frontiers* magazine (Volume XI, Issue X), chief project engineer Mike Sinnett described one of the tests that validated the cascading failure analyses:

> “Sinnett described one particularly challenging test that demonstrates the overall robustness of the 787 design and its capability to maintain safe conditions in the presence of multiple failures. ‘We intentionally failed one of the three air-data systems that provide key information on speed and altitude,’ Sinnett explained. ‘After that, we caused the remaining two systems to disagree.’ When the two remaining systems disagree, it means there is no known valid source of speed and altitude data. That is when the backup systems kick in. ‘Pilots see an annotation that they are getting this information from backup systems, but they never lose data on the primary flight display,’ Sinnett continued. Altitude is provided from

> the Global Positioning System (GPS) system. Known conditions from a variety of systems and inputs, including aircraft gross weight, angle of attack, high-lift configuration and other parameters, allow the airplane to back-calculate airspeed from the lift equation and display it on the flight deck. ‘This represents a significant advancement in safety and crew awareness in the presence of multiple failures,’ he said” [C3].

C.7 SCENARIO #7

Scenario #7 involved system-level requirements that did not correctly anticipate flight crew actions or responses to specific conditions or failures. This scenario covers a deliberate action by the flight crew that was not necessarily anticipated by the system designers. Note that it is understood that the designers can never fully protect an airplane from doing something totally wrong or unexpected, particularly if it is not consistent with crew procedures or training. For example, an autopilot design did not anticipate the flight crew making control inputs into the flight control system without first disconnecting the autopilot.

On July 13, 1996, a MD-11 experienced an in-flight upset near Westerly, Rhode Island. On June 8, 1997, a different MD-11 experienced an in-flight upset near Nagoya, Japan. Per National Transportation Safety Board (NTSB) Recommendations A-99-39-44 [C4], these in-flight upsets were caused when the flight crewmembers made manual flight control inputs while the autopilot system was engaged. Per the airplane flight manual, they should not have made manual flight control inputs when the autopilot was engaged. Doing so results in a sudden and abrupt movement of some flight control surfaces; when the autopilot disengages, there is an unpredictable airplane response.

In both in-flight upsets, the crewmembers took actions that they believed were appropriate to address their concerns (in one case, concern that the airplane might not level off at assigned altitude, creating a need to slow the rate of descent; in the other case, concern that the airplane would accelerate beyond the maximum operating airspeed). However, in both cases, the crewmembers made manual control inputs prior to disengaging the autopilot.

The NTSB recommendations ranged from revising airplane flight manuals/company flight manuals to improve awareness to requiring all new transport-category airplane autopilot systems to be designed to prevent flight upsets when manual inputs to the flight controls are made [C4].

C.8 SCENARIO #8

In Scenario #8, all system-level requirements were initially complete and correct. However, a change was made in one area, such as a specific aircraft system, function, or sub-function, and that change was not adequately analyzed so that the change adversely affected the operation of another aircraft system or function. This would be an instance of a requirements conflict. In addition, this is an instance of the system-level change impact analysis (CIA) not being performed completely or correctly.

These results are sometimes referred to as “change on change.” After a change is implemented in one system, it has unanticipated, unexpected effects on other systems, resulting in the need to drive additional changes. Having a robust CIA is the best way to mitigate this issue. In general, this tended to happen when there was a subtlety in the design change implementation that was not clearly understood by all impacted systems’ teams.

C.9 SUMMARY OF PRELIMINARY FINDINGS

Anything that involves humans can result in human errors. Discussions with software and airborne electronic hardware (AEH) SMEs validated that errors can occur in software and AEH that are not related to higher-level requirements errors or omissions (i.e., the requirements had been properly allocated to hardware and software, but there were errors in the detailed implementation). These discussions highlighted the following:

- Mistakes can happen anywhere in the development space.
- Design assurance reviews can never be 100%.
- Design assurance reviews still cannot guarantee a perfect product because the reviewer can make mistakes, too. The purpose of having the robust processes in place is to minimize errors.

The research also revealed that there could be cases in which higher-level requirements/constraints were not identified/communicated to the software and AEH developers. From an industry guidelines perspective, there is some room for improvement to mitigate this from occurring.

The purpose of the ARP4754A [C5] development assurance (DA) process is to address the increased integration of systems. Boeing has practical experience validating and verifying complex and highly integrated systems. In addition, Boeing participated in the creation of Aerospace Information Report (AIR) 6110, Contiguous Aircraft/System Development Process Example [C6]. The purpose of this AIR was to provide a practical example of an implementation of ARP4754A (and its interrelationships with ARP4761 [C7]). This AIR, though consistent with ARP4754A guidance, lacked key integration activities (the systems integration guidance contained in Section 4 of ARP4754A could be improved). Additional research could examine the horizontal and vertical integration guidance provided in ARP4754A to assess whether additional guidance might be recommended. This research would also include potential process improvements in the direct links among ARP4754A and ARP4761; DO-178 [C8]; and DO-254 [C9].

Stated differently, there is room for process improvement in industry guidelines related to horizontal and vertical integration:

- Airplane-level V&V
- Intersystem V&V
- Intrasystem V&V
- Component-level V&V

From an industry guideline perspective, this could impact the robustness level of integrated V&V programs, including robustness of testing at component, subsystem, system, and system-of-systems levels.

The systems architecture and integration activities are an integral contributor to DA. There are interfaces between the systems architecture and integration activities and the safety assessment activities. This interaction is important to identify design constraints for other interfacing systems (and their lower-level hardware and software). As systems become more integrated, it is more likely that systems will be levying requirements and constraints on other systems (more so than in a federated systems architecture). Improving/clarifying the interactions between system development and the safety assessment process (particularly related to the integration of different systems) could be beneficial.

This is not meant to imply that manufacturers and suppliers have not developed internal processes to analyze the systems architecture at its different levels. It just acknowledges that this information is not explicitly or clearly contained in the existing industry guidelines. If this is not done correctly, it increases the likelihood that DO-178 and DO-254 will not begin with a complete and correct set of requirements. As has been observed in numerous articles, the software is generally doing exactly what it was designed to do (which also supports the general adequacy of DO-178). When there are problems, they are usually caused by flawed (incomplete or incorrect) requirements.

White Paper 2 contained additional information on methods to help validate missing requirements from an integration perspective.

Another area of improvement in ARP4754A is providing additional guidance on the modification of existing systems. The majority of ARP4754A is written as if the system being developed is a “clean sheet” system. However, most systems are either modifying an existing system or using an existing system in a new environment. Again, this is not meant to imply that manufacturers and suppliers have not developed their internal change impact assessment processes to support this type of activity; it is just an acknowledgement that there is a potential area for improvement in the industry guidelines.

The final recommended area for further investigation is identifying when the existing guidelines would not be adequate for the more integrated systems. For example, the research team identified cases in which:

- All of the failures (first order and cascading effects) are acceptable from a systems perspective (acceptable loss of redundancy, degraded performance, etc.). However, the cumulative effect of acceptable systems-level effects is catastrophic at the airplane level.
- All of the failures (first order and cascading effects) are acceptable for a given airplane-level functional hazard assessment (FHA). Cumulative effect of acceptable, individual airplane-level FHA is catastrophic when viewed from a multi-airplane level FHA perspective.

Boeing recognized process gaps in the existing industry guidelines (particularly in ARP4754A and ARP4761). It does not believe that it would have found systems architecture deficiencies for highly integrated systems had it had simply followed industry guidelines.

C.10 REFERENCES

C1. FAA. (September 9, 2005). *AD 2005-18-51*.

C2. Australian Transport Safety Bureau. (August 1, 2005). *Transport Safety Investigation Report, Aviation Occurrence Report* (ATSB Publication No. 200503722).

C3. Gunter, L. (2011). Dream flights: Extreme measures. *Boeing Frontiers*, *IX*(X), 34-36.

C4. National Transportation Safety Board. (May 25, 1999). A-99-39-44, Safety Recommendation. Retrieved from http://www.ntsb.gov/safety/safety-recs/recletters/A99_39_44.pdf.

C5. SAE International. (December 21, 2010). SAE ARP4754A/EUROCAE ED-79A, Guidelines for Development of Civil Aircraft and Systems.

C6. SAE International. (December 16, 2011). SAE, SAI AIR6110, Contiguous Aircraft/System Development Process Example.

C7. SAE International. (1996). SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems.

C8. RTCA. (2001). DO-178B/C, Software Considerations in Airborne Systems and Equipment Certification. Washington, DC.

C9. RTCA. (April 19, 2000). DO-254, Design Assurance Guidance for Airborne Electronic Hardware. Washington, DC.

APPENDIX D—WHITE PAPER 4 EXTRACT

The following subsections detail research findings for each of the selected real-world avionics scenarios provided in appendix C.

D.1 SCENARIO #1 FINDINGS

There was a requirement for the transition time for the handshake between primary flight controls and autopilot. As part of the requirements validation process, the content of the requirement was reviewed by the subject matter experts (SMEs), who determined that the handshake time requirement was correct. The requirement was then baselined, allowing the design, build, and verification process to proceed for this system. As part of the overall verification process, a test matrix was developed that included both nominal and off-nominal cases. One of the off-nominal cases—single engine out testing on an upward sloping runway—showed that the handshake time requirement was too long. It should be noted that this condition was very unique to the flight-testing regime. During flight test programs, profiles are flown which are outside of normal operations to gather data and test conditions that will not be experienced by operational airlines. For example, data can be collected for conditions beyond the normal operational boundaries to validate behavior. By doing this, the flight test program helps verify that the airplane will support the performance of all functions relative to performance in revenue service.

Source data for this scenario included SME interviews, Boeing Commercial Airplanes product development flight squawks, and problem reports (PRs).

This scenario highlights the potential need for additional industry guidance in the examination of processes to ensure that original equipment manufacturers (OEM) and suppliers are working toward a complete and correct set of requirements to the greatest practical extent.

D.2 SCENARIO #2 FINDINGS

The software made by one supplier had a bug introduced into it through a coding error in which a data field associated with the number of flights between operational tests was used without initialization. This data field is initialized when a system test is performed but not otherwise. When a new software data load was performed to update the equipment, this field was not initialized. This was really a two-part error. The first part was to make the coding error of using uninitialized space. This escaped software-level verification testing because the sequence of testing would have included a step that did the proper initialization. The second error was the decision to fail the system when the counter reached a certain value. The correct action should have been to annunciate the condition but continue to operate. The software was peer reviewed by the supplier and approved by the supplier. In further investigations to successfully resolve the PR, it was validated that the requirements were complete and correct; the software needed to be modified.

Source data for this scenario included SME interviews, test squawks, and PRs.

This scenario highlights the potential need for additional industry guidance in identifying potential gaps that may exist with processes to validate and verify requirements for both single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.

D.3 SCENARIO #3 FINDINGS

The air data inertial reference unit (ADIRU) software was Document-178B (DO-178B) compliant. The anomaly in the original ADIRU software, which allowed inputs from a known faulty accelerometer to be processed by the ADIRU and used by the flight computer, autopilot, and other aircraft systems, was not detected during testing.

Accelerometer #5 failed with erroneous high output values. The ADIRU software disregarded the erroneous high output value from accelerometer #5; it was programmed to use the values from backup systems. However, the restart of the ADIRU masked the initial failure of accelerometer #5; the power cycle on the ADIRU occurs on each occasion the aircraft's electrical system is shut down and restarted. In addition, a latent software error that allowed the ADIRU to use input of an accelerometer had failed. When accelerometer #6 failed, the previously failed accelerometer #5 output was used, resulting in the in-flight upset [D1].

This scenario highlights the potential need for additional industry guidance in the following areas:

- Examine processes to ensure that OEMs and suppliers are working toward a complete and correct set of requirements to the greatest practical extent.
- Identify potential gaps that may exist with processes to validate and verify requirements for both single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.
- Evaluate failure conditions on system functions and assurance of requirements to resolve undesirable combinations affecting aircraft/system performance.

D.4 SCENARIO #4 FINDINGS

Based on interviews with Boeing design SMEs and requirements experts and reviews of problem reports, it was determined that this scenario can occur when either the required resolution/required tolerance are not properly specified. This can become a problem in normal operations. It becomes even more of a problem when the required resolution/required tolerance is not specified for unexpected operations or failure conditions. This scenario highlights the importance of considering off-nominal and failure modes as a critical part of requirements validation and verification (V&V).

Source data for this scenario included SME interviews, test squawks, and PRs.

This scenario highlights the potential need for additional industry guidance in the following areas:

- Investigate processes to help identify missing requirements during the requirements validation phase, particularly those related to horizontal integration.
- Examine processes to ensure that OEMs and suppliers are working toward a complete and correct set of requirements to the greatest practical extent.
- Consider potential process improvements to address cumulative effects of otherwise acceptable individual systems-level cascading effects.

D.5 SCENARIO #5 FINDINGS

Based on interviews with Boeing design SMEs and requirements experts and reviews of problem reports, it was determined that this scenario can also occur when the required resolution/required tolerance are not properly specified, particularly from an integration perspective. This can sometimes happen when changes are made to a voting algorithm. For example, if a system changes its voting algorithm to make its data invalid based on a +/- tolerance of 10° C, it will cause problems if an interfacing system is expecting data to be invalid if the tolerance is +/- 1° from the agreed-upon constraint. There are several reasons why this can occur. If the requirements are not validated to be complete and correct, then problems can occur. In addition, there can be problems from both a horizontal and vertical integration perspective. Some of the required tolerances may be in place to support safety analyses. If the vertical integration and requirements traceability is missing, there is the possibility that the key requirements will not be identified. As a result, an interfacing system may change its tolerance without understanding the impact on other systems. If the horizontal integration is not adequately performed, the interfacing systems will not be aware of the required constraints the systems are imposing on each other.

Source data for this scenario included SME interviews, test squawks, and PRs.

This scenario highlights the potential need for additional industry guidance in the following areas:

- Examine processes to ensure that OEMs and suppliers are working toward a complete and correct set of requirements to the greatest practical extent.
- Identify potential gaps that may exist with processes to validate requirements for both single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.
- Consider establishing an approach to validate and verify intrasystem functionality to determine that proper function, content, and performance exist:

    - Include consideration of intersystem functionality verification.
    - Include consideration of aircraft-level failure modes and effects.

- Investigate the potential need to improve horizontal and vertical integration for V&V processes at the component, intrasystem, intersystem, and airplane levels.

D.6 SCENARIO #6 FINDINGS

The example above provides a “positive” example (as opposed to a “negative” example, which is discovered as a PR). It also emphasizes the importance of having good intrasystem, intersystem, and failure analyses to validate the system’s architecture. Requirements are an integral part of the design process. However, it is also important to conduct the systems architectural analyses. Doing so can help validate that the requirements are complete and correct.

Source data for this scenario included SME interviews, test squawks, and PRs.

This scenario highlights the potential need for additional industry guidance in the following areas:

- Identify potential gaps that may exist with processes to validate requirements for both single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.
- Consider establishing an approach to validate and verify intrasystem functionality in order to determine that proper function, content, and performance exist:
    - Include consideration of intersystem functionality verification.
    - Include consideration of aircraft-level failure modes and effects.
- Investigate potential process improvements to facilitate requirements validation for the modification of existing systems.
- Investigate the potential need to improve horizontal and vertical integration for V&V processes at the component, intrasystem, intersystem, and airplane levels.
- Consider potential process improvements to address cumulative effects of otherwise acceptable individual systems-level cascading effects.

D.7 SCENARIO #7 FINDINGS

The autopilot was designed with the assumption that the flight crew would not provide manual inputs when the autopilot was engaged. The airplane flight manual directed that this should not occur. However, pilots did provide manual inputs with the autopilot engaged. System complexity was determined to be the key contributing factor for the example above. It was not necessarily the system complexity of the system by itself. It was the broader aspect of system complexity that considers how the system operates in both normal and failure conditions and unexpected flight crew actions [D2].

This scenario highlights the importance and challenges when considering potential unexpected pilot actions. It is not possible to consider all potential unexpected pilot actions (e.g., not following training associated with the required crew procedures for an annunciated message). It is also expected that the crewmembers will follow established procedures. A possible area for future research is the design of systems that interface with humans to monitor the human-machine interface and respond to inputs not within the boundaries of normal operations.

This scenario highlights the potential need for additional industry guidance in the following areas:

- Investigate processes to help identify missing requirements during the requirements validation phase.
- Identify potential gaps that may exist with processes to validate requirements for both single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.

D.8 SCENARIO #8 FINDINGS

After interviews with requirements management SMEs and change/configuration management experts, it was determined the key contributing factor that causes this scenario is increased systems complexity. As systems become more highly integrated, the impact of a change on other systems may not be readily apparent without a rigorous change impact analysis (CIA). Some key areas to consider as part of the CIA include the impact on:

- Functionality
- Performance
- Interfaces (particularly with other systems)
- Safety analyses
- Resource utilization
- Emerging system behavior

If the cross-functional impact is not considered when changes are implemented, it is possible there will be a subsequent “change on changes.” This can occur when proper consideration is not given to the cross-functional impact of a given change. The change fixes the original problem; however, the change now also introduces new problems, precipitating the need for another change.

Source data for this scenario included SME interviews, test squawks, and PRs.

This scenario highlights the potential need for additional industry guidance in the following areas:

- Examine processes to ensure that OEMs and suppliers are working toward a complete and correct set of requirements to the greatest practical extent.
- Identify potential gaps that may exist with processes to validate requirements for both single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.
- Consider establishing an approach to validate and verify intersystem functionality to determine that proper function, content, and performance exist. This would include resource utilization and emerging system behavior:
    - Include consideration of intersystem functionality verification.
    - Include consideration of aircraft-level failure modes and effects.

- Investigate potential process improvements to facilitate requirements validation for the modification of existing systems.

D.9 WHITE PAPER 4 CONCLUSIONS

The eight scenarios summarized in this White Paper identify the following potential areas for root-cause investigation required by White Paper 5:

- Scenario 1: This scenario highlights the potential need for additional guidance in examining processes to ensure that OEMs and suppliers are working toward a complete and correct set of requirements to the greatest practical extent.
- Scenario 2: This scenario highlights the potential need for additional guidance in identifying potential gaps that may exist with processes to validate requirements for both single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.
- Scenario 3: This scenario highlights the potential need for additional guidance in the following areas:

  - Examine processes to ensure that OEMs and suppliers are working toward a complete and correct set of requirements to the greatest practical extent.
  - Identify potential gaps that may exist with processes to validate requirements for both single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.

- Scenario 4: This scenario highlights the potential need for additional guidance in the following areas:

  - Investigate processes to help identify missing requirements during the requirements validation phase.
  - Examine processes to ensure that OEMs and suppliers are working toward a complete and correct set of requirements to the greatest practical extent.
  - Consider potential process improvements to address cumulative effects of otherwise acceptable individual systems-level cascading effects.

- Scenario 5: This scenario highlights the potential need for additional guidance in the following areas:

  - Examine processes to ensure that OEMs and suppliers are working toward a complete and correct set of requirements to the greatest practical extent.
  - Identify potential gaps that may exist with processes to validate requirements for both single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.
  - Consider establishing an approach to validate and verify intrasystem functionality to determine that proper function, content, and performance exist.

    - Include consideration of intersystem functionality verification.

        - Include consideration of aircraft-level failure modes and effects.

    - Investigate the potential need to improve horizontal and vertical integration for V&V processes at the component, intrasystem, intersystem, and airplane levels.

- Scenario 6: This scenario highlights the potential need for additional guidance in the following areas:

    - Identify potential gaps that may exist with processes to validate requirements for both single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.
    - Consider establishing an approach to validate and verify intrasystem functionality to determine that proper function, content, and performance exist.

        - Include consideration of intersystem functionality verification.
        - Include consideration of aircraft-level failure modes and effects.

    - Investigate potential process improvements to facilitate requirements validation for the modification of existing systems.
    - Investigate the potential need to improve horizontal and vertical integration for V&V processes at the component, intrasystem, intersystem, and airplane levels.
    - Consider potential process improvements to address cumulative effects of otherwise acceptable individual systems-level cascading effects.

- Scenario 7: This scenario highlights the potential need for additional guidance in the following areas:

    - Investigate processes to help identify missing requirements during the requirements validation phase.
    - Identify potential gaps that may exist with processes to validate requirements for both single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.

- Scenario 8: This scenario highlights the potential need for additional guidance in the following areas:

    - Examine processes to ensure that OEMs and suppliers are working toward a complete and correct set of requirements to the greatest practical extent.
    - Identify potential gaps that may exist with processes to validate requirements for both single-system/function and intersystem/cross-function levels, including pilot evaluation of aircraft-level operation.
    - Consider establishing an approach to validate and verify intrasystem functionality to determine that proper function, content, and performance exist.

    - Include consideration of intersystem functionality verification.
    - Include consideration of aircraft-level failure modes and effects.

  - Investigate potential process improvements to facilitate requirements validation for the modification of existing systems.

The research team’s initial approach for Phase 2 research involved the examination of possible reasons that might cause or contribute to requirements errors, omissions, and conflicts in light of the eight scenarios outlined in Phase 1.

During Phase 1, the research team reviewed the nine possible reasons listed in the Task Order 22 performance work statement and found that they had potential applicability to the research. In addition, the research team identified two additional possible reasons involving horizontal and vertical integration for incomplete and incorrect requirements. All 11 possible reasons are addressed in appendix E, section E.2.

The initial approach to Phase 2 research involved evaluating each scenario for applicability of these 11 possible reasons. This effort led to the creation of table D-1 to identify possible patterns of repetition. Additional research involving a questionnaire was conducted in Phase 2. This information is presented in appendix E, section E.1.

Table D-1. Scenario/possibility mapping summary

	Possibilities that might cause or contribute to requirements errors, omissions, and conflicts	1	2	3	4	5	6	7	8	9	10	11
WP 3 Scenario #	Description											
1	Incorrect requirement discovered during V&V	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Yes	Not a contributor	Not a contributor	Not a contributor	Not a contributor
2	Incorrect translation/implementation of a correct requirement	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Yes	Yes	Not a contributor	Not a contributor
3	Anomalous system operation requirement not specified	Yes	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Yes	Not a contributor	Yes	Not a contributor	Not a contributor
4	Requirements not correctly specified for unexpected operation/failure conditions	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Yes	Yes	Not a contributor	Yes	Not a contributor
5	Standalone system requirements are incompatible with integrated systems operations	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Yes	Not a contributor	Yes	Yes	Yes
6	Inadequate or missing V&V of cascading failure conditions	Yes	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Yes	Yes	Yes
7	Requirements do not anticipate (non-standard) expected crew actions	Yes	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Not a contributor	Yes	Not a contributor	Not a contributor	Not a contributor	Not a contributor
8	Standalone system design changes not analyzed for effects on interfacing systems	Yes	Not a contributor	Yes	Not a contributor	Not a contributor	Not a contributor	Yes	Yes	Yes	Yes	Not a contributor

D.10 REFERENCES

D1. Australian Transport Safety Bureau. (August 1, 2005). *Transport Safety Investigation Report, Aviation Occurrence Report* (ATSB Publication No. 200503722).

D2. National Transportation Safety Board. *A-99-39-44*, *Safety Recommendation*. Retrieved from http://www.ntsb.gov/safety/safety-recs/recletters/A99_39_44.pdf.

APPENDIX E—WHITE PAPER 5 EXTRACT

The following sections detail the Phase 2 questionnaire, responses from subject matter experts (SMEs), and the findings and results as referenced in section 5.1.

E.1 PHASE 2 QUESTIONNAIRE

The following is the Phase 2 questionnaire:

Inputs on Requirements and V&V Questionnaire

Background:

Boeing was awarded a research study contract by the FAA known as 'Task Order 22' (TO-22), which is part of a broader umbrella contract known as Systems Engineering 2020 (SE 2020).
The objective of TO-22 is to identify possible issues and shortcomings with the current process used by the commercial aviation industry regarding requirements definition, validation and verification for aircraft digital system requirements. We are currently working to classify and categorize identified issues and shortcomings, and determine associated root causes.

Preamble:

Please consider responding to this questionnaire during a few quiet moments. Suggest focusing on first-order/primary considerations that come to mind quickly. Lengthy responses (more than a few sentences) are not required.
Your response will be included in the TO-22 study; as such, they will be documented in a publically released report.
Pending the results of this phase of TO-22, the FAA may request Boeing to identify approaches to mitigate these occurrences.
The FAA has expressed that the results of this research may be used to formulate proposed changes to industry guidance material and FAA advisory circulars.

Questions:

- Where are current digital systems requirements development, validation and verification processes ~~are~~ breaking down? Can you suggest an example scenario (or two) to illustrate your response?
- What possibilities might cause or contribute to digital systems requirements errors, omissions and conflicts? Perhaps they may have to do with growth of Digital System Complexity or System Integration?
- Why do problems with digital systems requirements for aircraft continue to occur? Can you suggest or do you know root cause(s)?
- Based on your experiences and knowledge of problem reports, how would you Pareto out the distribution of the following problems:
    - Problem #1 - The system-level requirement was initially specified incorrectly and implemented according to that requirement. The error was not discovered during the validation process, or else the validation requirements at that level did not occur. This would be an example of a requirements error, as well an error in the validation of that requirement.
    - Problem #2 - Incorrect translation of a correct system-level requirement when assigning that requirement to a specific implementation. For example, a "+" input into a control law summing

junction was incorrectly implemented as a “–” input. This would be an example of a requirement error, as well as an error in the verification of that requirement. This differs from Problem #1 in that an error in the translation or transcription of requirements occurred. The initially defined requirement was correct.

- Problem #3 - A requirement that would have addressed an anomalous system operation was never specified (requirement was omitted). For example, the power-up process while the aircraft was in the air did not specify certain latches, counters, and inputs that were to be initialized.

- Problem #4 - Requirements were correctly specified for normal operation were not correctly specified for unexpected operation or for failure conditions. This could include the situation where the system response to the unexpected operation or failure condition was specified but that response turned out to be undesirable, or the situation where the failure condition(s) was (were) not anticipated, and therefore the system response was undefined. This could be an example of a requirements error and/or omission, as well as an error in requirements validation.

- Problem #5 – Requirements were correct for operations for an individual system or systems, but the operation of the two or more interfacing systems—during normal operations or during failure conditions—were incompatible with each other. This would be an example of a requirements conflict between two systems.

- Problem #6 - Involved cascading failure condition(s) through multiple aircraft systems/functions due to an initial failure or set of failures that were not correctly identified.

- Problem #7 - System-level requirements where designers did not correctly anticipate potential flight crew actions. (Note: It is understood that the designers can never fully protect an airplane from doing something totally wrong or unexpected, particularly if it is not consistent with crew procedures or training).

- Problem #8 - All system-level requirements were initially complete and correct. However, a change was made in a specific system, function, or sub-function that was not adequately analyzed in terms of impacts to another system or function.

- Problem #9 – Inadequate horizontal integration is conducted, resulting in interfacing systems not being aware of design constraints that systems are imposing on each other.

- Problem #10 – Inadequate vertical integration is conducted during the development from aircraft to system to item. Errors are made as the parent requirements are decomposed and derived into lower level children requirements.

Note: this more of a qualitative assessment, in which you are assessing how percentage distribution for these problems. If you believe that there are additional types of problems which contribute to incorrect, incomplete, or missing requirements, please identify the additional scenario(s) and Pareto. The total of your percentages should equal 100%.
Please note to focus on the primary contributors when making this assessment (and not secondary problems).

Considerations: As you respond to the above questions, consider what possibilities might cause or contribute to aircraft digital system requirements errors, omissions and conflicts? Perhaps they may have to do with growth of System Complexity or System Integration?

Response: Please forward your input directly to Dan Fogarty. If you have any questions, please email or call Dan directly.

Final Question: Any other concerns related to possible issues and shortcomings with the current process used by the commercial aviation industry regarding requirements definition, validation and verification for aircraft digital system requirements? Please respond below:

E.1.1 Findings and Results

Questions from the Phase 2 questionnaire appear as the primary bullet points and the SME responses appear in subsequent bullet points:

- Where are current requirements development, validation and verification processes breaking down? Can you suggest an example scenario (or two) to illustrate your response?

    - Observations

        - Validating the completeness of requirements for new and novel systems. Especially where those systems are complicated.
        - Improvements can be made in establishing plans that are enough (but not too complex) to generate unambiguous life cycle data. It is important to allocate the required resources to execute the plans.
        - It is important to ensure that there are rigorous up-front development and validation processes/activities.
        - Excessive or exclusive reliance on review of requirements as a means of up-front validation. Peer reviews are necessary, but not sufficient. They will catch only a limited set of errors.
        - Failure to recognize the inherently iterative nature of development. For example, requiring 100% of content for interface control data, prior to any real design work. Some data can and should be captured as soon as possible, but other data (e.g., detailed Built-in Test Equipment [BITE] reports) cannot be fully defined and validated until lower-level design is underway.
        - Lack of a uniform definition and training on what constitutes validation and what the expectations are, at each phase of design. The result is varying levels of coverage, and rigor during reviews, analysis, and test.
        - There's a very broad span of opinion and practice about what is the appropriate level of requirements definition and what should be defined as a requirement.
        - Fidelity of highly integrated lab testing equipment and thoroughness of such test procedures.
        - It is important to clearly establish roles, responsibility, and authority.
        - Software is built on the assumption of hardware behavior. If the hardware doesn't behave as expected, there will be software/airborne electronic hardware (software/AEH) problems.

  - Examples

    - Missed requirement resulted in later design change. Network gateway signals are used to enable dataloading of airplane systems. During the early development, the requirement for the need for certain signals to be gatewayed even when a switch was not known to have a valid configuration installed for its location on the aircraft, the requirement was missed for the need to gateway those signals required to enable dataload when the network system was going through an update. If a network system upgrade service bulletin was incorrectly installed, the airplane would be grounded until preloaded spares could be added. (Note: this had no impact on safety; at no time were incorrect software configurations loaded. The effect would be an increase in the required maintenance times).
    - A program used to generate takeoff performance numbers was noted to take an excessive amount of time to calculate on the test vehicle. It was discovered that the same behavior was noted in lab testing but the tester did not flag the problem because the pass / fail criteria of the test did not specify a time requirement for the calculation. It was taking 2.5 minutes to compute takeoff numbers.

- What possibilities might cause or contribute to requirements errors, omissions and conflicts? Perhaps they may have to do with growth of System Complexity or System Integration?

  - Observations

    - Most commonly, these problems occur where multiple organizations and/or companies must develop requirements that work together to perform some functions while also operate independently to develop their other requirements. In essence, the team focus can sometimes be more immediately on what they need and less urgently on the coordinated activity.
    - Change is another “environmental” consideration. What assumptions did the developer make about changes that happen around them? Can their system detect when they could be affected by a change? Do they understand line replaceable unit (LRU) hardware/app software/airplane system/airplane compatibility issues that can arise when one or more parts change?
    - Often due to insufficient system requirements, failure/lack of thorough reviews, insufficient domain knowledge.
    - Requirement errors, omissions, etc., are merely the human factor. Requirement development and validation methods, and the recognized effort to define a correct, complete, and appropriate set of requirements

        haven't always adjusted to the increased integration of the systems architectures.

    - It is important to understand the fidelity of models/simulations being used.

  - Examples

    - It is important to consider environmental impacts such as Single Event Upset (SEU) upset. This gets to a key question: how do you find out whether assumptions about changes in the environment are valid? Some questions to help drive out requirements: Is your hardware susceptible to Single Event Effects (SEE)? What kinds of SEE is it susceptible to? Does your system design handle all of these effects? Have you assessed the secondary effects of your systems mitigation activities for SEE? What assumptions did the design make to manage redundancy? Have you assessed the secondary effects of your redundancy management actions?
    - The simulations used to model the hydraulic system pressures were not accurate in a specific flight-test condition (outside the bounds of normal airplane operation). When the test vehicle performed a similar condition in flight, Engineering subsequently discovered that their hydraulic system pressure model was not accurate. After updating the model, it was shown that a system logic change was required to preclude the unnecessarily triggering of the subsystem.
    - The ice detection system on the test vehicle was noted to display a transient failure during certain test maneuvers. The sensor probes were known to be sensitive to rapid changes in angle of attack or angle of sideslip. The corrections derived from analysis had not been fully tested in the wind tunnel due to technical and economic practicalities. The requirements to which the probes were designed did not consider the extreme and prolonged maneuvering performed during flight testing. The filtering of parameters had to be re-evaluated to ensure no such erroneous behavior would occur within the normal envelope of operations expected in service. (Note: this occurred during cascaded stalls and sideslips (i.e., outside the normal airline operating environment).

- Why do problems with digital systems requirements for aircraft continue to occur? Can you suggest or do you know root cause(s)?

  - Observations

    - Specification validation of interfaces between systems is frequently not executed in a way that is commensurate with the inevitable evolutionary nature of this complex problem. It is common for instance to require complete definition of all interfaces in one or two iterations prior to the point in development where the systems function is defined sufficiently to allow for a complete definition.

    - Problems can sometimes occur because the requirement is too prescriptive at the system/subsystem or higher. Having requirements that are too prescriptive can drive requirements changes/churn.
    - Sometimes the requirement does not have the connection to the intent. As result, the requirements verification focuses on the letter of the law (instead of the spirit). This can be mitigated by capturing the intent as the requirements rationale or creating a parent requirement which clearly captures the intent.
    - As traditionally federated systems move to integrated modular avionics architectures, it is important for systems to understand the digital domain. As systems start including a significant software component, it is important to understand some of the issues that digital processing can introduce (sampling artifacts, how significant digits are affected by error terms, etc.).
    - It is important for the system designers to have a good understanding of the environment in which their system will be operating in.

  - Examples

      - One system assumed that because the values they were keeping track of should be changing slowly that the digital behavior would also be immune to sampling artifacts. It turned out that some signals were transient and the low sampling rates would cause one copy to see the signal and another copy to miss it.

- Based on your experiences and knowledge of problem reports, how would you Pareto out the distribution of the following problems:

  - Attempts to Pareto examples of problems along the lines of the questionnaire are not the correct way to look at the overall problem. Rather, the responses to the earlier questions provide the needed information.

- Any other concerns related to possible issues and shortcomings with the current process used by the commercial aviation industry regarding requirements definition and validation and verification (V&V) for aircraft digital system requirements? Please respond below:

  - We did not receive any inputs to this question; however, SME input to prior questions addressed possible issues and shortcomings.

These findings emphasize the importance of having validated, complete, and correct requirements and recognizing the iterative nature of requirements validation. The following is a summary of common trends offered by the SMEs that may help identify potential areas of improvement:

- Improving the validation (completeness and correctness) of requirements, particularly for new, novel, and/or complex systems.
- Recognizing the inherently iterative nature of development. Re-evaluating plans and requirements content predicated on a linear design process. For example, a linear design process may require 100% of the content for interface control data to be specified prior to any real design work. Some data can, and should, be captured as soon as possible, but other data (e.g., detailed BITE reports) cannot be fully defined and validated until lower-level design is underway. Program management practices (including organizational structure) may need to evolve with the non-linear nature of developing highly complex, integrated digital systems.
- Optimizing level of detail for development of plans in a disciplined fashion.
- Optimizing level of technical oversight to ensure plans are executed in a disciplined fashion.
- Looking to the future as designs grow in complexity, consider prototyping to help with validating the completeness and correctness of requirements against preliminary design architectures. The prototyping process can augment the peer-review process, which will remain necessary. Prototype tools can include model-based design (MBD), simulation, and simulated distributed tests, particularly for integrating across multiple systems.
- Providing a uniform definition and training approach on what constitutes validation and what the expectations are at each phase of the design. Without this in place, it is possible for varying levels of coverage and rigor during reviews, analysis, and tests. In light of the growth of complexity and integration, there is a need to iterate to an integrated solution. An analogy is the spiral software process.
- Developing an optimum level of fidelity in highly integrated lab testing equipment and test procedure completeness to accelerate learning and reduce the cost of problem discovery on the aircraft.
- Validating assumptions about the environment.

Sections E.1.2–E.1.8 provide research findings from the Phase 2 questionnaire responses.

E.1.2 Systems Complexity and Systems Integration

To achieve increased functionality and improved performance, systems architectures are becoming more centralized and automated, with avionics designers integrating more functions and capabilities that reflect new technologies and increasing customer expectations.

As a result of the evolution of airplane architectures, airplane functions traditionally supported by individual systems may now be integrated on a common computing platform with a common communication infrastructure (e.g., an integrated modular avionics [IMA] architecture). These architecture changes provide several benefits to the airlines, pilots, and passengers. Integrated architectures can result in a reduction in parts, wiring, and weight that directly relates to decreased maintenance costs and, in the case of weight, decreased fuel burn. Increased integration and high reliance on software can also create more flexibility when system changes are needed, reflecting new technologies and increasing customer expectations.

Adoption of IMA architecture and new electrical designs are two significant changes in airplane systems architectures. Moving to IMA architecture and introducing more electrically powered systems help improve performance and reduce overall airplane weight, but these design decisions also greatly increase system interface complexity. For the IMA architecture, airplane functions traditionally supported in a federated manner are now integrated on a common platform. For example, the electrical system moved from a traditional centralized bus design to a remote distribution design.

The benefits of the highly integrated systems architectures also come with a challenge: managing an order of magnitude increase in data traffic. Calculations that were once carried out in individual systems can now be executed in an IMA. Raw data are collected at the source, packaged, sent to the IMA, processed, and the results repackaged and sent to subscribers. Detailed information about IMAs can be found in DO-297, “Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations.” This type of architecture increases signal traffic and makes data networks more intricate. Data management challenges of these new architectures include ensuring the network meets all timing, latency, and bandwidth requirements, because an individual signal may now have to cross 5–10 nodes on its path from source to subscriber.

The increased systems integration and complexity increases the importance of requirements development. Problems related to iterative integration generally do not occur for self-contained (i.e., federated) functions with little or no integration. The problems occur when multiple systems have to participate in an airplane function such as power-on scenarios, data load, and the like.

To help mitigate integration issues later in the program, it would be very beneficial for new and novel systems (IMA, remote power distribution, etc.) to develop requirements for the other airplane systems on how to use these resource systems as one of their first priorities. This would need to cover nominal and failure scenarios. With new and novel systems, a preliminary recommendation is to first prioritize the integration requirements for other systems.

Requirements development and validation methods—and the recognized effort to define a correct, complete, and appropriate set of requirements—have not always adjusted to the more integrated systems architectures. For example, a supplier decides to implement using a multitasking operating system of its own design. Such a design requires certain implementation practices to work robustly. The engineer writing the high-level requirements and designing the architecture does not identify the shared resources and the behaviors that the tasks need to follow. The engineer reviewing the requirements does not spot the problem either. The design/code is reviewed at a module rather than at an integrated level. There is no specific requirement attached to the desired behavior, so verification testing does not catch the problem until it is discovered later during lab integration testing.

From a software process perspective (defined as taking a system specification and turning it into executable code), experience seems to indicate that industry is good at ensuring the code matches the specification. For example, the processes and execution are generally very good at ferreting out problems in which there is an incorrect translation of a correct systems-level requirement when assigning that requirement to a specific implementation. This type of problem would be least likely to occur during integration and flight test.

E.1.3 New/Novel Technology/New Environments

Problems can arise when the engineers preparing the specification/conducting V&V are not familiar with the digital domain (even if they are familiar with the airplane function). Experience with the digital domain can be increasingly important. If the engineer does not foresee some of the issues that digital processing can introduce (sampling artifacts, how significant digits are affected by error terms, etc.), problems can occur during early testing. As another example, a system could assume that because the values being tracked should be changing slowly, the digital behavior would also be immune to sampling artifacts. Some signals can be transient and the low sampling rates would cause one copy to see the signal and another copy to miss it. If there was a better understanding, this problem would not remain undiscovered until testing and could be mitigated.

The operating environment also needs to be considered. For example, the following questions would help ensure a more complete understanding of the operating environment and acceptable systems behavior:

- Is the hardware susceptible to single event effects (SEE)?
- To what kinds of SEE is it susceptible?
- Does the system design handle all of these effects?
- Have secondary effects of the systems mitigation activities for SEE been assessed?
- What assumptions did the design make to manage redundancy?
- Have the secondary effects of the redundancy management actions been assessed?

Change is another “environmental” consideration. What assumptions did the developer make about changes that happen with integrated systems and any new environments (e.g., high-intensity radiated field, etc.)? Does the developer understand line replaceable unit hardware/application software/airplane system/airplane compatibility issues that can arise when one or more parts change?

E.1.4 Organizational Impediments

There is not a single organizational structure that, by itself, mitigates requirement V&V issues. It is helpful if the organizational structure reflects the integrated nature of the product. It is important to clearly establish roles and responsibilities. Large-scale systems integration means ensuring that the entire system works. Integration problems, by definition, are usually outside the exclusive domain of a single organization. There are multiple ways in which this can be organized. For example, the following approach is one (but not the only) way in which this can be addressed:

- Propulsion integration team–responsible for all of the integration within propulsion systems.
- Systems integration team–responsible for all the integration with systems (e.g., flight controls, hydraulics, electrical).
- Interiors integration team–responsible for all the integration with interiors systems.
- Airplane-level integration team–responsible for all the integration between propulsion, interiors, and systems.

Most commonly, requirements problems occur when multiple organizations/companies must develop requirements that drive systems design to meet system/aircraft performance. Design teams can sometimes focus more immediately on what they need from an intrasystem perspective and less urgently on the integrated, coordinated activity. A preliminary recommendation is to have a systems integration organization that will proactively coordinate and validate that there is an integrated solution. In addition, this system integration organization would lead efforts to ensure technical adequacy of requirements definition/validation, architecture refinement, interface control specification revision, and development assurance (DA)/requirements verification plans as they are revised during the course of iterative development.

E.1.5 Sufficient Planning

DA requires the following plans to be created:

- Safety assessment
- Requirements capture
- Requirements validation
- Implementation verification
- Configuration management
- Process assurance
- Certification and regulatory authority coordination

There are two aspects that will improve the success of these plans: timing and level of detail. The earlier the plans are developed and integrated, the less chance there will be that any aspects of requirements definition and V&V will be missed. The levels of detail in the plans need to be sufficient to generate unambiguous life-cycle data, allocate the required resources and time to execute the plans, and provide sufficient technical oversight of resources. Just as requirements continue to be developed, balanced, and refined during iterative integration into the complete aircraft or system, the plans must be refined to match. The overlying jumps from architecture selection to design, modeling, and implementation must be reflected in the evolving plans. As iterative integration drives the complexity higher and emerging system characteristics impact existing requirements, continuing refinement of plans and requirements must be accomplished. Iterative integration includes the complex interactions, controls (such as configuration management), design refinements, design requirements, and the coalescence of requirements and system implementation that achieves successful aircraft/system development and operation.

The plans need to recognize the inherently iterative nature of development. For example, requiring 100% of content for interface control data, prior to any real design work, does not recognize the integrated nature. Some data can, and should, be captured as soon as possible. However, other data (e.g., detailed BITE reports) cannot be fully defined and validated until lower-level design is underway.

E.1.6 Published Industry Guidance and Procedures

Advisory Circular (AC) 20-174 recognizes Aerospace Recommended Practice (ARP) 4754A as an acceptable DA process. AC20-115 and AC20-152 invoke, respectively, DO-178 and DO-254. Development programs also typically have issue papers (IP). The ACs and IPs must be successfully addressed to achieve certification. Therefore, there can be no shortcuts.

However, industry experience with actually implementing ARP4754A is somewhat limited. As the industry gains more experience and collects lessons learned, there will be more harmonization on its application (particularly for minor model programs).

E.1.7 Requirements Validation

The impact of incomplete, incorrect, or missing requirements is well understood. The process of ensuring requirements are completely correct is not easy; intentionally not including requirements is not a contributing factor. One way to improve the difficult job of validation is to have uniform definition and training on what constitutes validation and what the expectations are at each phase of design. This can help ensure the proper level of coverage and rigor during reviews, analysis, and tests.

In addition, it is helpful to ensure that the entire life cycle and downstream operators are being considered during requirements validation. For example, a program used to generate takeoff performance numbers was noted to take an excessive amount of time to calculate on the test vehicle. The same behavior was noted in lab testing, but the tester did not flag the problem because the pass/fail criteria of the test did not specify a time requirement for the calculation. This delayed timing effect had no safety impact and was fixed during the test program.

The existing processes point to traceability as a key method of ensuring requirements completeness. As an example, detailed traceability analyses could be conducted to look for missing requirements. Parent-child requirements relationships would be established, validated, and integrated in a tool such as a dynamic object-oriented requirements system. As designs become more complex in the future, there are tools that could augment traceability, analyses, and peer reviews. Modeling and prototyping of the digital system provides an opportunity to improve integration. Modeling provides the ability early on to ask, “Is this how you want the system to behave?” The follow-on question, “Is this how the system behaves?” also must be asked.

In addition, if the requirement does not have the connection to the intent, problems can occur. As a result, the requirements verification focuses on the letter of the law (instead of the spirit). This can be mitigated, as needed, by capturing the intent as the requirements assumption/rationale or by creating a parent requirement that clearly captures the intent. This is equivalent to developing a missing system-level requirement from lower-level technically detailed/derived requirements. Grouping lower level requirements to give context and intent for integration into higher level requirements can be considered.

E.1.8 Requirements Implementation Verification

It is important to establish properly scoped verification activities. In addition, it is important to have optimum fidelity of the integrated lab testing equipment and thorough test procedures. This will help accelerate finding problems early in the program. As an example, simulations that model a system may not be accurate in a specific condition (that is only accomplished during the flight test program and not seen in revenue service). Engineering initially believes it is limited only to the specific ground testing being performed. When the test vehicle performs a similar condition in flight, the subsystem is unnecessarily triggered. Engineering subsequently discovers that its system model is inaccurate for this flight-test condition. After updating the model, it is shown that a system logic change is required to preclude unnecessarily triggering the subsystem. This type of situation illustrates the important relationship between modeling, simulation, and testing with respect to ensuring all elements are harmonized. By doing this, the flight test program helps verify that the airplane will support the performance of all functions relative to performance in revenue service.

E.2 EVALUATION OF REAL-WORLD SCENARIOS AND POSSIBLE REQUIREMENTS IMPACTS CANDIDATE REQUIREMENTS ISSUES AND POTENTIAL SHORTCOMINGS

This research evaluated each of the eight scenarios identified in White Paper 3 to determine which possibilities might cause or contribute to requirements errors, omissions, and conflicts. The eight scenarios were chosen, with input from Boeing SMEs, as representative occurrences illustrating possible problems with requirements definition and V&V processes. Multiple problem reports across multiple design disciplines and programs were considered by Boeing SMEs prior to down-selecting to the eight scenarios.

Each possibility was considered on a standalone basis; that is, any of the eight scenarios could have one or more corresponding possibilities selected.

The possibilities that might cause or contribute to requirements errors, omissions, and conflicts were considered as follows:

1. System complexity. Is the system too complex for the designer to understand how it is to operate in normal conditions, failure conditions (including multiple failure conditions), and pilot unexpected actions, such that it is extremely difficult for the designer to fully specify the system?
2. Organizational impediments. Are there organizational impediments, such as a large number of design groups or companies involved in developing significant portions of the system or systems, which could contribute to requirements errors, omissions, or conflicts? Would these organizational impediments make it more difficult for the designers to understand how the system will operate separately and when integrated with other aircraft systems, including failure conditions and pilot unexpected actions, such that it would be extremely difficult for the designer to fully specify the system? Though these organizations will be using current tools, processes, and the like, they will also be using tools and processes unique to different organizations. This can raise the question of whether the lack of integrability of organization-unique toolsets and processes may be part of the requirements shortcoming. Integration conversations and hand-offs between original equipment manufacturers and suppliers are very important to ensure design integrity. This takes precedence over common tools. There has also been an increased ability in recent years to share data across different toolsets, thereby reducing the potential problems in this area. Achieving tool commonality across the aviation industry would be a very challenging task.
3. Sufficient planning. Are the planning documents detailed enough to specify the responsibilities for all design groups and companies involved so that there is little chance that any aspect of the requirements definition/ V&V could “fall through the cracks” without being recognized? The term “document” should not preclude the use of tools such as MBD. A certain amount of documents and artifacts are required for DA verification evidence. Modeling, simulation, and documentation all have valuable uses. The research shows that the key issues are timing, level of detail, and updating. The earlier the plans are developed and integrated, the less chance there will be that any aspects of requirements definition/V&V will be missed. The levels of detail in the plans need to be sufficient to generate unambiguous life-cycle data, allocate the required resources to execute the plans, and provide sufficient technical oversight of resources. Finally, the plans need to recognize the inherently iterative nature of development.
4. Following published guidance and procedures. Are the design groups and companies following the agreed-upon guidance material (e.g., an FAA AC or IP) regarding how the system is developed and all the requirements validated and verified prior to final system approval? Are there any shortcuts being taken or any activities not being accomplished? Current industry standards are adequate for validating individual requirement’s correctness/completeness, particularly for federated systems. Complex integrated systems, however, require each company to develop its own processes, because industry guidelines and standards do not exist with sufficient fidelity (earlier white papers identified this gap and suggest new standards be considered).
5. Program schedules. Do program schedules allocate the necessary time to allow system designers to fully specify their system and then validate and verify those requirements? Is there any buffer built into the program schedules to allow designers and V&V engineers to complete their assignments if the program falls behind?

6. Experienced personnel. Do aircraft system development and V&V activities include personnel with experience in those tasks so that there are always skilled, experienced people either performing or directing critical development and V&V tasks? This can raise the following questions: If new tools and related skills are required to resolve the requirement shortcomings, how will the need for experienced personnel be met? If new approaches, such as model-based systems engineering (MBSE), require significant research and development—and standards and guidelines must be based on repetitive, long-term development of the tools, processes, and emerging knowledge of how they may be used to mitigate requirements shortcomings in systems development—how will they be applied and accepted for certification prior to the accumulated technical understanding and standards development? The most important consideration in this area is the training of personnel—including the use and application of tools—and specific knowledge of systems, integration with other systems, and overall understanding of digital data behavior. This, along with knowledge of applicable environments and DA requirements and practices, will lead to capable staff. The implementation of MBSE, which primarily focuses on the logical architecture, would be analogous to the advances made in 3D physical modeling. In both cases, training is an integral aspect.
7. Requirements validation. Is attention being given to the issue of validating the system requirements, so that each defined requirement has been assured of being complete and correct? Is attention being given to any requirement that may not actually have been specified but should have been?
8. Requirements verification. Is the system design being properly verified once all requirements have been implemented?
9. System integration. Is attention being given to integration of aircraft systems, so that erroneous, missing, or conflicting requirements can be identified? How do or will we know when the reconfigured requirements are sufficient to support all of the life-cycle processes? Section 6 of ARP 4754A addresses modifications to systems and aircraft; however, a universal consensus across the industry on its application does not yet exist.

The team also included additional considerations for horizontal (with increasing levels of integration as one system may impose requirements on other systems) and vertical integration (hierarchical system decomposition from aircraft, to system, to item as corresponding requirements are decomposed and derived).

10. Horizontal integration for incomplete and incorrect requirements. Extensive literature sources document that incomplete/incorrect requirements cause or contribute to development errors. A simplistic (and unrealistic) response would be to “just get the requirements right” and that the occurrences of incomplete, missing, or incorrect requirements (and their associated development errors) will be significantly minimized.

    However, it is important to acknowledge the difficulty of obtaining a “complete and correct” set of requirements. SAE ARP4754 [E1] acknowledged it is virtually impossible to validate that requirements (and assumptions) are complete and correct for complex systems.

When requirements changes result in late design changes, it adversely affects cost, schedule, and, potentially, safety. There is a vested interest throughout the aviation industry to have complete and correct requirements. However, that is easier said than done; no one intentionally has incorrect or incomplete requirements. There are a number of situations in which late design changes can impact the product development life cycle from design through certification and into service operation. These include:

a. Requirements addressing timing and resource allocation. Development of system architecture, functionality, design, and component selection can result in changes to these requirements as the reality of the system/aircraft resources to be shared becomes more defined. Multiple allocations on specific resources (e.g., bandwidth on communications networks; computer processing priorities; and time, power, and weight allocations) can result in competition for available resources.
b. Measurement and evaluation of the implemented systems may result in resources (or use of resources) that do not achieve, or overuse, the expected, required, or advertised resource levels.
c. Emerging characteristics of the aircraft/system may reveal limitations that were not foreseen during the design process and can result in derived requirements and the possibility of additional or modified system-level requirements.
d. Additions of new requirements or changes to existing requirements, including additional requirements identified during the aircraft development, can exacerbate the competition for available resources.
e. Even the addition of resources due to component selection, design, or architecture changes can reverberate through the requirements and initiate ripples of requirements change. This may include additional functionality or the addition of new requirements justified by the growth of shared resources. Multiple domain organizations within the system/aircraft development/integration may simultaneously try to take advantage of the added resources.

This suggests that a change impact analysis be conducted in light of the iterative process of requirements changes and additions (note content regarding the importance of recognizing the iterative nature of requirements validation in section E.1.1.1, SME Questionnaire Findings).

Many of the existing guidelines focus on validating the existing requirements set. There are rather extensive guidelines on different methods for validating the completeness and correctness of requirements (e.g., recommended validation matrix questions or attributes). However, there is not a significant amount of industry guidance on how to identify “missing” requirements. To a certain extent, this becomes axiomatic. If the requirement were known, it would be captured and communicated. However, if the requirement is unknown, it is difficult to capture. There are techniques for analyzing existing requirements to evaluate completeness and accuracy. For example, requirements can be linked by organizational responsibility, functionality, architecture allocations, resources, verification methods, system requirements (decomposition), and derived requirements (including synthesis).

Even with existing requirements, the potential exists for the requirement to be misinterpreted or misunderstood. Because most requirements are text-based, there is always the possibility that two people will read it and reach different conclusions. This is one reason why requirements reviews exist. It is also the reason for the use of logical annotation languages and related tools for architectural design, system design, requirements engineering analyses, executable modeling language, simulation languages, and related tools. There are additional possibilities for applying consistency checking with these tools and techniques.

Figure E-1 shows a simplistic example in which a flight management system expert develops requirements, which, to the best of the individual's ability, reflect a complete and correct set of requirements. This information is passed on to the flight management software engineer, who in turn develops the flight management software.

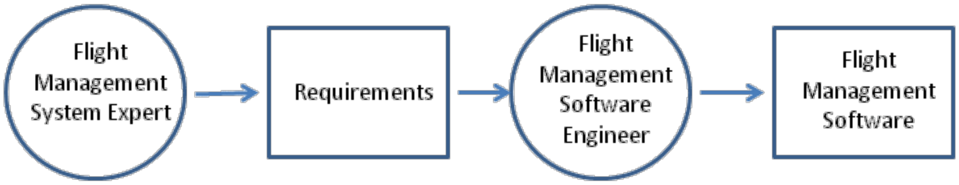

Flight Management System Expert
Requirements
Flight Management Software Engineer
Flight Management Software

Figure E-1. Abstraction/mental model to software

The following steps are involved:

a. Capture
b. Communicate
c. Comprehend

If there are any gaps in terms of capturing, communicating, or comprehending the requirements, it will increase the chance that requirements will be missed or misinterpreted.

With the increasing level of integration between aircraft functions and the systems that implement them (see figure E-2), one system may impose requirements on other systems (e.g., performance, design constraints). If this is not done correctly, it can increase the possibility of a development error.

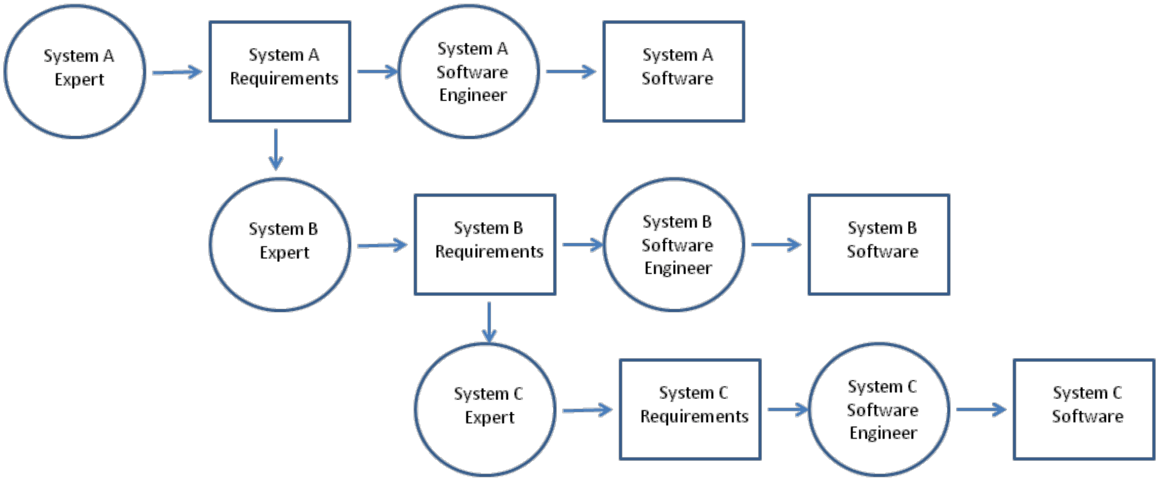


Figure E-2. Integrated systems

Figure E-2 is a simplistic example designed to illustrate requirements interrelationships in the systems engineering domain and does not attempt to show resource interrelationships in the architecture/design domain. It is not intended to imply that one system imposing requirements on other systems covers the entire spectrum. For example, system resources may be shared with multiple system functions/systems/subsystems. Requirements controlling resource behavior must be shared with all users of those resources. The design activities must be aware of this and establish derived lower-level requirements in cognizance of system architecture, design, and their relationship with system-level requirements (both existing and the additional system-level requirements that must be created to achieve complete and accurate requirements).

11. Vertical integration for incomplete and incorrect requirements. In addition to needing to understand the “horizontal integration,” there is also a need to understand the “vertical integration.”

As shown in figure E-3, the DA processes are defined from a hierarchical system decomposition, going from aircraft, to system, to item. At each level, requirements are decomposed and derived. Higher-level parent requirements are decomposed into lower-level children requirements. In addition, some requirements may be derived directly from design decisions and are not directly traceable to higher-level requirements.

Safety analyses are conducted at each respective level, resulting in derived safety requirements.

If there are any errors or omissions at the higher level, these can manifest in lower levels, resulting in undesirable or unpredicted behavior.

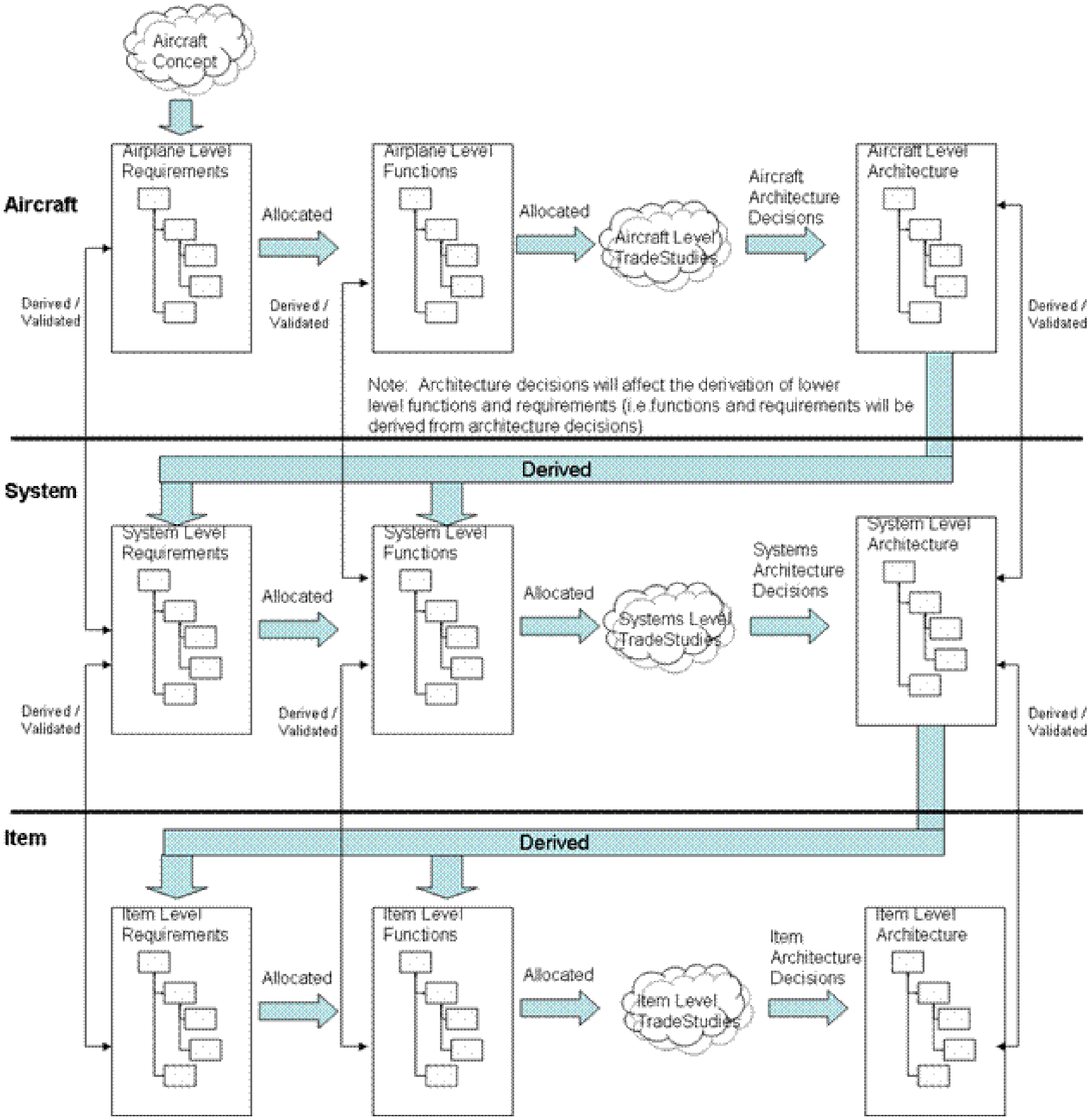

Aircraft Concept
Aircraft
Airplane Level Requirements
Allocated
Airplane Level Functions
Allocated
Aircraft Level TradeStudies
Aircraft Architecture Decisions
Aircraft Level Architecture
Derived / Validated
Derived / Validated
Derived / Validated
Note: Architecture decisions will affect the derivation of lower level functions and requirements (i.e functions and requirements will be derived from architecture decisions)
Derived
System
System Level Requirements
Allocated
System Level Functions
Allocated
Systems Level TradeStudies
Systems Architecture Decisions
System Level Architecture
Derived / Validated
Derived / Validated
Derived / Validated
Item
Derived
Item Level Requirements
Allocated
Item Level Functions
Allocated
Item Level TradeStudies
Item Architecture Decisions
Item Level Architecture

Figure E-3. Vertical integration of requirements

DO-178 [E2] and DO-254 [E3] assume that a complete and correct set of requirements have been allocated to the software and airborne electronic hardware.

The interactions between different systems, if not properly understood, can be a source of problems.

E.3 REFERENCES

E1. SAE International. (1996). SAE ARP4754/EUROCAE ED-79, Certification Considerations for Highly Integrated or Complex Aircraft Systems.

E2. RTCA. (2001). DO-178B/C, Software Considerations in Airborne Systems and Equipment Certification. Washington, DC.

E3. RTCA. (April 19, 2000). DO-254, Design Assurance Guidance for Airborne Electronic Hardware. Washington, DC.

APPENDIX F—SCENARIO MAPPING

F.1 INTEGRATION OF REAL-WORLD AVIONICS SCENARIOS AND PHASE 2 SME QUESTIONNAIRE RESPONSES

A comparison of subject matter expert (SME) questionnaire responses and findings for potential additional guidance for each of the real-world avionics scenarios (outlined in appendices C and D) was made to look for common elements, as listed in figure F-1. An evaluation of this comparison suggests:

- The predominant common element between SME responses and potential additional guidance was in the area of working toward a complete and correct set of requirements.
- Another significant common element was identifying missing requirements.
- A third element that was emphasized by this comparison was identifying potential gaps that may exist with processes to validate and verify requirements.

Each of these common elements aligned to multiple inputs from the SMEs and multiple real-world scenarios. In addition, these common elements align with incomplete, incorrect, or missing requirements as a major root-cause category of the requirements issues and shortcomings described in section 5.1.2.

Figure F-1. Questionnaire responses combined with the eight scenarios

SME Question	Questionnaire Response	**Potential need for additional guidance in the following areas:**	Work to a complete and correct set of requirements (Scenarios 1, 3, 4, 5, 8)	Identify potential gaps that may exist to V&V equirements (Scenarios 2, 3, 5, 6, 7, 8)	Evaluate failure conditions to resolve undesirable aircraft/system performance (Scenario 3)	Investigate processes to help identify missing requirements (Scenario 4, 7)	Consider process improvements to address cumulative effects of individual systems-level cascading effects (Scenario 4, 6)	Consider approach to V&V intrasystem functionality to determine that proper function, content, and performance exist (Scenario 5, 6, 8)	Improve horizontal and vertical integration for V&V @ component, intrasystem, intersystem, and airplane levels (Scenario 5, 6)	Investigate potential process improvements to requirements validation for the modification of existing systems (Scenario 6, 8)	Other
Where are current requirements development, validation and verification processes breaking down? Can you suggest an example scenario (or two) to illustrate your response?											
	Validating the completeness of requirements for new and novel complex systems.		X								
	Improve plans to generate unambiguous life cycle data; then allocate the required resources to execute the plans.										Iterative Nature of Development & Training
	Ensure rigorous up-front development and validation processes/activities.		X			X			X		Iterative Nature of Development & Training
	Varied opinons on appropriate level of requirements definition and what should be defined as a requirement.		X	X		X				X	
	Fidelity of highly-integrated lab testing equipment and thoroughness of test procedures.										Increased fidelity of test lab equipment and associated test procedures to discover & resolve problems prior to aircraft test (@ lower cost)
	It is important to clearly establish roles, responsibility and authority.										Org structure (Programmatic Practices)
	If hardware doesn't behave as expected, there will be SW/AEH problems.		X								
What possibilities might cause or contribute to requirements errors, omissions and conflicts? Perhaps they may have to do with growth of System Complexity or System Integration?											
	Problems can occur where multiple organizations/companies develop both interdependant and independent requirements.		X	X				X	X		Org structure (Programmatic Practices)
	System developers need to address potential impacts of changes to other systems on their system and understand LRU hardware/app software/airplane system/airplane compatibility issues.		X		X	X					
	Often due to insufficient system requirements, failure/lack of thorough reviews, insufficient domain knowledge.		X			X		X			Training
	Adjust requirement development, completeness, and validation methods to the increased integration of the systems architectures.		X	X		X				X	
	It is important to understand the fidelity of models/simulations being used.										Fidelity of models
Why do problems with digital systems requirements for aircraft continue to occur? Can you suggest or do you know root cause(s)?											
	Definition of all interfaces may require one or two iterations prior to the point in development where the systems function is defined sufficiently to allow for a complete definition.		X	X							Programmatic & design practices for iterative development.
	Having requirements that are too prescriptive can drive requirements changes/churn.		X	X							
	As systems increase in software components and evolve into IMA, it is important to understand digital processing (sampling artifacts, how significant digits are affected by error terms, etc.) and also the operational environment.		X			X		X			Environments & assumptions

APPENDIX G—PHASE 3 QUESTIONNAIRE

The following subsections detail the Phase 3 Questionnaire, responses from subject matter experts (SME), and the findings and results, as referenced in section 5.2.

G.1 PHASE 3 QUESTIONNAIRE

The following is the Phase 3 questionnaire:

QUESTIONNAIRE: Safety Issues with Verification and Validation Processes and Practices

Background:

This questionnaire request is to support an FAA research study contract known as 'Task Order 22 (TO-22) Safety Issues with Verification and Validation Processes and Practices,' which is part of a broader umbrella contract known as Systems Engineering 2020 (SE 2020).

The objective of TO-22 is to identify possible issues and shortcomings with the current process used by the commercial aviation industry regarding requirements definition, validation and verification for aircraft digital systems. We have classified and categorized issues and shortcomings and determined associated root causes.

The goal of this questionnaire is to get your recommendations on specific changes to address and mitigate the identified root causes of requirements shortcomings.

Preamble:

Please consider responding to this questionnaire in the two blank columns below during a few quiet moments. Lengthy responses (more than a few sentences) are not required.

Your response will be included in the TO-22 study; as such, they will be documented in a publically released report.

Your responses will not be specifically identified by name, organization, or company. Responses can be sent to either Dan Fogarty of The Boeing Company, or if preferred anonymously, Chuck Kilgore of the FAA who will remove the contact information before forwarding to Dan. Contact information for both Dan and Chuck is at the bottom.

The results of this research may be used to propose changes to either industry standards or regulatory guidance.

Root Cause	Recommendation(s) to Address Root Cause	Additional or Improved Standards/Guidance Needed (id existing document revision or suggest new document required)
Incomplete, Incorrect, or Missing Requirements		
Incomplete, Incorrect, or Missing Requirements of new technologies, particularly with respect to timing (e.g., latency and jitter).		
Incomplete, Incorrect, or Missing Requirements associated with handoffs between ARP4754A development assurance (DA) activities and DO178. and DO254 activities.		
Incomplete, Incorrect, or Missing Requirements in light of potential failure conditions and/or unexpected pilot actions.		
Incomplete, Incorrect, or Missing Requirements associated with systems integration.		
Incomplete, Incorrect, or Missing Requirements due to assumptions about the environment.		
Incorrect Implementation of Otherwise Correct Requirements		
Incorrect Implementation of Otherwise Correct Requirements.		
Failure to detect software or hardware implementation bugs.		
Incomplete, Inadequate Change Impact Analysis		
Incomplete, Inadequate Change Impact Analysis for new, novel, and/or complex systems and new environments.		
Incomplete, Inadequate Change Impact Analysis for the modification of existing systems or functions.		
Incomplete, Incorrect Programmatic and Technical Planning		
Incomplete, Incorrect Programmatic and Technical Planning for complex/iterative development.		
Incomplete, Incorrect Programmatic and Technical Planning with respect to incomplete technical oversight to ensure plans are executed in a disciplined fashion.		

Final Question: Do you have any root causes or recommendations with the current processes used by the commercial aviation industry regarding requirements definition, validation and verification for aircraft digital systems not included above?

Response: Please forward your input directly to daniel.j.fogarty@boeing.com. If you have any questions, please email or call Dan directly (425-280-4780). Alternatively, anonymous responses can be sent to Charles.Kilgore@FAA.gov.

G.1.1 Findings and Results

The findings and results of the Phase 3 questionnaire are summarized in table G-1.

Table G-1. Phase 3 questionnaire results

Root Cause	Recommendation(s) to Address Root Cause	Additional or Improved Standards/Guidance Needed (identify existing document revision or suggest new document required)
Incomplete, Incorrect, or Missing Requirements		
Incomplete, Incorrect, or Missing Requirements of new technologies, particularly with respect to timing (e.g., latency and jitter).	• System level requirement standard including suggestions on the types of requirements that should be considered – essentially cues to assess completeness of requirements. • Well-defined process for requirements reviews involving peers and non-advocates.	See comment at left.
Incomplete, Incorrect, or Missing Requirements associated with handoffs between Aerospace Recommended Practice 4754A (ARP4754A) DA activities and Document 178 (DO178) and DO254 activities.	• Root cause is essentially a failure to do correct/ appropriate top-down tracing and bottom-up audit (i.e., do the children completely satisfy the parent?). • Ensure the validation process for the equipment-level system requirements is improved (checklist, review, safety review of derived). • Ensure that the requirements directly provided by original equipment manufacturer (OEM) to the item level are validated at OEM level.	• No new documents required. • Possibly examples or discussion in a system-level requirement standard about appropriate trace mappings (training).

Table G-1. Phase 3 questionnaire results (continued)

Root Cause	Recommendation(s) to Address Root Cause	Additional or Improved Standards/Guidance Needed (identify existing document revision or suggest new document required)
Incomplete, Incorrect, or Missing Requirements in light of potential failure conditions and/or unexpected pilot actions.	• Single and multiple failure analyses conducted by safety group, crew ops, pilot community.	• Boost/improve the validation and safety sections of in future update of ARP4754A. • Create safety questionnaire/ checklist.
Incomplete, Incorrect, or Missing Requirements associated with systems integration.	• Well-defined and thorough intrasystem and intersystem analyses. • Better definition of integration requirements (internal and external). • Better definition of the coordination between OEM and systems and ensure the proper validation & verification work statement is defined.	• Add subsection to requirements management section of ARP4754B.
Incomplete, Incorrect, or Missing Requirements due to assumptions about the environment.	• Lack of validation of assumptions. • Consider assumptions as derived requirements at the system level and address them as the derived requirements.	• Boost the existing assumptions section of ARP4754A. Add assumptions review to system safety plan and preliminary airplane safety assessment/ preliminary system safety assessment.

Table G-1. Phase 3 questionnaire results (continued)

Root Cause	Recommendation(s) to Address Root Cause	Additional or Improved Standards/Guidance Needed (identify existing document revision or suggest new document required)
Incorrect Implementation of Otherwise Correct Requirements		
Incorrect Implementation of Otherwise Correct Requirements.	• Late or inadequate verification of requirement compliance. • Proper verification process at the system and equipment level. • Introduce clear definition of verification credit and coverage analysis.	• Improve existing Section 4.6 (System Implementation) of ARP4754A.
Failure to detect software or hardware implementation bugs.	• Root cause analysis as part of problem report activity – process failure, inadequate verification, or is it one of those unique scenarios that current methods cannot detect? The first two are quality issues (expect corrective action), the latter has to be considered in the context of likelihood of similar escape (more rules won't solve).	• Tracing and coordination between OEM/system – provider needs to improve, but no need for new regulations/ guidance.

Table G-1. Phase 3 questionnaire results (continued)

Root Cause	Recommendation(s) to Address Root Cause	Additional or Improved Standards/Guidance Needed (identify existing document revision or suggest new document required)
Incomplete, Inadequate Change Impact Analysis		
Incomplete, Inadequate Change Impact Analysis for new, novel, and/or complex systems and new environments.	• Issue is undetected impact and resulting erroneous/unintended behavior. See comments above about inadequate requirements, failure to detect bugs, etc. • Increase understanding of systems and their interrelationships. • Ensure that there is a robust process in place to monitor and assess changes. • Establish and properly document modification impact analysis (MIA) at both the OEM and system level. • Ensure that equipment and item level changes are addressed in that MIA.	• Improve existing Section 6 (System Implementation) of ARP4754A.
Incomplete, Inadequate Change Impact Analysis for the modification of existing systems or functions.	• Issue is undetected impact and resulting erroneous/unintended behavior. • Increase understanding of systems and their interrelationships. • Ensure that there is a robust process in place to monitor and assess changes. • Establish and properly document MIA at both the OEM and system level.	• Improve existing Section 6 (System Implementation) of ARP4754A.

Table G-1. Phase 3 questionnaire results (continued)

Root Cause	Recommendation(s) to Address Root Cause	Additional or Improved Standards/Guidance Needed (identify existing document revision or suggest new document required)
Incomplete, Incorrect Programmatic and Technical Planning		
Incomplete, Incorrect Programmatic and Technical Planning with respect to incomplete technical oversight to ensure plans are executed in a disciplined fashion.	• Provide sufficient resources for the oversight. • Provide resources skilled in the oversight process. • Provide resources knowledgeable in the system being overseen. • Project plan should address this topic. Also, supplier oversight plan (part of process assurance [PA] plan) needs to be detailed – may need the addition of a checklist. • Decision flow to address the change impact analysis (CIA) process.	• May need to add the section to ARP4754A/reuse section to address the program plan expansion in order to address this topic. • Also improve PA plan, oversight section. • Society of Automotive Engineers' ARP4754A should be clarified and Advisory Circular 20-174 (AC20-174) should be aligned with the ARP in their guidance regarding CIA, or the CIA description should solely exist in AC20-174. • While SAE ARP4754A initially describes a common concept for an MIA, Section 6.3, it appears to create variations in those evaluations and the criterion by which certain changes would be considered acceptable. • Further, there is guidance overlap between the AC20-174 "traditional techniques" concept and ARP Section 6, which does not clarify if they are redundant or distinct concepts.

APPENDIX H—PROCESS ASSURANCE REVIEW CRITERIA

This appendix provides a recommended checklist and acceptance criteria for the four structured process assurance (PA) reviews. The assessment checklist and acceptance criteria for the assessments are contained in the tables below. The execution order of the following assessment tasks is at the discretion of the assessment team. Note that planning review criteria in the tables below contain references to applicable sections in Aerospace Recommended Practice (ARP) 4754A.

H.1 Development Assurance Review-1 (Planning)

This checklist was developed as a tool to conduct an onsite review of supplier design team development assurance (DA) planning documents and then to conduct an onsite review to validate that appropriate infrastructure, tools, and processes/procedures are defined as described in the planning documents.

Table H-1. Planning review criteria

Data Item	ARP4754A Objective Table A-1	Planning Review Criteria
Planning documents	1.1, 1.2	Review planning documents to confirm: a. The planning documents address all system development and integral processes to meet ARP4754A objectives defined in Appendix A, Section 1.0. b. Transition criteria and interrelationship among processes are defined in the planning documents. c. DA process boundaries where transition to Document-178 (DO-178)/DO-254 processes will take place is defined (4.6.1.1). d. Reference to the top-level processes/command media for the supporting processes and their mapping to each of the ARP4754A Appendix A objectives are included (5.8.4.3).

Table H-1. Planning review criteria (continued)

Data Item	ARP4754A Objective Table A-1	Planning Review Criteria
System Development and Requirements Management Plan	1.1, 1.2	Review planning documents to confirm that: a. The planned development cycle and associated key events are identified (5.8.4.3). b. Organizational structure and key individual responsibilities supporting the development are included (5.8.4.3). c. Process to capture and control requirements, including transmittal to supplier/sub-tier supplier, is defined (5.3). d. Process to capture and control requirements traceability records (both source/parent and children requirements identification) is defined (5.4.6a). e. Process to capture allocation of requirements to architecture elements or hardware/software items (4.1.7, 4.5). f. Methods to capture derived requirements rationale and OEM review of derived requirements are defined. g. Plan for integration of items within the scope of the planning document is defined (4.6.3, 4.6.4). h. Adequate description of the requirements capture process is provided to assess that, if the plan is followed, the ARP4754A objectives defined in Appendix A, Section 2.0 will be met. i. Requirements management plan has been reviewed by all organizations who will follow the plan or who will use the data produced by the activities in the plan. j. Outputs/artifacts of development and requirements processes are identified and their planned contents and configuration controls methods are per ARP4754A Appendix A, Section 2.

Table H-1. Planning review criteria (continued)

Data Item	ARP4754A Objective Table A-1	Planning Review Criteria
Safety Program Plan	1.1, 1.2	Review planning documents to confirm the following contents: a. Process to define and uniquely identify safety requirements (5.1.5, 5.3.1.1, 5.3.2). b. Roles and responsibilities of safety team and its relationship with other design teams (5.1.5). c. Description of safety activities (FHA, PSSA, CCA, etc.), and deliverables (5.1.5). d. Project milestones for which safety reports are required (5.1.5). e. Validation plan for the safety requirements (5.1.5). f. Verification plan for the safety requirements (5.1.5). g. Links with other DA plans (5.1.5). h. Adequate description of the safety assessment process is provided to assess that, if the plan is followed, the ARP4754A objectives defined in Appendix A, Section 3.0 will be met. i. Safety plan has been reviewed by all organizations who will follow the plan or who will use the data produced by the activities in the plan. j. Outputs of safety assessment process are identified and their planned contents and configuration controls methods are per ARP4754A Appendix A, Section 3.

Table H-1. Planning review criteria (continued)

Data Item	ARP4754A Objective Table A-1	Planning Review Criteria
Validation Plan	1.1, 1.2	Review validation planning documents to confirm: a. Description of validation methods and guidance to assign one or more validation methods for the requirement is included (5.4.6, 5.4.7.1a, table 6). b. Identification and description of validation process outputs/artifacts are included (5.4.7.1b, c). c. Format and minimum contents of validation matrix are identified and the contents are sufficient to meet ARP4754A objectives (5.4.7.2). d. Process to revalidate requirements in case of requirements changes is defined (5.4.7.1e). e. Roles and responsibilities in the validation process are defined (5.4.7.1f). f. Schedule of key validation activities is defined (5.4.7.1g). g. Managing of assumptions, if used, is defined (5.4.7.1h). h. Process independence between requirements definition and validation activities is defined per system DA level (5.4.7.1i). i. Adequate description of the process is provided to assess that, if the plan is followed, the ARP4754A validation objectives defined in Appendix A, Section 4.0 will be met. j. Validation plan has been reviewed by all organizations who will follow the plan or who will use the data produced by the activities in the plan. k. Configuration control method for validation artifacts is per ARP4754A Appendix A, Section 4.

Table H-1. Planning review criteria (continued)

Data Item	ARP4754A Objective Table A-1	Planning Review Criteria
Verification Plan	1.1, 1.2	Review planning documents to confirm: a. Role and responsibilities associated with conducting the verification activities are included (5.5.6.1a). b. Description of independence between design and verification activities is included and per ARP4754A Appendix A, Section 5 (5.5.6.1b). c. Definition of verification methods and guidance to assign one or more verification methods for the requirement is included (5.5.5, 5.5.6.1c, table 7). d. Identification and description of verification process outputs/artifacts are included (5.5.6.1d). e. Identification of key verification activities or setups and sequence of dependent activities (5.5.4f, 5.5.6.1e). f. Schedule of key verification activities (5.5.6.1f). g. Criteria for taking system verification credit from hardware or software verification activities (5.5.6.1g). h. Method used for capturing configuration tested, test setup, and special hardware or software used (5.5.4b). i. Format and contents of verification matrix are defined and the contents are sufficient to meet ARP4754A objectives (5.5.6.3). j. Process to re-verify (e.g., regression testing) requirements or design changes implemented after a verification baseline is established. k. Adequate description of the process is provided to assess that, if the plan is followed, the ARP4754A objectives defined in Appendix A, Section 5.0 will be met. l. Verification plan has been reviewed by all organizations who will follow the plan or who will use the data produced by the activities in the plan. m. Configuration control method for verification process outputs/artifacts is per ARP4754A Appendix A, Section 5.

Table H-1. Planning review criteria (continued)

Data Item	ARP4754A Objective Table A-1	Planning Review Criteria
Configuration Management Plan	1.1, 1.2	Review planning documents to confirm that the plan: a. Identifies tools, methods, roles, and responsibilities for configuration management (5.6.2.1). b. Identifies configuration items (design and DA data items) and the control category that will be used for each item is defined (5.6.1b, 5.6.2.2, table 8). c. Define process for establishing configuration baseline (5.6.2.3). d. Define control process to change an established baseline (5.6.2.3). e. Process to capture and resolve issues uncovered during reviews, validation, and verification activities (5.6.2.4). Method to share (PR) with OEM for system and airplane-level effects evaluation is defined. f. Define the process to make the configuration items retrievable (5.6.2.5). g. Adequate description of the process is provided to assess that, if the plan is followed, the ARP4754A objectives defined in Appendix A, Section 6.0 will be met. h. Configuration management plan has been reviewed by all organizations who will follow the plan or who will use the data produced by the activities in the plan. i. Outputs of configuration control process are identified and their planned contents and configuration control method are per ARP4754A Appendix A, Section 6.

Table H-1. Planning review criteria (continued)

Data Item	ARP4754A Objective Table A-1	Planning Review Criteria
PA Plan	1.1, 1.2	Review planning documents to confirm that: a. PA activities are conducted with independence from the system development process (5.7). b. PA activities include verifying that adequate plans are developed and maintained during the project (5.7.1a). c. PA reviews are planned to ensure that development activities are conducted in accordance with the defined plans (5.7.1b). d. Outputs of PA process are identified and its planned contents and configuration control method are per ARP4754A Appendix A, Section 7 (5.7.1c). e. PA activities are defined to verify that the scope and contents of other planning documents are consistent with the DA level of the system (5.7.2a). f. Sufficient PA reviews are planned to timely detect process issues that may lead to development errors (5.7.2d). g. PA review of project plans includes that applicable processes/procedures are documented (5.7.3). h. PA review of project plans includes that the procedures for plan updates are defined (5.7.3).

OEM = original equipment manufacturer; FHA = functional hazard assessment; PSSA = preliminary system safety assessment; CCA = common cause analysis; PR = problem report

H.2 DA Review-2 (Validation)

This checklist was developed as a tool to conduct an onsite review of original equipment manufacturer (OEM) or supplier design team artifacts and assess adherence to the applicable system development, requirements management, validation, safety, configuration management, and PA plans (see table H-2).

Table H-2. Validation review criteria

Data Item	ARP4754A Objective Table A-1	Validation Review Criteria
Previous DA Review Results	7.1, 7.2	Completed checklist is available from previous DA Review. Any findings and action items from DA review are closed or in-work per agreed upon schedule (5.7.4).
System Requirements	2.3, 2.4, 3.7, 6.2, 6.3	Review sample data to confirm: a. New and modified supplier/OEM requirements are controlled per process defined in configuration management plan (5.6.2.6). b. If used, identification of DA compliance applicable requirements is per the criteria referenced in a DA planning document. c. A controlled database or document contains requirements traceability records (both source/parent and children requirements identification). d. Upon review, a requirement is reasonably accomplished by its children requirement and there are no unrelated children requirements (Section 5.4.4.1a). e. For derived requirements, an adequate rationale statement is provided. Supplier provided derived requirements to the design team for assessing system-level effects (4.4).
System Description	2.5	Review system description to confirm that it: a. Contains (5.8.4.4): i. Intended functions provided by the system. ii. System architecture and design features implemented to meet safety requirements. iii. Fault or failure containment means. iv. New or novel design elements, if any. b. Is controlled per the configuration management plan (5.6.2.6).
Requirements Allocation	2.6	Review sample data to confirm: a. Requirements are adequately allocated to architectural elements or hardware/software items and the allocation is controlled. b. Evidence exists to show that the allocation was reviewed by appropriate SMEs for completeness and correctness. c. Requirements allocations are tracked for correct and complete implementation or are captured in lower-tier requirements.

Table H-2. Validation review criteria (continued)

Data Item	ARP4754A Objective Table A-1	Validation Review Criteria
Requirements Validation		Review sample data to confirm: a. A controlled validation matrix or tracking document is used to plan and record completion of validation activities for all new and modified airplane to component-level requirements. b. Validation methods identified for the requirement are per definition and guidance in supplier requirements processes or planning documents. c. Review of the validation artifacts shows that the validation activity was sufficient for the requirement. d. Applicable requirements for interfacing systems performance (e.g., electrical or hydraulic power, data latency or jitter) were reviewed and concurred by system SMEs. e. Configuration control of the validation matrix is per the configuration management plan (5.6.2.6).
Safety Analysis	3.1, 3.3	Review sample data to confirm: a. FHA and PSSA are conducted and safety requirements are captured from the results of these analyses (5.1.1, 5.1.2, 5.3.2). b. FDAL and IDAL assignments are defined per process described in the safety program plan (5.2.3, 5.2.4). c. Preliminary CCA are conducted and necessary independence requirements are defined based on the CCA results (5.1.4). d. Safety requirements are uniquely identified (5.3.1.1). e. Derived safety requirements are defined with adequate rationale (5.3.1.4). f. Availability and integrity requirements for interfacing systems are captured (5.4.4.1). g. Traceability is established between safety analysis (FHA, PSSA, CCA) and safety requirements (5.4.6).
Supplier PA Review Results	7.1, 7.2	Review data to confirm: a. Results from supplier-conducted PA reviews are available. b. Findings and actions, if any, captured during the supplier reviews are tracked for timely resolution.

SME = subject matter expert; FHA = functional hazard assessment; PSSA = preliminary system safety assessment; FDAL = function development assurance level; IDAL = item development assurance level; CCA = common cause analysis

H.3 DA Review-3 (Verification)

This checklist was developed as a tool to conduct an onsite review of OEM or supplier design team artifacts and assess adherence to the applicable system development, verification, safety program plans, configuration management, and PA plans.

Table H-3. Verification review criteria

Item No.	Data Item	ARP4754A Objective Table A-1	Verification Review Criteria
1.	Previous DA Review Results	7.1, 7.2	Completed checklist is available from previous DA review. Any findings and action items from DA review are closed or in-work per agreed upon schedule (5.7.4).
2.	Implementation Verification	5.1–5.5, 6.2, 6.3	Review sample data to confirm: a. A controlled verification matrix or tracking document is used to plan and ensure verification completion of all new and modified requirements. b. Verification methods identified for the requirement is per definition and guidance in supplier verification processes or planning documents. c. Verification test procedures contain success criteria or expected results (5.5.5.4 test procedure d). d. The procedure provides sufficient setup and execution steps to make it repeatable. e. The test cases provide verification coverage consistent with the plan in the verification matrix. f. Verification procedure reference requirements covered by the test (5.5.5.4d). g. Verification procedures are controlled per configuration management plan (5.6.2.6).

Table H-3. Verification review criteria (continued)

Item No.	Data Item	ARP4754A Objective Table A-1	Verification Review Criteria
3.	Requirements Verification Results including Verification Matrix	5.1–5.5	Review sample data to confirm: a. Verification matrix or tracking document provides tracing between requirements and verification results (5.5.6.3). b. Verification results capture the test procedure version, configuration of the design and, if applicable, test setup (5.5.5.4). c. Verification results are documented with pass/fail determination or identification of problem reports where issues or failure are captured (5.5.5.4 test results d). d. The verification results provide sufficient coverage consistent with the plan in the verification matrix (5.5.6.2). e. Verification tests demonstrate that the system performs its intended functions and provides confidence that the system does not perform unintended functions (5.5.5.4). f. Verification results and the verification matrix is controlled per project configuration management plan.
4.	Systems Safety Analysis	3.4, 3.6	Review sample data to confirm that system safety analysis contains (5.1.3): a. System description or reference to system description that is used for safety analysis. b. Summary of failure condition and the associated hazard classification (FHA, FDAL). c. IDAL for electronic hardware and software items. d. Qualitative and quantitative analysis for the failure conditions. e. CCA results summary. f. Safety-related maintenance tasks and intervals. g. Traceability between safety requirements and sections of the system safety assessment, where compliance to the requirement is shown. h. Reference to tests conducted for failure mode and effect analysis validation.

Table H-3. Verification review criteria (continued)

Item No.	Data Item	ARP4754A Objective Table A-1	Verification Review Criteria
5.	Aircraft and Systems Integration	2.7	Review sample data to confirm: a. Electronic hardware and software integration activities are performed using appropriate test setup (4.6.3). b. System integration activities are performed using appropriate lab or flight test airplane to verify system performs intended functions and does not perform unintended functions (4.6.4). c. System-to-system integration activities are performed to ensure that the systems operate correctly individually or together as installed on the airplane (4.6.4).
6.	Problem Reports	5.6, 6.3	Review sample data to confirm: a. Problem reports are used to capture and manage issues uncovered during verification activities (5.6.1c, 5.6.2.4). b. Deferred problem reports were assessed for their impact on safety impact (5.5.6.4). c. Problem reports and their resolution are recorded. (5.6.1c). d. Supplier has established a process to provide problem reports to the design teams for system- and airplane-level effects evaluation.

Table H-3. Verification review criteria (continued)

Item No.	Data Item	ARP4754A Objective Table A-1	Verification Review Criteria
7.	Configuration Management Records (including Change Impact & Regression Analysis)	6.1–6.4	Review sample data to confirm: a. Baseline is established for configuration items identified in configuration management plan (5.6.2.3). b. Requirements or design change is traceable to previous baseline (5.6.2.3). c. Requirements or design change is implemented per authorized change records (e.g., change request/notice) (5.6.1, 5.6.2.4). d. Change records include assessment of impact to applicable configuration items, including requirements, interfaces, safety analyses, and validation and verification data items (5.6.2.4). e. Change to applicable configuration items is tracked for completion (5.6.2.4). f. Change records are controlled, archived, and retrievable per project configuration management plan (5.6.2.5). g. Supplier has a process for notifying OEM of internal design or requirements changes for system- and airplane-level effects evaluation.
8.	Supplier Data Review Results	7.1, 7.2	Review data to confirm: a. Results from supplier-conducted PA reviews are available. b. Findings and actions, if any, captured during the supplier review(s) are tracked for timely resolution.

FHA = functional hazard assessment; FDAL = function development assurance level; IDAL = item development assurance level; CCA = common cause analysis

H.4 DA Review-4 (Final)

This checklist was developed as a tool to conduct an onsite review of supplier design team artifacts and assess adherence to the applicable system development, verification, safety, configuration management, and PA plans.

Table H-4. Final review criteria

Item No.	Data Item	ARP4754A Objective Table A-1	Final Review Criteria
1.	Previous DA Review Results	7.1, 7.2	Completed checklist is available from previous DA review. Any findings and action items from DA review are closed or in-work per agreed upon schedule (5.7.4).
2.	Verification	5.3, 5.5, 6.2, 6.3	Review sample data to confirm: a. Verification is conducted on TC/amended TC system configuration or change record (including regression record) exists to show that verification conducted on previous configuration is valid for TC/amended TC configuration (5.5.6.4). b. Verification conclusion (pass/fail) for each requirement is captured in verification matrix (5.5.6.3). c. Verification matrix is under configuration control per the configuration management plan (5.5.6.4).
3.	Safety analysis	5.4, 6.2, 6.3	Review sample data to confirm: a. Safety requirements verification is complete or tracked for completion before system safety analysis document release for TC/amended TC. b. Safety analysis document is under configuration control and the completed sections are valid for the TC/amended TC system and item configurations (5.5.1).
4.	Open Problem Reports	5.6, 6.3	Review sample data to confirm: a. Criteria for problem reports disposition for TC and amended TC is defined. b. Any open problem reports are tracked for disposition before TC or amended TC. c. Supplier safety-related open problem reports have been reviewed and dispositioned by the Boeing design team.
5.	Configuration Index	8.1	Review sample data to confirm: a. Configuration of system equipment including software and airborne electronic hardware items are defined (5.8.4.2). b. Physical and functional interfaces with other systems are defined (5.8.4.2). c. Certification maintenance requirements and safety-related limitations, if any, are defined (5.8.4.2).

Table H-4. Final review criteria (continued)

Item No.	Data Item	ARP4754A Objective Table A-1	Final Review Criteria
6.	Accomplishment Summary	8.1	Review accomplishment summary to confirm: a. Summary confirms that the DA data artifacts identified in the planning documents are generated and archived (5.8.4). b. Any deviation from the planning documents is included with adequate rationale for its acceptance (5.8.3). c. A summary of DA review results is included (5.8.3). d. A statement of compliance that DA objectives are met, per agreed upon methods, is included (5.8.3).
7.	Supplier Data Review Results	7.1, 7.2	Review data to confirm: a. Results from supplier-conducted PA reviews are available. b. Findings and actions, if any, captured during the supplier data reviews are tracked for timely resolution.

TC = type certification

APPENDIX I—POTENTIAL FUTURE WORK CONCEPTS

The purpose of this appendix is to recommend potential future research on the possible benefits and use of model-based design (MBD), virtualization, distributed test, and interoperability-based testing for improving validation and verification (V&V) of complex integrated digital systems.

I.1 The MBD

The MBD is an approach to design that emphasizes the injection of additional formalism into pre-existing design processes. These formalisms can be introduced at a variety of levels of abstraction of design. At each level, the formalisms enable a number of new analytic capabilities:

- Analyses of individual systems (e.g., demonstrating their conformance to requirements).
- Analyses of interactions between systems (e.g., demonstrating their conformance to communication protocol requirements).
- Analyses of the emergent behavior created by the combination of individual systems into a greater system of systems (SOS) (e.g., demonstrating properties of the SOS given properties of the systems themselves).

Future research is recommended to evaluate the benefits, limitations, applications, and uses to improve V&V practices of complex, highly integrated digital systems.

I.2 Virtualization

Virtualization is an emerging technology that provides capabilities to facilitate early evaluation of requirements at both component (line replaceable module [LRM]/line replaceable unit [LRU]) and integration levels. Depending on the fidelity or the virtualization construct, the early evaluation could be used to facilitate validation of requirement content, to be followed by verification of actual requirements.

The capabilities of virtualization are met by developing a very high fidelity simulation of the underlying hardware (LRM/LRU processor) and associated software. MBD and virtualization are complementary technologies; future research is recommended to evaluate their benefits, limitations, applications, and uses to improve V&V practices of complex, highly integrated digital systems.

I.3 Distributed Test

The distributed test capability enables the test of interoperability attributes and performance characteristics of complex, networked SOS. This capability was developed after recognizing that traditional test and evaluation (T&E) methodologies for SOS environments were inadequate. As the complexity of open architecture, networked systems increases, the difficulty in developing and validating these systems increases as the system elements are developed and tested in disparate locations with varying requirements, program milestones, and system maturity.

Significant benefits can be achieved when T&E and systems engineering jointly participate in developing V&V requirements, particularly in defining test approaches that are appropriate for integration and V&V. This includes helping to ensure the system concepts, requirements, architectures, designs, and operations are valid, feasible, affordable, producible, and testable. Ultimately, this helps programs identify and mitigate risks earlier in the product life cycle, decrease risks and costs, and shorten the time to operational readiness.

Future research is recommended to evaluate distributed testing for benefits, limitations, applications, and uses to improve V&V practices of complex, highly integrated digital systems, including those associated with the Next Generation Air Transportation System.

I.4 Interoperability Testing

Interoperability testing focuses on the importance of multiple elements (components, subsystems, platforms, and/or SOS) operating in an integrated fashion, hereto referred to as interoperability. Test planning should include interoperability considerations (e.g., for possible development cycles/spirals depending on program or project size and complexity).

At the top level, interoperability testing ensures the ability of systems to operate together/exchange information in the same environment without disrupting any participant's ability to perform its intended, independent function.

Interoperability testing is the ability of a system of interest (SOS, systems, platforms, subsystems, components, and environments [e.g., units, forces, atmospheric conditions]) to interact with all aspects of the test system (e.g., physical interfaces, environmental conditions, command, people [e.g., semantics, understanding], power, and data [e.g., processes, security, data sharing]) and accept the same from the other components of the systems of interest to enable them to operate effectively together. Interoperability testing includes both the technical exchange of information and end-to-end operational effectiveness of that exchanged information as required for regulatory and operational requirements. Interoperability testing should consider the level of standards compliance of existing implementations and new systems to be incorporated. To achieve maximum benefit, interoperability testing should be performed in the most operationally realistic environment possible, determining whether the system of interest conforms to applicable standards and ensures data collected are adequate for evaluating interoperability issues.

Future research is recommended to evaluate the benefits, limitations, applications, and uses of interoperability testing to improve V&V practices of complex, highly integrated digital systems.