NASA/CR–2014-218550

Regulatory Compliance in Multi-Tier Supplier Networks

Emray R. Goossen and Duke A. Buster
Honeywell International Inc., Albuquerque, New Mexico

November 2014

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Report Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at *http://www.sti.nasa.gov*

- E-mail your question to help@sti.nasa.gov

- Fax your question to the NASA STI Information Desk at 443-757-5803

- Phone the NASA STI Information Desk at 443-757-5802

- Write to:
  STI Information Desk
  NASA Center for AeroSpace Information
  7115 Standard Drive
  Hanover, MD 21076-1320

NASA/CR–2014-218550

Regulatory Compliance in Multi-Tier Supplier Networks

Emray R. Goossan and Duke A. Buster
Honeywell International Inc., Albuquerque, New Mexico

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

Prepared for Langley Research Center
under Contract NNL13AA04B

November 2014

Acknowledgment

.
This contract work was awarded by NASA under Contract No. FCSR-NNL13AA04B, Task Order No. NNL13AC66T. The NASA technical monitor for this task is Mr. Wilfredo Torres-Pomales.

Available from:

NASA Center for AeroSpace Information
7115 Standard Drive
Hanover, MD 21076-1320
443-757-5802

ABSTRACT

Regulatory Compliance in Multi-tier Supplier Networks

Over the years, avionics systems have increased in complexity to the point where 1st tier suppliers to an aircraft OEM find it financially beneficial to outsource designs of subsystems to 2nd tier and at times to 3rd tier suppliers. Combined with challenging schedule and budgetary pressures, the environment in which safety-critical systems are being developed introduces new hurdles for regulatory agencies and industry. This new environment of both complex systems and tiered development has raised concerns in the ability of the designers to ensure safety considerations are fully addressed throughout the tier levels. This has also raised questions about the sufficiency of current regulatory guidance to ensure: proper flow down of safety awareness, avionics application understanding at the lower tiers, OEM and 1st tier oversight practices, and capabilities of lower tier suppliers. Therefore, NASA established a research project to address Regulatory Compliance in a Multi-tier Supplier Network.

This research was divided into three major study efforts:

1. Describe Modern Multi-tier Avionics Development
2. Identify Current Issues in Achieving Safety and Regulatory Compliance
3. Short-term/Long-term Recommendations Toward Higher Assurance Confidence

This report presents our findings of the risks, weaknesses, and our recommendations. It also includes a collection of industry-identified risks, an assessment of guideline weaknesses related to multi-tier development of complex avionics systems, and a postulation of potential modifications to guidelines to close the identified risks and weaknesses.

REGULATORY COMPLIANCE IN MULTI-TIER SUPPLIER NETWORKS

HONEYWELL

Objective: Assess risks and guideline weaknesses in successful multi-tier development of increasingly complex avionics systems, and provide recommended adjustments to guidelines.

Contents

Table of Figures

Table of Tables

1 Purpose

Over the years, avionics systems have continued to increase in complexity to the point where 1st tier suppliers to an aircraft OEM have found it financially beneficial to outsource designs of subsystems to 2nd tier and at times to 3rd tier suppliers. Combined with challenging schedule and budgetary pressures, the environment in which safety-critical systems are being developed introduces new hurdles for regulatory agencies and industry. This new environment of both complex systems and tiered development has raised concerns in the ability of the designers to ensure safety considerations are fully addressed throughout the tier levels. This has also raised questions about the sufficiency of current regulatory guidance to ensure: proper flow down of safety awareness, avionics application understanding at the lower tiers, OEM and 1st tier oversight practices, and capabilities of lower tier suppliers. Therefore, NASA established a research project to address Regulatory Compliance in a Multi-tier Supplier Network.

1.1 Abbreviations and Acronyms

AIR	Aircraft Certification Service
ARC	Aviation Rule Making Committee
ASA	Aircraft Safety Assessment
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance
CCA	Common Cause Analysis
CI	Configuration Item
CMA	Common Mode Analysis
DAR	Designated Airworthiness Representative
DER	Designated Engineering Representative
DoDAF	Department of Defense Architecture Framework
DMIR	Designated Manufacturing Inspection Representative
EUA	Early User Assessment
FCSR	Flight Critical Systems Research
F-FMEA	Functional Failure Modes and Effects Analysis
FFPA	Functional Failure Path Analysis
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
FSDO	Flight Services District Office
FTA	Fault Tree Analysis
HCMP	Hardware Configuration Management Plan
HDVP	Hardware Verification Plan
HHA	Health Hazard Analysis
HQAP	Hardware Quality Assurance Plan
HRD	Hardware Requirements Document

HW	Hardware
ICD	Interface Control Document
KPP	Key Performance Parameter
MBD	Model Based Design
MIDO	Manufacturing Inspection District Offices
ODA	Organization Designation Authorization
O&SHA	Operating and Support Hazard Analysis
OEM	Original Equipment Manufacturer
OMT	Organization Management Team
PAH	Production Approval Holder
PASA	Preliminary Aircraft Safety Assessment
PHA	Preliminary Hazard Analysis
PHAC	Plan for Hardware Aspects of Certification
PHL	Preliminary Hazard List
PRA	Probabilistic Risk Assessment
PSAC	Plan for Software Aspects of Certification
PSCP	Project Specific Certification Plan
PSP	Partnership For Safety Plan
PSSA	Preliminary System Safety Assessment
PSyAC	Plan for Systems Aspects of Certification
RAA	Responsibility, Accountability, Authority
RHA	Requirements Hazard Analysis
SCD	Specification Control Drawing
SCMP	Software Configuration Management Plan
SDP	Software Development Plan
SE-CMMI	Systems Engineering Capability Maturity Model Integration
SHA	System Hazard Analysis
SPP	Safety Program Plan
SQAP	Software Quality Assurance Plan
SSHA	Subsystem Hazard Analysis
SVP	Software Verification Plan
SW	Software
TRL	Technology Readiness Level

1.2 Definitions

COMPLEXITY: A reflection of the difficulty and effort required to understand, implement, and verify a system. It is not measured in the number of components or in the number of source lines of code, but in the difficulty in understanding and development of the system.

CONTRACTOR: The Corporation executing the development of a system or component.

ESCAPES: Errors in the system which escape verification and validation to appear at the next higher tier or aircraft integration level.

ITEM: A hardware or software element having bounded and well-defined interfaces.

LEGACY: Systems, architectures, and technology from previously fielded products.

MASTERY OF COMPLEXITY: The ability to constrain the growth of complexity or to define and describe it so that it can be simply understood and shown to meet safety objectives.

MULTI-PEER: A group of suppliers at the same tier that participate in the development of a system as subcontractors to the same contractor or applicant.

MULTI-TIER SUPPLIER NETWORK: A tiered set of suppliers that together construct individual subsystem components and integrate those subsystems into the desired top tier system.

OUTSOURCING TRANSITION: The decision: to move, the activity of movement, and the oversight of the development activities for a subsystem or item.

OVERSIGHT VISIBILITY: The level of visibility into: design details and development processes throughout all tiers of a development network.

PRIME: The top level OEM contractor

SUPPLIER: A subsystem or component developer

SYSTEM DEVELOPMENT CANVAS: A virtual space in which all the activities of a design interact.

TIER: Levels of contracted corporations in which a contracting corporation has let a contract to a developer for a subsystem component or item.

TRANSLATION LAYER: Any point in a development activity in which information from one domain, one discipline, one corporation, or one individual is transferred to another.

WORLDVIEW: The sum of experiences, training, and cultural influences that form a foundation for behavior

2 Structure of This Report

Figure 1 below shows the steps and tasks we performed for the study.

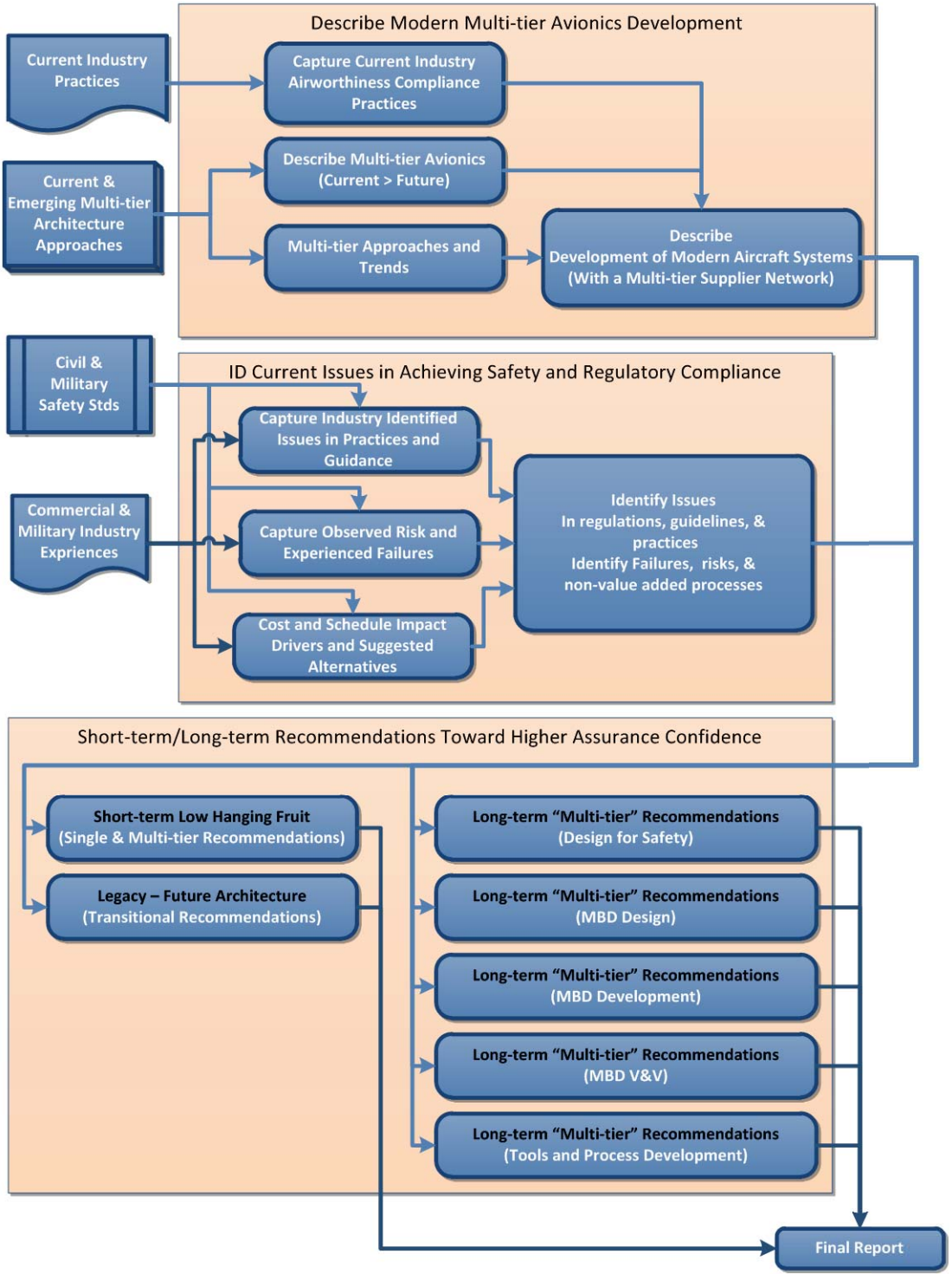


Figure 1. Study steps and tasks

The majority of the information, risks, and recommendations came from two steps – an analysis of the safety standards (regulations and guidelines), and interviews with industry experts regarding current practices and experiences. See Appendix A for the regulatory guidelines assessment. See Appendix B for the risks and recommendations from industry.

Appendices C, D, and E capture other material we produced in the course of the study: how well do ARP4754A and DO-331 address model-based design (MBD); current trends in avionics that will affect the guidelines; and an overview of the certification process with a bias towards avionics and suppliers.

As we executed the tasks, we formed a mind map that captures the flow leading to the findings of the study. See Figure 2 below.

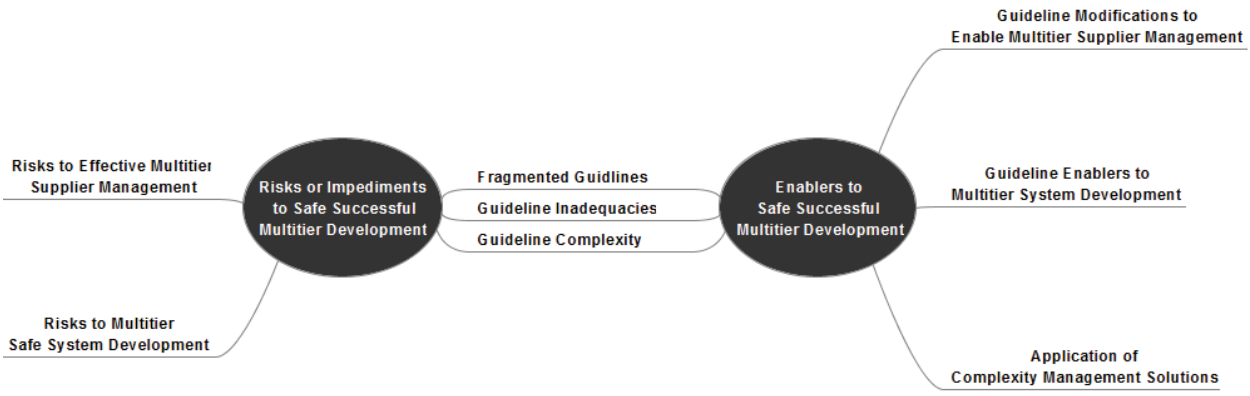


Figure 2. Map of Study Findings

We first extracted two major categories of risks to safe multi-tier avionics development – management of suppliers and lack of a systems emphasis. Then we looked at how the existing regulations and guidelines do or don't address the risks. We finished with regulatory and guideline actions that would lead to greater safety in multi-tier developments.

As you go through the sections in this report, you will see expansions of this map.

3 Summary of Findings and Recommendations

The findings and recommendations are grouped under the categories of:

- Risks to multi-tier supplier management
- Risks to multi-tier systems development
- Guideline weaknesses
- Recommendations

3.1 Risks to Multi-tier Supplier Management

Good multi-tier supplier management is as important to developing safe systems as are the technical processes because it establishes the responsibilities, the resources, and the means of accomplishing the work.

Failure to Understand Outsourcing Risks: Industry contributors to this study identified outsourcing failures as a major safety area. Seemingly unmanageable growth in complexity and the associated development costs has prompted industry to seek specialized suppliers that are less expensive than internal organizations. Companies often assume (for the hope of reducing cost) that suppliers' knowledge is equal to internal experienced personnel and their "across-the-hallway" day-to-day discussions. There are some resulting failures:

- Suppliers are not accurately assessed regarding their system integration capability and experience in design for safety. Companies accept suppliers' claim of experience from similar past efforts, and accept suppliers' self-assessments.
- Suppliers fail to correctly interpret requirements because they lack application experience or knowledge about systems' higher level functions.
- Technical solutions that boast of cost reductions and competitive advantages are often overrated for sales, and end up adding to complexity.
- Companies using suppliers do not understand the level of internal expertise that must be maintained to provide proper oversight of suppliers. Experienced personnel are dropped as suppliers are brought on, and then companies cannot perform oversight properly.
- When outsourcing, especially to another country, there are cultural differences that are not recognized. First-time expectations between a company and its supplier are wrong because their cultures are different.

Inadequate Contracting: The most obvious result of the missed risks above is inadequate contracting between companies and their suppliers. The contracts lack assignments of system functions and safety responsibilities, do not establish processes for passing clear specifications, and lack oversight focused on safety.

Responsibilities and boundaries that are not defined and funded will not be worked on. Further, boundaries that are not defined from a system perspective will let functional and safety requirements

slip through. A contract should clearly assign responsibility, authority, and accountability (RAA) at the company's level to provide the context a supplier needs.

For companies and suppliers that are not effective at multi-tier work, oversight is often viewed incorrectly. Companies view it as increasing the cost of execution, or use oversight as a tool to reduce the costs of suppliers. Suppliers view oversight as additional regulatory burdens and another checkbox to fill before shipping a product. In these cases, companies expect design and safety oversight to take place through requirements flow down and a few design reviews.

With multiple tiers of suppliers, there is a question about how much visibility should be available to the company at the top through all the tiers, and how that can be accomplished without compromising intellectual property. Often, visibility is provided only after a supplier fails to perform.

In the course of this study, we did not find any guidelines to industry that provided a clear contracting approach to: outsourcing decisions, supplier assessments, supplier management and oversight, and proper contracting of these activities.

3.2 Risks to Multi-tier Systems Development

Struggles towards Mastery of Complexity: Design of safe avionics requires that there be clarity in understanding the system. Complexity makes understanding harder. Einstein had a great quote, "If you can't explain it simply, you simply don't understand it." Unfortunately, there is a common tendency to consider complexity as admirable in customers' eyes and an indicator of a supplier's accomplishments.

Outsourcing makes complexity worse in terms of safety by adding multi-tier "translation layers". Translating system knowledge across company boundaries abstracts developers further from the systems architects who are supposed to understand the system.

Product complexity can be put into two buckets – essential and nonessential being further categorized as clearly explained and poorly described. A company and its suppliers must understand the essential complexities. They should consider eliminating or segregating nonessential complexity for cost and safety reasons. There are risks that a developer will not properly manage its product complexity because:

- The developer lacks a clear system view of what functions are essential and nonessential.
- The developer does not maintain the system view through development, allowing boundaries and high-level requirements to drift.
- The developer's teams and suppliers begin work before system definitions are known.
- The developer's design tools do not handle complexity well.
- There are regulatory processes that have some promise to illuminate complexity, but the processes are unnecessarily constrained.

Incomplete/Inadequate Requirements Development and Translation: All of the study participants agreed that the major source of design and safety error was in the requirements translation, interpretation, and flow-down. Guidelines and processes have worked quite well for implementation of designs. However, attention and processes are needed at the system decomposition boundaries to transfer the requirements and system intent to multi-tier suppliers. These boundary risks include:

- Level of understanding the system and its application by developers on both sides of a multi-tier boundary.
- Availability and use of design tools and industry standards that are sufficient for conveying design requirements.
- Clear and concise requirements that prevent interpretation error, particularly in higher level system intent.
- Carefully defined interfaces. Companies should not rely on "compliance" with industry standards to properly define interfaces.

Inadequate Systems Processes: Both industry and regulatory experts raised the concern of a decay in the fundamental systems responsibilities in the avionics industry. The risk sources are:

- System interface definition, system level testing, and unintended function testing have been starved of resources due to the regulatory and industry focus on software and lower level processes. System-level assessment is traded for an assumption that extensive low level testing prescribed by the guidelines will provide adequate coverage. This fails particularly at system boundaries and boundaries between tiers of suppliers.
- Multi-tier oversight is dependent on the strength of a company's safety organization. When additional tiers are added, the demands on that safety organization increase without the resources to match – funding, technically savvy personnel, and personnel with subcontractor oversight experience.
- Low-level items begin to define system objectives. Systems objectives should be the source from which requirements are decomposed and allocated. With a process emphasizing software over systems, the lower level implementers have few boundaries and "discover the design".

3.3 Guideline weaknesses

Appendix A, Regulatory Guideline Assessment, holds our assessment of how well the current regulatory guidelines address avionics development in a network of multi-tiered developers. We looked at documents from ARP, RTCA, FAA Orders, Advisory Circulars, and a few other peripheral documents.

It is difficult to grasp the available resources, content, and applicability of the current guidelines. Newcomers to the avionics industry must get a significant amount of tribal knowledge from experienced companies. Even the experienced DER's and safety process experts we spoke with hesitated to say they had a full picture of the safety processes outlined in the many guidelines.

Fragmented Guidelines: The regulatory guidelines can be likened to a collection of roadmaps generated by various cartographers, each with partial terrain information and each with their own particular region and destination in mind. A newcomer in the multi-tier development environment will typically be told to start with the fundamental documents of ARP4754A, DO-178C, and DO-254. After that, a newcomer will labor for some time before being made aware of the existence and applicability of Advisory Circulars and FAA Orders. Then, time is required to wade through the guidelines figuring out how they apply to the newcomer's work.

The issue of fragmentation was pointed out by a previous Aviation Rulemaking Committee (ARC) assessment of FAA initiatives to improve aircraft certification and approval processes (online ARC Recommendation Report dated May 22, 2012). Their study pointed out that many initiatives to improve certification efficiency have been implemented; however the initiatives are not cohesive.

Guideline Inadequacies: This study identified 8 guideline weaknesses related to multi-tier, newcomer, and even experienced industry developers as follows:

1. Hidden Guidance Methods: The reader of the guidelines is not likely to stumble on to all the useful material scattered throughout the RTCA, ARP, Advisory Circulars, FAA Orders, SAE papers, IEEE papers, etc. that could be useful to the developer. What appears to be missing is a top level view of the guidelines themselves with an organized structure around a clearly defined roadmap to the objectives.
2. Inadequate Systems Guidance: Industry experts indicate the current safety escapes are at the systems design and testing levels rather than at the low level implementation. ARP4754A was only recently (2011) recognized by the FAA as an acceptable means of compliance, even though ARP4754 was published in 1996. This document, however, remains in conflict with the Industry Guide to Product Certification. System safety is given lip service, but the focus on software and its processes has caused industry to devalue systems design.
3. Inadequate Multi-tier Oversight Methodology: Out of the most heavily used regulatory documents (ARP4754A, DO-178C, and DO-254), only DO-178C calls out areas for supplier oversight and control. FAA Order 8110.49 speaks to multi-tier development and the need for oversight, but this document is not widely recognized and used by industry. The guidelines do not promote effective oversight. Most companies implement oversight as periodic "fly-by" assessments of suppliers' work at reviews. The required oversight does not promote tiers working towards the same system intent.
4. Weak Multi-tier Requirements Development Guidance: Flow-down of clear and complete requirements is critical when each company tier adds a requirement translation layer. Some of the documents promote graphical descriptions for requirements in addition to text because they are clearer. The guidelines should be updated to describe how to use graphical requirements for multi-tier tasks.
5. Missing Model-Based Design (MBD) Guidance: MBD can be used from upper systems level down through software and hardware component levels. Currently, DO-331 is the primary guide for MBD because ARP4754A recognizes it. However, DO-331 was written as a software document under DO-178C, so its guidance for MBD is directed at software. The reader is left with a lack of clarity as to what is permitted in systems vs software modeling. See Appendix D,

ARP4754A and DO-331 Model Based Design Guideline Adequacy, for further discussion on the issues of MBD.

6. Missing/Weak Tiered Supplier Management Guidance: As we mentioned in Section 3.1 above (multi-tier supplier management), strong contracts are necessary for safety. The issue is not the legalese in contracts, but the behaviors and partnerships in the development effort. The guidelines do not say anything to industry about evaluating suppliers' capabilities, defining methods and means of transferring information (both directions), establishing Responsibility, Accountability and Authority.
7. Weak Guidance for Handling Translation Layers: Translation layers are the places in the design process where technical and management information is transferred from one organization to another. Any time information jumps from one company to another, there is a risk that it will not be complete. These translations should be minimized and/or managed to assure accuracy in the translation. The guidelines are weak in their recognition of these high risk points and in guidance as to how to manage proper translation. ARP4754A acknowledges the requirements allocation and includes a verification loop but not much more than that.
8. Inadequate Guidance on System Complexity Minimization: Growing complexity is the prime driver of multi-tier development teams, and it is the primary reason for increased risk in multi-tier development. Increased risk comes with complexity in the form of: a lack of full system understanding, increased information translation boundaries, and the entry of inexperienced developers into the avionics arena. Complexity issues are recognized in at least one document, Order 8110.49, which actually does a nice job of outlining the concerns. However the guidelines could provide additional assistance in complexity minimization or in the design of necessarily complex systems in a safe manner.

Guideline Complexity: Guidelines provide considerable tutorial material but are not clearly organized towards a goal or series of accomplishments the developer should follow. Without the tutorial of an experienced safety specialist or a DER, a multi-tier newcomer would not quickly grasp the intended objectives outlined within the guideline. Take for example the Plan for Software Aspects of Certification (PSAC) and Plan for Hardware Aspects of Certification (PHAC) – there is an outline of each of these mandatory documents in the respective guidelines, but the guidelines themselves are not organized with a focus towards the development of a PSAC and PHAC.

3.4 Summary of Recommendations

We addressed the risks identified above from the perspective of the overall purpose and intent of regulatory guidelines. Potential enhancements to the collection of guidelines were then postulated as illustrated in Figure 3.

The result is five recommendations that fall into the categories of multi-tier supplier management and multi-tier system development.

The five recommendations are:

1. **Development of a Multi-tier Contracting Guideline**
2. **Development of a Hierarchal Guide to the Guidelines**
3. **Product-Driven Guideline Structure Modifications for DO-178C and DO-254**
4. **Specification of a Systems Plan for Certification**
5. **Development of a System MBD Guideline**

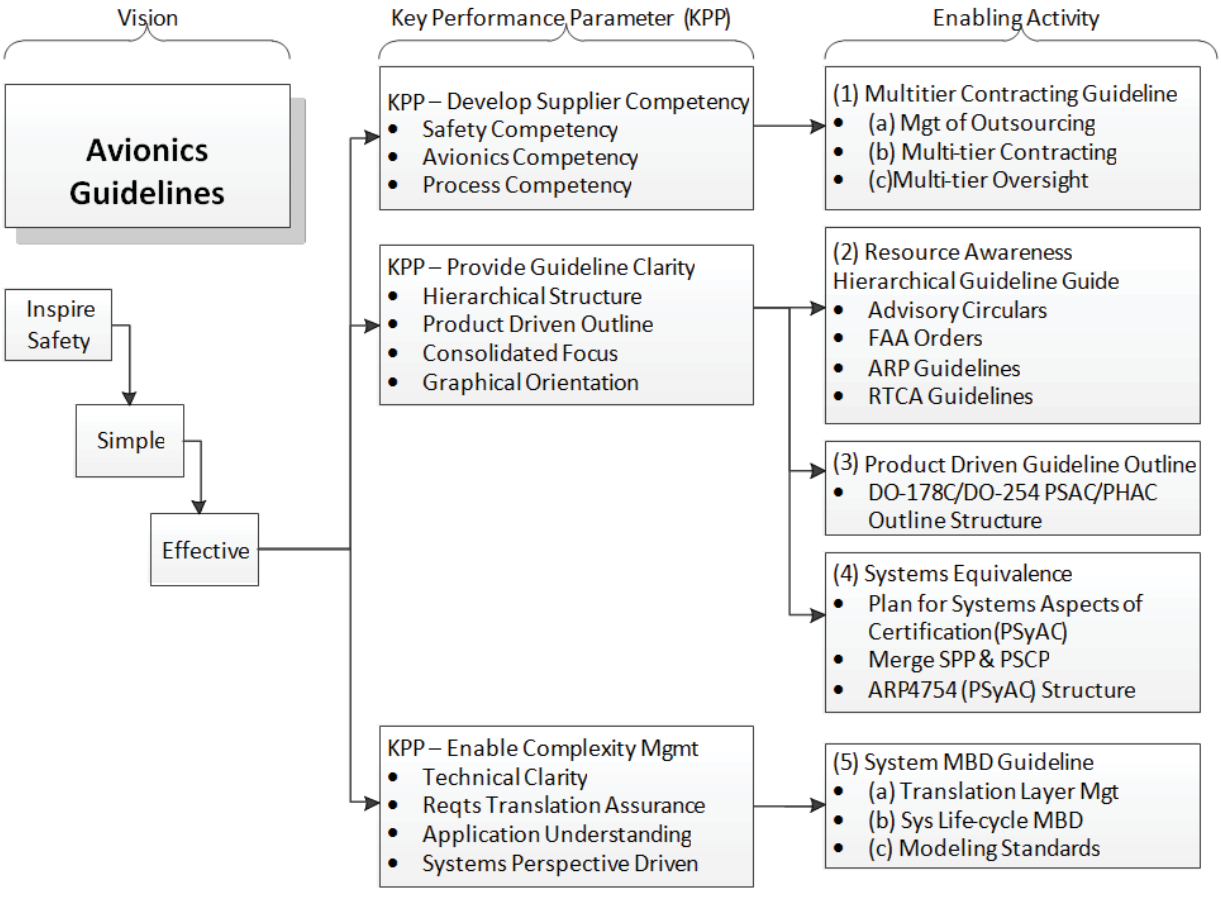


Figure 3. Guideline Intent and Recommended Enhancements

Recommendation 1: Multi-tier Contracting Guideline

Several weaknesses were identified in the guidelines relating to management of multi-tiered suppliers: assessing suppliers, defining multi-tier responsibilities in contracts, day-to-day management practices, and inadequate oversight of suppliers. There are resources for multi-tier management in some FAA internal orders (to FAA AIR), but these are not widely recognized by industry.

To address these issues, we propose a new guideline with three sections:

a) **A guide for management of outsourcing: guidance for assessing potential supplier capabilities; guidance in the transition to outsourcing in terms of requirements rigor and skill retention; and awareness of potential impacts from corporate and cultural differences and how do deal with them.**
b) **A guide for multi-tier supplier contracting: a model contract with the basic elements; guidance for establishing boundaries in Responsibility Accountability and Authority (RAA); flow-down of system, software, and hardware prescriptive plans.**
c) **A guide for multi-tier supplier oversight: oversight agreements established prior to contract authorization; agreements on oversight visibility throughout the tier levels; and a continual focus on technical oversight.**

Recommendation 2: Hierarchical Guide to the Guidelines

Help developers find the appropriate regulatory guidance, and provide resource awareness through a hierarchical guideline document.

We recommend the development of a hierarchical guide to the guidelines showing interrelationships and dependencies between Advisory Circulars, FAA Orders, ARP guidelines, RTCA guidelines and key industry guidelines.

During this process there should also be an effort to close the missing cross reference holes found in the various guidelines.

Recommendation 3: Product Driven Guideline Structure

We recommend a restructure of DO-178C and DO-254 to match the section outlines of the PSAC and PHAC which the developer must generate. There is a PSAC outline (DO-178C Section 11.1) and PHAC outline (DO-254 Section 10.1.1) in the two guidelines. However, the explanatory material in the RTCA documents defining the content of the PSAC and PHAC is not organized according to the outlines of the PSAC or PHAC.

Recommendation 4: Systems Plan for Certification

Strengthen the system role in complex multi-tier developments.

We recommend a Plan for Systems Aspects of Certification (PSyAC) be established along with the PSAC and PHAC.

The PSyAC would replace the SPP and PSCP. The benefits would include:

- Resolving discrepancies between the FAA and Industry Guide to Product Certification (PSCP) and the ARP4754A System Safety Program Plan (SPP). See Figure 20, page 48 for a comparison of the two differing outlines.
- Maintaining focus on system objectives, overall system safety, architectural changes, system requirements, and design clarity.
- Addressing the entire life-cycle of the system (hardware and software developers generally focus on the implementation phase of the V-diagram).
- Provide oversight over all of the tiered supplier networks.
- A single plan defining the system safety analyses and assessments.

Recommendation 5: System Model-Based Design (MBD) Guideline

We believe MBD is a way to reduce the number of translation layers and the impact of any remaining translation layers. MBD is much more than the application of a graphical compiler to generate code from a clearly understood picture of a function or process. MBD applies from the concept through the validation stage of a development where virtual execution of models as they develop direct their requirements specification within the MBD environment and their Early User Assessment (EUA) validation of the developing system.

MBD over the entire life-cycle must be addressed by the guidelines.

It is important that MBD be understood as:

> Model-Based Design (MBD) is a mathematical and visual method of addressing problems associated with designing complex control, signal processing and communication systems. Rather than relying on physical prototypes and textual specifications, model based design uses a system model as an analyzable specification throughout development. It supports system- and component-level design and simulation, automatic code generation, and continuous test and verification. In Model-Based Design, a system model is at the center of the development process, from requirements development, through design, implementation, and testing

We recommend a System MBD Guideline to address the full life-cycle of the development effort and to provide a system perspective of MBD.

First, the guideline should address "translation layer management". The objectives of translation layer management are the reduction of the number of layers and the clarity by which information transitions the translation layer.

This is the jump of a concept, requirement, or design to another tier or group. Figure 4 illustrates the addition of translation layers in a single sub-tier development. A part of addressing translations is modeling standards that can be exchanged across tier boundaries.

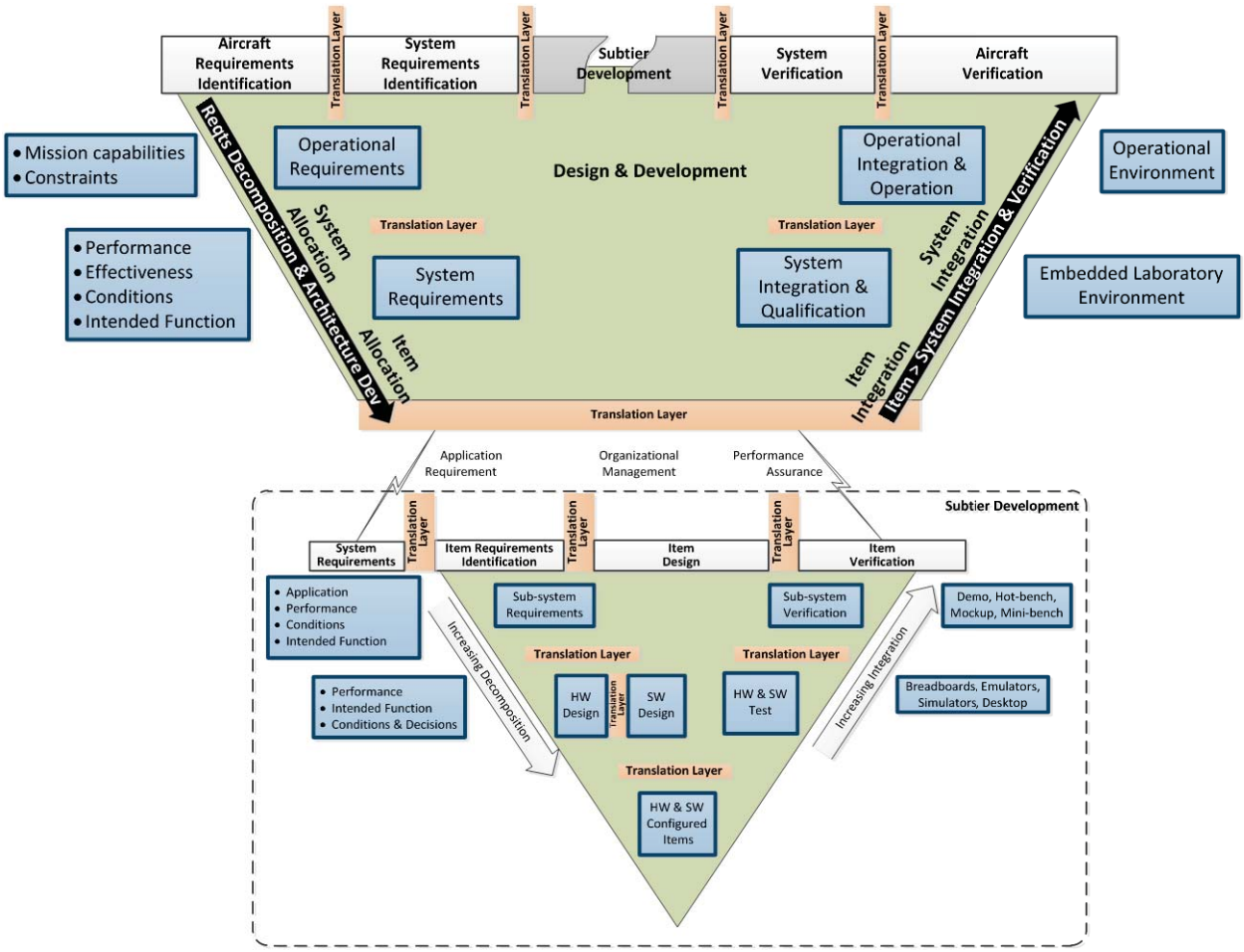


Figure 4. V-Diagram Translation Layers

Second, the MBD guideline should address the full development life-cycle, concept to delivery, from a system perspective which DO-331 does not provide (it only maps DO-178 into a MBD context).

Figure 5 below modifies the traditional V-Diagram illustration to identify the MBD activities over the full life-cycle of a program. It is also drawn to show interactions between a primary developer and the 1st supplier tier.

During development, there must be a continual sharing and open model exchange between the specifier and the developer. This iterative process is another form of EUA that validates interpretations of application intent, performance, and behavior.

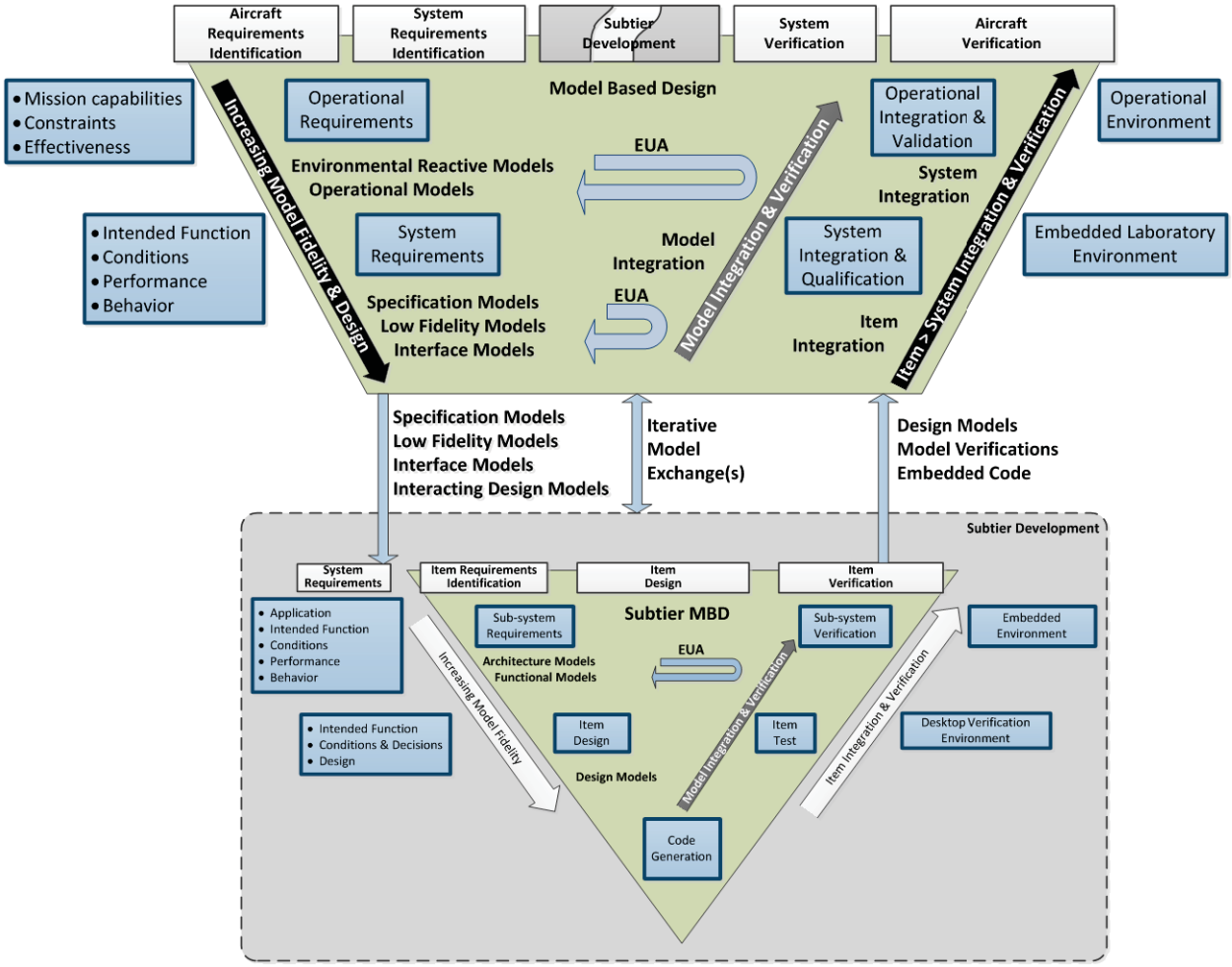


Figure 5. System Model Based Design

3.5 Final Observations

Multi-tier development in an environment of increasing avionics complexity and cost-cutting increases the risk to safe systems developments. However, approaching each aspect of the overall development from a systems perspective will relieve most of the concerns through:

- Organizing the guidelines from an overall systems perspective. This includes how the documents address each other, and the outlines in the documents themselves.
- Application of systems analysis to contracting mechanisms. Contracting mechanisms and approaches that implement agreements on processes, techniques, and oversight to address all tasks and information flow from a multi-tier network model.
- Application of a systems driven design. Application of MBD principles throughout the system development life-cycle through all tiers. Oversight and management of all tiered systems, software, and hardware activities.

We would prioritize the recommendations as follows:

1. Major impact, significant effort: PSyAC and Systems MBD Guideline (Recommendations 4 & 5)
2. Medium impact, low effort: Hierarchical Resource Guideline, DO-178C/DO-254 restructure directed towards the PSAC/PHAC outline (Recommendations 2 & 3)
3. Medium impact with significant effort: Multitier Contracting Guideline (Recommendation 1)

4 Risks or Impediments to Safe Successful Multi-tier Development

Figure 6 breaks out the risks to multi-tier supplier development and safe system development identified by industry. Sections 4.1 and 4.2 provide an explanation of these items.

This collection of multi-tier risks was developed through a review of the regulatory and industry guidelines, and on industry comments identifying weak mechanisms in the safety development processes.

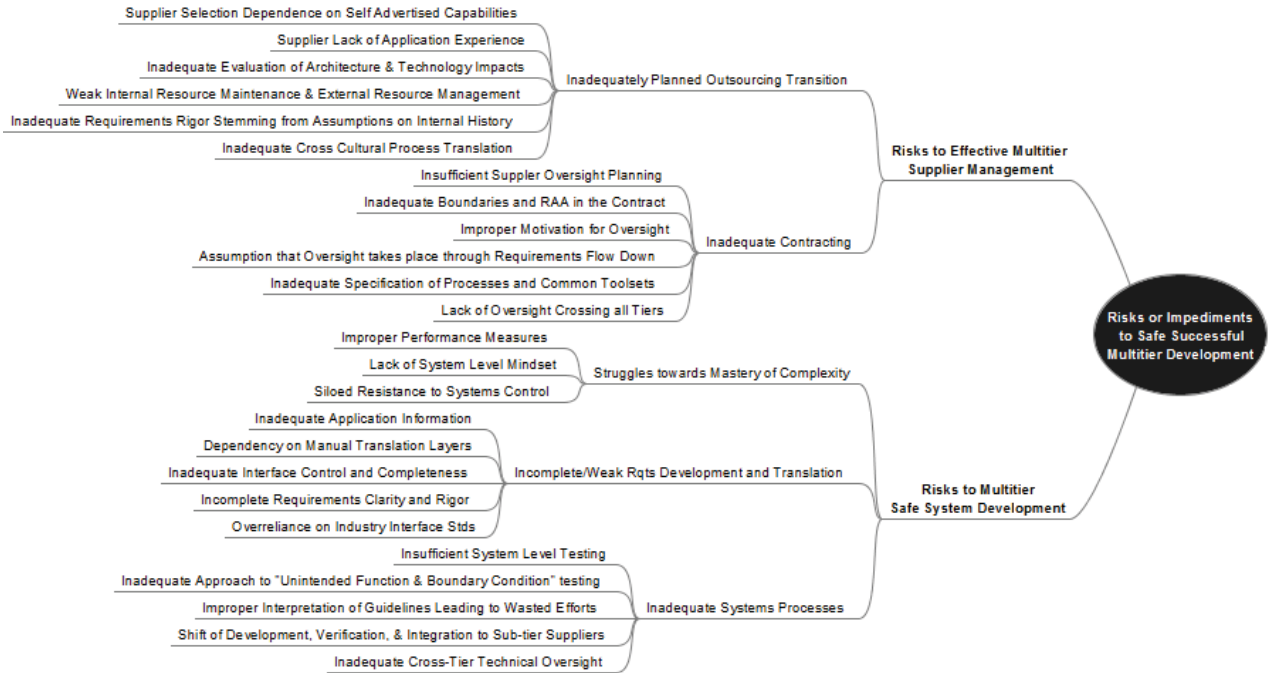


Figure 6. Risks to Multi-tier Development

4.1 Risks to Multi-tier Supplier Management

Table 1 lists those risks collected during this research associated with management of multiple tiers, and provides a short description of that risk.

Table 1. Multi-tier Risks from Inadequate Management

Risks to Multi-tier Supplier Mgt
Inadequately Planned Outsourcing Transition: Companies outsource development for two primary reasons – reduce their own internal costs (requested by management), and deal with complexity by dividing the work. Shifting the work externally can add safety risks if the technical aspects of the transition are not carefully planned and the potential issues addressed prior to the transition. The outsourcing transition adds another tier and the associated translation layers in the technical, process, and management areas. Along with this comes the added effort to ensure that information is clearly transferred to the multi-tier supplier.

Risk Source	Description
Supplier Selection Dependent on Self Advertised Capabilities	Contractor accepts suppliers' marketing of their capabilities and suppliers' self evaluations of capability. As a result, the contractor skips their independent evaluations of potential suppliers.
Supplier Lack of Application Experience	Common causes: 1) a supplier is knowledgeable in his functional area, but has little understanding of next level application; 2) the contractor assumes the supplier is qualified for different area of avionics development based on demonstrated capability in a specific application. Gaps in the supplier's understanding are not filled because the contractor assumes the supplier knows the application.
Inadequate Evaluation of Architectural and Technical Impacts	Contractors may accept solutions that sound good to save time and risk. Program risks may actually increase with the decision to outsource when coupled with unawareness of the complexity consequences and the safety implications.
Weak Internal Resource Maintenance and External Resource Management	Outsourcing for financial or partnership reasons will usually include a reduction of internal resources at the contractor level. An inadequate understanding of the level of internal technical skills needed by contractor to maintain oversight of the subtier developer may result.

Risk Source	Description
Inadequate Requirements Rigor Stemming from Assumptions on Internal History	Transition of contractor's formerly internal technical work to supplier may be based on contractor's historical internal operations and specification rigor. Assumptions of previously highly coupled teams, common processes, and levels of experience are applied to requirements and process flow down as if they were still within the contractor's facility and organization. Failure to complete early user assessment closure on design progress does not catch the potential gaps.
Inadequate Cross Cultural Process Translation	There may be a tiered failure to clarify and train cross-cultural methods and processes to attain a common ground. Design behavior norms and design freedoms stemming from assumptions of the foreign (and even US) contractor's cultural norms if not addressed with the developer can result in gaps and errors.

Inadequate Contracting: The contractual management of tiered developments is an important aspect of safe system development in defining boundaries and responsibilities while giving the prime contractor necessary oversight and insight throughout the development. It also assists the tiered developer in application clarity.

Risk Source	Description
Insufficient Supplier Oversight Planning	Insufficient oversight agreements and planning during the establishment of supplier contract. Subsequent unfilled expectations result in weak oversight, disputes, and cost increases.
Inadequate Boundaries and Supplier Responsibility, Accountability, and Authority (RAA) in the Contract	Inadequate description of supplier RAA in the contract results in uncertainties, assumed responsibilities, and gaps in the design process.
Improper Motivation for Oversight	Contractor mindset towards oversight goals of continual reduction of the oversight burden resulting from a cost reduction objective and technical dislike for executing the oversight management activities. Results in oversight through metrics measuring supplier, design "escapes" and errors not detected by supplier quality assurance and testing, and completed task performance rather than personal involvement in the design during the development effort.

Risk Source	Description
Assumption that Oversight takes place through Requirements Flow Down	Contracting assumption that written flow-down of processes and requirements provides sufficient oversight. Overreliance on written procedures and periodic design reviews without frequent technical and management guidance to clarify and correct the suppliers design directions. An aloof attitude towards accomplishing the design objective without real design participation by the contractor.
Inadequate Specification of Processes and Common Toolsets	Inadequate agreements on processes, requirements flow-down methodologies, and common toolsets at contract initiation. Disparate processes and toolsets force contractors and suppliers to translate, and this is where specification errors are most likely to occur.
Lack of Oversight Crossing all Tiers	Failure to contract visibility and oversight through all levels of tiers from the top can lead to application and requirements divergence at the lower tiers.

4.2 Risks to Multi-tier Systems Development

Table 2 lists those risks collected during this research associated with systems development in a multi-tier environment, and provides a short description of that risk.

Table 2. Multi-tier Risks from Weak System Development

Risks to Multi-tier Systems Development
Struggles toward Mastery of Complexity: Complexity is the primary driver of outsourcing and multi-tier network development. However, the added tiers introduce additional complexity that must now also be managed. So, complexity must be described in a humanly understandable fashion that provides clarity and control of the system. This requires an understanding of the difference between necessary complexity and unnecessary complexity, which can only be found at a top level view of the system's application and requirements, and must be followed with an oversight mindset towards simplification that overcomes the natural tendencies towards unnecessary complexity.

Risk Source	Description
Improper Performance Measures	Contractors and suppliers find rewards in developing systems that perform over and above what is sufficient. They readily accept and promote more complex systems with functionality beyond the intended function.

Risk Source	Description
Lack of Systems Level Mindset	Contractors lack experience in clearly describing systems. The lack comes from a long trend of dropping systems design in deference to strong software design - software design does not capture system priorities and behavior. Results in weak boundary definitions, incomplete or inaccurate requirements, added translation layers, weakened verification, and loosely contained designs at each subsequent tier.
Siloed Resistance to Systems Control	Development teams tend to stay with familiar local methods, and do not want to spend additional time and money considering overall project benefits.

Incomplete/Inadequate Requirements Development and Translation: Clear simple understandable requirements development comes from a full understanding of the application. The translation from the composer to the reader is hampered by differences in interpretation, differing experiences between the two developers, assumptions regarding guidelines, specifications, and differing "world views". Multi-tier networks compound this risk by jumping across company boundaries, adding to the risk of missed interpretation, and further distancing the developer from the top level system designer.

Risk Source	Description
Inadequate Application Information	Suppliers are given limited information about the higher tier system purpose and operational characteristics. Can result in improperly implemented requirements and erroneous derived requirements.
Dependency on Manual Translation Layers	Manual translation of requirements driven by specification methodologies that require human interpretations.
Inadequate Interface Control and Completeness	Lack of focus on the criticality of accurate and unambiguous interface specifications.
Incomplete Requirements Clarity and Rigor	Textual driven requirements that have not been validated for completeness and accuracy, or Design Specifications that have not been validated.
Overreliance on Industry Interface Standards	Companies assume interface standards suffice as complete interface definitions in a system. This is particularly a problem for standards that set the format of data exchanged, but not the content.

Inadequate Systems Processes: System level validation and verification is not completely covered by V&V of components such as software routines .

Risk Source	Description
Insufficient System Level Testing	A prime contractor assumes testing by lower tiers capture the behavior of the avionics system. However, suppliers do not have enough information on other suppliers' components to create system-level tests. System failures are not noted until experimental flight tests.
Inadequate "Unintended Function" and Boundary Condition Testing	Causes: 1) industry avoids these tests because the tests are hard to define or take too much effort; 2) contractors lose systems level application expertise over time to outsourcing.
Improper Interpretation of Guidelines Leading to Wasted Effort	Individual erroneous perception and interpretation of guidelines leading to unnecessary efforts or complexity in compliance.
Shift of Development, Verification, and Integration to Sub-tier Suppliers	Management in contractors wants to reduce their infrastructure costs, so they shift systems and integration work to suppliers. However, contractors do a poor job of describing their system processes to suppliers. This is aggravated again by the suppliers' lack of system knowledge.

5 Guideline Weaknesses

An examination of the guidelines, see Appendix A, was performed to assess their adequacy in providing guidance to complex avionics development in a multi-tier developer environment. Incomplete closure of an identified multi-tier risk is a weakness in the regulatory guidelines. Figure 7 groups the findings of the guideline assessment into three categories:

1. Fragmented Guidelines
2. Guideline Inadequacies
3. Guideline Complexity

The paragraphs below will dive into more detail on these groups and where the safety risks of execution of a development in a multi-tier network of suppliers may be propagated through the existing guidelines and industry practices. Any weaknesses in the guidelines are exacerbated by multi-tier suppliers as they add another dimension to oversight and information clarity management.

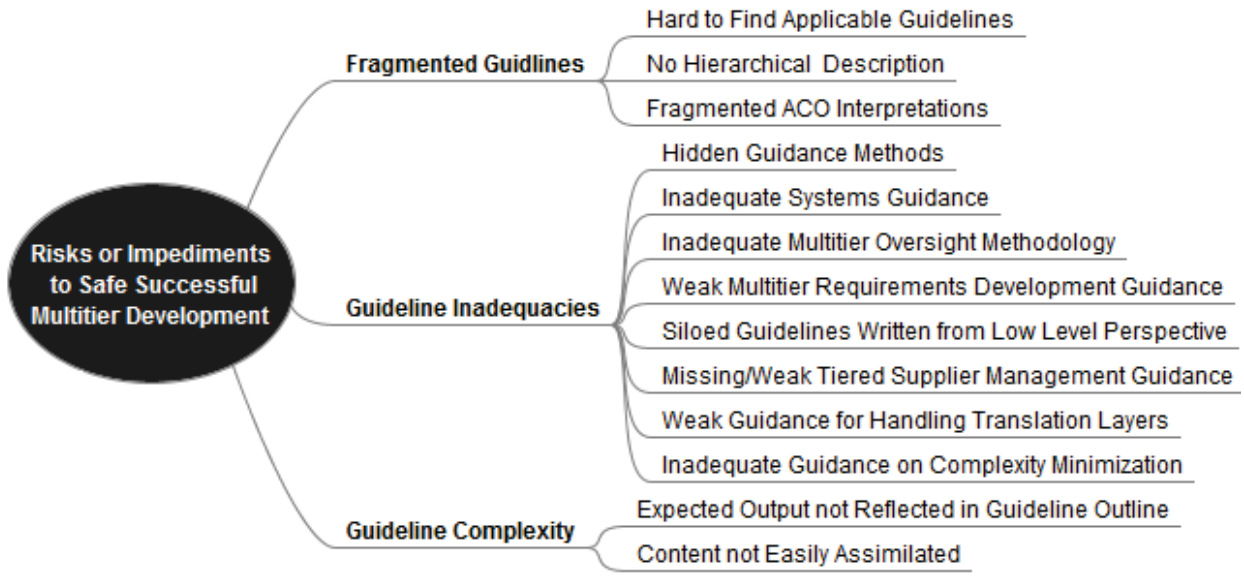


Figure 7. Guideline Weaknesses

5.1 Fragmented Guidelines

Table 3. Fragmented Guideline Weaknesses

Fragmented Guidelines	
Guideline Weakness	**Description**
Hard to Find Applicable Guidelines	We found no organized system or hierarchical view of the Advisory Circulars, Orders, RTCA guidelines, ARP guidelines, or industry guidelines. A multi-tier newcomer will have difficulty in finding applicable guidelines, wading through them, and assimilating an understanding of applicable content.
Inadequate Clarity of Guideline Authority	There is no top level guidance providing means or sequences of design and artifact development that the regulatory agencies will be looking for. A few key guidelines are recognized by an FAA Order giving approval to that guideline's methods as an acceptable means of complying with safety objectives.
Fragmented ACO Interpretations	Regional offices differ in their interpretations of guidelines and acceptable approaches.

5.2 Guideline Inadequacies

Table 4. Guideline Inadequacies Weaknesses

Guideline Inadequacies	
Guideline Weakness	**Description**
Hidden Guidance Methods	Certain potentially useful guidance material (such as supplier capability evaluation and oversight recommendations found in Order 8110.105 and FAA and Industry Guide to Product Certification) is hidden in documents that have been defined as relevant only to the FAA AIR. Most suppliers will focus on the key guidance documents DO-178C and DO-254 and are likely to miss these resources.
Inadequate Systems Guidance	ARP4754A is virtually the only document giving systems guidance, and that document was only officially recognized in 2011 by FAA AC20-174. The FAA and Industry Guide to Product Certification PSCP and the ARP4754A PSP are in conflict as to content and that content is weak on the technical aspects of systems engineering. The use of systems level modeling and boundaries with lower level modeling is unclear.

Guideline Inadequacies	
Guideline Weakness	**Description**
Inadequate Multi-tier Oversight Methodology	FAA Order 8110.49 nicely expresses the concerns with multi-tier developments and focuses on initial supplier capability assessment and oversight but is targeted only to the AIR/DER audience. DO-178C addresses supplier oversight and control in a few sections for the developer of software. With these two exceptions, the remainder of the guidelines do not address oversight. Oversight reliance is therefore solely based on the contractor's integrity. Multi-tier technical oversight is generally limited to reviews and audits throughout all the guidelines. Therefore the quality of the oversight is constrained by the frequency and depth of the review and audit. The FAA has its own internal guidelines for oversight determination.
Weak Multi-tier Requirements Development Guidance	Thorough, complete and clear requirements development is as much about safety as it is about the functional design. Unclear requirements and their flow-down will hamper safety assessments and safety design. The guidelines have weaknesses in addressing the requirements and application understanding flow down to the lower tiered developer. Although there is excellent guidance on how to develop requirements in FAA DOT AR-08-32 Requirements Engineering Management Handbook, none of the industry RTCA or ARP documents reference it.
Siloed Guidelines Written from Low Level Perspective	Guidelines for the individual disciplines silo themselves from systems. With a weak systems guideline and this lower level perspective, discipline and functional boundaries can become gaps with no recognition of the systems aspects that each discipline developer should be responsible for to insure the gaps are bridged.
Missing/Weak Tiered Supplier Management Guidance	Contracting issues with multi-tier suppliers can have equal impact as a weak technical management process. Guidance for supplier contracting is weak or missing. Identification of items to address and contracting templates don't exist. There is no beginning point from which a contractor can obtain guidance that points to and references other relevant resources. Any materials associated with supplier capability assessments or oversight are scattered and do not complete the overall contracting practices that should be followed for multi-tier networks of suppliers. This leads to a dependency on OEM or contractor tribal knowledge.

Guideline Inadequacies	
Guideline Weakness	**Description**
Weak Guidance for Handling Translation Layers	Translation layers where understanding is intended to be transferred between individuals are a major risk area that becomes more critical in multi-tier environments. The guidelines are weak in identifying translation areas as high risk areas and do not provide sufficient guidance on how to manage the risk areas. In some cases there is a sense that the guidelines do the opposite by apparently imposing additional manual translation layers.
Inadequate Guidance on Complexity Minimization	Concerns over growing complexity are expressed in documents such as Order 8110.49 but minimization activities recommended are limited to measuring complexity and establishing a level of oversight. No guidance is given to generate a mindset for identifying nonessential complexity and then how do deal with it.

5.3 Guideline Complexity

Table 5. Guideline Complexity Weaknesses

Guideline Complexity	
Guideline Weakness	**Description**
Expected Output not Reflected in Guideline Outline	Guideline content is organized such that the reader must wade through all of the material before he begins to understand the compliance process. There is no clear guidance pointing to the objective for the developer to create a prescriptive process document that the FAA approves. The expected output of the documents, PSAC/PHAC, are treated as appendices as opposed to being the primary focus.
Content not Easily Assimilated	There are instances where the reader is left with uncertainties on what the guideline objective is thus leading to misinterpretations. Coupled with cases where guidelines contain material with questionable relevance while missing the core objectives the reader must spend extra effort to extract what is important. There is limited use of good systems practices utilizing graphics within the guidelines to aid understanding.

6 Recommendations

The intent of the regulatory guidelines is to inspire a safety mindset within the development community while doing so in an effective and simply understood manner. They are the means by which industry develops their plans for approval from the regulatory agencies. Our recommendations focus on enhancements to the regulatory documents, and hence industry plans, that alleviate the multi-tier risks identified earlier.

Figure 3 above illustrates how we selected the recommendations given the risks identified above plus key performance parameters (KPP) extracted from the guidelines. These three KPPs addressed the risks and weaknesses associated with this study.

Roughly half of the recommendations concern clarity in the guidelines. The other half adds to a systems perspective across multiple tiers.

After speaking with a number of industry experts, we extracted five recommendations which we believe are practical:

1) Add a guide for multi-tier contracting to help contractors establish good contracts and oversight.
2) Add a "guide to the guidelines", mapping the hierarchy and relationships between the regulations.
3) Re-arrange the outlines of DO-178C and DO-254 to the desired outlines for PSAC's and PHAC's.
4) Add a Plan for System Aspects of Certification (PSyAC) to go along with PSAC's and PHAC's.
5) Add a Systems MBD guideline to address the full development life-cycle.

The guidelines provide carefully thought tutorials and guidance, but tend to do so in silos, excluding themselves from other domains. There was a temptation to recommend that we throw away the bulk of the guidelines and just maintain an example PSAC, PHAC, and add a Plan for Systems Aspects of Certification (PSyAC). These three documents would have reflected the contents of DO-178C, DO-254, and ARP4754 respectively. All important and relevant material from all the other documents would have been collected into these three. Any developer could then extract the relevant content for his effort to create his executable document. However, the recommendations are towards a reorganization of the document outlines directed toward the products they expect to be generated.

The inputs and guideline weaknesses were broken out with high level content in the groups as illustrated in Figure 8 below.

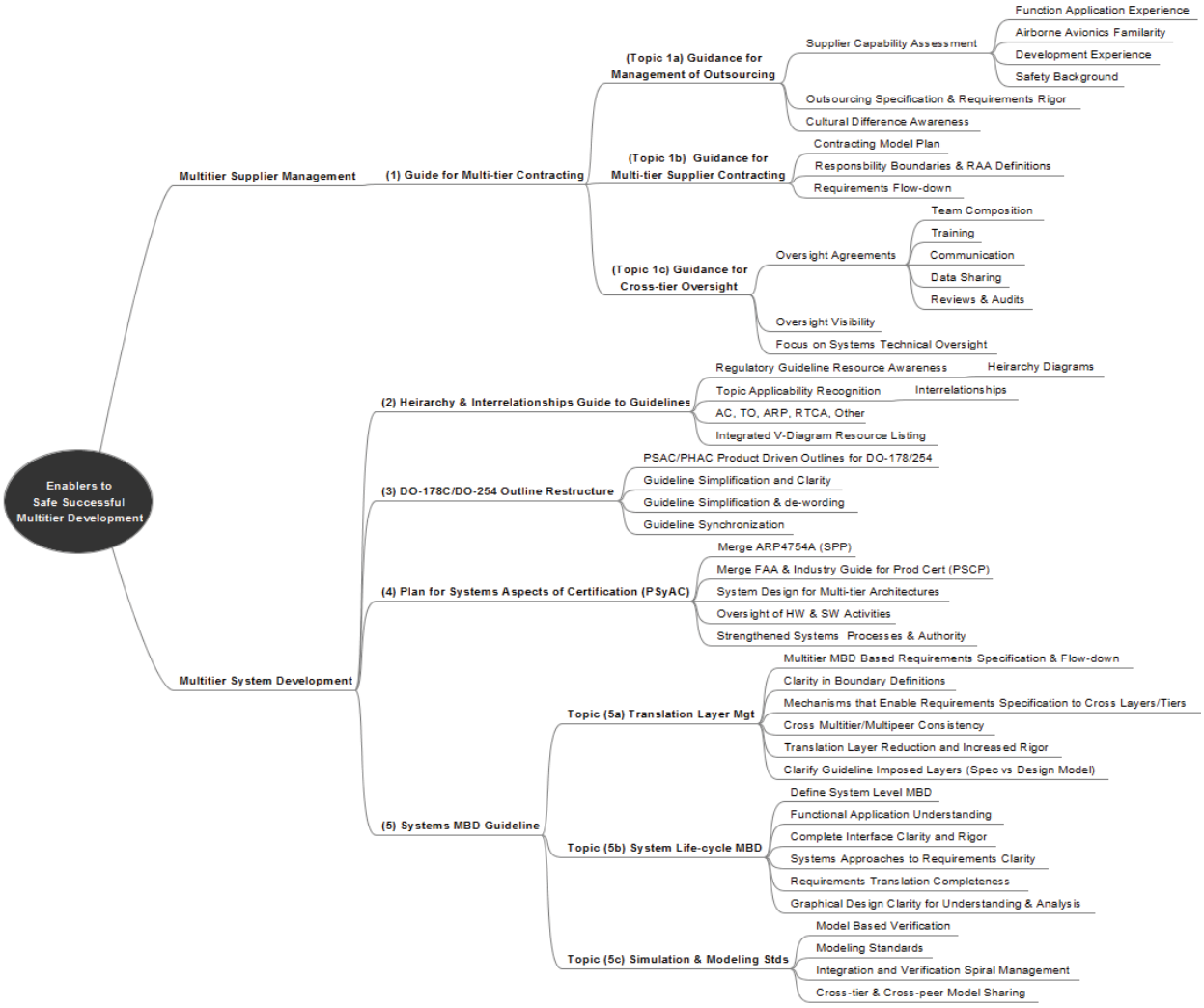


Figure 8. Enablers for Safe Multi-tier Development

6.1 Context for the Recommendations

A simple view of the major activities and influences on an avionics development is reflected in Figure 9. The major drivers are the system requirements, safety and security regulations, and the design. All three merge and interact with each other in the "system development canvas". There are three other outside influences that have indirect effects on the activities within the canvas: technology advancements, legacy systems foundations, and business drivers.

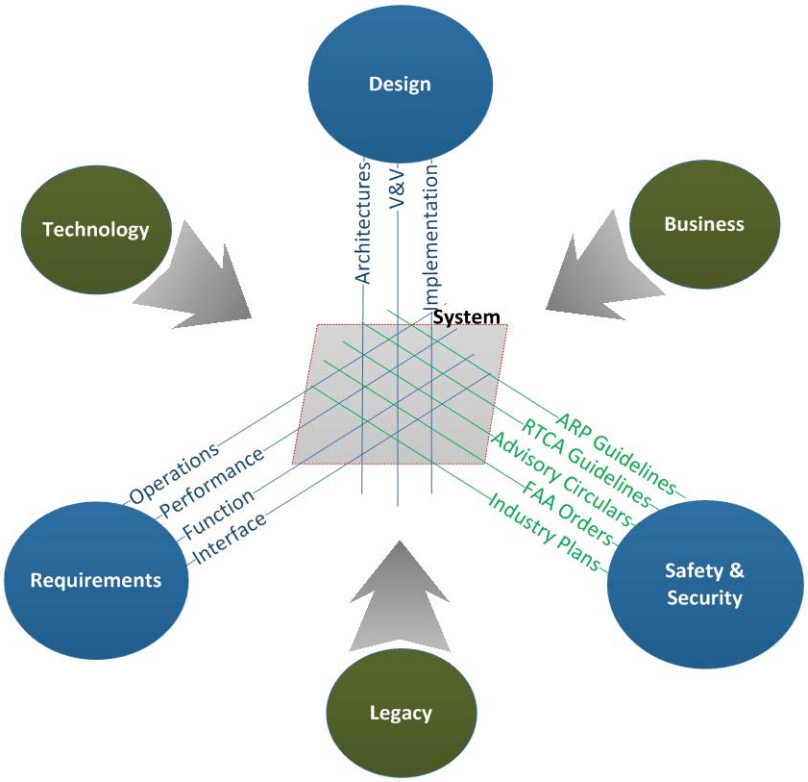


Figure 9. Simple "one company" development effort

This relatively simple diagram becomes complicated quickly when the development effort is spread across tiers of contractors and suppliers.

Figure 10 below shows how the primary flow down of information occurs through the functional requirements and safety requirements. The figure also shows the points where the recommendations apply.

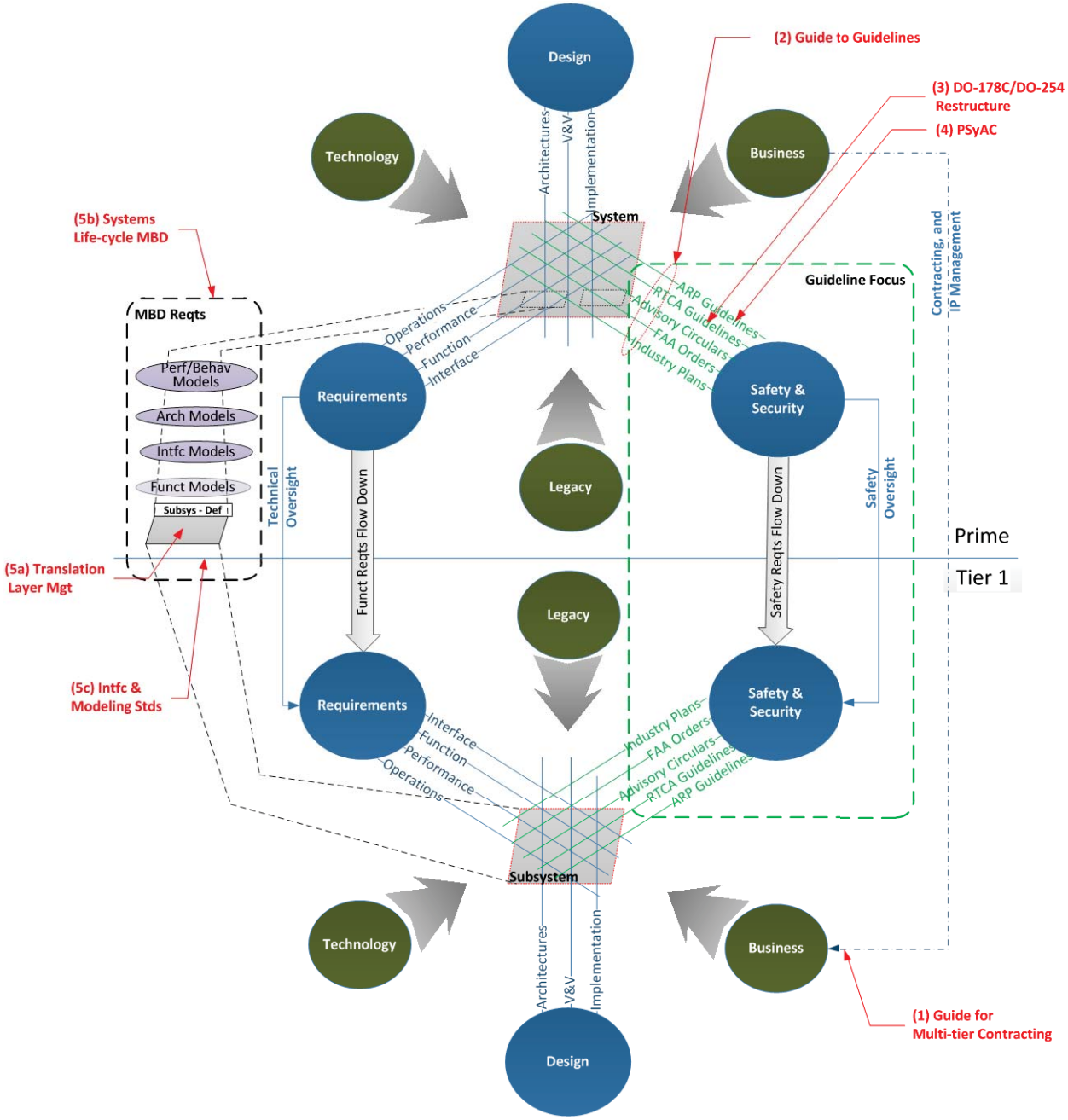


Figure 10. Development efforts spread across tiers, and where the recommendations apply

The regulatory activities that are expected to take place within the system development canvas over the life-cycle of the development are illustrated in Figure 11 below. The key regulatory guidelines and key artifact outputs are overlaid on the traditional V-diagram.

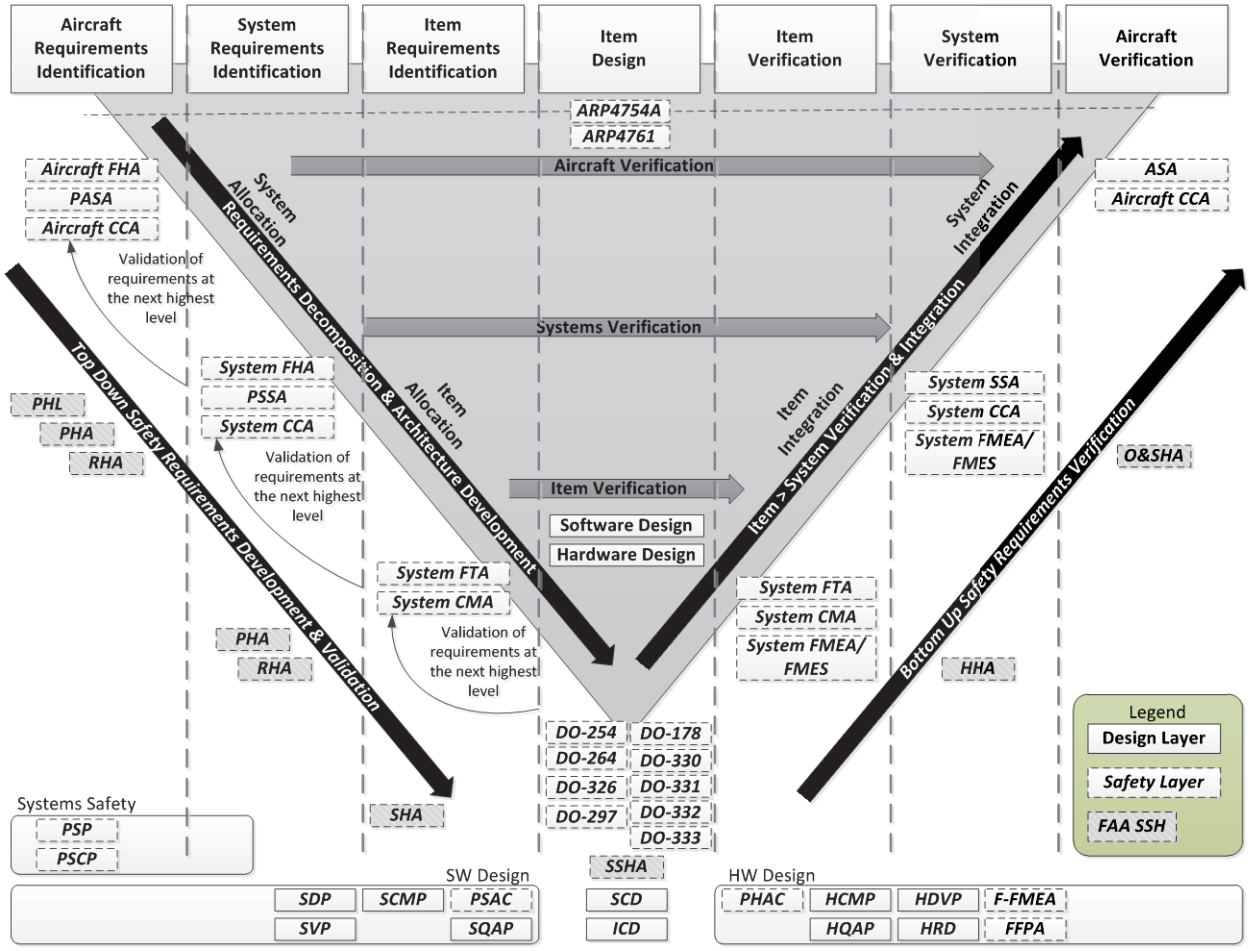


Figure 11. Guideline Expressed Regulatory Activities

6.2 Recommendation #1 – Guide for Multi-tier Contracting

Recommendation 1: To address these three issues a new guideline is proposed with three sections:

- **A guide for management of outsourcing**
- **A guide for multi-tier supplier contracting**
- **A guide for multi-tier supplier oversight**

Three primary weaknesses were identified in the guidelines relating to management of multi-tiered suppliers:

1. Weak multi-tiered supplier management guidance material that would assist in: pre-contract assessments, contractual agreements on multi-tier operations, and good day-to-day management practices. What is available is not clearly assembled to aid in the establishment of an effective network of multi-tier suppliers.
2. There is an inadequate level of multi-tier oversight methodology that would educate those new to multi-tier outsourcing and would streamline good contracting. Oversight methods are mentioned in a number of guidelines but implementation of good oversight practices is not thoroughly taught.
3. There are some resources to multi-tier management and contracting buried in documents such as FAA orders that are generally meant for the FAA AIR.

6.2.1 Guide topic: Management of Outsourcing

Table 6 lists the key enablers to address weaknesses noted during this study regarding industry comments and guideline content in the preparation for outsourcing a system design and development to multi-tier suppliers.

Table 6. Guide for Management of Outsourcing

Category	Description
Supplier Capability Assessment	Develop guidelines to assist a contractor in the assessment of potential supplier capabilities that press beyond contractor advertized capabilities and look at specific system application knowledge and experience. Leverage Order 8110.49 and 8110.105 for supplier capability assessments.
Outsourcing Spec and Requirements Rigor	Provide guidance to transitioning formerly internally developed systems or items to an external developer. Address the rigor necessary and internal skills that must be retained to transition to external design and development. Assist in identifying historical but unrecognized internal working relationships and assumptions that must be retained or replaced in a tiered relationship.
Cultural Difference Awareness	Provide awareness alerting the candidate contractor to ask the right questions and perform the right assessments that will illuminate potential cultural design process difference that can impact a development. Cultural differences affecting design approaches and norms are not just across national or language boundaries but across corporate boundaries as well.

Supplier Capability Assessment: All stakeholders of the fielded system development and its performance, from the prime down through the multi-tier contractor and to the multi-tier supplier, including the certification agencies desire an assurance at the onset that a multi-tier supplier is capable of developing the product to the proper design assurance levels. A potential supplier must exhibit:

- Functional application experience
- Airborne avionics design and development familiarity
- Functional safety assessment background
- Verification and integration experience

These go beyond the normal evaluations of:

- Quality control systems
- Software development processes
- Financial and progress reporting processes
- Etc.

All of these are necessary attributes of a potential multi-tier suppler. The guideline should outline all the necessary attributes and suggested means of assessing the potential supplier. FAA Order 8110.49 and 8110.105 are resources that can be used to launch the content of a guideline for industry.

Outsourcing Specification and Requirements Rigor: The purpose of this section is to make the contractor aware of the pitfalls with multi-tier outsourcing in regards to specification and requirements and to provide guidance for management of the outsourcing activities. Guidance to assist management of technical aspects of development in the following areas would be helpful:

- Awareness of the investment issues associated with transitioning formerly internally developed items to a supplier. Management must be aware that the systems role must be stepped up and maintained to achieve the rigor necessary to transmit requirements externally. Management must be aware of what levels of internal staffing will be required to be maintained throughout the development to manage requirements and specification accuracy and clarity.
- Recommended approaches and activities in anticipation of an outsourcing activity that will illuminate general and technical issues with multi-tier outsourcing as well as unique organizational issues that may arise. Alternative suggestions to counter the potential risks that may arise should be provided.
- Fewer and fewer management personnel have come up through the ranks today. As a result they are likely to overlook the technical aspects of outsourcing when under financial pressures. There does need to be an awareness of the potential risks and the rigor required in outsourcing design and development. Solid technical oversight must be maintained within the contracting organization.

These may seem like a management 101 course in business management, however, the avionics industry has specialized requirements and the complexities require a level of expertise be maintained at all tiers. There are avionics industry paradigms, risks, and practices that are not taught at business schools.

Cultural Differences Awareness: The approach taken by a designer to solve a problem, the method and level of documentation, and the verification approaches will differ between individuals even though they are educated at the same university. This is true even when they come from the same nationality and culture. When they are embedded in different corporations or work in different countries these differences can diverge even more. This issue is therefore not so much about nationality cultural differences but an awareness of characteristics that may emerge when working with anyone. The business and technical manager should be made aware of certain characteristics that may emerge and best ways to deal with those characteristics. For example:

- There may be a "worldview" that the contractor is the authority and should never be questioned. As a result the developer or supplier may not raise issues with requirements or designs that clearly have technical errors. The developer designs exactly what was specified without question.
- Another "worldview" is that everything should be questioned and that the supplier not only has the freedom to question but freedom to deviate without informing the contractor. The contractor is not likely to get what he asked for.
- There may be a reluctance to show work in progress because of the embarrassment associated with criticism of a work that is not yet complete. This supplier may not provide materials for interim reviews and could result in major error at the final integration.

Recognition of these potential characteristics at the contracting phase can be countered with oversight activities within the originating contract.

6.2.2 Guide topic: Multi-tier Supplier Contracting

Table 7 list aids useful to the establishment of a multi-tier supplier contract.

Table 7. Multi-tier Supplier Contracting

Multi-tier Supplier Contracting	
Category	**Description**
Contracting Model Plan	Outline the basic elements of a good contracting approach in the form of a contract model. Address all the content of the recommended Guide for Multi-tier Contracting.
Responsibility Boundaries and RAA Def	Provide guidance addressing contractual methods of defining and contracting design boundaries for appropriate Responsibility, Accountability, and Authority
PSAC, PHAC, PSyAC Flow-down	Provide guidance for the contractor in providing clarity to the tiered developer on what is "prescriptive" in nature from the guidelines that the FAA will expect to review and approve. There should be guidance on the use of prescriptive documents and relationships to the guidelines that request them and define them i.e. PSAC in DO-178C, PHAC in DO-254, "PSyAC" in ARP4754A" [PSCP or SPP].

Contracting Plan Model: The contracting model plan is a template containing the key elements for the establishment of a contract that puts in place the agreements between the contractor and supplier prior to execution. The model plan focuses on the aspects of issues to be agreed upon that impact multi-tier development activities beginning with the lists contained in Table 7 and Table 8.

Responsibility Boundaries and RAA Definitions: Clear definitions and understanding of Responsibility, Accountability, and Authority (RAA) insure there are no conflicts or gaps. There is a need to reestablish the concepts of RAA and so it is recommended that the Multi-tier Guide for Supplier Management address this topic. For the guide it will be a list of issues to be defined in each of the three categories of RAA.

PSAC, PHAC, "PSyAC" Flow-down: It is the responsibility of the contractor to flow down the correct content of the PSAC, PHAC, and PSyAC (recommended guideline) to the multi-tier supplier and to insure the necessary content is flowed down to any further tiers of suppliers. Best practices in the content of these prescriptive documents and assurance of the information flow is a useful guide to the contractor of multi-tier suppliers.

6.2.3 Guide topic: Multi-tier Oversight

Table 8 lists three key management guidance elements for effective oversight of multi-tier developers.

Table 8. Multi-tier Oversight

Multi-tier Oversight	
Category	**Description**
Oversight Agreements	Provide guidelines for contractual agreements that address proper levels of oversight and insight into the design during the development. Pre-contract agreements that all parties agree to. Leverage Order 8110.105 in the determination not only of how much oversight is needed but what kind of oversight should be considered. Include oversight team composition, communication, data sharing, and reviews and audit agreements.
Oversight Visibility	Support for contractor visibility accessibility throughout all tiers of the supply chain and visibility into cross-peer developers. Must address intellectual property protection and balance between control and delegation.
Focus on Systems Technical Oversight	Create a mindset towards systems technical management and oversight through a top down guidance of systems engineering oversight of technical developments. Begin with transference of the application operational understanding. Set a standard for technical oversight as a participatory partnership between contractor and supplier. This is an oversight discipline that is more than just critical point reviews. It encourages collaborative design.

Oversight Agreements: There are too many examples of failures that have resulted in the contractor having to place personnel at the supplier sight to resolve performance issues and provide design direction. Why not approach oversight from a preventive perspective rather than a corrective action perspective? There should be an encouragement towards continual participatory oversight as opposed to a periodic metric/questionnaire type of oversight.

What level of oversight, where, and how it is to be conducted should be agreed to at the time of contract initiation. Along with the PHAC, PSAC, and "PSyAC" the contract should lay out the agreements. Both contract performance and technical design oversight must be performed. Guidelines such as DO-178C list areas where oversight is to be applied but do not define how they are to be conducted other than periodic design reviews. Resources such as FAA Order 8110.105 can be used to provide additional insight that can be combined into a guideline for industry oversight.

Oversight Visibility: There is value in top-down oversight visibility through all tiers from the prime contractor down to the lowest level multi-tier supplier. Course corrections may need to be applied at any level because of the loss of application objectives as the requirements are translated between layers. Requirements specifications are not perfect. The contract flow down should outline what and how this oversight will be accomplished. Conversely trusted supplier and acknowledged expertise at the lower tier may suggest oversight be provided from the lower tier to the higher tier and the prime contractor. Intellectual property protection mechanisms and trust are key enablers toward establishment of what should be a partnership in oversight. There is precedence for open partnerships recommended for guidance. Documents such as Partnerships for Safety Plans between industry and the FAA reflect successful trusted partnerships.

Focus on Systems Technical Oversight: The purpose of this guidance is to counteract the natural tendency to perform oversight from a contractual performance perspective and technical touch points. The tendency is towards reducing oversight as the design progresses because the performance metrics are acceptable. Unfortunately it is also a tendency to not report issues or the truth from a protective instinct. The developer would much rather solve his own problems than share his "failings" with the contractor.

Contractual performance oversight is good. However, system development oversight is critical. The RTCA guidelines recommend supplier oversight be captured in the PSAC pointing to the planning documents as the location for oversight processes but go no further. Coupled with recommended design reviews one might assume technical oversight is covered. However, the reviews are targeted at verification of work already accomplished.

6.3 Recommendation #2 – Guide to the Guidelines

Recommendation 2: Publish a hierarchical guide to the guidelines document showing interrelationships and dependencies between Advisory Circulars, FAA Orders, ARP guidelines, RTCA guidelines and key industry guidelines. During this process close the missing cross reference holes found in the various guidelines. Consideration should be given to an electronic guideline system.

Note: In an attempt to provide examples that would assist the multi-tier developer, we generated some sample hierarchical diagrams included below. These are just samples, and are not complete.

At present there is no overall top down organization of the guidelines, ACs, and Orders documents that would provide an overview of the "safety system". Related or relevant documents can only be found by searching the references within the guidelines, orders, and advisory circulars. For example: It may take some time for a developer to stumble onto the CPI Guide, which contains valuable guidance and models for the creation of a PSP and PSCP. AC23.1309-1E calls out Order 8110. Order 8110.4C Change 5 calls out the CPI guide a number of times. However neither AC25.1309-1A nor AC23.1329-1B reference Order 8110.4C. None of the ARP documents or RTCA documents reference Order 8110.4C. So, unless the developer begins with AC23.1309-1E or stumbles onto 8110.4C he is likely to be unaware of the FAA and Industry Guide to Product Certification.

Around half of the references made are just that, references. The other half provide some meat as to why the reference is made and what the reference provides. At least they point to other sources of guidance. There are some notable reference absences:

- DO-326 not being mentioned by the ARP documents.
- The age of AC 25.1309 is showing by missing references that are found in AC 23.1309.

We could not find any existing hierarchical guideline reference documents that would guide a multi-tier supplier in understanding the safety processes. Experienced DER and Safety Specialists felt these kinds of graphics would be useful aids to them and experienced developers.

When there is difficulty in extracting requirements or guidelines, it heightens the risk that all guideline requirements will not be followed. Therefore, we have identified the deficiency in the clarity of guideline interrelationships as a critical enhancement to enable multi-tier developer understanding of regulatory guidance. Figure 12 below illustrates what might appear to the tiered developer as a forest of documentation he must wade through, assuming he found these. Figure 12, however, is much more organized than the tiered developer will find. It already reflects a pass through documents extracting relevant referenced documents from within them.

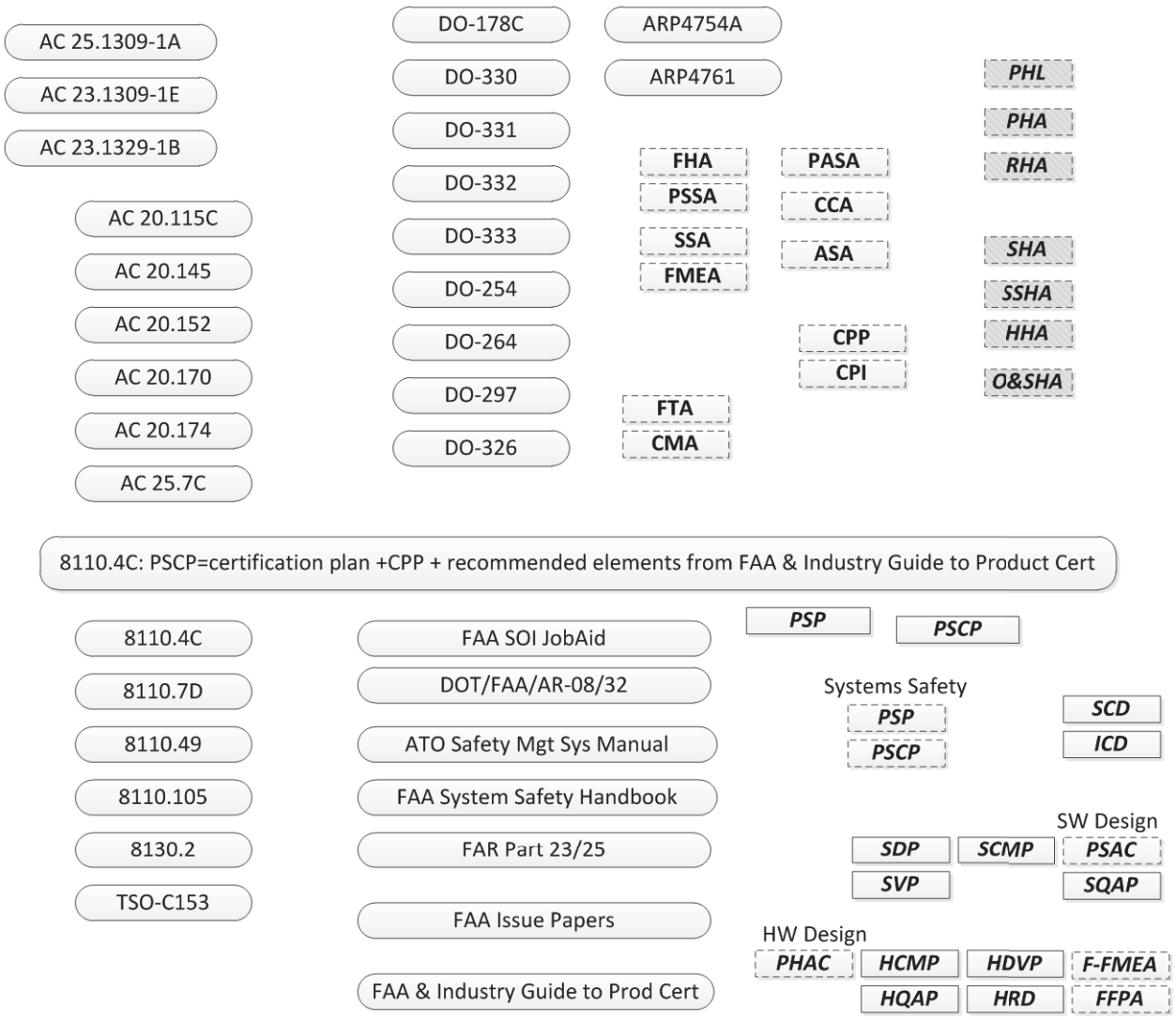


Figure 12. Document Forest

The most useful existing guideline interaction diagram is “Figure 1- Guideline Documents Covering Development and In-Service/Operational Phases” found in ARP4754A, shown below in Figure 13.

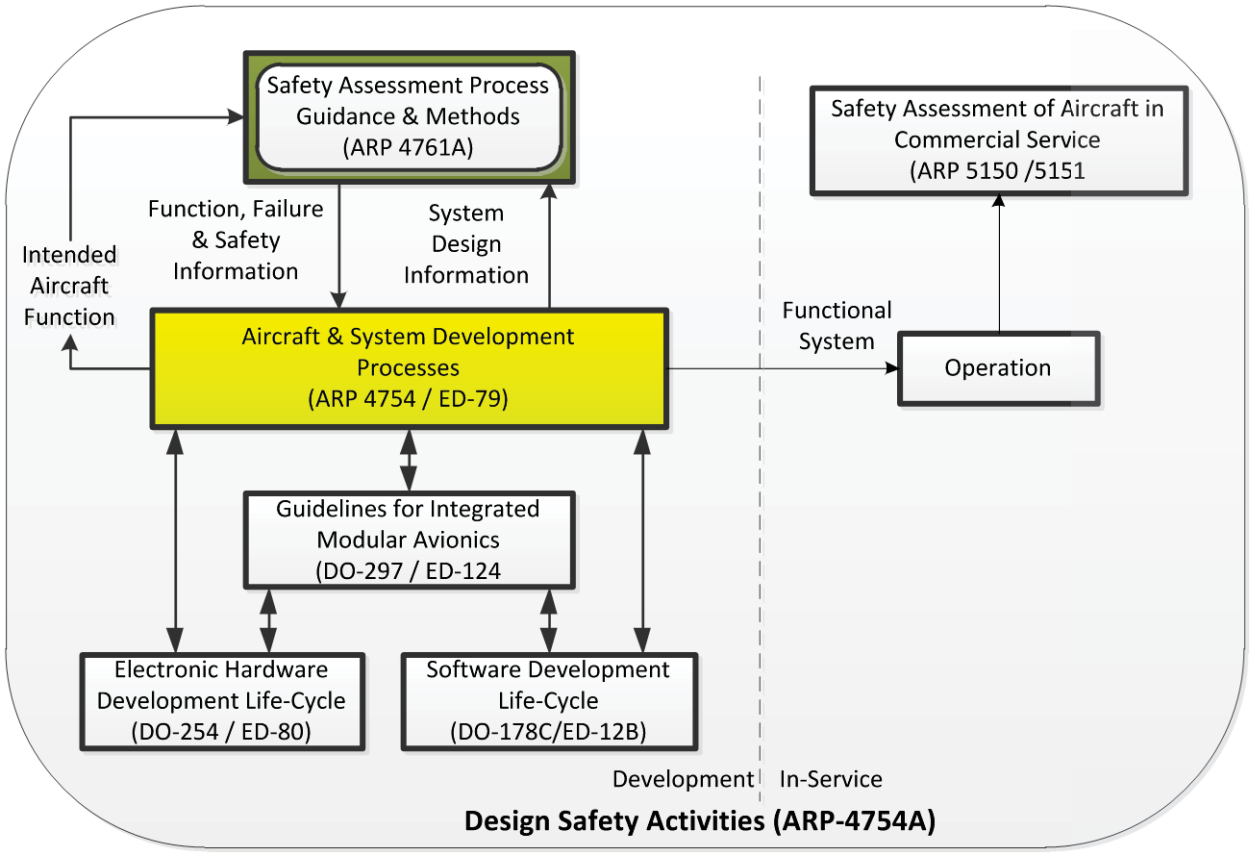


Figure 13. ARP 4754A Document Interrelationship

Figure 13 is however limited to the interactions between ARP-4754A and ARP-4761A, DO-254, DO-178C, and DO-297.

There are many more relationships to ARP-4754A as illustrated in Figure 14 below. Those in boldface include a reference to ARP-4754.

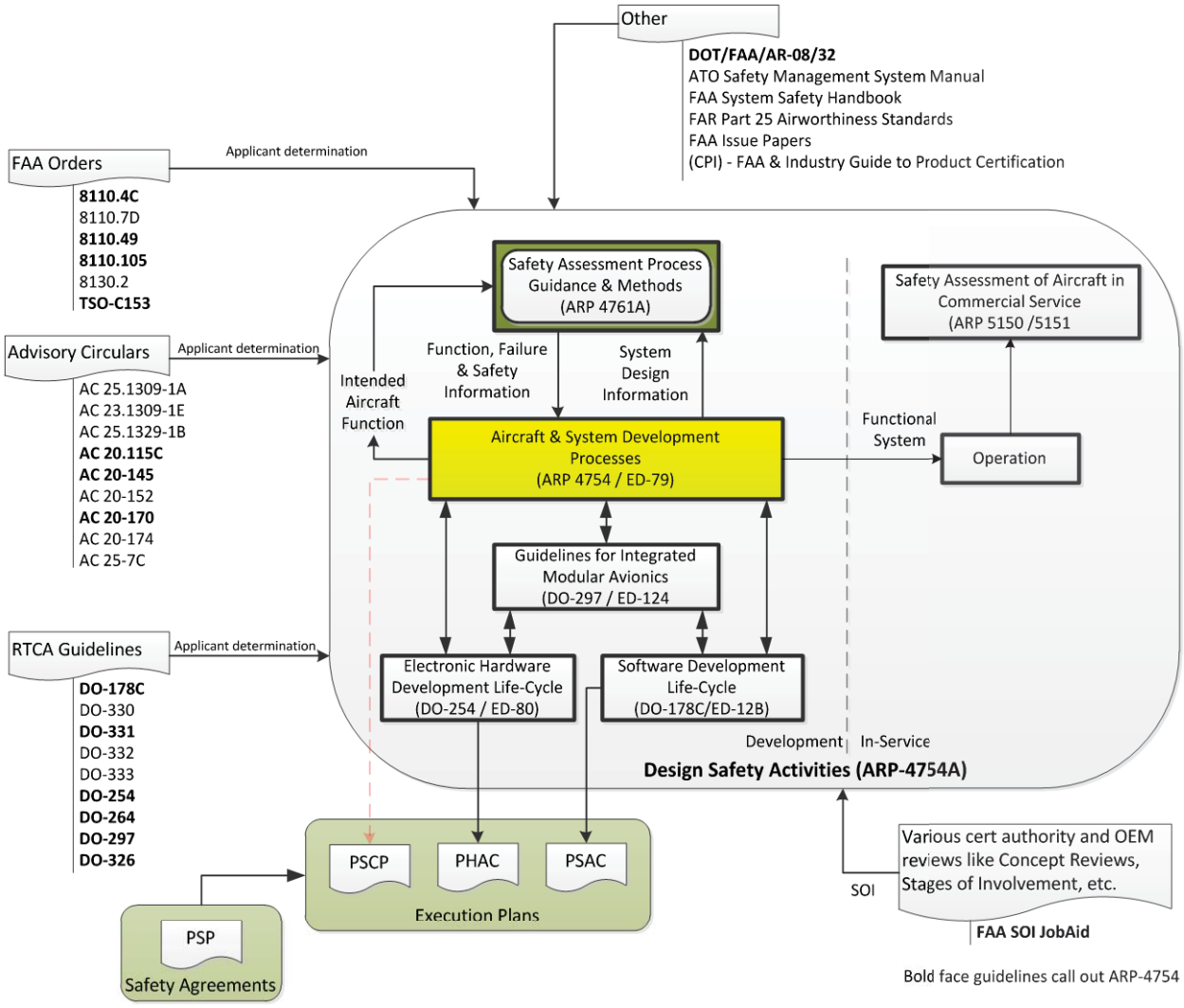


Figure 14. ARP4754A figure augmented with other documents

Figure 14 still does not capture the relationships between all the guidelines.

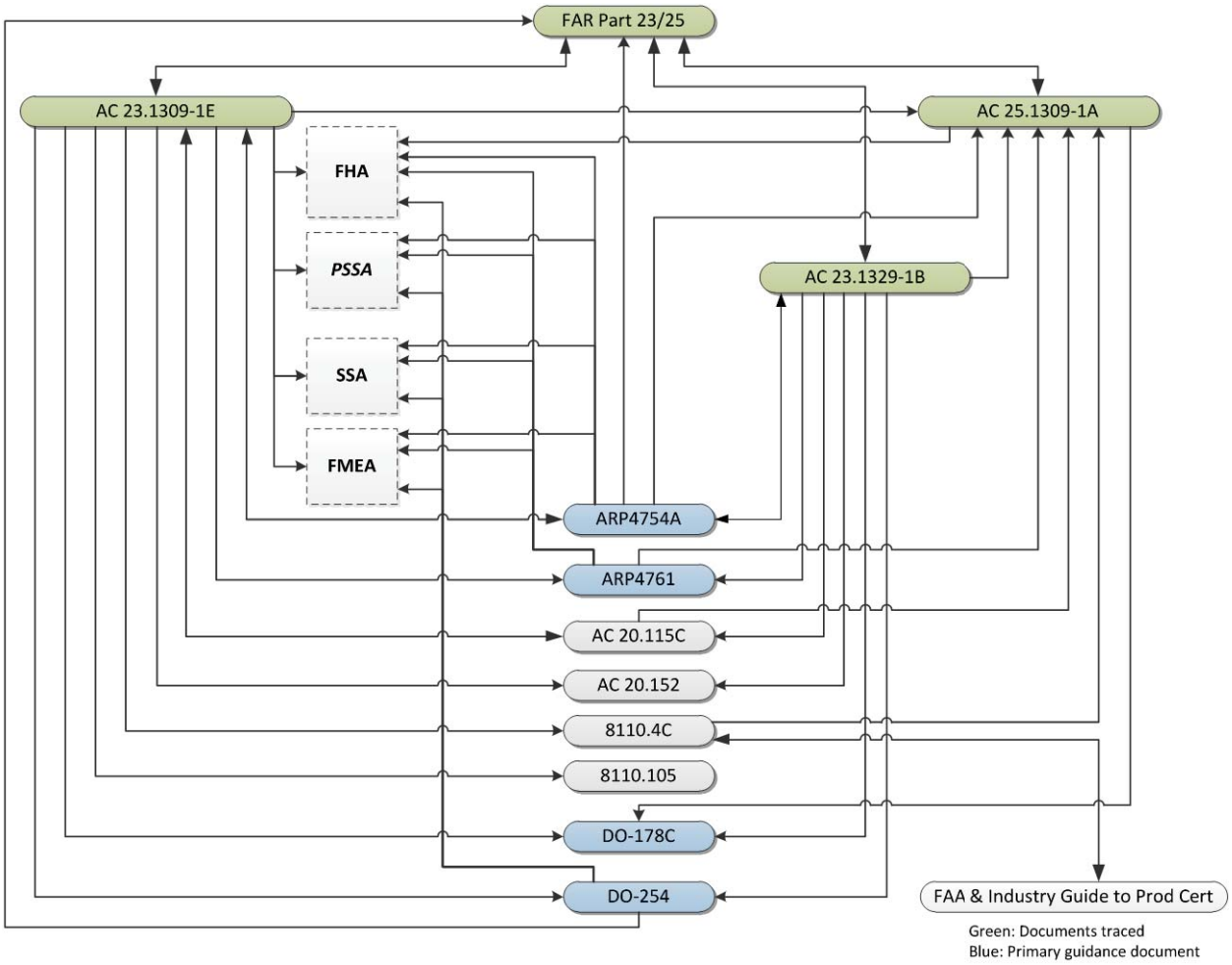


Figure 15. FAR and Top Level AC Guideline Cross-references

Figure 15 provides an assessment of FAR Part 23/25, AC 23.1309-1E, AC 23.1329-1B, and AC 25.1309-1A references to guidelines and the call back or reference of those guidelines to these regulations. Also included are analysis products that were listed in these ACs and the call back from the guidelines to these same analysis products. Interrelationships between the called out guidelines are not reflected on this diagram. It must be noted that there are many more ACs and guidelines not covered by this study, which is focused on electronic avionics development in a multi-tier environment.

Though not completely clear from this kind of diagram, the ARP documents begin to emerge as primary guidance materials.

Context Interrelationship Diagram Observations:

- Both AC 23.1309-1E and AC 23.1329-1B call out AC 25.1309-1A but the converse is not true.
- AC 23.1309-1E calls out four products: FHA, PSSA, SSA, and FMEA. AC 25.1309-1A only calls out the FHA. AC 23.1329-1B does not reference any analysis products.
- AC 23.1309-1E and AC 23.1329-1B both call out ARP4754A and ARP4761. AC 25.1309-1A does not call out either of the ARP documents.

- ARP4754A calls out all three of the AC documents as well as referencing the FAR. ARP4761 only calls out AC 25.1309-1A. (There is current activity to update 4761 to 4761A, so perhaps 4761A will reference 4754A.)
- AC 20.115C calls out both AC 23.1309-1E and AC 25.1309-1A. Itself is called out by the both the AC 23.xx documents but not the AC 25.1309-1A.
- DO-254 calls out all four analysis products: FHA, PSSA, SSA, and FMEA. DO-178C does not.
- Even though these cross references are made in these documents, the reason, purpose, or content of the reference (the flow of information) is generally missing except in the cases of the ARP documents.

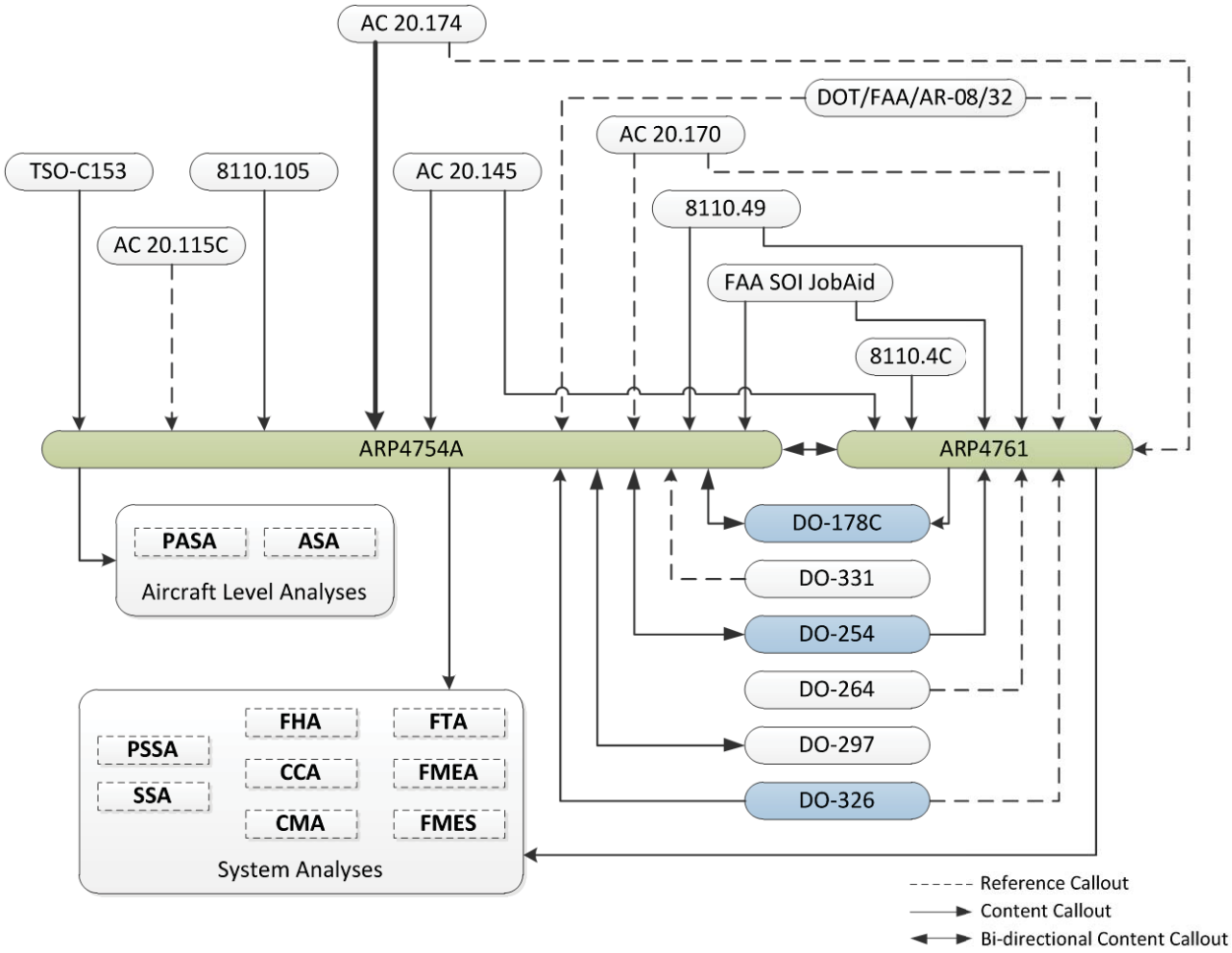


Figure 16. ARP 4754 ARP4762 Guideline Cross References

Figure 16 breaks out the cross references from ARP-4754A and ARP-4761 to the advisory circulars, orders, and RTCA documents. Also included in the diagram are artifacts described in ARP-4754A and ARP-4761 that should be generated.

ARP Guideline Cross Reference Observations:

- AC 20-174 recognizes the ARP documents as an acceptable method for establishing a development assurance process.

- Half of the advisory circulars call out the ARP documents by name only with no specific purpose or content.
- The ARP documents are consistent in their call out of artifacts.

Figure 17 below provides a hierarchical reference graphic of DO-178C, DO-254, and DO-326 from the advisory circulars, orders, ARP, and primary RTCA documents. Artifacts identified by the individual RTCA documents are included with a flow to what document gave them reference.

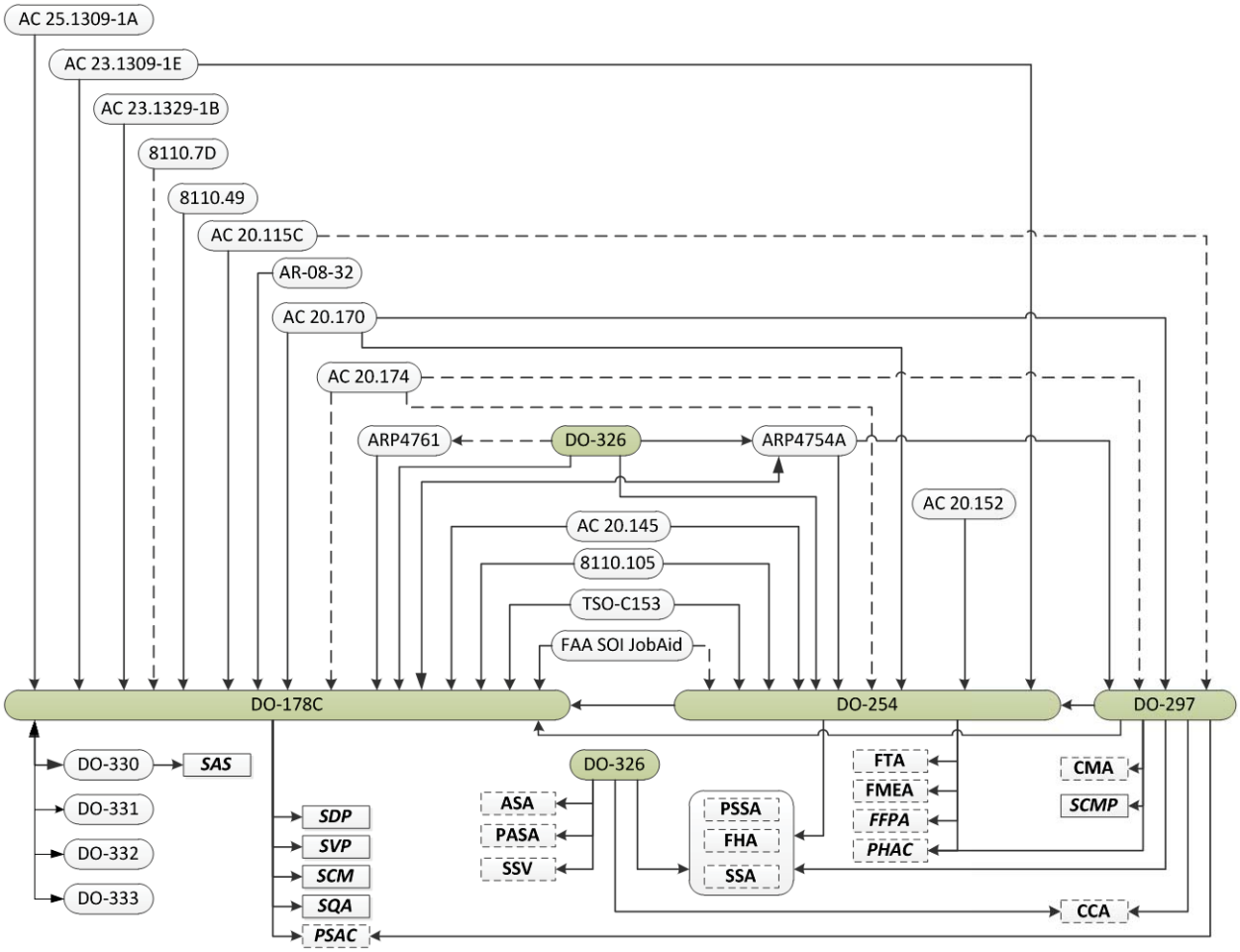


Figure 17. RTCA Guideline Hierarchy

RTCA Guideline Hierarchy Observations:

- Some references are to specific revision numbers. Later documents are generic: XXX-()
- AC 25.1309-1A stands out as missing references here as well
- DO-326 appears the most complete in its referencing
- Some slight differences exist in artifact titles ex: SCM/SCMP

6.4 Recommendation #3 – DO-178C/DO-254 Outline Restructure

Recommendation 3: Since the PSAC and PHAC are the operational product to which the FAA and developer will agree and execute the development, then DO-178C and DO-254 should be organized in accordance with the outlines of the PSAC and PHAC.

All relevant explanatory material should be captured under that outline. At the same time this restructure is performed, each tutorial and explanatory statement should be evaluated for keeping it simple but sufficient to reduce unnecessary content the simplest level. The hope is that this restructuring would enable clarity to new multi-tier developers.

Einstein said, "Everything should be made as simple as possible but not one bit simpler". This perspective goes for the regulatory guidelines as well as the description of the system being designed. If you can't explain it simply, then how can you expect the developer to execute the desired process or design the desired system? Anything that obscures the desired outcome is not part of the solution.

The structures of DO-178C and DO-254 contain obscurants, at least in the way they are assembled. If it is true as stated in DO-178C that "the PSAC is the primary means used by the certification authority for determining whether an applicant is proposing a software life cycle that is commensurate with the rigor required for the level of software being developed" then paragraph 11.1 of DO-178C should be the upfront master plan for the structure of the DO-178C document. The rest of the document then is subservient to the outline of the PSAC within Para 11.1. Then only that which serves to guide execution of Para 11.1 should be retained.

Likewise in DO-254 the PHAC "defines the processes, procedures, methods, and standards to be used to achieve the objectives of this document and obtain certification authority approval for certification of the system containing hardware items." Para 10.1.1 should be the upfront master plan and the rest of the document be subservient and explanatory to the outline of the PHAC in Para 10.1.1. Only that which serves to complete or explain the content of Para 10.1.1 should be retained.

Figure 18 and Figure 19 below provide quick assessments of what this would mean for each of DO-178C and DO-254. The figures reflect that the major paragraphs remap quickly. However, we made no effort yet to reduce the content to an appropriate level within this outline for the PSAC and PHAC. These are for concept evaluation only at this time.

This is also an opportunity to update the major guidelines to resolve discrepancies in responsibilities and boundaries, particularly differences between the FAA System Safety Handbook and ARP4754A. Some documents like 25.1309-1A have not been updated recently.

Sometime in the future, the guidelines should be restructured for website electronic access with hyperlink between references driven by topic much like the recommended DO-178C/254 restructuring. Access to the site could be through subscription as much of the material is currently sold.

Figure 18. Suggested DO-178(x) and PSAC Outline Structure

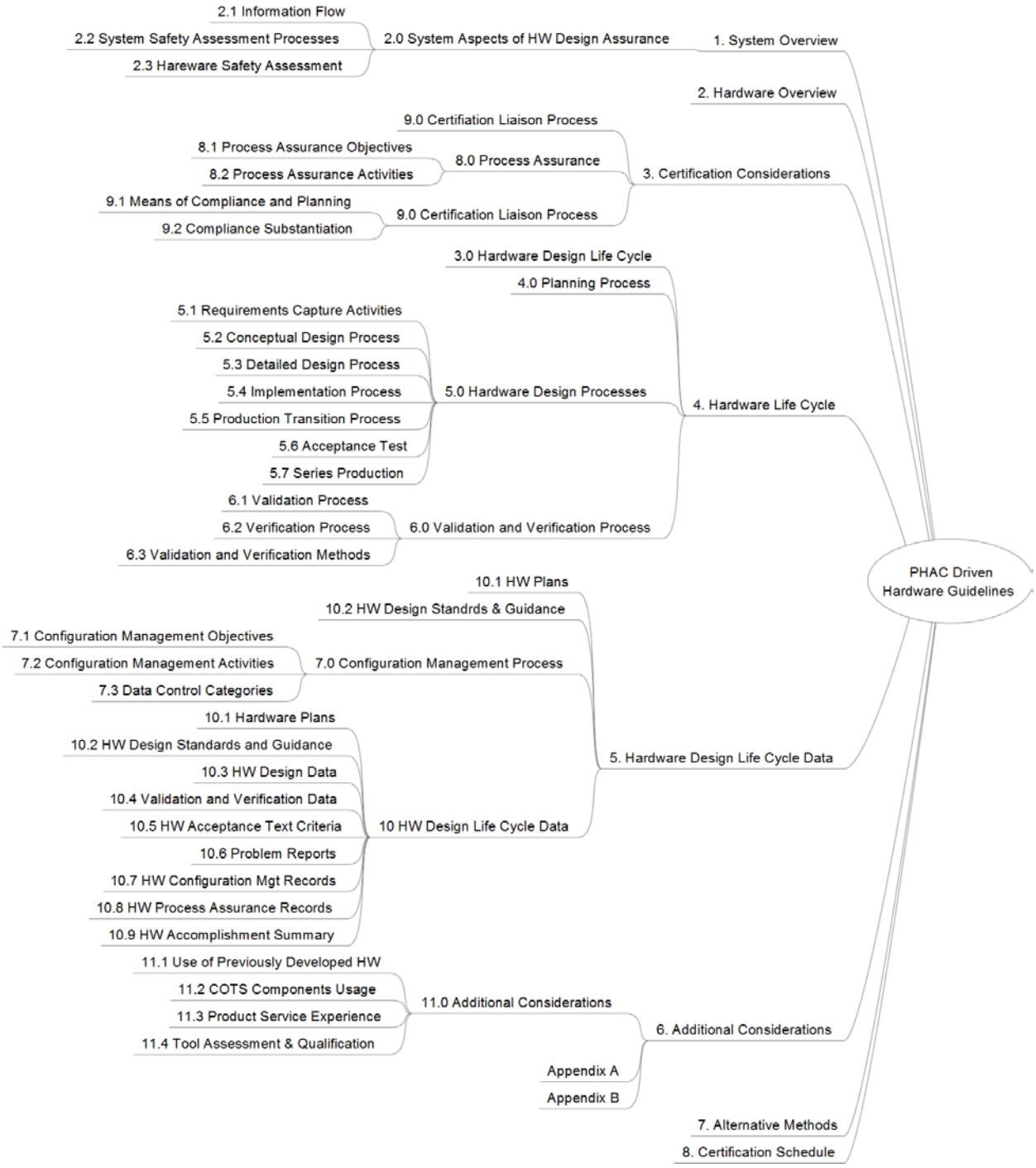


Figure 19. Suggested DO-254 and PHAC Outline Structure

6.5 Recommendation #4 – Plan for Systems Aspect of Certification (PSyAC)

Recommendation 4: We recommend systems be put on an equal footing with software and hardware through: 1) the development of an equivalent PSyAC; and 2) clarify the boundaries of authority between ARP4754A, DO-178, and DO-254.

> ***Tom Simonite (Microsoft)****: People seem to equate programming with coding, and that's a problem. Before you code, you should understand what you're doing. If you don't write down what you're doing, you don't know whether you understand it, and you probably don't if the first thing you write down is code. If you're trying to build a bridge or house without a blueprint—what we call a specification—it's not going to be very pretty or reliable. That's how most code is written. Every time you've cursed your computer, you're cursing someone who wrote a program without thinking about it in advance.*
>
> *There's something about the culture of software that has impeded the use of specification. We have a wonderful way of describing things precisely that's been developed over the last couple of millennia, called mathematics. I think that's what we should be using as a way of thinking about what we build.*

We would add that the aircraft industry has done the same – the culture of software has impeded the use of systems specifications and methods in avionics.

Tom's statement above alludes to a lack of understanding of the system application or function and to jumping to implementation before the system design is complete. Much of the avionics industry would say "we don't do that". However, some old-timers would vigorously disagree, pointing out the degrading of system value that has slowly but progressively taken place since software implementation of systems functions entered the avionics arena.

The more complex systems become, the greater is the need for a strong systems engineering design approach to implement the proper design for the application. Although ARP4754A has been officially recognized (AC 120.74 dated 9/30/2011), years have passed during which this lack of recognition has degraded the value of systems engineering in the industry. In some organizations, systems engineering has become a task of requirements decomposition and requirements tracing. Some contractors even relegate verification to suppliers or low level software and hardware implementer. The result is a loss of application expertise, loss of system guidance, and the exclusion of system level verification and validation activities which are critical for complex systems.

ARP-4754A provides guidance towards a System Safety Program Plan (SPP) for system development. The FAA and Industry Guide to Product Certification provides guidance towards a Project Specific Certification Plan (PSCP) for system development. Either one of these could be assumed by industry as providing the systems equivalent to the PSAC and PHAC. However, the ARP-4754A SPP differs significantly in content with the PSCP described in the FAA and Industry Guide, see Figure 20 below.

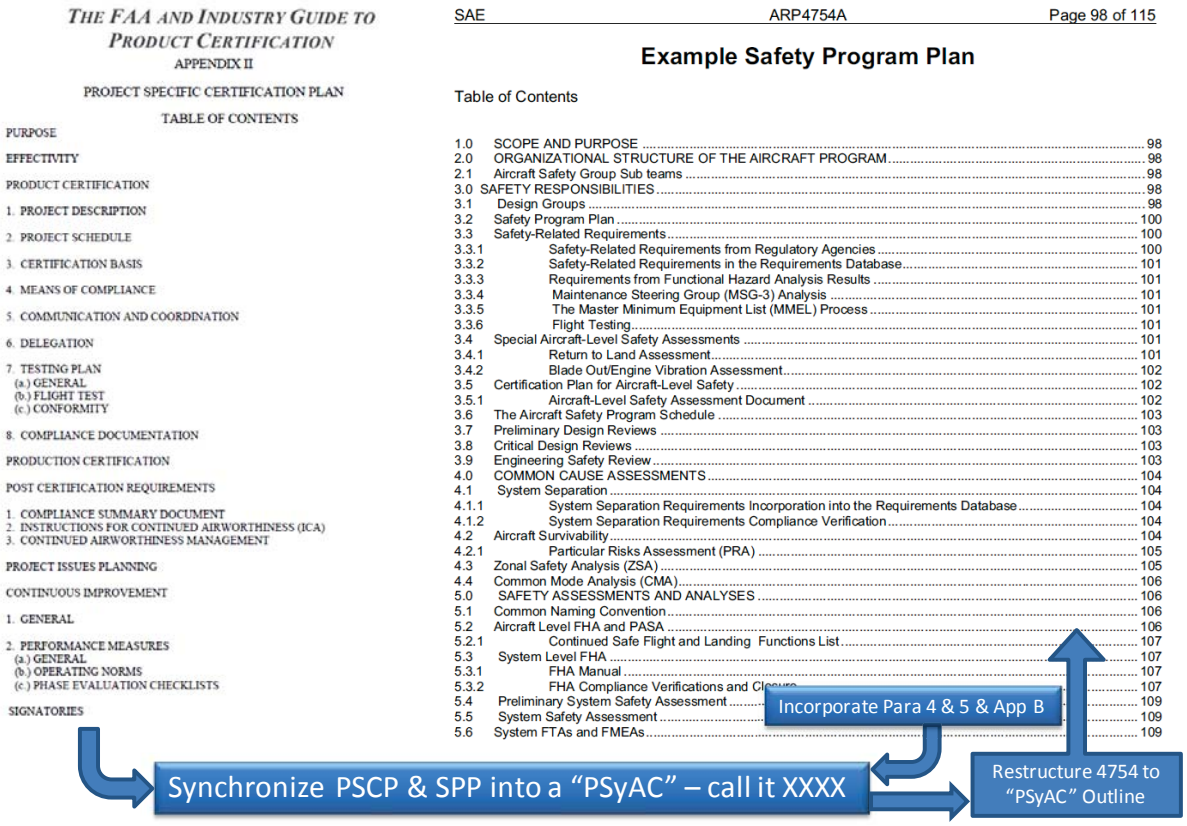


Figure 20. Proposed PSyAC Construction Resources

The PSyAC ties to ARP4754A as a PSAC ties to DO-178(x). The rationale for a PSyAC is:

- The discrepancies between the FAA and Industry Guide to Product Certification (PSCP) and the ARP4754A System Safety Program Plan (SPP) need to be resolved. See Figure 20 for a comparison of the two differing outlines.
- It gives a single document where prescriptive agreements for the system and plans for system certification are recognized. The systems plan is more critical than the PHAC and PSAC for highly complex systems.
- The use of multi-tier suppliers requires solid systems practices and application guidance throughout the tiers.
- Increasingly complex systems need disciplined focus on the objectives, continual architectural guidance, continual collaborative safety design, and requirements and resulting design clarity.
- It is systems responsibility to provide oversight into both software and hardware designs.
- It is systems responsibility to integrate the various avionics components and to validate their compliance with safety regulations and compliance to application requirements.
- Systems is the primary certification agency liaison and provides the system safety analyses and assessments.
- Systems is responsible for the entire life-cycle of the system. Hardware and software responsibilities are generally focused on the implementation phase of the V-diagram.

6.6 Recommendation #5 – Systems Model-Based Design (MBD) Guideline

We see MBD as a practical means to share systems knowledge across tiers. It can capture functions and component relationships in clear graphical formats. This is very useful for complex systems being developed across tiers. The important caveat is that models be used properly and in the right scope – they can be mis-used the same as text requirements. The current regulatory guidelines for MBD do not look at it as a systems tool, but more for software.

MBD holds opportunities to address clarity in understanding, clean requirements flow-down, boundary interface rigor, handling system complexities, all the while providing motivation to the developer through cost control.

Consequently, we recommend a guideline describing MBD for passing system knowledge across tiers.

Recommendation 5: Development of a Systems Model-Based Design Guideline addressing:

- **Translation layer management.**
- **System life-cycle MBD.**
- **Simulation and modeling standards.**

6.6.1 MBD Guideline Topic – Translation Layer Management

Every translation of a concept, a definition, or a requirement to another person or organization is a point where information may not be properly transferred. The probability of error insertion is the greatest at translation and interpretation, not during implementation. This responsibility of correctness in translation and interpretation assurance again falls on the shoulders of good systems practices. Unfortunately the trend towards outsourcing and multi-tier developments increases the number of translation points and variability in interpretation styles, methods, and languages. Figure 21 below illustrates the addition of translation layers in a single tier development scenario.

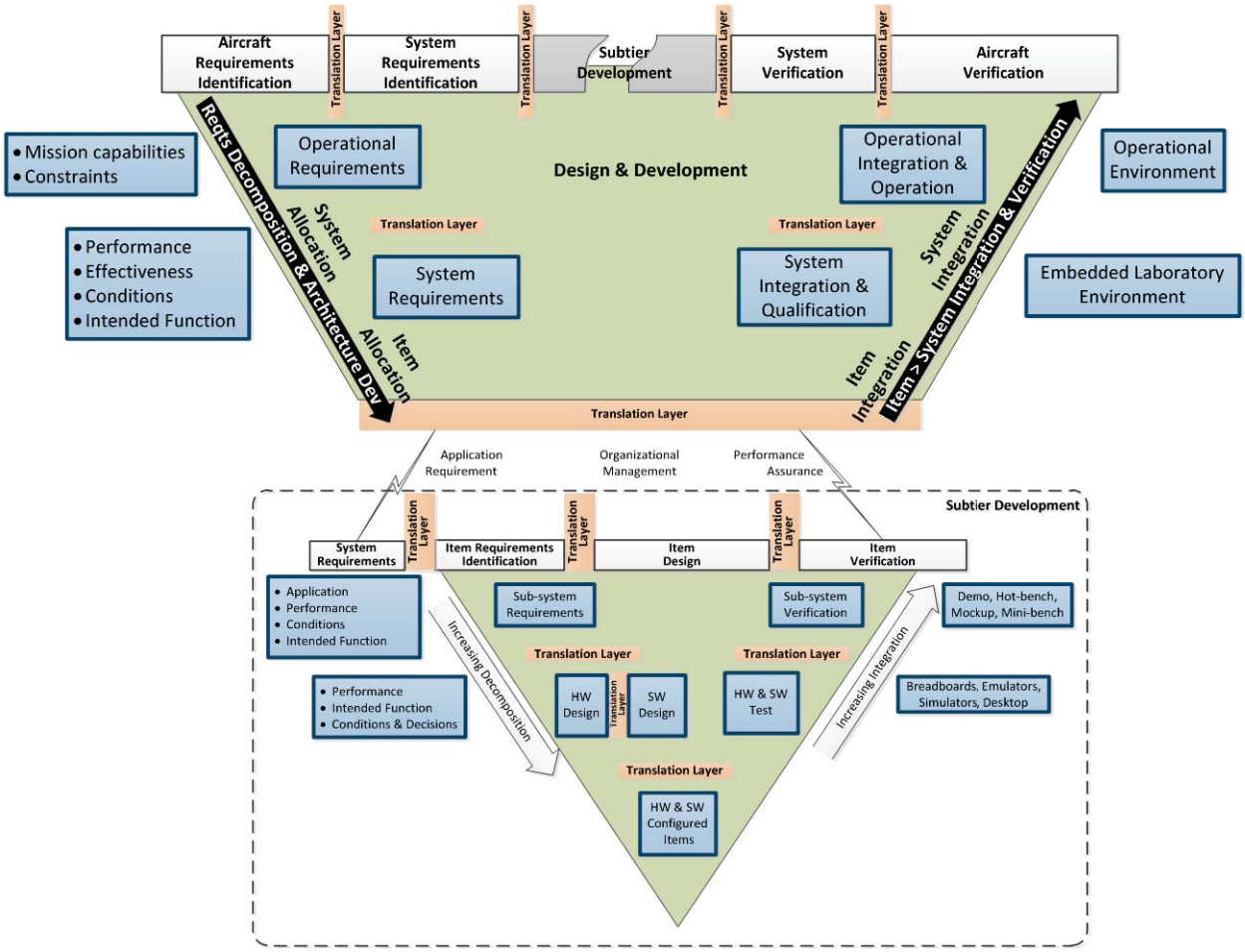


Figure 21. V-Diagram Translational Layers

The guidelines recognize the need for accurate requirements and address these issues primarily through rigorous requirements traceability methods. However, requirements traceability and the guidelines do not address if the requirement is interpreted correctly by a supplier or if the supplier's component fits the application purpose.

Accuracy, completeness, and singleness of interpretation of all the requirements is critical to the sufficiency of application objectives and safety assurance objectives. Therefore, every effort should be made to eliminate translation points. If they cannot be eliminated, then the transfer "language" (textual, graphical, or model) must be carefully chosen and executed.

How, and with what mechanism, does a developer eliminate translation layers or reduce the impact of the translation layers he cannot eliminate?

It seems like the major solution is to get the human out of the translation process. Beginning in its infancy machine coding was replaced with assembly coding which was later replaced with coding in higher-order languages. As a picture is worth a thousand words and as models are usually represented as pictures, the next step must naturally be an acceptance of graphical compilers. Machine code validation gives way to statement validation, and statement validation gives way to model validation

during the design process. In all cases embedded testing remains as the final validation for delivery of the product.

It also appears that moving towards MBD as a mechanism for requirements development and communication is a way to both reduce the number of translation layers and the impact of any remaining translation layers. The impact towards reducing translation layers is illustrated in Figure 22. This figure assumes a graphical model that can be compiled to executable embedded code. The translation layers and associated analyses that were necessary to validate software requirements translation and design interpretation, 6, 7, and 8 are eliminated.

The flow-down to the multi-tier developer includes: higher level architecture models instructing the developer in application usage, performance and behavior specification models, high fidelity interface models describing interfaces between individual sub-systems, and may include low fidelity functional models to assist in the description of the functional requirements.

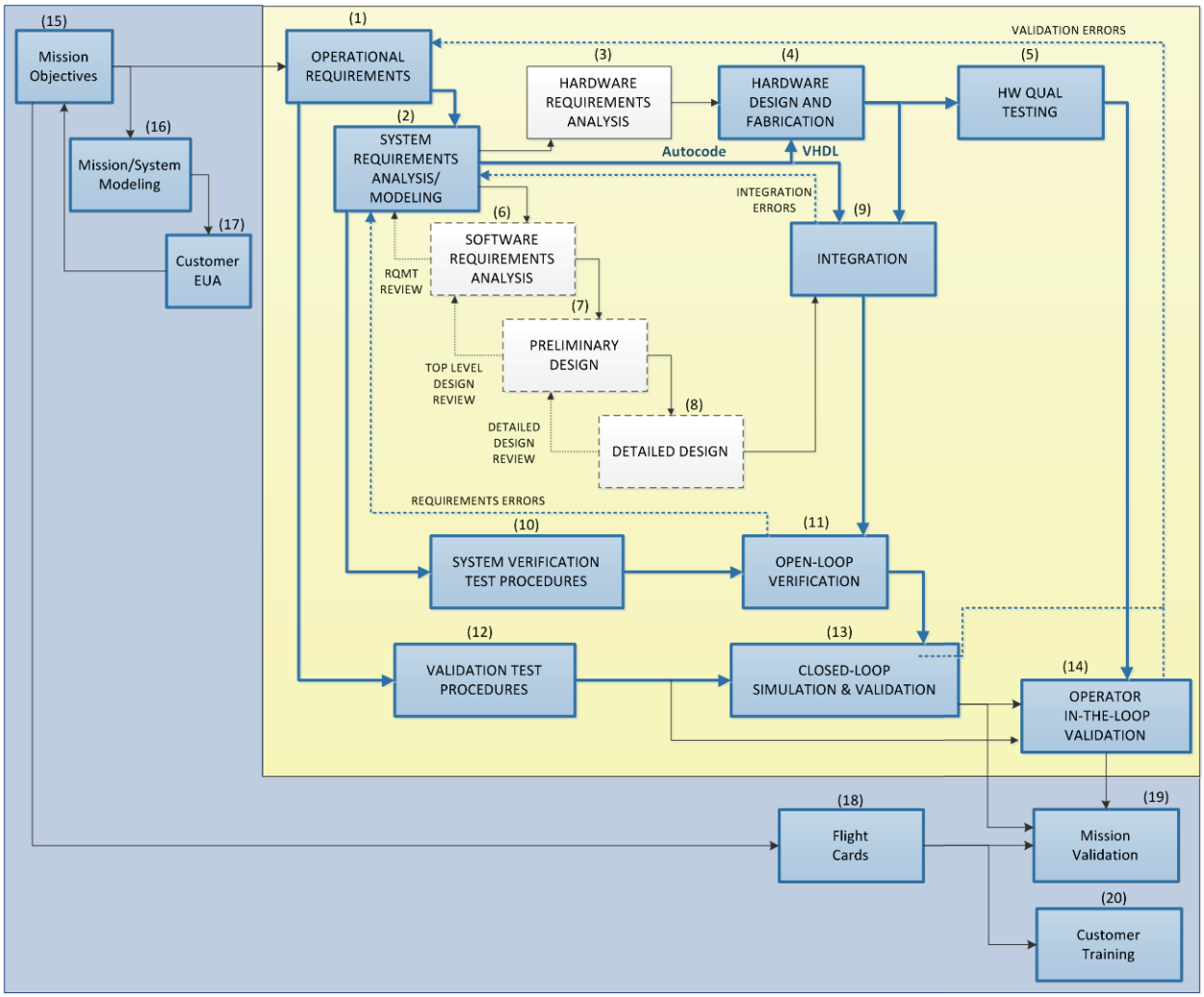


Figure 22. Development Waterfall

The capabilities exist today for this change from the typical waterfall process. This pushes the design modeling details to the system level and therefore increases the need for a system level MBD guideline. It must address the full life-cycle apart from DO-331 which was intended by the authors to address the implementation phase of software modeling.

Still missing from the guidelines, general practices, and tool capabilities is the capability to exercise application performance and validate behavior against the requirements. This would seem to fit the specification model paradigm described in DO-331. However, there is a gap in understanding exactly what the intent is and how to implement that intent. There must be a means to validate that the requirements accurately define the intended application performance and behavior. Individual requirements should be unique, resulting in one interpretation – not necessarily one implementation. However, a specified stimulus should result in a unique and deterministic response.

6.6.2 MBD Guideline Topic – System Life-cycle

There is a need for a Systems Guide to MBD that addresses the full life-cycle of a system development from concept to certification. MBD is much greater than the item development phase addressed by DO-331. MBD also should not impose artificial constraints on the process because of historical approaches. It must expand the ability to clearly describe the concepts and requirements while at the same time providing the means to validate the design at the current decomposition level. System, software, and hardware design boundaries will shift as a result.

Almost all of our industry interviewees recognized MBD as a valuable mechanism for improving development while at the same time reducing cost. MBD is considered by a large segment of industry as a game changer to avionics development. Yet, even though the 1st MBD certification of an avionics system occurred more than 15 years ago, there still remains an uncertainty and division on a broad application of MBD principles.

Weaknesses remain in:

- The definition of what MBD is
- Industry holding to a software view of MBD
- Poor understanding of which modeling methodologies support MBD objectives
- Interpretations detracting from MBD objectives
- Model sharing inadequacies
    - Weak or non-existent MBD modeling standards
    - Wide variation in modeling methodologies and toolsets
    - Variation in the design level application of MBD
    - Cross-tier management barriers
    - Guideline constraints
- Weak provision for performance and behavior modeling methodologies
- Weak usage of MBD in requirements flow-down

The guidelines should first clarify the definition of MBD. Our definition would be:

> *Model-Based Design (MBD) is a mathematical and visual method of addressing problems associated with designing complex control, signal processing and communication systems. Rather than relying on physical prototypes and textual specifications, model based design uses a system model as an analyzable specification throughout development. It supports system- and component-level design and simulation, automatic code generation, and continuous test and verification. In Model-Based Design, a system model is at the center of the development process, from requirements development, through design, implementation, and testing.*

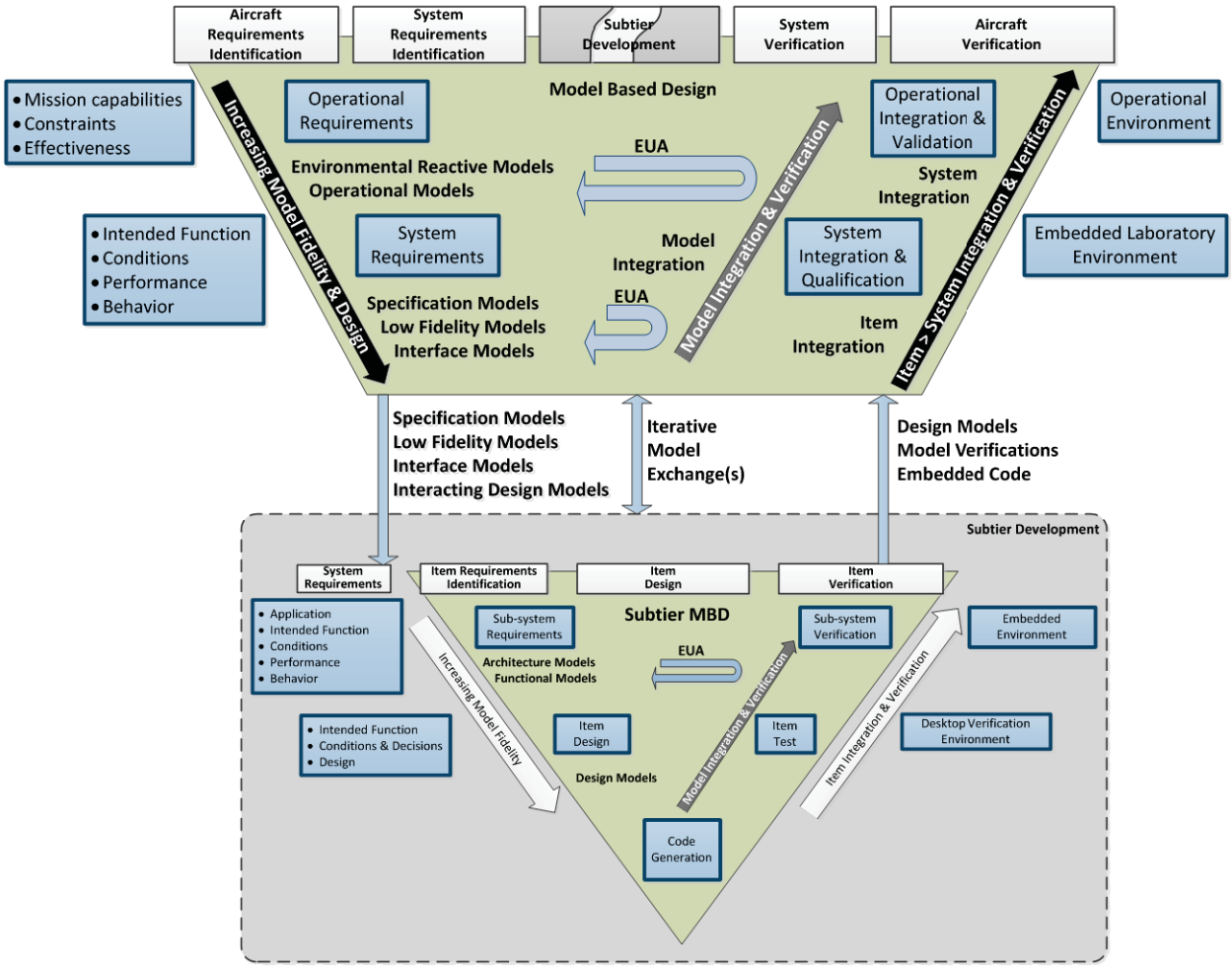


Figure 23. System Model Based Design

Figure 23 modifies the traditional V-Diagram to illustrate the MBD activities from a systems perspective over the full life-cycle of a program. It is also drawn to show interactions between a primary developer and one supplier tier. Hopefully, it will assist in showing why we believe approaching MBD from a software perspective is inadequate.

Modeling could and should begin with mission concepts and operation objectives that define constraints and objectives. This includes the establishment of environmental reactive models against which early models and final models are played for Early User Assessments (EUA) all along the design process. There are two paths shown on the integration up-slope: one serves the purpose of evaluating models as they are developed and refined and the second serves the purpose of accomplishing the final integration, verification and validation activities. This EUA process is one of the greatest benefits of MBD towards removing defective requirements and defective models early in the process.

Models may begin as specifications against which a design model is evaluated or as low fidelity design models which morph into the detailed design models. These are used to develop the system requirements in a graphical modeling format. Application usage, intended function, conditions, performance, and behavior are all captured at the system requirements modeling stage.

Before these models are passed on to the subsystem development and/or next tier level the interfaces between all interacting models are defined. The interface models must be at a higher TRL level than the intended functional model to be developed.

During development there must be a continual sharing and open model exchange between the specifier and the developer. This iterative process is another form of EUA that validates interpretations of: application intent, performance, and behavior.

The sub-system developer converts the low fidelity design model into a high fidelity model or develops a design model from the given specification models. The sub-system developer eventually generates embedded code from the models that flow up through the test models developed during the item design process. During this verification process test scripts run against the models in the EUA assessments form foundations for development of final verification test scripts run in an embedded environment.

An alternative view of this process is illustrated in Figure 24 below. The prime or contractor builds a modeling environment of the aircraft and desired functional items as Configuration Items. He may have multiple low fidelity CI-(x) items Specification Models in his environment or a mix of low fidelity Design Models, Specification Models, and full maturity Design Models.

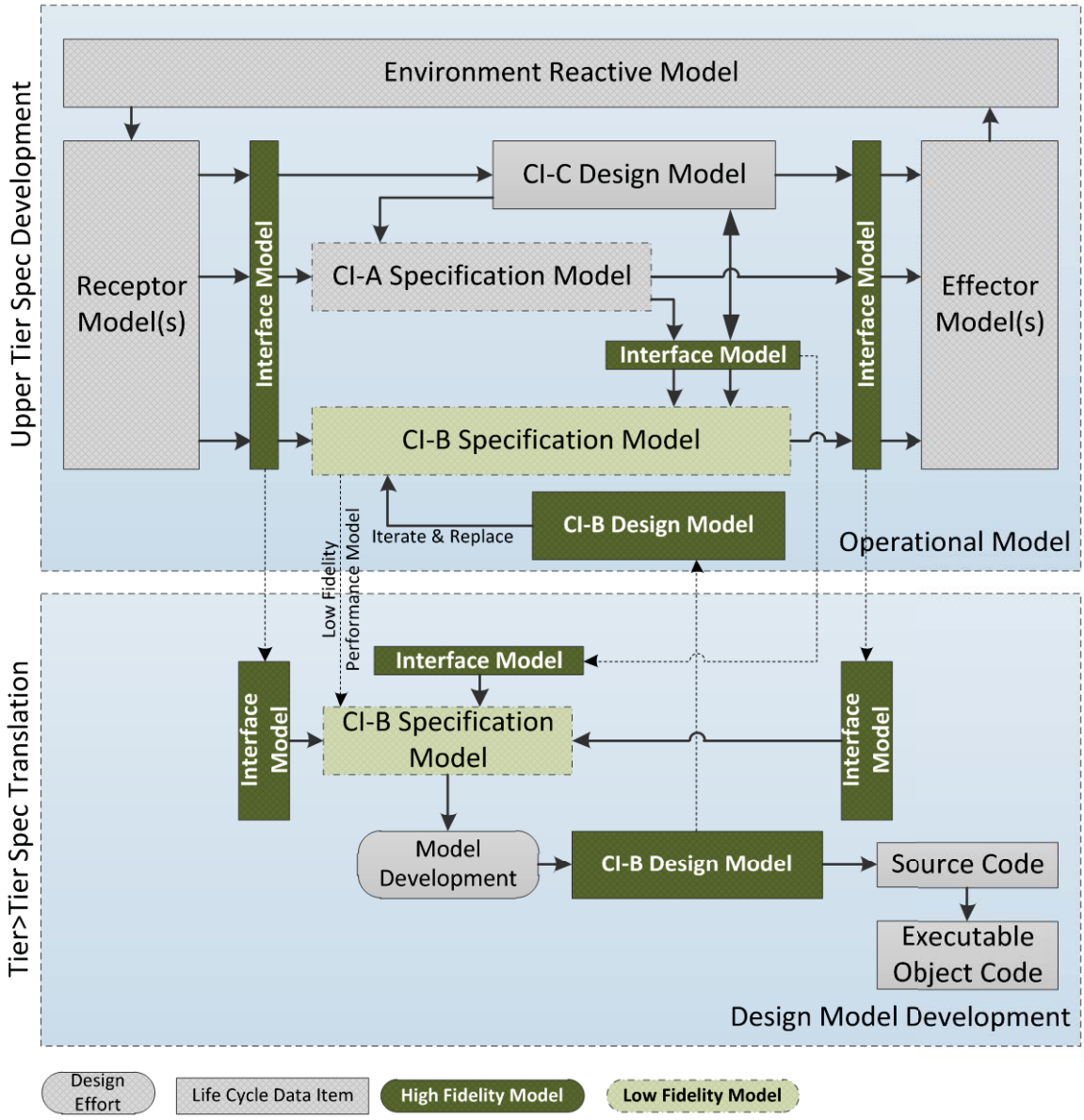


Figure 24. System MBD Process

A critical component the prime or contractor develops is the Interface Model. Most likely the interface model would be in the form of a high TRL maturity Design Model in order for the multiple developers to have clarity in interfaces.

The prime or contractor passes the high fidelity Interface Design Models and the low fidelity Specification/Design Model to the developer. When completed, or in an iterative fashion, the developer passes the developing Design Model of CI-B back to the Prime for integration and validation. The low fidelity Specification/Design Model is focused on functional performance requirements of CI-B avoiding detailed design and CI-B internal architectures.

6.6.3 MBD Guideline Topic – Simulation and Modeling Standards

Modeling standards are needed that enable cross-tier model sharing, early user assessment of the design as it progresses, application understanding propagation through the tiers, verification and validation development during the design process, and verification and validation during the integration process

To insure cross-tier and cross-peer modeling consistency, there must be modeling standards established that support model sharing. Simulations must be sufficient at each tier level to capture the application operational intent, performance, and behaviors in order that EUA's can be performed at each design spiral. These same simulations and models must support the development of test scripts that can be translated into embedded testing for final verification and validation.

This is a large topic that we did not have the time or scope to delve into for this study.

It may be useful to establish a "Systems Engineering Capability Maturity Model Integration" (SE-CMMI) measure of MBD capability for candidate supplier selection purposes.

APPENDIX A

Regulatory Guideline Assessment

Objective: Assess regulatory guidelines and industry practices for management and control of safety aspects of complex avionics design in a multitier supplier network.

Contents

Table of Figures

1 Purpose

Over the years, avionics systems have continued to increase in complexity to the point where 1st tier suppliers to an aircraft OEM have found it financially beneficial to outsource designs of subsystems to 2nd tier and at times to 3rd tier suppliers. Combined with challenging schedule and budgetary pressures, the environment in which safety-critical systems are being developed introduces new hurdles for regulatory agencies and industry. This new environment of both complex systems and tiered development has raised concerns in the ability of the designers to ensure safety considerations are fully addressed throughout the tier levels. The growth in avionics complexity and the increase in the number of developers in a multitier developer community raise questions about the sufficiency of current regulatory guidance to insure; proper flow down of safety awareness, avionics application understanding at the lower tiers, OEM and 1st tier oversight practices, and capabilities of lower tier suppliers. Therefore, NASA established a research project to address Regulatory Compliance in a Multitier Supplier Network.

The research was divided into three major study efforts:

1. Describe Modern Multi-tier Avionics Development
2. Identify Current Issues in Achieving Safety and Regulatory Compliance
3. Short-term/Long-term Recommendations Toward Higher Assurance Confidence

This document summarizes civil and military safety standards, and current commercial and military industry practices. It provides an assessment of regulatory guidelines and industry's application of regulatory guidance to address the issue of complex systems development in a multitier supplier environment.

2 Documents Reviewed

Standards and guideline documents reviewed for the NASA Flight Critical Systems Research (FCSR) study are listed below. The review focused on determining the level of guidelines, if any, for managing complex system designs in a multitier supplier network environment.

The documents were searched for the keywords: tier, multitier, supplier, developer, complex, compliance, certification, experience, proficiency, oversight, delegation, assessment, qualitative, quantitative, and (including references to DO, ARP, TC, STC and use of shall, will, must) providing an assessment of guidance content as it applies to multitier avionics development.

Attention was also given to references of: requirements, allocation, trace, model, interface, interop, trace, and design as an assessment of functional requirements management.

The list below is organized for documents classified as: system level guidelines, RTCA Documents, FAA advisory circulars, FAA Orders, Mil Standards, industry practices, and papers relevant to the topic.

Systems Level Guidelines

- DoDAF 2.0, DoD Architecture Framework
- FAA System Safety Handbook

- DOT/FAA/AR-08/32, Requirements Engineering Management Handbook
- FAA Air Traffic Organization Safety Management System Manual
- FAR Part 25, Airworthiness Standards: Transport Category Airplanes
- ARP 4754A, Guidelines for Development of Civil Aircraft and Systems
- ARP4761, Guidelines and Methods for Conducting Safety Assessment on Civil Airborne Systems and Equipment

RTCA Documents

- DO-178C, Software Considerations in Airborne Systems and Equipment Certification
    - DO-330, Software Tool Qualification Considerations
    - DO-331, Model Based Development and Verification Supplement to DO-178C
    - DO-332, Object-Oriented Technology and Related Techniques Supplement to DO-178C
    - DO-333, Formal Methods Supplement to DO-178C
- DO-254, Design Assurance Guidelines for Airborne Electronic Hardware
- DO-264, Guidelines for Approval of Provision and use of Air traffic Services supported by Data Communications
- DO-297, Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations
- DO-326, Airworthiness Security Process Specification

Advisory Circulars

- AC 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes
- AC 25.1309-1A, System Design and Analysis
- AC 25.1309 Arsenal, - System Design and Analysis
- AC 25.1329-1B, Approval of Flight Guidance Systems
- AC 20.115C, Airborne Software Assurance
- AC 20-145, Guidance for IMA that implement TSO-C153 Authorized Hardware Elements
- AC 20-152, Design Assurance Guidance for Airborne Electronic Hardware
- AC 20-170 IMA development, Verification, Integration, and Approval using DO-297 and TSO-C153
- AC 20-174 Development of Civil Aircraft Systems
- AC 25-7C, Flight Test Guide for Certification of Transport Category Airplanes

FAA Orders

- Order 8110.4C, Type Certification
- Order 8110.7D, Aircraft Certification Systems Evaluation Program
- Order 8110.49, Software Approval Guidelines
- Order 8110.105, Simple and Complex Electronic Hardware Approval Guidance
- Order 8130.2, (Draft) Airworthiness Certification of Aircraft and Related Products
- TSO-C153, Integrated Modular Avionics Hardware Elements

Mil Standards

- MIL-STD-882E Standard Practice for System Safety

Industry Practices

- The FAA and Industry Guide to Product Certification
- Sample Contractor Supplier Assessment and Oversight process
- Sample Contractor Partnership for Safety Plan
- Sample Developer PSAC
- Sample Developer PHAC
- INCOSE-TP-2003-002-03.2.1 System Engineering Handbook

Studies and Papers

- 787 Case Study – Tang and Zimmerman
- Use of Safety Cases in Cert and Regulation –Leveson
- Reliance on Development Assurance Alone for Complex Criticality - CAST
- Certification Concerns of IMA Avionics Systems - Bartley and Lingberg
- Complexity Concept Causes and Control – McDermid
- The Impact of RTCA DO-178C on Software Development - Reddy
- Transitioning to DO-178C and ARP 4754 for UAV SW development using MBD - Erkkinen
- Complying with DO-178C and DO-331 using MBD - Potter

Other resources

The following document was defined by NASA (Wilfredo Torres-Pomales) as outside the boundaries of this study. It was included here for reference only. The NASA System Safety Handbook was reviewed so as to obtain another perspective.

- NASASP2010580, NASA System Safety Handbook

The following are included for reference only.

- *NASA/SP-2007-6105, NASA Systems Engineering Handbook, Washington, DC*
- *NASA. NPR 8715.3C, NASA General Safety Program Requirements, Washington, DC. 2008.*
- *NASA. NPD 8700.1, NASA Policy for Safety and Mission Success, Washington, DC. 2008.*
- *NASA. NPR 7123.1A, NASA Systems Engineering Processes and Requirements, Washington, DC. 2007.*
- *NASA. NASA-STD-7009, Standard for Models and Simulations, Washington, DC. 2008.*
- *Quality assurance plans and processes SAE Aerospace Standard (AS) 9100 [27]*

3 Summary of Findings

3.1 Relationship of the Documents

A graphical representation of the sources of guidance available to the avionics developer is shown in Figure 1 below. The documents listed on this figure and those examined in this research do not address all available regulatory guidance sources but focus on those that impact the development of avionics systems and their safety aspects as related to the topic of this study – complex avionics systems development in a multitier environment. One might conclude from the accident-incident databases that

the occurrence of avionics generated incidents is very rare (no accidents have been reported due to avionics failures alone) that the certification processes are quite effective. Indeed they have served the aerospace industry well. However, the growth in complexity has reached a new level and the introductions of multitier suppliers has been recently increasing with some reports of failed performance – managed by the OEM or 1st tier contractor, nevertheless raising a concern. It should be noted that the accident/incident databases contain insufficient data details to make a proper assessment of the potential risks from complex avionics systems.

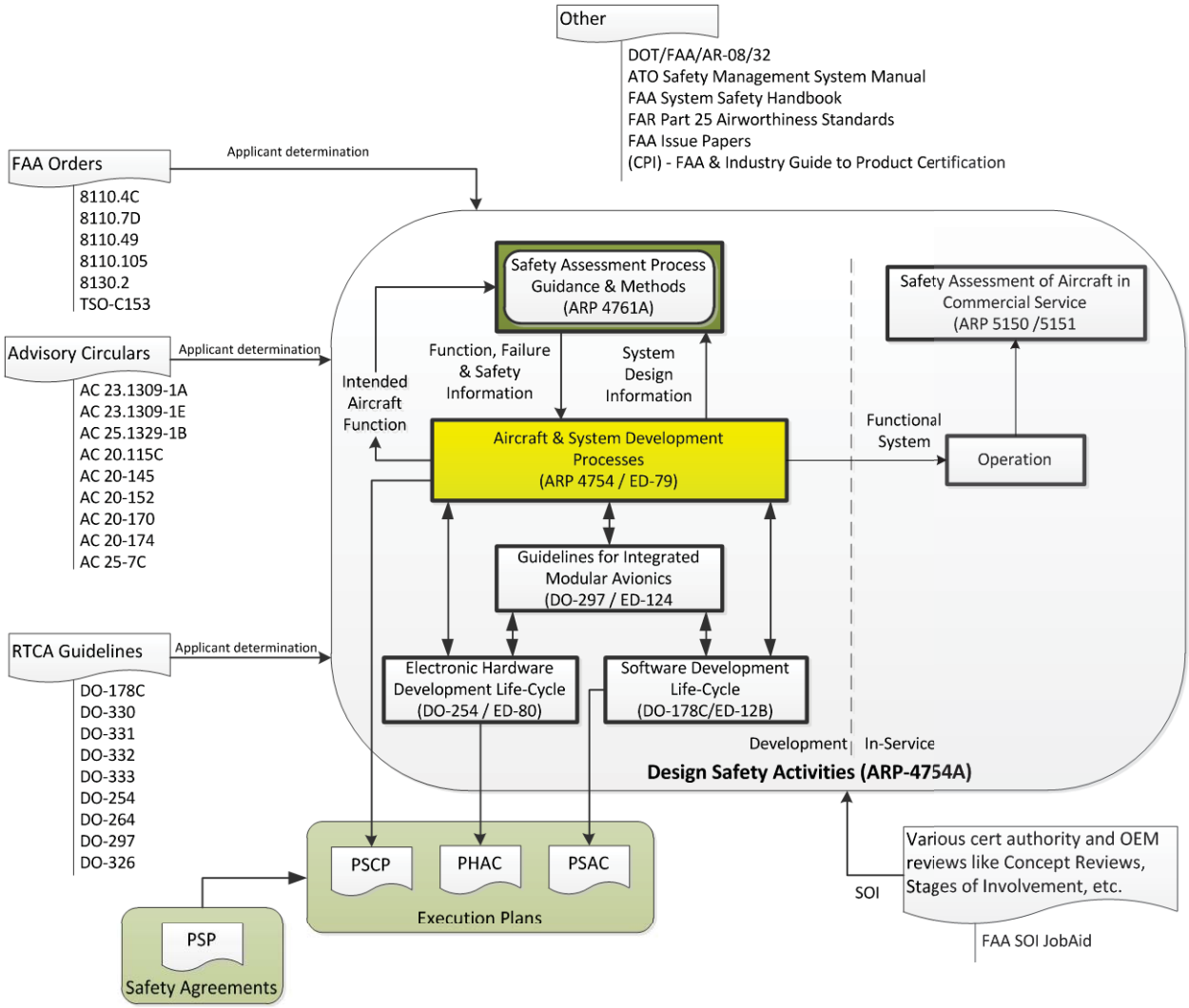


Figure 1. Safety Regulations and Guidelines (Context)

We have found that OEM and supplier experience on relevant certification programs is a key factor in successfully applying regulatory guidance and achieving regulation compliance. We found no top level document or hierarchical figure that gave complete guidance to a developer regarding which regulatory guidelines would apply to a development. Neither is there much guidance regarding what topics within

the guidelines are applicable to the developer. The developer must sort through the various documents to find those items that may apply on his/her own application or depend on the contractor, an OEM, or the ACO office to guide him. For a sub-tier contractor new to avionics systems and the safety aspects of the various guidelines this is likely to cause difficulty in execution because the information is spread over so many documents. The content of the guidelines is not easily assimilated by inexperienced suppliers. The sub-tier contractor is likely to do only what s/he is told to do in a statement of work (SOW) and may not know what questions to ask before beginning work. A major threat to safety is introduced when an experienced supplier switches to outsourcing for profit or development magnitude reasons. The experienced supplier is likely to place a contract based on assumptions on the knowledge and experience of the lower tier developer translated from his own internal organization's experience. The FAA has some internal documents that guide them on determining developer oversight but this kind of evaluation is not provided as a guideline for oversight to the industry. It is very dependent on the insight of the contracting OEM or developer.

A considerable amount of material must be assimilated in order to plan and execute a cost-effective approach to developing and certifying complex avionics systems. The FAA, EASA, ICAO and sovereign states have various ways of issuing guidance that pertain to certification processes and demonstrating compliance with applicable airworthiness regulations. Regulatory agencies issue policies, orders, notes, advisory circulars, issue papers, SARPs (Standards and Recommended Practices), and CRIs (Certification Review Items) along with TSOs and ETSOs to ensure safety and interoperability across the spectrum of national and international rules and regulations. When a lower-level supplier is unaware or inexperienced at showing compliance, the risk to the overall program may not be recognized until later when the cost, in terms of schedule and effort, can be much greater. This issue must be recognized and addressed by the contracting supplier with sufficient oversight in application knowledge and regulatory process guidance.

It should be noted that the regulatory guidance is intentionally non-prescriptive. The developer's interpretation of the guidelines, in the form of an approved Plan for Software Aspects of Certification (PSAC) and Plan for Hardware Aspects of Certification (PHAC), provides the processes the developer will follow. This approach allows applicants to use their own processes, methods, and tools to develop products and take advantage of improvements as development progresses. However, regulatory agencies need to have confidence that the process, methods, and tools used to develop a product will result in a certifiable product. To address this concern, early in the development life cycle the OEMs and suppliers develop these certification plans and seek acceptance of the system, software, and hardware development plans from the RAs. Figure 1 utilizes the ARP 4754A Design Activities diagram as the core process description to develop a context diagram into which the regulatory guidelines flow.

In collecting the documents listed in Figure 1 relevant to this study, it was beneficial to visually represent the developer's activities by overlaying development documents identified in the various guidelines in Figure 2 because of differences in activities between documents such as the FAA Systems Safety Handbook (SSH) and ARP-4754A. These were overlaid on the ARP-4754A Interaction Between Safety and Development Process figure in the form of a design layer, safety layer, and FAA SSH layer.

The goal was to extrapolate the elements that impact multitier development from existing guidance and use this to guide improved regulatory guidance mechanisms for complex multitier avionics developments of the future.

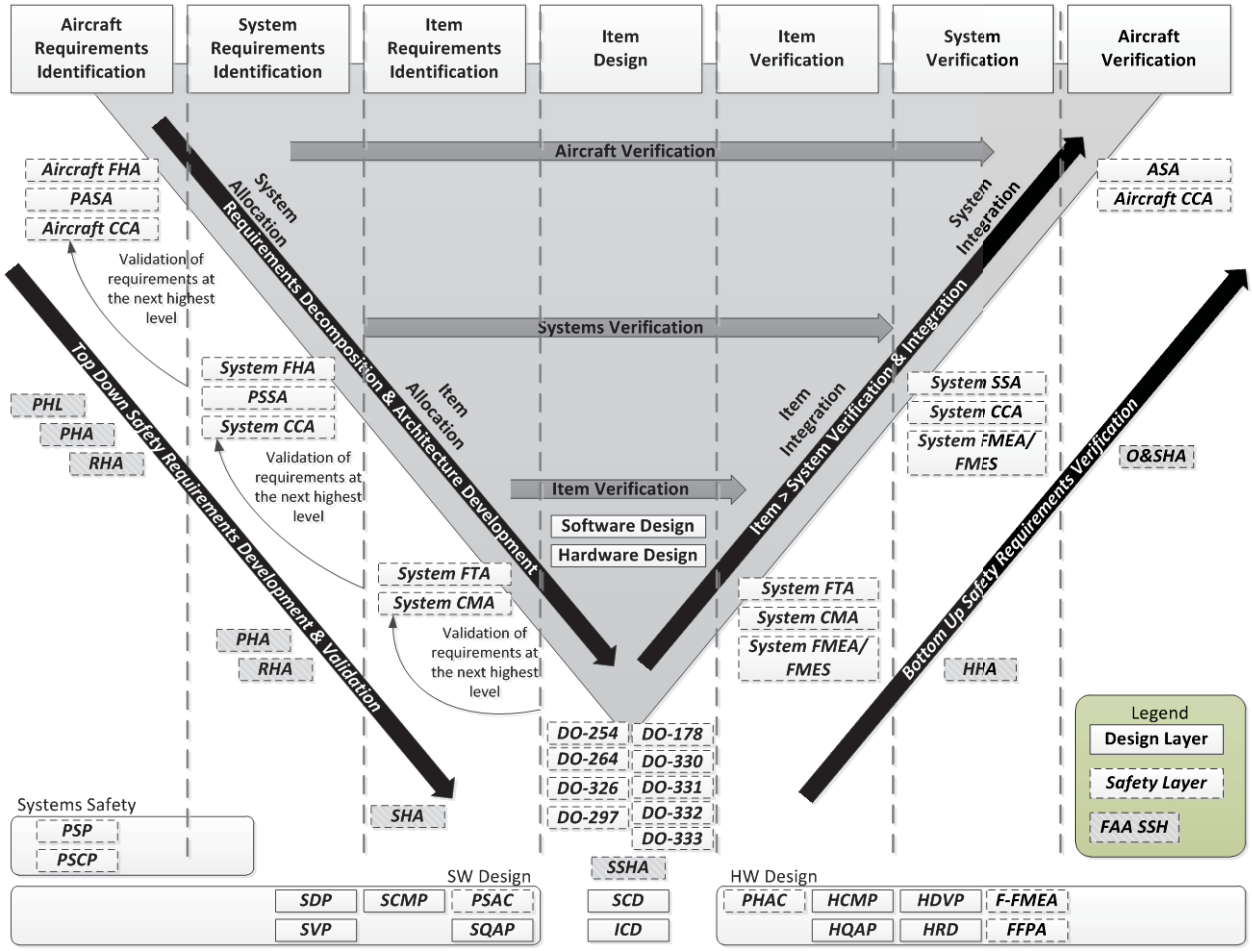


Figure 2. Development Safety Documents

The safety guidance within the various FAA Advisory Circulars, FAA System Safety Handbook, ARP4754A, ARP4761, and the DO-documents is intentionally designed to be non-prescriptive. However, this leaves complex systems and multitier supplier network developments dependent on FAA and OEM DER oversight, industry experience, and product knowledge. More recent releases, such as DO-178C, have specifically called out the need for oversight.

3.2 Multitier Notes

Of the documents reviewed, DO-297, DO-178C, DO-254, and Order 8110.49 provide greatest amount of guidance to multitier development. From an overall system perspective, DO-297 by its very nature of the architecture must address a multitier supplier development environment approach to safety. It outlines multitier overarching responsibilities. From an implementation development perspective DO-178C and its supplements specifically addresses lower tier supplier responsibilities better than any of the other documents. Order 8110.49 nicely expresses the issues of this study: complex systems being

developed in a multitier environment focusing on the oversight of the suppliers. Although meant for the FAA it can be useful to the applicant in determining suppler and sub-tier supplier capabilities.

Where written guidance does not exist, then oversight from an ACO and each supplier using a subcontractor is necessary to enforce safety in design and V&V. Each group will be accounting for roles and responsibilities (set in contracts) and intellectual property as well as technical interfaces. The FAA will usually expect proposals to be made by the applicant to address the rules and regulations.

The adequacy of any identified safety assurance guidance is dependent on the level of prescription deemed appropriate. The safety assurance approaches and processes determined from the guidelines by the OEM or 1st tier supplier that are turned into prescriptive processes are translated by humans tier to tier. These are judgment calls based on experience. Just as any requirements translation from English to English is subject to quality concerns so are the guidance mechanism translations. When provided to a foreign supplier there is a cultural difference that may also undermine communication assumptions.

In general it is cumbersome for the developer to extract the safety assurance objectives from the guidelines in order to define what will become the prescriptive processes he will follow. Developers often generate tables or checklists from the guidelines to guide themselves in assessment of compliance with the guidelines. For a number of the documents it would be helpful if the guideline structures were more succinct and to the point - subscribe to a Keep It Simple but Sufficient (KISS) principle. Digging through the excess information to find the value added information in this volume of documentation is not straightforward, especially since so much unwritten experience-based knowledge exists. This tends to make this the domain of the experienced and so adding multitier suppliers increases risk.

3.3 Individual Document Summaries

The following paragraphs summarize the insights gained in searching through the guidelines for written direction to the potential developer of complex systems utilizing tiered suppliers.

3.3.1 Systems Level Guidelines

DoD Architecture Framework (DoDAF)

The primary value of C4ISR was the mechanisms to insure clear requirements interpretation. DoDAF 2.0 appears to depart from these values in DoDAF 1.0, taking instead a focus on business information to aid a manager in making decisions. As a result the values of the graphical representations of a systems design for complex avionics are diminished. The C4ISR utility for design of complex avionics systems is gone.

FAA System Safety Handbook (SSH)

The FAA SSH loosely addresses multitier suppliers by suggesting that the contractor should impose SSP requirements on suppliers, including a System Safety Working Group (SSWG). It also has a section defining contractor oversight containing principles which could be considered applicable for guidance of multitier suppliers.

DOT/FAA/AR-08/32

The document presents a set of recommended practices on how to collect, write, validate, and organize requirements. The document does not favor high-level modeling or model driven requirement development. The perspective is from the software engineering low-level modeling. It has no perspective on tiered or supplier-developed requirements, therefore does not address the concerns raised over complex avionics development in a multitier environment. There is no discussion regarding flow down to other suppliers, delegation, or oversight in any form. It does follow the C4ISR style of decomposition of requirements; system overview, identification of boundaries, definition of operational concepts, development of the functional architecture, and definition of the software requirements. It does refer to ARP 4754, ARP 4761, and DO-178B.

FAA Air Traffic Org Safety Mgt Sys Manual

The document discusses oversight from a number of FAA perspectives. It does not address applicant oversight of suppliers or sub-tier suppliers. Complexity is discussed from a NAS perspective. There are no guidance mechanisms suggested to address complex systems development in a multitier environment. Although our study focuses on the avionics aspect of this issue, it seems like the NAS would have a common issue with complex systems and multitier/multipeer suppliers.

FAR Part 25

*FAR Part 25 contains rules and regulations that must be complied with distinguishing it from the guidelines which give approaches by which compliance may be shown. FAR Part 25 addresses the use of safety equipment and the safety design of the installed systems in terms of performance hazards they might produce. It contains no references to ARP, RTCA, or AC guidelines. However, 1309 specifies a number of items that "**must**" be achieved which by implication might cause a supplier to flow down requirements and assessments to lower tier suppliers. However, FAR Part 25 provides no guidance control for supplier or multitier supplier networks safety management.*

ARP-4754A

ARP-4754A is one of the primary documents which address the complete lifecycle of a system development. ARP-4754A safety assurance control authority is through the Aircraft Safety Group which is to establish and communicate safety requirements to all tiers. There is mention of tiered development but it does not address supplier oversight. However it develops a good system safety perspective. The style of the document is like all the guidelines, it provides a recommended means of compliance but does not prescribe a specific approach. So, although it does not specifically address complex development in a multitier supplier network the principles, it outlines excellent guidance for the applicant to implement. Oversight mechanisms, though not spelled out, could be extrapolated from the content of the document. Enhancements to the document to address multitier oversight are recommended.

ARP-4761

ARP-4761 does not address multitier developments specifically, therefore it provides no multitier guidance material. The described mechanisms could, however, be applied to lower tiered subsystems much as the aircraft requirements are assessed with system requirements. It neither precludes nor informs on multitier developments. However there is inherent tiered hierarchy within the FHA and FTA. An FMES is compiled including supplier's FMEAs.

3.3.2 RTCA Documents

DO-178C

DO-178C calls out multiple oversight areas for lower tier supplier critical processes. Yet there are holes in the system level requirements validation. The document excludes itself from the validation of any system requirements allocated to hardware so in a manner it creates a gap between the system and the sub-system. It is these interfaces between a contractor and supplier where system understanding and requirements boundaries cause the greatest error. There is also no guidance on managing the impact of an in-experienced developer. No assessment of supplier lack of experience in aircraft systems, real-time, and design of safety critical systems is given.

DO-330

DO-330 is a supplement to DO-178C focused on software tool qualifications. It reflects the same level of supplier oversight established in DO-178C and so does address the issue of multitier supplier development to that level.

DO-331

The definition of what model-based development is and how it is applied will vary greatly over the industry and between disciplines. ARP 4754A is referenced as defining the system life cycle processes.

DO-332

DO-332 is identical to DO-331 in terms of guidelines and wording in relation to this study. The notes from DO-331 apply to DO-332.

DO-333

DO-333 discusses Formal Methods as a verification method. It contains no guidance or control mechanisms related to complex multitier network of suppliers.

DO-254

The document does not address tiered level developments but does consider aspects of COTS hardware provided by a commercial vendor. In that requirements are to be traceable to the next level of requirements, there might be some level of control of the developer even though the idea of a supplier and/or sub-tier supplier is not mentioned. Furthermore, the document excludes itself from the validation of any system requirements allocated to hardware. Effectively, DO-254 provides no guidance for tiered development. Like DO-178C, DO-254 defines objectives that should be satisfied in order to establish compliance with airworthiness requirements. Relevant objectives need to be flowed down to suppliers who provide hardware and/or software for the system.

DO-264

DO-264 does not address multitier or a supplier base in any way and so does not provide any guidance for multitier supplier oversight. However, the document has good process guidance and stakeholder interaction definitions that could be expanded to address multitier supplier oversight and design requirements control.

DO-297

DO-297 guides a IMA system development so by its nature addresses an environment that will involve multiple suppliers and potentially tiers. It has a number of guidance statements regarding supplier control including references to DO-178 that could provide some management guidance of sub-tier suppliers. However, considering the environment is that of multitier or multipeer development it is weak in providing guidance directions towards sub-tier supplier oversight.

DO-326

DO-326 does not address multitier or supplier base. The relevant airworthiness security requirements need to be flowed-down to suppliers of system components.

3.3.3 Advisory Circulars

AC 23.1309-1E

The AC clearly states that it is neither mandatory nor is it a regulation. However, the AC also states that "While these guidelines are not mandatory, they are derived from extensive FAA and industry experience in determining compliance with the relevant regulations. Whenever an applicant's proposed method of compliance differs from this guidance, the proposal should be coordinated with the Small Airplane Directorate Standards Staff, ACE-110". So there is an implication of prescription imposition. Any potential multitier guidance found could therefore be interpreted as more than just recommendations. However, the AC does not address multitier supplier networks or oversight of suppliers. The document does provide potential guidance awareness of areas for supplier or multitier supplier networks safety management. The AC references: ARP 4754A, ARP 4761, DO-178B, and DO-254.

AC 25.1309-1A

Throughout the document, AC 25.1309 addresses complexity concerns and means of assuring safety through analyses. The document addresses qualitative assessment and failure risk and consequence assessment decision rationales. It takes exception to its applicability to software errors stating "it is not feasible to assess the number or kinds of software errors, if any, that may remain after completion of system design, development, and test", instead referring to DO-178A. The use of experienced judgment is clearly the cornerstone of the hazard assessments. Any new tier supplier is very likely not to have that necessary experience. The last issue of this document is 1988. An update to AC 25.1309-1A was drafted in 2002 (draft ARSENAL revised) but a revision has not yet been released for Part 25 aircraft. It does not address supplier oversight or tiered supplier management.

AC 25.1309 Arsenal

AC/AMJ No. 25.1309 (draft ARSENAL revised) was reviewed in terms of differences that might provide guidance for complex multitier avionics systems design and safety assurance. Certain enhancements within the document are also noted. No enhancements were added that address complex systems or multitier management. It did invoke the ARP safety guidelines and additional DO documents.

AC 25.1329-1B

AC25.1329-1B acknowledges the growth in complexity but does not offer control mechanisms in response other than alerts to higher risks. The AC is pretty specific on flight control system modes and their assessment. ARP 4754, ARP 4761, DO-178B, DO-254 are referenced. The document expresses the need to examine and test interfaces between systems in a manner which reflects a system functional and performance examination of the exchange of data between the systems where the greatest risk of failure reside. However, it does not address the multitier or supplier aspects of a system development.

AC 20-115C

This AC was written to recognize DO-178C and it supplements and to provide guidance for transitioning to DO-178C. It also explains the use of DO-178C for TSO authorizations. It does not, however, address any of the issues associated with complex system design in multitier environments. This AC references a number of DO and AC documents as well as ARP 4754A.

AC 20-145

Control of third party production of hardware is discussed. It is recommended that, because of the complexity, applicants conduct a structured formal analysis in accordance with ARP 4754 and ARP 4761. The appropriate design assurance should be achieved for each complex electronic device using DO-254. The use of third party software is not addressed by this AC. Although third party suppliers are discussed there really is little implication of oversight management of the design process of third party suppliers.

AC 20-152

This AC addresses complex micro-coded components with design assurance levels of A, B, and C airworthiness appropriateness for the intended function. DO-254 is called out as the primary guidance document. The AC does not provide guidance for management or oversight of complex system design in multitier environments.

AC 20-170

DO-297 is an integral part of AC 20-170. The AC applies to systems developed by a single company as well as those developed by multiple companies. However, this document does not address the issues associated with complex systems development in a multitier environment. It does reference DO-297 which by the nature of an IMA system considers the use of multitier suppliers even though DO-297 is weak in its description of oversight management of suppliers.

AC 20-174

The purpose of this AC is to recognize ARP-4754A as an acceptable method for establishing a development assurance process. The AC addresses the concern of possible development errors stemming from the ever increasing complexity of modern aircraft systems taking the route that ARP-4754 provides a structured methodology to address these concerns. There is, however, no additional guidance as to managing complexity or the development of systems in a multitier supplier environment. References are made to a number of RTCA documents: DO-178B, DO-254, and DO-297.

AC 25-7C

AC 25-7C provides no oversight or management guidance of supplier or multitier supplier networks safety management. The AC is not mandatory nor does it constitute a regulation. Safety discussions are limited to performance related issues. The only reference to guidelines is to DO-160. Any modeling discussions are at the aircraft level.

Order 8110.4C

TO 8110.4C is primarily written for internal use by the FAA, its designees, and delegated organizations. The order provides procedures and policy for the type certification of products. The document provides a high-level model of the certification events that typically make up the life cycle of an aircraft but does not address multitier aspects of avionics development and safety.

Order 8110.7D

The purpose of this document is to apply standardized systems evaluations to the continued integrity of the design data after initial approval by the FAA at the PAH and associate facilities. It does not reevaluate previously approved design or safety data. It forms a good basis for production multitier supplier management assessments. However, the focus is on production quality assurance rather that design and development safety compliance assurance. As such it provides no guidance to the design and development of complex avionics systems in a multitier supplier network. Elements of production control and oversight could be redirected to form a basis of enhanced supplier control during the design phase.

Order 8110.49

This order establishes procedures for evaluating and approving aircraft software and software changes to approved aircraft software. It guides Aircraft Certification Service (AIR) field offices and Designated Engineering Representatives (DER) on how to apply DO-178B. It is applicable to TC, STC, ATC, ASTC, and TSO. ***This document nicely expresses the issues being addressed in this study: complex systems being developed in a multitier environment****. It does not provide additional insight on solutions to the issues but focuses on the use of oversight of the supplier and the conduct of reviews to address the concerns. It does not address MBD. Included is a supplier assessment table, although meant for the FAA, which could be useful to an applicant in determining a supplier and sub-tier supplier capability. It should be updated in light of DO-178C use of oversight.*

Order 8110.105

Order 8110.115 is primarily written for internal use by the FAA. It assists in determination of FAA involvement in a project, types of reviews, and how much delegation of oversight is given to designees. This document includes an assessment checklist of developer experience to determine the level of involvement necessary by the FAA that could be useful to the industry as a potential supplier capability assessment. It does not provide guidance for the complexity issues and multitier development issues of this study, although the checklist accesses the system complexity when determining oversight. The use of MBD is not addressed.

Order 8130.2

This order is focused on processes for airworthiness certification and maintenance activities and responsibility assignments, but all at the aircraft level. With the focus on the high level applicant, FAA interaction, and designee responsibilities it does not address the multitier design and development issues of complex avionics. There are a few items of delegation discussed.

TSO-C153

There is no mention of suppliers, oversight, or delegation in the document. Neither is complexity, requirements management, or model based development addressed. It therefore does not provide any guidance for complex avionics developed in a multitier supplier environment.

3.3.4 Mil Standards

Mil-Std-882E

In place of the terms suppliers, oversight, or delegation the document discusses the responsibilities of the developer and the interaction with the program manager. Oversight is discussed in the form of monitoring the developer's system safety activities with review and approval of the delivered artifacts. Complexity, requirements management, or model based development are not addressed. As such, the document addresses the safety management between the manager and the developer at one tier. The principles described between the manager and developer could be applied at the developer and sub-tier developer as well. The use of model simulation for safety testing is allowed, however, the subject of MBD is not addressed.

3.3.5 Industry Practices

FAA and Industry Guide to Product Certification

This document has quite a bit of discussion on management of design and safety for a system development. Oversight and delegation guidelines are given throughout the document; however they only address the first tier supplier. Although it does not specifically address multitier supplier development the principles could be applied by the applicant and the supplier. It fails on the count of multitier in that it focuses on foreign suppliers almost to the exclusion of the management of US suppliers. Although it contains considerable valuable guidelines its adherence or enforcement is not clear. It is up to the applicant to develop the content of a Partnership for Safety Plan (PSP) and Project Specific Certification Plan (PSCP). The PSP and PSCP will need to detail the sub-tier supplier assessment and oversight management processes that will be followed. The document references DO-160 and DO-178B but no ARP documents.

Contractor Supplier Assessment and Oversight Processes

If a contractor has a supplier assessment and oversight process their oversight process will generally summarize the methods and processes to be used by the contractor to perform supplier assessments and determine the level of technical oversight, citing assessment of the suppliers control of the design process for compliance with ARP 4754, DO-178, DO-200, and/or DO-254. Supplier selection and management processes may be declared outside the scope of the Supplier Assessment and Oversight Process leaving those controls to be managed through a flowed down PSCP, PSAC, and PHAC.

Weaknesses found in these oversight processes are in:

1) *the assumption that management and technical oversight will take place through the flow down of the PSCP, PSAC, and PHAC,*
2) *they tend to focus on-going supplier performance assessment that will determine and adjust the percentage of oversight deemed necessary with a bent towards reducing oversight and design participation through a sampling metric,*
3) *they generally fall short of providing supplier oversight guidance save in the assessments of their performance after they are on contract,*
4) *the net impetus of this approach is a focus on supplier defect leakage rather than on supplier design oversight.*

INCOSE-TP-2003-002-03.2.1 System Engineering Handbook

The document recognizes that complexity is a major issue but does not provide a means to manage complexity other than rigor in the decision gate review and assessment processes. There is only recognition of a single layer of suppliers. No oversight of suppliers is mentioned. No references to any RTCA or ARP documents are made. INCOSE provides no insight on the topic of this research.

3.3.6 FAA Issue Papers

Issue papers are generally project specific so do not provide assistance to industry across the board for guidance. So, no issue papers were reviewed.

3.3.7 Papers

787 Procurement Case Study - Tang and Zimmerman

Under the 787, Boeing instituted a risk sharing approach and tiered supply chain to contracting approximately 50 tier-1 suppliers who also served as integrators of subsystems produced by tier-2 suppliers. These tier-1 suppliers were responsible for delivering complete systems to Boeing. The paper highlights two primary issues with Boeings institution of this multitier network of suppliers that are applicable to any structure with multiple tiers of suppliers: 1) care in selection of tier-1 supplier experience and capability, and 2) oversight through the multi-levels of the resulting tiered structure. It also brings out several issues with assumptions: 1) assumed alignment in technical and management with the OEM goals and principles, 2) lack of understanding cultural impacts, 3) capability and experience of the supplier including the engineering expertise as well as the depth of resources within the supplier. As a paper it does not provide regulatory guidance, however it highlights issues associated with the use of multitier developers and recommends greater level of OEM involvement in tier-1 supplier selection of sub-tier suppliers. It also recommends an oversight working team with visibility across the tiers. These recommendations apply to this study.

Use of Safety Cases in Cert and Regulation - Leveson

This paper does not address multitier supplier issues or complexity directly. Neither does it address delegation of design tasks or integration of subsystems and the oversight of these activities, although it does allude to local government oversight through inspections and audits. It does not reference any RTCA papers or ARP documents and procedures. There are however, certain elements identified in the paper that that are applicable to increasing the safety of multitier complex systems.

Reliance on Development Assurance Alone for Complex Criticality - CAST

The document does not address multitier supplier development and does not discuss oversight or delegation. It recognizes the ARP and RTCA documents as a means to provide assurance through a development process. The paper takes a position that the regulations and policy are not sufficiently explicit (prescriptive). The greater discussion on the use of diversity (dissimilarity) implies guidance towards the use of diversity as a means to supplement development assurance. It does not provide guidance towards complex avionics developed in a multitier environment.

Certification Concerns of IMA Avionics Systems – Bartley and Lingberg

By its nature an IMA system may be made up of multitier suppliers of the individual components and functions. This paper raises many of the concerns relevant to development of complex systems in a multitier environment. It states that the existing regulatory guidance material, though fragmented, provides sufficient guidance to accomplish the necessary safety design and assessments. The concern is that a fragmented supplier development base will exacerbate the issue by inadvertently missing certain aspects of the design and analysis.

Complexity Concept Causes and Control – McDermid

The paper is focused on the issue of complexity and how to manage and asses the system. The paper provides nothing new or of value but rather proposes some unacceptable means of dealing with assessments for avionics. Not useful to this study.

The Impact of RTCA DO-178C on Software Development - Reddy

The document provides a nice summary of the impact of DO-178C. It is a concise description of the changes made from DO-178B to get to DO-178C. It has no direct value to this study but is recognized as an aid to someone wanting to understand DO-178C structures.

Transitioning to DO-178C and ARP 4754 for UAV SW development using MBD - Erkkinen

This paper takes a look at the changes in DO-178C and supplement DO-331 in regards to the use and processes of MBD. The use of MBD to capture requirements, model the design, and generate code from the model is now clearly acknowledged as an acceptable means to certification by the governing standards. A long standing issue wherein DO-178B provided an uncertainty in mapping objectives to MBD artifacts is now clarified. DO-178C, supplement DO-331, calls out ARP4754A recommendations for MBD requirements capture, modeling, simulation, analysis, and validation. Also noted is that DO-331 defines a design model that is used to not only capture and analyze but to generate embedded code for both hardware and software implementations.

So as it relates to this study this paper provides insight into guideline support for use of MBD as a means, although not stated, by which complex multitier systems requirements can be captured, modeled, tested, and coded. The paper does not outline this system design management approach but establishes that the regulatory documents contain the acknowledgment of MBD that can enable guidelines that raise the bar on multitier development. [This flows into our pre-conceived thoughts that the use of MBD and systems control can be strengthened to address the issues].

Complying with DO-178C and DO-331 using MBD - Potter

This document is basically the same as the paper on Transitioning to DO-178C and ARP 4754 for UAV SW development using MBD with a few noted differences.

3.3.8 Other Resources

NASASP2010580, NASA System Safety Handbook Volume 1

Although this document is out of the scope of assessing the regulatory guidelines for management and oversight of multitier supplier development of complex systems, this document was reviewed for an alternate perspective. The document defines complexity as one of the primary reasons for its purpose, to provide a safety framework with a holistic assessment of the aggregate sources of risk. It does not specifically address multitier supplier network risks: experience, interpretation, boundary issues, etc. However, the purpose of the document is intended for those with oversight responsibilities. The overall framework could easily be applied to multitier suppliers. The document does not reference any ARP or DO documents, but references Mil-STD-882D, Mil-HDBK-217F and a number of NPR documents.

4 Guideline Reviews

What follows is a collection of relevant statements to complexity, multitier, and the use of modeling from the documents. Each collection for that document is preceded by a short summary and relevance assessment of the guideline or practice towards the issue of multitier developments. The summaries were collected into paragraph 3.3 for a quick review by the reader.

4.1 Systems Level Guidelines

4.1.1 DoDAF 2.0, DoD Architecture Framework

The primary value of C4ISR was the mechanisms to insure clear requirements interpretation. DoDAF 2.0 appears to depart from these values, taking instead a focus on business information to aid a manager in making decisions. As a result the values of the graphical representations of a systems design for complex avionics are diminished. The C4ISR utility for design of complex avionics systems is gone.

DoDAF as outlined in the C4ISR methodology was considered a very good systems practice approach to be recommended and followed throughout industry to define complex systems.

- **However**; the direction within DoDAF V2.0 which has replaced C4ISR and DoDAF 1.0 makes its focus management tools for control - departing from a technical guidance purpose.
- DoDAV 2.0 quotes:
  - "DoDAF V2.0 focuses on architectural "data", rather than on developing individual "products"
  - "The major emphasis on architecture development has changed from a product-centric process to a data-centric process designed to provide decision-making data organized as information for the manager."
  - "The three major viewpoints of architecture described in previous version (e.g., Operational, Technical, and System) have been changed to more specific viewpoints that relate to the collection of architecture-related data which can be organized as useful information for the manager in decision-making"
  - "Architecture development is a management tool that supports the decision-making process"
  - Any discussion regarding allocation and delegation is limited to organizational structures within the government.

4.1.2 FAA System Safety Handbook

The FAA SSHB loosely addresses multitier suppliers by suggesting that the contractor should impose SSP requirements on suppliers, including an System Safety Working Group (SSWG). It also has a section defining contractor oversight containing principles which could be considered applicable for guidance of multitier suppliers.

- Section 5.3.11 The contractor must impose requirements on suppliers that are consistent with and contribute to the SSP.
- Subcontracted systems impacting safety are required to implement an SSP.
- The prime contractor has responsibility for integrating the overall SSP.
- The SSP should indicate how the contractor or prime plans to effect integration and procedures.
- Section 5.4 describes an integrated SSP, although very loose in its construction and execution.
  - Organization
  - Formation of a System Safety Working Group (SSWG).
  - Risk hazard identification and risk resolution
  - Integrated safety V&V
  - Integrated Audit program

- Section 6.4 outlines Managing Contractor System Safety (Contractor Oversight)
  - It does not address multitier management, although these principles are useful to lower tier management
- Appendix D discusses the use of OOA/OOD modeling to specify requirements and formal inspections of specifications.

4.1.3 DOT/FAA/AR-08/32, Requirements Engineering Management Handbook

The document presents a set of recommended practices on how to collect, write, validate, and organize requirements. The document does not favor high level modeling or model driven requirement development. The perspective is from the software engineering low level modeling. It has no perspective on tiered or supplier developed requirements, therefore does not address the concerns raised over complex avionics development in a multitier environment. There is no discussion regarding flow down to other suppliers, delegation, or oversight in any form. It does follow the C4ISR style of decomposition of requirements; system overview, identification of boundaries, definition of operational concepts, development of the functional architecture, and definition of the software requirements. It does refer to ARP 4754, ARP 4761, and DO-178B.

- The document is not a fan of MBD: "There are other ways that the requirements could be specified besides shall statements. One approach is to use a graphical model to define the ideal value function and supplement it with the tolerances and latencies for each controlled variable. One disadvantage of this approach is that it is no longer obvious what constitutes an individual requirement."
- The Handbook describes the following 11 main-level recommended practices that allow developers to progress from an initial, high-level overview of the system to be developed to a detailed description of its behavioral and performance requirements.
  1. Develop the System Overview
  2. Identify the System Boundary
  3. Develop the Operational Concepts
  4. Identify the Environmental Assumptions
  5. Develop the Functional Architecture
  6. Revise the Architecture to Meet Implementation Constraints
  7. Identify System Modes
  8. Develop the Detailed Behavior and Performance Requirements
  9. Define the Software Requirements
  10. Allocate System Requirements to Subsystems
  11. Provide Rationale
- Input-Function-Output requirement clarity must be translated to the developer.
- A good requirement specification should describe everything necessary to produce the correct system—and nothing more. This succinctly states the balance that requirements need to achieve. A KISS description.
- The document recommends a system overview be generated and be generated early. Use context diagrams, describe external entities, identify system boundaries, and capture preliminary system goals. Include operational concepts.

- The document outlines the development of a functional architecture. Use data flow diagrams, define interfaces, minimize coupling, provide rationale etc.
- Then the document acknowledges spiral maturation as design details are refined and original specifications are revised.
- Requirements are to be traceable back to system goals.

4.1.4 FAA Air Traffic Organization Safety Management System Manual

The document discusses oversight from a number of FAA perspectives. It does not address applicant oversight of suppliers or sub-tier suppliers. Complexity is discussed from a NAS perspective. There are no guidance mechanisms suggested to address complex systems development in a multitier environment. Although our study focuses on the avionics aspect of this issue, it seems like the NAS would have a common issue with complex systems and multitier multipeer suppliers.

- Complete elimination of risk is unachievable considering the complex interplay of human, material, and environmental factors.
- Recognizing the critical role that humans and human error play in complex systems and applications has led to the development of the human-centered design approach. This human-centered design approach is central to the concept of managing human errors that affect safety risk.
- An accident rarely results from a single failure or event. They often result from degrading events that may be complex and involve primary, secondary, or even tertiary events.
- A correct requirement is unambiguous and verifiable. Controls can be complex or simple.
- If an organization is too complex or the attitude is such that information is not shared readily or willingly, safety could suffer.
- The section on incident reporting and its value raises an issue we ran into during this study – the data available in the accident/incident databases is very hard to search for avionics faults and has virtually no information as to the cause of the incident or its corrective action. Their utility for this study was of little value.
- A safety culture, Figure 3, is promoted in which the individual and group values, attitudes, competencies, and patterns of behavior determine commitment to safety.

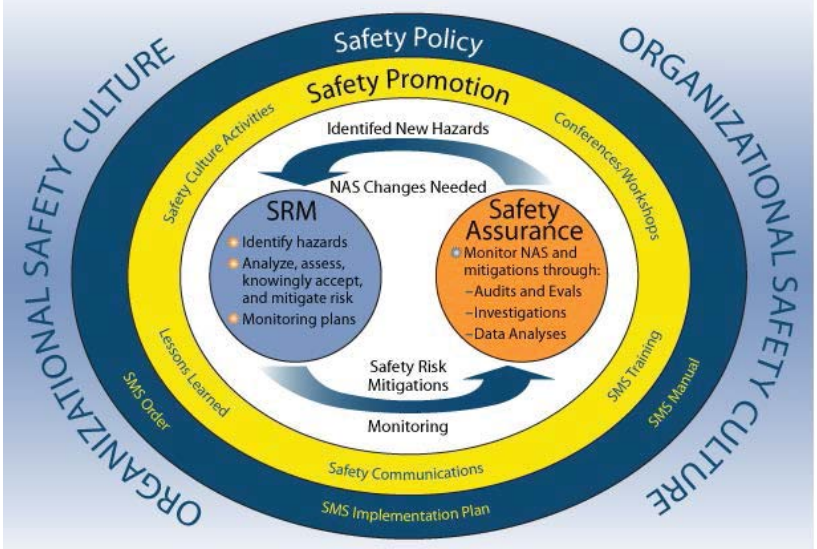


Figure 3. Organizational Safety Culture

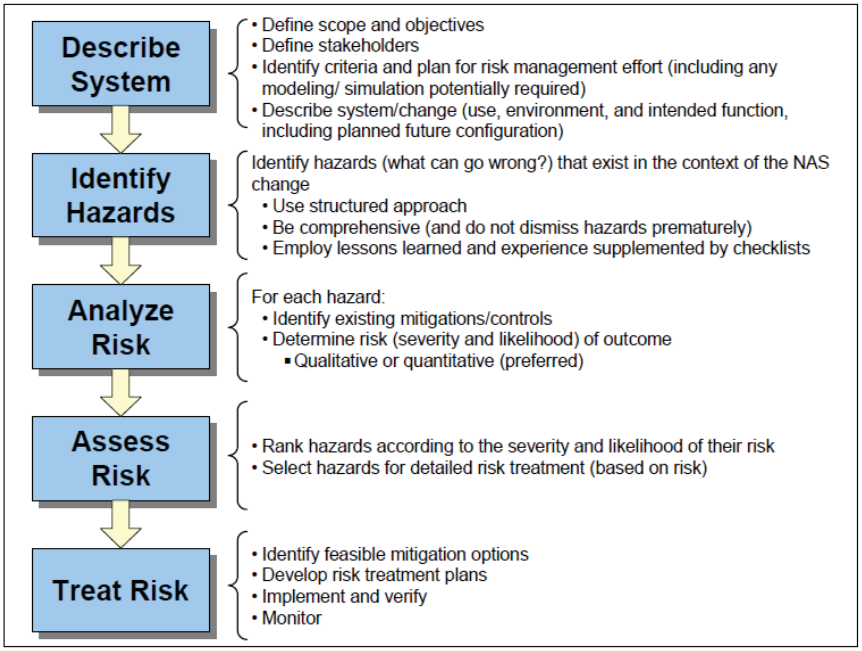


Figure 3.5: SRM Safety Analysis Phases

Figure 4. SRM Safety Analysis Phases

4.1.5 FAR Part 25, Airworthiness Standards: Transport Category Airplanes

FAR Part 25 contains rules and regulations that must be complied with distinguishing it from the guidelines which give approaches by which compliance may be shown. FAR Part 25 addresses the use of safety equipment and the safety design of the installed systems in terms of performance hazards they

*might produce. It contains no references to ARP, RTCA, or AC guidelines. However, 1309 specifies a number of items that "**must**" be achieved which by implication might cause a supplier to flow down requirements and assessments to lower tier suppliers. However, FAR Part 25 provides no guidance control for supplier or multitier supplier networks safety management.*

- There is a general statement that the airplane design may not have design features or details that experience has shown to be hazardous or unreliable. Generally the document discusses aircraft systems design in terms of performance hazards generated by systems.
- Electrical wiring interface system safety requires that 1) each catastrophic failure condition be extremely improbable and does not result from a single failure, 2) each hazardous failure condition is extremely remote.
- Electrical equipment and installations must not result in one system adversely impacting another system.
- The design **must** prevent occurrences of any failure that could prevent continued safe flight, reduce the capability of the crew or airplane to cope with adverse operating conditions and must provide the crew appropriate warnings.
    - Compliance with these requirements **must** be shown by analysis, simulator, or flight tests.

4.1.6 ARP-4754A, Guidelines for Development of Civil Aircraft and Systems

ARP-4754A is one of the primary documents which address the complete lifecycle of a system development. ARP-4754A safety assurance control authority is through the Aircraft Safety Group which is to establish and communicate safety requirements to all tiers. There is mention of tiered development but it does not address supplier oversight. However it develops a good system/safety perspective. The style of the document is like all the guidelines, it provides methods as means but does not prescribe any. So, although it does not specifically address complex development in a multitier supplier network the principles it outlines provide excellent guidance for the applicant to implement. Oversight mechanisms, though not spelled out, could be extrapolated from the content of the document. Enhancements to the document to address multitier oversight are recommended.

- The complete development cycle is described and guidance for functional allocation, design, requirements management, validation, and etc is outlined.
- Frequently, significant elements systems are developed by separate individuals, groups or organizations. These systems require added design discipline and development structure to ensure that safety and operational requirements can be fully realized and substantiated. A top down iterative approach from aircraft level downwards is key to initiating the processes.
- The Safety Program Plan section suggests that the plan may include the project safety organization responsibilities and its relationship with partners and/or suppliers with respect to the safety process.
- When discussing FDAL/IDAL acknowledges: "Note that the boundaries between systems and items may not coincide with the boundaries between aircraft manufacturers and suppliers, or between suppliers and sub-tier suppliers or with physical packaging."

- Specifies the responsibility for the Aircraft Safety Group (which has responsibility for performing and monitoring program safety tasks) to: “Establish and communicate the safety requirements at all tiers of definition”
- Multitier developments is recognized: “Note that the boundaries between systems and items may not coincide with the boundaries between aircraft manufacturers and suppliers, or between suppliers and sub-tier suppliers or with physical packaging.”
- A Safety Program Plan is defined that should be developed which identifies the project safety organization and defines responsibilities within this organization and its relationship with partners and/or suppliers with respect to the safety process.
- While the format of the validation effort is left to the developer, a structured process should be defined in the validation plan.
- Allocation of functions and requirements development is discussed at a high level.
- Modeling is a tool recognized in the integration and validation phases.
- When graphical requirements capture is planned the use of the models/modeling should be identified and the intended tools should be specified along with modeling standards.
    - The use of MBD for requirements development, flow down of requirements, and tiered developer management is not excluded but is also not developed as a method.
- There is an implied but not defined tier boundary crossing by the “Integral Processes” of Fig 6 in ARP-4754A flowing from aircraft functions down to sub-systems. A cross-tier control organization and process should be defined to address this but ARP-4754A does not describe such a function or organization.
- ARP-4754A relinquishes development guidance of the design process to DO-178 and DO-254 at the point where requirements are allocated to hardware and software – pg 29.
- One of the primary questions posed to multitier development is in the safety assessments in Para 5.1 on ARP-4754A page 31. How are these analyses managed through the multitier levels? Neither does Fig 7 page 33 address multitier developments.
    - A key part of the multitier FHA/PASA/PSSA/ASA/SSA is 1) how the identified failure conditions are specified as flow down to the lower tiers as causes of that failure condition, 2) how the verification and validation of those identified failure conditions and causes is executed, and 3) how lower level tiers maintain awareness of safety so as to identify previously unidentified failure conditions impacting the higher level systems and aircraft.
- A multitier development requires that a means to track, collect, and unify validation artifacts to show compliance at the aircraft level be used. This should fall into a systems oversight discussion justifying a paragraph on this topic.

4.1.7 ARP-4761, Guidelines and Methods for Conducting Safety Assessment on Civil Airborne Systems and Equipment

ARP-4761 does not address multitier developments, therefore it provides no multitier guidance material. The described mechanisms could, however, be applied to lower tiered subsystems much as the aircraft requirements are assessed with system requirements. It neither precludes nor informs on multitier developments. However there is inherent tiered hierarchy within the FHA and FTA. An FMES is compiled including supplier’s FMEAs.

- The bottom-up SAA process collects the necessary source data from suppliers as specified in the FHA/PSSA, FMEA/FMES, study results, etc.
- All safety requirements should be traceable and validated at each level of derivation. A good way to accomplish this is to create a table of derived requirements based on design decisions. Once the high level requirements have been identified, they may be used to generate lower level requirements as part of the PSSA process for the systems or items.

4.2 RTCA Documents

4.2.1 DO-178C, Software Considerations in Airborne Systems and Equipment Certification

DO-178C calls out multiple oversight areas for lower tier supplier critical processes. Yet there are holes in the system level requirements validation. The document excludes itself from the validation of any system requirements allocated to hardware so in a manner it creates a gap between the system and the sub-system. It is these interfaces between a contractor and supplier where system understanding and requirements boundaries cause the greatest error. There is also no guidance on managing the impact of an in-experienced developer. No assessment of supplier lack of experience in aircraft systems, real-time, and design of safety critical systems is given.

- The guideline applies to the applicant and to any subtier suppliers. The applicant is responsible for oversight of the suppliers.
- Planning should address supplier oversight.
- The SQA objective includes oversight of suppliers software life cycle process compliance with approved plans and standards.
- Certification reviews may take place at supplier's facilities. Certification reviews may involve discussions with suppliers.
- The PSAC outline defined in 11.1 includes Section h. Supplier oversight: This section describes the means of ensuring that supplier processes and outputs will comply with approved software plans and standards.
- The SCMP outline defined in 11.4 includes Section e. Supplier control: The means of applying SCM process requirements to suppliers.
- The SQAP outline defined in 11.5 includes Section g. Supplier oversight: A description of the means of ensuring that supplier's processes and outputs will comply with the plans and standards.
- The SW Accomplishment Summary defined in 11.20 includes Section g. Supplier oversight: This section describes how supplier processes and outputs comply with plans and standards.
- Systems processes are defined as responsible for refinement and allocation of system requirements to hardware and/or software as determined by the system architecture.
- 2.5.6 states that guidance for system verification is beyond the scope of DO-178. ARP-4754A does not give clear guidance for software/system verification either. There appears to be a gap on systems development guidelines and system verification.
    - Section 6.3.1 describes a review and analysis of high level requirements. The objective is to ensure that the system functions to be performed by the software are defined and

that the functional performance and safety-related requirements of the system are satisfied by the high level requirements and that derived requirements and the reason for their existence are correctly defined.

4.2.2 DO-330, Software Tool Qualification Considerations

DO-330 is a supplement to DO-178C focused on software tool qualifications. It reflects the same level of supplier oversight established in DO-178C and so does address the issue of multitier supplier development to that level.

- If tool life cycle activities will be performed by a supplier then configuration management activities should be applied to the supplier.
- The Tool Quality Assurance Process objectives provide confidence that the tool life cycle development and integral processes produce a tool that conforms to approved tool plans and standards.
- Third party or COTS tool qualification data is generated to acquire certification as specified in the PSAC.
- The tool qualification plan should include a means of ensuring supplier processes and outputs comply with approved tool plans and standards.
- The tool configuration management plan includes supplier TCM control of supplier processes.
- Supplier oversight is part of the Tool Quality Assurance Plan and the Tool Accomplishment Summary.
- Tool design standards include complexity restrictions ex: maximum level of nested calls or conditional structures, use of unconditional branches, and number of entry and exit points of code components.
- Hardware/software integration testing is clearly defined as needing to be done on the target computer environment with a focus on requirements based testing of the high level functionality, the hardware/software interfaces, and the error sources associated with the software operating within the target computer environment.
- Tool selection evaluations: The aspects of tool history to be evaluated include the level of experience and /or training in the use of the tool on the part of the applicant. The tools stability and maturity is examined.
- The document alludes to the greater use in the future of formal methods, model-based development and other tool-intensive methodologies. It states: The increased risk that these tool-intensive methodologies brings leads to the conclusion that an intermediate level of tool category between the two DO-178B tool categories is needed in order to address all tool types and define the appropriate TQLs. The two categories are; 1) development tools, and 2) verification tools. It is not, however, clear what this means.
- Automatic Code Generator (ACG) is discussed in its potential application. Here it states that an ACG must be qualified under DO-178C section 12.2 criteria 1 (since it could insert an error into the airborne code). This argument could be questioned where the verification is performed on the embedded code.

4.2.3 DO-331, Model Based Development and Verification Supplement to DO-178C

As does DO-178C this document provides some guidance to multitier supplier control in the form of recommended supplier oversight and compliance with design processes and quality management. The guideline requires oversight of any lower tier software supplier, however, there is no guidance on the managing the impact of experience on the developer. No assessment of supplier lack of experience in aircraft systems, real-time, and design of safety critical systems is given. The definition of what MBD is and how it is applied will vary greatly over the industry and between disciplines. ARP 4754A is referenced as defining the system life cycle processes.

- If software development activities will be performed by a supplier DO-331 states planning should address supplier oversight.
- Software quality assurance processes include assurance that suppliers comply with approved software plans, standards.
- Supplier processes and outputs should be assured by the SQA process to comply with approved plans and standards.
- The PSAC outline includes a section entitled: Supplier oversight describing the means of ensuring that the supplier processes and outputs will comply with approved software plans and standards.
- The SCM outline contains a section entitled: Supplier control describing a means of applying SCM process requirements to suppliers.
- It is stated that constraints and rules on development, design, and coding methods can be included to control complexity. Potentially using defensive programming practices.
- Complexity definition is not stated, however, complexity includes the degree of coupling between software components, the nesting levels for control structures, and the complexity of logical or numeric expressions.
- It is stated that the current state of software engineering does not permit a quantitative correlation between complexity and the attainment of system safety objectives. Complexity should be avoided however.
- The conformance to standards includes evaluation of the software design to complexity restrictions and constraints.
- Reviews are used to detect and report requirements errors introduced during the software requirements development process. This includes top level system requirements, low level software requirements, derived requirements, and the software architecture.
- The PSAC defines the proposed means of compliance.

4.2.4 DO-332, Object-Oriented Technology and Related Techniques Supplement to DO-178C

DO-332 is identical to DO-331 in terms of guidelines and wording in relation to this study. The notes from DO-331 apply to DO-332.

- If software development activities will be performed by a supplier DO-332 states planning should address supplier oversight.

- Supplier processes and outputs should be assured by the SQA process to comply with approved plans and standards.
- The PSAC outline includes a section entitled: Supplier oversight describing the means of ensuring that the supplier processes and outputs will comply with approved software plans and standards.
- The SCM outline contains a section entitled: Supplier control describing a means of applying SCM process requirements to suppliers.
- The use of classes in managing complexity is more powerful when they are related to each other through a class hierarchy.
- It is stated that constraints and rules on development, design, and coding methods can be included to control complexity. Potentially using defensive programming practices.
- It is stated that the current state of software engineering does not permit a quantitative correlation between complexity and the attainment of system safety objectives. Complexity should be avoided however.

4.2.5 DO-333, Formal Methods Supplement to DO-178C

DO-333 contains no guidance or control mechanisms related to complex multitier network of suppliers.

- In the review process: If high-level requirements and low-level requirements are formally modeled then formal analysis can be used to show compliance.

4.2.6 DO-254, Design Assurance Guidelines for Airborne Electronic Hardware

The document does not address tiered level developments. In that requirements are to be traceable to the next level of requirements there might be some level of control of the developer even though the idea of a supplier and/or sub-tier supplier is not mentioned. Furthermore the document excludes itself from the validation of any system requirements allocated to hardware. Effectively, DO-254 provides no guidance for tiered development.

- It acknowledged that COTS component suppliers may not have followed design safety processes outlined in DO-254.
- Section 2.3.5 states that a PHAC be developed outlining the design assurance approach and strategy. Section 9.1 outlines PHAC liaison with the cert authority. However, there is no tiered supplier guidance here or in the PHAC outline Section 10.1.1. COTS is to be addressed but there is no topic for developers.
- Section 9.2 states that Certification authority reviews may take place at the applicant's facilities or applicant's supplier's facilities.
- Requirements should be traceable to the next higher hierarchical level or requirements.
- Just like DO-178C, page 37, DO-254 excludes validation of system requirements allocated to hardware – assuming that they are validated as part of the systems process. It also states that not all hardware derived requirements need to be validated.

4.2.7 DO-264, Guidelines for Approval of Provision and use of Air traffic Services supported by Data Communications

DO-264 does not address multitier or a supplier base in any way and so does not provide any guidance for multitier supplier oversight. The document has some process guidance and stakeholder interaction definitions that might be expanded to address multitier supplier oversight and design requirements control.

- This document has a good focus on the development processes ex: Section 1.3.3 provides a relationship of guidance material to standards and evidence, Section 2.0 provides a description of the processes.
    - Although the document does not invoke "shall", "will" ("should" is used) in its guidance the focus on processes and guidance is of a nature that achieves prescriptive effects without being prescriptive.
- Complexity is recognized as an issue for data communications in operational issues that must be coordinated. The document states there is a need for a certification agency/industry accepted guidance process for coordinating implementation requirements and qualifying approaches.
- The document specifies that stakeholders should be identified. The question is if anyone will call a sub-tier supplier a stakeholder.
- There are some natural positions in the sequence of requirements – design – validation process description and Figs 2-3, 2-4, and 2-6 with the associated multitier oversight could be inserted.

4.2.8 DO-297, IMA Development Guidance and Certification Considerations

DO-297 guides a IMA system development so by its nature addresses an environment that will involve multiple suppliers and potentially tiers. It has a number of guidance statements regarding supplier control including references to DO-178 that could provide some management guidance of sub-tier suppliers. However, considering the environment is that of multitier or multipeer development it is weak in providing guidance directions towards sub-tier supplier oversight.

- The primary objective is for satisfying airworthiness with the ability to obtain incremental acceptance of individual items (including the core software) and hosted applications without compromising system safety.
- Makes a point in the purpose section that the certification applicant for a TC or STC should develop an effective system of communication among developers and system integrators. Very critical to programs where suppliers are from differing companies.
- The allocation of aircraft functions should be addressed in the IMA system architecture to ensure availability, integrity, and safety requirements are satisfied.
- Section 2.4 outlines tasks and outputs of the various stakeholders – at a high level general topic (interfaces, shared resource definitions, results of V&V, etc. **However**, the information flow is supplier up, not giving responsibility to the applicant or integrator for controlling the supplier designs.
- Section 3.4 makes the point of hosted applications coming from multiple suppliers using differing toolsets. It states that an IMA platform user's guide be provided to all application developers.

- Each developer is given responsibility for identifying potential failure modes of their application. Response to fault actions required by the platform should be identified.
- Module suppliers may develop the Module Requirements Specification based on assumptions for intended use. Assumptions should be documented in the MRS and validated during V&V.
- Section 4.6.2 a change management process should be established and coordinated between all stakeholders. The process should identify how levels of developers, suppliers, integrators, and certification applicants will coordinate and address changes.
- Requirements traceability should be performed.
- Section 5.1.2 The IMA system integrator is responsible for consolidation of results of system safety assessments performed by all suppliers ensuring the SSA results are consistent and compatible with the IMA SSA. Includes verifying PSSA/SSA results with testing of resource management, health monitoring, fault management and other protection features.
- Section 5.1 **defines stakeholder responsibilities** for safety assessments. Listing key items to be addressed and describes failure mode analyses requirements for each component of IMA. References ARP4754 and ARP-4761.
- Section 5.2 describes system development assurance guidelines and mechanisms. References DO-178 and DO-254.
- Fig 5 outlines a hierarchical layered functional/module/application layered PSAC and PHAC.
- The IMA system development process should consider the primary characteristics of IMA: flexible, reusable, and interoperable.

4.2.9 DO-326, Airworthiness Security Process Specification

DO-326 does not address multitier or supplier base.

- The document references DO-254, DO-178, ARP-4754, and ARP-4761 but does not address multitier or supplier aspects in development or in safety assurance. It spends some time providing an interaction with ARP-4754 so in a dependent fashion there is some indirect development guidance. It contains a diagram reflecting consistency with ARP 4754.
- Relative to DO-178 it does not make use of it but rather distinguishes levels of security from levels of safety as viewed in DO-178
- There is a flow of requirement validation artifacts up to the certification evidence.

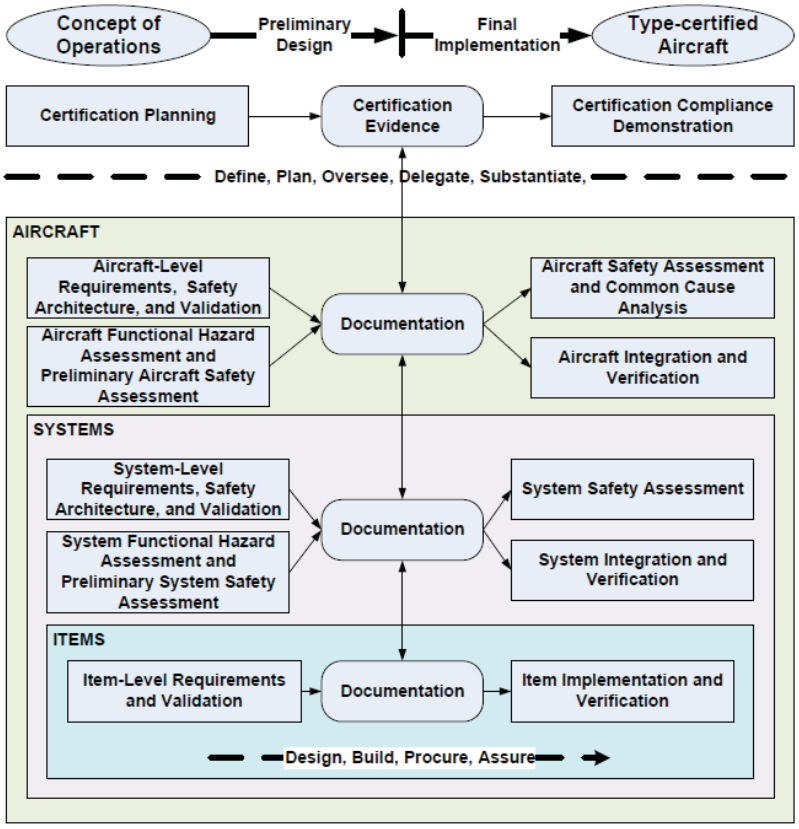


Figure 1-2 Generic Activities for Airworthiness Safety Process for Aircraft Development and Certification

Figure 5. DO-326 Airworthiness Safety Activities

4.3 Advisory Circulars

4.3.1 AC 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes

The AC clearly states that it is neither mandatory nor is it a regulation. However, the AC also states that "While these guidelines are not mandatory, they are derived from extensive FAA and industry experience in determining compliance with the relevant regulations. Whenever an applicant's proposed method of compliance differs from this guidance, the proposal should be coordinated with the Small Airplane Directorate Standards Staff, ACE-110. So there is an implication of prescription imposition. Any potential multitier guidance found could therefore be interpreted as more than just recommendations. However, the AC does not address multitier supplier networks or oversight of suppliers. The document does provide potential guidance awareness of areas for supplier or multitier supplier networks safety management. The AC references: ARP 4754A, ARP 4761, DO-178B, and DO-254.

- 1309 alludes to increasing complexity and integration difficulties experienced in assessing hazards that could result from complex systems.
- Complexity is defined as: "A system is "complex" when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods or structured

assessment methods." "Increased system complexity is often caused by such items as sophisticated components and multiple interrelationships."
    - FMEA and FTA are examples of such structured assessment methods.
    - A portion of compliance may be shown by the use of DAL's processes within DO-178 and DO-254.
    - The applicant is advised to perform analyses commensurate with the levels of complexity – however there is no definition of complexity levels.
- It is necessary to conduct a qualitative functional FTA or FMEA to show malfunctions are indeed remote in systems of high complexity.
- For simple and conventional installations it may be possible to assess a hazardous or catastrophic failure on the basis of experienced engineering judgment using only qualitative analysis.
- Installed systems should be evaluated by performing a safety assessment as shown in this AC.
- A four-tier set of aircraft classes is defined and associated levels of safety the aircraft must meet.
- In order to show compliance with the requirements of FAR Part 23.1309(a), (a)(1), (a)(2), and (a)(3) it will be necessary to verify that the installed systems and each item will cause no unacceptable adverse effects…
- The applicant should conduct bench, ground, and/or flight testing when necessary to validate hazard classifications
- The applicant must also discuss with the project ACO what aspects of this testing will need to be included in the FAA certification testing
- Compliance with § 23.1309(c) may be shown by analysis and, where necessary, by appropriate ground, flight, or simulator test.
- The applicant is responsible for identifying and classifying each failure condition and choosing the methods for safety assessment

4.3.2 AC 25.1309-1A, System Design and Analysis

Throughout the document AC 25.1309 addresses complexity concerns and means of assuring safety through analyses. The document addresses qualitative assessment and failure risk and consequence assessment decision rationales. It takes exception to its applicability to software errors stating "it is not feasible to assess the number or kinds of software errors, if any, that may remain after completion of system design, development, and test instead referring to DO-178A. The use of experienced judgment is clearly the cornerstone of the hazard assessments. Any new tier supplier is very likely not to have that necessary experience. The last issue of this document is 1988. An Arsenal update was attempted in 2002 but the effort was apparently abandoned. It does not address supplier oversight or tiered supplier management.

- The document addresses the difficulty in assessing hazards with the increase in the degree of system complexities, integration, and number of safety critical functions performed by systems.
    - For these reasons, structured means for showing compliance were introduced with 25.1309(b) and the associated guidance of 25.1309(b), (c), and (d).

    - These are the selective use of rational analyses to estimate quantitative probabilities, and the development of related criteria based on historical data of accidents and hazardous incidents caused or contributed to by failures expressed as numerical probability ranges associated with the terms used in 25.1309(b).
    - Both qualitative and quantitative assessment techniques are allowed.
- 1309 defines failure conditions in terms of severity; Minor, Major, Hazardous, Catastrophic. It defined an analysis of each level of severity, see Figure 6.
- Tests are not required to verify failure conditions that are postulated to be catastrophic.

Figure 1: Probability vs. Consequence Graph

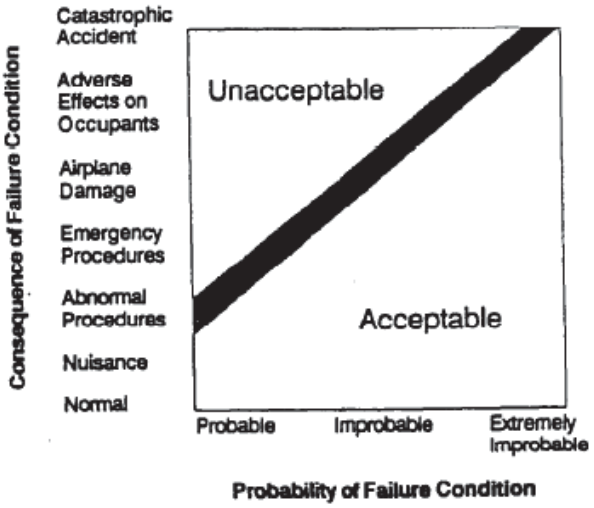


Figure 6. AC25.1309 Probability of Failure Condition Assessment

- Complexity is defined as: A system is considered to be complex if structured methods, of analysis are needed for a thorough and valid safety assessment. A structured method is very methodical and highly organized. Failure modes and effects, fault tree, and reliability block diagram analyses are examples of structured methods. Determination of complexity is an engineering judgment. **Note**: the judgment of complexity drives much of the subsequent hazard assessment and hazard mitigation effort and techniques.
- RAA: The responsibility for applying criteria, experienced operational judgment, and engineering judgment to identify and classify failure conditions is the applicant's responsibility.
    - The cognizant certification office provides oversight in providing concurrence with the applicant's assessments.
- It requires a safety assessment be made and specifies safety levels in qualitative terms. 7.b and 7.d are intended to insure an orderly and thorough evaluation of the effects on safety of any foreseeable failures.
    - Common cause and cascading effects should be considered.
- It allows that techniques can include the use of service experience data of similar previously approved systems through a qualitative analysis.

- A “fail-safe” design concept from Part 25 is outlined: integrity and quality, redundancy or backup system, isolation, proven reliability, failure warning, flight crew procedures, designed in failure effect limits, designed in failure path control, margins or safety factors, and error tolerance.

4.3.3 AC 25.1309 Arsenal, System Design and Analysis

The abandoned AC25.1309 Arsenal version was reviewed in terms of differences that might provide guidance for complex multitier avionics systems design and safety assurance. Certain enhancements within the document are also noted. No enhancements were added that address complex systems or multitier management. It did invoke the ARP safety guidelines and additional DO documents.

- The Arsenal version of AC 25.1309 references DO-178B, DO-160D, ARP 4754, and ARP 4761 and the complementary EUROCAE documents.
- Complexity is defined as: A system is Complex when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods.
    - The document alludes that some complex systems may be too difficult for exhaustive testing as a means of showing compliance. An alternate technique is allowed through the use of Development Assurance. Considerations for systems architectures for this purpose are appropriate.
    - It is recommended that a top down approach to assessing hazards is taken for complex systems.

4.3.4 AC 25.1329-1B, Approval of Flight Guidance Systems

AC25.1329-1B acknowledges the growth in complexity but does not offer control mechanisms in response other than alerts to higher risks. The AC is pretty specific on flight control system modes and their assessment. ARP 4754, ARP 4761, DO-178B, DO-254 are referenced. The document expresses the need to examine and test interfaces between systems in a manner which reflects a system functional and performance examination of the exchange of data between the systems where the greatest risk of failure reside. However, it does not address the multitier or supplier aspects of a system development.

- A system is complex when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods.
- The AC uses the term “should” and “should not” when discussing compliance to the AC itself, as the AC represents one, but not the only method of complying with the regulations. It uses “must” and “may not” when discussing compliance to 25.1329 and other rules as compliance to a rule is not optional.
- A design philosophy is espoused where the applicant should establish, document, and follow a design philosophy that support the intended operational use regarding FGS behavior, modes of operation, the pilot interface with controls, indications, alerts, and mode functionality.
- In demonstrating the intended function and performance of both the FGS and systems providing outer loop commands, the applicant needs to address potential inconsistencies between limits provided by the two different systems.
- The applicant should demonstrate the intended function and performance of the FGS across all possible functional interfaces.

- The use of simulator (which is a model of the systems installation environment) for demonstrations is an accepted means of aircraft/pilot situational evaluation.

4.3.5 AC 20-115C, Airborne Software Assurance

This AC was written to recognize DO-178C and it supplements and to provide guidance for transitioning to DO-178C. It also explains the use of DO-178C for TSO authorizations. It does not, however, address any of the issues associated with complex system design in multitier environments. This AC references a number of DO and AC documents as well as ARP 4754A.

- The AC states it was written for applicants, design approval holders, and developers of airborne systems and equipment containing software for type certificated aircraft, engines, and propellers. We recommend developers of TSO articles use this AC for software assurance (see paragraph 7).
- The AC recommends industry upgrade processes to DO-178C because DO-178B has areas that are not adequately addressed.
- Systems that have utilized earlier versions of DO-178 are referred to as legacy systems.
- The applicant PSAC should identify how DO-178C supplements will be applied.
- 8.c. If you are using models as defined in DO-331, section MB.1.0, as the basis for developing software, you should apply the guidance in DO-331. Section MB.6.8.1 identifies certain objectives and describes the activities for using model simulation to satisfy those objectives.

4.3.6 AC 20-145 Guidance for IMA that implement TSO-C153 Authorized Hardware Elements

Control of third party production of hardware is discussed. It is recommended that because of the complexity applicants conduct a structured formal analysis in accordance with ARP 4754 and ARP 4761. The appropriate design assurance should be achieved for each complex electronic device using DO-254. The use of third party software is not addressed by this AC. Although third party suppliers are discussed there really is little implication of oversight management of the design process of third party suppliers.

- Third party manufacturers are suppliers to the TC/STC/ATC/ASTC applicant and must be controlled during production by the applicant's quality assurance organization.
    - For this AC, a third-party manufacturer is a developer of a hardware module to be installed into a rack or cabinet that has TSO-C153 authorization, and who is not the rack or cabinet manufacturer nor the IMA system integrator.
    - Third-party hardware modules may or may not obtain TSO-C153 authorization. In order to not violate the TSO-C153 authorization granted for the rack or cabinet, the third-party manufacturer's hardware module must be shown to meet the environmental, interoperability, configuration management, and regulatory requirements of the installation
- Third party hardware module and/or software installed in the IMA system compliance to regulations is the responsibility of the applicant.
- Functional partitioning is recognized as a mechanism to reduce complexity and provide fault containment.

- The fidelity of simulator testing must be commensurate with the complexity of the task and degree of system integration at the aircraft level.
- **System Safety Assessment (SSA).** A systematic, comprehensive evaluation of the functions implemented by the IMA system, as installed in the aircraft, should be conducted to show that the relevant safety requirements identified in the PSSA have been met

4.3.7 AC 20-152, Design Assurance Guidance for Airborne Electronic Hardware

This AC addresses complex micro-coded components with design assurance levels of A, B, and C airworthiness appropriateness for the intended function. DO-254 is called out as the primary guidance document. The AC does not provide guidance for management or oversight of complex system design in multitier environments.

4.3.8 AC 20-170, IMA Dev, Verification, Integration, and Approval using DO-297 and TSO-C153

DO-297 is an integral part of AC 20-170. The AC applies to systems developed by a single company as well as those developed by multiple companies. However, this document does not address the issues associated with complex systems development in a multitier environment. It does reference DO-297 which by the nature of an IMA system considers the use of multitier suppliers even though DO-297 is weak in its description of oversight management of suppliers.

- This AC is intended to address IMA developer, integrator, and IMA application/component supplier.
- The applicant for a TSO authorization must control the design and quality of the parts, processes, and services provided by any supplier to the applicant.
- Complexity is defined as: Attribute of systems or items that makes their design and/or operation difficult to comprehend.
- The AC uses the term “should” when discussing compliance to the AC itself, as the AC represents one, but not the only method of complying with the regulations. It uses “must” when discussing compliance to the regulations, as compliance to a regulation is not optional.

4.4 AC 20-174 Development of Civil Aircraft Systems

The purpose of this AC is to recognize ARP-4754 as an acceptable method for establishing a development assurance process. The AC addresses the concern of possible development errors stemming from the ever increasing complexity of modern aircraft systems taking the route that ARP-4754 provides a structured methodology to address these concerns. There is, however, no additional guidance as to managing complexity or the development of systems in a multitier supplier environment. References are made to a number of RTCA documents; DO-178B, DO-254, and DO-297.

- This AC is not mandatory: and is not a regulation.
- This advisory circular (AC) recognizes the Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754A, Guidelines for Development of Civil Aircraft and Systems,

dated December 21, 2010, as an acceptable method for establishing a development assurance process.

- The AC was written for manufacturers who are seeking certification of their aircraft or aircraft system including Line Replaceable Units (LRU) and components.
- This AC addresses the concern of possible development errors due to the ever increasing complexity of modern aircraft and systems. In order to address this concern, a more structured methodology to mitigate development errors is described in SAE ARP 4754A.

4.4.1 AC 25-7C, Flight Test Guide for Certification of Transport Category Airplanes

AC 25-7C provides no oversight or management guidance of supplier or multitier supplier networks safety management. The AC is not mandatory nor does it constitute a regulation. Safety discussions are limited to performance related issues. The only reference to guidelines is to DO-160. Any modeling discussions are at the aircraft level.

- The use of FMEA is indicated for braking systems, multi-axis AHRS faults, anti-skid system, and control system failure assessments.
- It may be agreed that a simulation will be used to establish compliance with the performance and handling requirements. This simulation must be of a type and fidelity appropriate for the task and be validated by flight test data for the conditions of interest.
- The level of substantiation of the simulator to flight correlation should be commensurate with the level of compliance (i.e., the closer the case is to being non-compliant, the higher the required fidelity of the simulation).

4.5 FAA Orders

4.5.1 Order 8110.4C, Type Certification

TO 8110.4C is primarily written for internal use by the FAA, its designees, and delegated organizations. The order provides procedures and policy for the type certification of products. The document provides a high-level model of the certification events that typically make up the life cycle of an aircraft but does not address multitier aspects of avionics development and safety.

- The FAA encourages applicants to develop a plan for working with their geographic ACO that considers all safety aspects.
  1. Is a tool that helps determine how much attention the various safety aspects warrant and helps the FAA establish priorities that best promote safety,
  2. Addresses the unique characteristics of the applicant's affiliation with the FAA,
  3. Remains independent of specific projects,
  4. Identifies expectations and develops specific interface procedures between the applicant and the FAA, within the limits of FAA regulations and policy, and
  5. Helps the FAA build a constructive relationship with the applicant, including how the FAA and the applicant hold each other accountable.
- The document acknowledges that information will be lacking for complex projects at the time of the writing of a certification plan that is required at the time of application.

- The document alludes to the "experienced" applicant recognition of the value of addressing safety aspects. The implication is that the in-experienced will not. Project team members must build on their experience to identify critical issues – would be lacking in the in-experienced.
- Oversight and delegation is addressed (pg 37) as it relates to a DER. The level of FAA involvement will vary as the level of experience of a applicant or designee varies.
- The document references ARP-4761, and DO-160 only.

4.5.2 Order 8110.7D, Aircraft Certification Systems Evaluation Program

The purpose of this document is to apply standardized systems evaluations to the continued integrity of the design data after initial approval by the FAA at the PAH and associate facilities. It does not reevaluate previously approved design or safety data. It forms a good basis for production multitier supplier management assessments. However, the focus is on production quality assurance rather that design and development safety compliance assurance. As such it provides no guidance to the design and development of complex avionics systems in a multitier supplier network. Elements of production control and oversight could be redirected to form a basis of enhanced supplier control during the design phase.

Here just a few example evaluation statements. There are many.

- Section 6 Supplier Control
    - The term supplier includes distributors
    - Approved suppliers and criteria for supplier approval is evaluated.
    - Supplier's quality systems are reviewed.
    - How is authority for major inspection/material review delegated.
    - Section 6.11 asks the question if the evaluated facility flows down applicable technical and quality requirements to both US and international suppliers
    - AIR directorates implement an Aircraft Certification Systems Evaluation Program (ACSEP).
        - The ACSEP team leader may extend an ACSEP evaluation at PAH to key suppliers and subtier suppliers to verify that the Production Approval Holder (PAH) is satisfactorily controlling its suppliers.
    - The supplier audit records of its own suppliers is audited by the ACSEP.
- The supplier control mechanisms used for production if redirected could form a basis for enhanced supplier control during the design phase.

4.5.3 Order 8110.49, Software Approval Guidelines

This order establishes procedures for evaluating and approving aircraft software and software changes to approved aircraft software. It guides Aircraft Certification Service (AIR) field offices and Designated Engineering Representatives (DER) on how to apply DO-178B. It is applicable to TC, STC, ATC, ASTC, and TSO. ***This document nicely expresses the issues being addressed in this study: complex systems being developed in a multitier environment****. It does not provide additional insight on solutions to the issues but focuses on the use of oversight of the supplier and the conduct of reviews to address the concerns. It does not address MBD. Included is a supplier assessment table, although meant for the FAA, which could be useful to an applicant in determining a supplier and sub-tier suppler capability. It should be updated in light of DO-178C use of oversight.*

- This document is the only one that literally uses the words sub-tier suppliers.

- Chapter 13 “Properly Overseeing Suppliers”
  - This policy applies when an applicant uses suppliers and sub-tier suppliers to perform system and software development, verification, and certification activities. Confer with FAA system and software specialists as required.
  - Contemporary issues are listed
    - “Many TC/STC/TSOA applicants have shifted system and software development, verification, and certification activities onto their aircraft system suppliers and **sub-tier suppliers**. In the past, these suppliers participated in compliance activities only at their respective system, subsystem, or component levels. With airborne systems becoming increasingly more complex and integrated, and suppliers and sub-tier suppliers accepting these new responsibilities, **we are concerned that their lack of expertise could result in incomplete or deficient certification activities**.”
    - “Each responsibility that the applicant delegates to a supplier creates an interface with that supplier that needs to be validated and verified to ensure that the transition from the supplier’s processes to the applicant’s processes (or vice-versa) is accomplished correctly and accurately. Lack of proper validation and verification of life cycle data at the transition point has resulted in issues with regard to requirements, problem reporting, changes, etc.”
    - “Some certification tasks and activities may be performed in a foreign country. We can review the bilateral agreement with that country to determine if the certification authority may be able to help us in making a determination of compliance to the applicable FAA regulations. We can’t, however, request the certification authority of a country with which we do not have a bilateral agreement in place to assist us in making a determination of compliance to FAA regulations.”
      - **Note**: this does not address the additional issue of cultural differences affecting the engineering process. Assumptions that the engineering thought process, rigor, open questioning/challenges to design and understanding are the same as in the US even for those educated in an American college are the same is often wrong.
    - “Finally, retention of substantiating data, such as software life cycle data and other certification and compliance data, is a critical part of the certification process. When this data is retained by a foreign supplier, it may not be readily available to us. This may also affect the continued operational safety of the aircraft and its systems, especially with regard to in-service problems (service difficulties), problem resolution (service bulletins), and mandatory corrections (airworthiness directives).”
  - “The applicant should create oversight plans and procedures that will ensure all suppliers and sub-tier suppliers will comply with all regulations, policy, guidance, agreements, and standards that apply to the certification program.” This includes all the publications that the applicant is responsible to comply with ACs, Orders, Issue papers, etc.
    - The past experience, knowledge of the certification process, software development capability, and application complexity determine the level of oversight deemed necessary from the FAA.
  - The type and number of software reviews will depend on the software level of the project, the amount and quality of DER support, the experience and history of the applicant and/or software developer, service difficulty history, and several other factors. Chapter 3 of this order covers specific guidelines for determining the level of FAA involvement.

- The applicant's planning documents, such as certification plans and PSACs, should describe how the applicant will have visibility into their suppliers' and sub-tier suppliers' activities. This includes commercial off-the-shelf software component suppliers and vendors.
  - The plan should address how the applicant will ensure that all applicable regulations, policy, plans, standards, issue papers, partnership for safety plans, and memoranda of agreement are conveyed to, coordinated with, and complied with by prime and sub-tier suppliers.
  - The plan should address how the system components will be integrated, and who will be responsible for validating and verifying the software and the integrated system.
  - The plan should identify who the designees are and what their responsibilities are, who the focal points are, and how their activities will be coordinated and communicated.
  - The plan should establish a system to track problem reports. It should describe how problems will be reported between the applicant and all levels of suppliers. The plan should describe how the designee(s) will oversee problem reporting.
  - The plan should identify who will be responsible for ensuring that all integration verification activities between all levels of suppliers comply with applicable guidance. It should describe how the designee(s) will oversee the verification process.
  - The plan should describe the procedures and tools to aid configuration management of all software life cycle data. It should describe how configuration control will be maintained across all sub-tier suppliers, including those in foreign locations, and how designees will oversee configuration management.
  - Compliance substantiation and data retention. The plan should describe how the applicant will ensure that all supplier and sub-tier supplier compliance findings are substantiated and retained for the program.
- The applicant's supplier management plan (or equivalent plans) should address the concern of newly created interfaces with a supplier when delegation occurs regarding the transition of life cycle data between the applicant's processes and the suppliers' processes.
- Sampling is the primary means of assessing the compliance of the software processes and data.
- Both low-level requirements are to be documented, reviewed, and be traceable to high-lvel requirements and system requirements.

- Chapter 14 Software Problem Reporting
  - This policy applies when an applicant's suppliers and sub-tier suppliers will be responsible for managing problems detected during the development of aircraft systems implemented with software.
  - The applicant's suppliers and sub-tier suppliers may not have the expertise to determine whether problems with their component(s) will have safety, functional, or operational impacts on the aircraft or airborne system in which they are used.
    - Due to these concerns, the applicant will need to actively participate in the oversight of problem reporting processes to ensure that problems are properly identified, reported, and resolved.
  - The applicant should discuss in their Software Configuration Management Plan, or other appropriate planning documents, how they will oversee their supplier's and sub-tier supplier's software problem reporting process. The plan should describe the supplier and

sub-tier supplier problem reporting processes, how notification of problems is flowed up the hierarchy, how appropriate disciplines will be involved in reviewing report resolutions, and establish the criteria for acceptability of closure or deferment.

- Figure 3-2 Other Relevant Data provides a good experience assessment table that may be useful to an applicant in determining supplier and sub-tier supplier capability in receiving a delegation of design authority. This is intended for FAA determination of Level of FAA Involvement (LOFI) but could be useful to industry.

4.5.4 Order 8110.105, Simple and Complex Electronic Hardware Approval Guidance

Order 8110.115 is primarily written for internal use by the FAA. It assists in determination of FAA involvement in a project, types of reviews, and how much delegation of oversight is given to designees. This document includes an assessment checklist of developer experience to determine the level of involvement necessary by the FAA that could be useful to the industry as a potential supplier capability assessment. It does not provide guidance for the complexity issues and multitier development issues of this study, although the checklist accesses the system complexity when determining oversight. The use of MBD is not addressed.

- This document was written to supplement DO-254 to give guidance for approving both simple and complex custom micro-coded components.
- There should be regular contact between the applicant, the supplier, and the cognizant FAA office. The FAA must monitor both the applicant and the hardware developer.
- AC 20-152 recognized RTCA/DO-254 as an acceptable means to gain FAA approval of complex custom micro-coded components; the AC doesn't recognize RTCA/DO-254 as an acceptable means to gain design assurance for COTS components.
- The TO distinguishes between COTS hardware (DO-254 Section 11.2) and COTS IP which DO-254 does not address. The topic here is the assurance that the applicant and developer show airworthiness compliance with the use of COTS IP.
    - As COTS IP is likely to have sufficient documentation to support assurance the applicant may need to utilize architectural mitigation, component verification, testing, analysis, and other life cycle data to demonstrate the IP is free from anomalous behavior and meets airworthiness requirements.
- The availability of experienced hardware designers is a consideration for hardware FAA involvement. The first three criteria in Figure 3-2 of 8110.105 are an assessment of the applicant, developer certification experience.
- Fig 3-2 is a score card of an applicant/Developer Hardware Certification Experience. Considering the dependence on experience from FAR, through 1309 and on to the ARP, and RTCA documents, an expansion of this guidance to industry as a key item for managing complex multitier developments should be considered.

4.5.5 Order 8130.2, (Draft) Airworthiness Certification of Aircraft and Related Products

This order is focused on: processes for airworthiness certification and maintenance activities, responsibility assignments, but all at the aircraft level. With the focus on the high level applicant, FAA interaction, and designee responsibilities it does not address the multitier design and development issues of complex avionics. There are a few items of delegation discussed.

- The document addresses responsibilities for a number of areas: ASI, designees, registration, etc.
- Delegation of authority (RAA): The FAA is authorized to delegate private persons or organizations to act as representatives and issue airworthiness certificates and related approvals under 14 CFR part 183. There is no discussion of subsequent delegation in the form of tiered DMIR or DAR (pg 2-1). Other than:
    - The authority of a DMIR must be specifically linked to a production approval holder (PAH) or PAH's approved supplier.
    - An organization designation authorization (ODA) may be approved to issue airworthiness certificates, airworthiness approvals, conformity certifications, and export approvals (pg2-2).
        - The organization management team (OMT) is the group of FAA personnel from the managing MIDO responsible for the oversight of the ODA.
    - A designated manufacturing inspection representative (DMIR) or designated airworthiness representative (DAR) may issue standard and special airworthiness certificates, airworthiness approvals.
    - The designee must obtain in writing from the regional MIDO, FSDO, or CMO any limitations on special airworthiness certificates before issuance.
    - Delegation of inspection and certification, relating to conformity, can be delegated to a supplier by the applicant – a letter of delegation must be submitted to the FAA (pg 3-2).
- Applicant is responsible for providing all supplier affidavits to the FAA.

4.5.6 TSO-C153, Integrated Modular Avionics Hardware Elements

There is no mention of suppliers, oversight, or delegation in the document. Neither is complexity, requirements management, or model based development addressed. It therefore does not provide any guidance for complex avionics developed in a multitier supplier environment.

- ARP 4754, DO160D, DO-254, and DO-178B are referenced
- An application to the ACO includes delivery of the PHAC and PSAC.

4.6 Mil Standards

4.6.1 Mil-Std-882E, Standard Practice for System Safety

In place of the terms suppliers, oversight, or delegation the document discusses the responsibilities of the developer and the interaction with the program manager. Oversight is discussed in the form of monitoring the developer's system safety activities with review and approval of the delivered artifacts. Complexity, requirements management, or model based development are not addressed. As such the

document addresses the safety management between the manager and the developer at one tier. The principles described between the manager and developer could be applied at the developer and sub-tier developer as well. The use of model simulation for safety testing is allowed, however, the subject of MBD is not addressed.

- The developer is to document an approved system safety engineering approach. This includes a description of how hazards and mishap risk are communicated to the acceptance authority.
    - Describe specific analysis techniques and formats to be used in qualitative or quantitative assessments of hazards, their causes, and effects.
- The document states it is impossible or impractical to design a complex system completely hazard-free.
- The document proposes a proficiency certification process be used as safety critical tasks may require personnel proficiency. Experience indicates that the degree of safety achieved in a system is directly dependent upon the emphasis given to application of professional knowledge and specialized skills together with the principles and methods of engineering design and analysis.
    - Safety critical tasks may require personnel proficiency; if so, the developer should propose a proficiency certification process to be used.
- Establish, plan, organize, implement, and maintain an effective system safety effort that is integrated into all life cycle phases
- Ensure that system safety planning is documented to provide all program participants with visibility into how the system safety effort is to be conducted.
- Establish definitive safety requirements for the procurement, development, and sustainment of the system.
- Monitor the developer's system safety activities and review and approve.
- Ensure that the appropriate system specifications are updated to reflect results of analyses, tests, and evaluations.
- Establish system safety teams to assist the program manager in developing and implementing a system safety effort.
- Quantitative requirements are usually expressed as a failure or mishap rate.
- Oversight is described in terms of: Monitor the developer's system safety activities and review and approve delivered data in a timely manner, if applicable, to ensure adequate performance and compliance with safety requirements.
- Where costs for safety testing would be prohibitive, safety characteristics or procedures may be verified by engineering analyses, analogy, laboratory test, functional mockups, or subscale/model simulation. Integrate testing of safety systems into appropriate system test and demonstration plans to the maximum extent possible.

4.7 Industry Practices

4.7.1 FAA and Industry Guide to Product Certification

This document has quite a bit of discussion on management of design and safety for a system development. Oversight and delegation guidelines are given throughout the document; however they only address the first tier supplier. Although it does not specifically address multitier supplier development the principles could be applied by the applicant and the supplier. It fails on the count of multitier in that it focuses on foreign suppliers almost to the exclusion of the management of US suppliers. Although it contains considerable valuable guidelines its adherence or enforcement is not clear. It is up to the applicant to develop the content of a Partnership for Safety Plan (PSP) and Project Specific Certification Plan (PSCP). It is off of these documents that an applicant is likely to generate the necessary sub-tier supplier assessment and oversight management. The document references DO-160 and DO-178B but no ARP documents.

- This guide is focused on large and complex systems. It identifies an FAA Chief Scientific and Technical Advisor who is to provide technical guidance.
    - The FAA Directorate will establish operating norms. These are affected by many factors including complexity and degree of delegation.
- The document provides guidelines for a management, delegation, and oversight structure in accordance and partnership with the FAA.
- The document discusses supplier identification, risk evaluation, and management but only in terms of foreign suppliers. Little if any is said regarding management of US suppliers.
- The experience of team members is relied upon to identify critical issues. The FAA determines its involvement based on that experience.
- The FAA maintains its control through oversight of the Designees. Descriptions of areas and mechanisms of oversight are given throughout the document.
    - Defined oversight criteria and defined delegations are deliverables to the FAA.
    - The FAA and the applicant agree to manage all designee activity within the regulations and policy regarding designee appointment, procedures, and oversight.
    - It is necessary to have all stakeholders in the delegation process agree on the extent of delegation, the procedures, and the degree of delegation oversight to be used in each project.
- Appendix VIII Delegation and Planning
    - The designee is given some guidance in classifying findings into categories for the purpose of determining the level of FAA oversight.
    - There is no multitier delegation guidance given.
- A number of documents are outlined that are along the lines of complex multitier supplier management.
    - Partnership for Safety Plan (PSP) is a document defining a working relationship between an applicant and the FAA. It addresses corporate planning, communication and coordination, delegation, and operating norms.

- Project Specific Certification Plan (PSCP) defines a certification plan between the FAA and the applicant. It defines the certification basis and means of compliance. Delegation and oversight is addressed only at the applicant tier.

4.7.2 Contractor Supplier Assessment and Oversight processes

If a contractor has a supplier assessment and oversight process their oversight process will generally summarize the methods and processes to be used by the contractor to perform supplier assessments and determine the level of technical oversight, citing assessment of the suppliers control of the design process for compliance with ARP 4754, DO-178, DO-200, and/or DO-254. Supplier selection and management processes may be declared outside the scope of the Supplier Assessment and Oversight Process leaving those controls to be managed through a flowed down PSCP, PSAC, and PHAC.

Weaknesses found in these oversight processes are in;

1) *the assumption that management and technical oversight will take place through the flow down of the PSCP, PSAC, and PHAC,*
2) *they tend to focus on on-going supplier performance assessment that will determine/adjust the percentage of oversight deemed necessary with a bent towards reducing oversight and design participation through a sampling metric,*
3) *they generally fall short of providing supplier oversight guidance save in the assessments of their performance after they are on contract,*
4) *the net impetus of this approach is a focus on supplier defect leakage rather than on supplier design oversight.*

- The purpose of this document is to define a process to assess the capability of a supplier to develop and verify airborne navigation/terrain databases, electronic hardware, software or systems. The assessment will result in a rating to be used as a guide for "Contractor" Project Teams to determine the level of Technical Oversight required for the suppliers. The results of the assessments can be used by the DER/AR/UM and PDQA organizations to determine the focus areas for their audits and to ensure that the appropriate level of Technical Oversight takes place.
- A multistep supplier assessment process is described in 2.1.
    - The assessment process will result in an Oversight Rating for suppliers. The Oversight Rating is generated through completion of the Supplier Ratings Tables, as described in the Supplier Assessment and Rating Form.
- **Supplier definition**: Any entity involved in the engineering development or verification of airborne navigation / terrain databases, electronic hardware, software or systems that is to be used in an airborne installation for Contractor and certified by the FAA or other regulatory authority.
    - This includes all levels of sub-tier suppliers.
    - This definition applies to Global Contractor Suppliers as well as Non-Contractor Companies.
    - This definition does not apply to Suppliers that are the TSO Leads or already hold the TSO.

- Suppliers that outsource to other suppliers must inform the Contractor Lead Site of their intent to outsource. If a sub-tier supplier at any level is selected for new work, then they must be assessed and receive oversight per this process to include technical, DER/AR/UM/TSO Specialist, and PDQA oversight. The sub-tier supplier will receive a rating and oversight percentage specific to their business location (e.g., the parent supplier at one location will be separately rated from their sub-tier supplier at another location). The Lead Site is responsible for oversight of all tiers of suppliers.
- Certification information addressing outsourcing and the use of suppliers will be documented per the Contractor Systems Certification Plan, PSAC, PHAC, SAS, and HAS templates as applicable.
- **Oversight Scope and Purpose**: This documents primary purpose is to assure oversight of suppliers and sub-tier suppliers occurs.
    - This document summarizes the methods and the process to be used to perform assessments and determine the level of Technical Oversight for suppliers that develop and/or verify airborne navigation/terrain databases, electronic hardware, software or systems for compliance with ARP 4754, RTCA/DO-178( ), DO-200( ) and/or DO-254( ).
    - The supplier ratings and oversight percentages generated by the assessments will be used by engineering organizations to provide appropriate Technical Oversight of a supplier's work and will provide information that will be used during the supplier selection process.
    - **HOWEVER**: The purpose statement states that: Supplier selection and management processes are outside the scope of the Supplier Assessment and Oversight Process. Yet a section 3 is included which describes the Oversight Process.
    - The purpose of this document is to define a process to assess the capability of a supplier to develop and verify airborne avionics systems. A rating is developed to be used as a guide for Applications Project Teams to determine the level of Technical Oversight required for the suppliers. The results of the assessments can be used to determine the focus areas for audits and to ensure that the appropriate level of Technical Oversight takes place.
- **Oversight Process:**
    - Supplier and sub-tier supplier oversight will be performed by the Lead Site/Non-Lead Site Oversight Engineers, PDQA, and the project DER/AR/UM.
    - The Lead Site that is applying for TSO, TC, or STC performs the supplier assessment.
- **Technical Oversight**:
    - Technical oversight consists of reviews conducted on a percentage basis of the supplier-produced artifacts. [Note: there is no mention of design participation]
    - Three review models are described:
        - Co-reviews, oversight engineer participates with supplier reviews but holds defects found until supplier discloses his/her defects found list.

        - Re-reviews, oversight engineer conducts a review on his own and discloses defects not identified by supplier (defect leakage) and records supplier performance data.
        - Co-Development, 100% of all technical reviews include oversight engineering in the role as a moderator. This model is not recommended as it does not develop supplier performance data.
    - A formula/table is provided to determine the level of oversight necessary based upon an oversight rating.
    - Oversight takes on the form of taking a sampling of the supplier produced artifacts.
    - Oversight engineer's qualification is defined as a highly competent engineer in the relevant product area.
- **DER Oversight**:
    - Per the Contractor DER Handbook DER/AR/UM oversight shall be conducted on the work produced by all suppliers.
        - The level of effort will include appropriate coverage of the following:
            - Higher criticality functions and safety features
            - Functional areas
            - Complex implementation
            - New or previously developed software or complex hardware
            - Work produced with and without Technical Oversight.
    - A representative sampling of the work performed by a supplier shall be audited.

4.7.3 Contractor Partnership for Safety Plan

An outline for this document can be found in FAA and Industry Guide to Product Certification, Appendix I. The document is a general MOA that the FAA and Contractor will work together in a certain manner. Generally non-prescriptive there are a number of "will" statements regarding execution. From a complex system multitier supplier perspective there is only a mention of "extent of delegation", and "supplier or supplier partner" internal requirements mentioned. As this PSP is directed only at defining the interfaces between Contractor and the FAA, it does not address supplier or developer control and management. It provides no guidance to this study of complex avionics being developed in a multitier environment.

- While at the highest levels, safety is of the utmost priority for both organizations, compliance to the regulations and conformance of products to the design as well as internal requirements will ultimately be the key drive to produce safe products.
- The document describes the organizations internal structure and responsibilities of each.
- Describes the framework for how programs requiring FAA approval or acceptance are to be conducted.
- Subservient document to regulations
- Contractor typical requirements:
    - Type Certificate (TC)
    - Supplemental Type Certificate (STC)
    - Technical Standard Order Authorization (TSOA)

- Production Certificate (PC)
- Parts Manufacturer Approval (PMA)
- DO-200 Letter of Acceptance (LOA)
- Major Repair, Major Alteration, and Airworthiness Function (MRA)

- FAA office interactions:
  - Aircraft Certification Offices (ACO)
  - Manufacturing Inspection District Offices (MIDO)
  - Aircraft Evaluation Groups (AEGs)
  - Flight Standards Office (FSDO)
- Organizational structures and responsibilities
  - Describes the Contractors overall organizational structure in general terms of function.

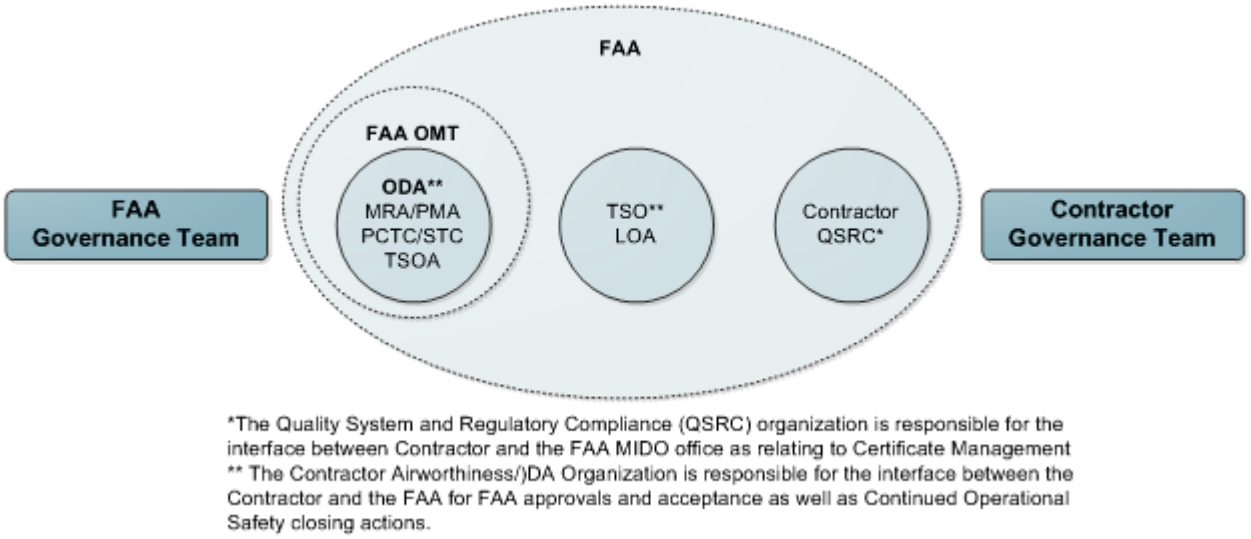


Figure 7. Safety Organization Interactions

  - Describes the Contractor governance team and describes top level responsibilities.
  - Describes the FAA governance team structure and primary responsibilities
- Communication and coordination
  - Defines types of communication: structured meetings, electronic information, telecommunication, management reviews, project specific technical coordination, regular project specific status awareness
  - Defines an issue resolution process
  - Operational safety database is described that collects history and issues
  - Accident/incident investigation activities are described and responsibility assigned.
- Gives an overview of compliance activities
- Gives an overview of production quality activities
- Defines critical effective program management: oversight, planning, communication, and documentation areas in:
  - Certification basis
  - PSCP

- Type design issues, production certification issues, and means of compliance
- Issue papers, exemptions, special conditions, equivalent safety proposals, limitations applicable in-service maintenance/operational history
- Pass/fail criteria for certification testing
- Critical assumptions, installation interface issues, data for Airworthiness Limitations Section of instructions for Continued Airworthiness
- Conformity inspection requirements which identify major/critical manufacturing processes, new materials and new technologies
- Extent of delegation
- Internal requirements (supplier or supplier-partners, international authorities involvement, validation needs, undue burden assessment

4.7.4 Developer PSAC

This PSAC was written for a project in which the 1st tier supplier to the applicant outsourced development of functions to sub-tier corporations located in the US, Europe, and Asia. It was a complex critical component for the aircraft. The document outlines oversight of the sub-tier suppliers in terms of SQA and DER artifact inspections with the 1st level suppliers DERs having oversight of the sub-tier supplier DERs. It is a good example of management of complex systems development in a multitier environment and reflects on the experience of the 1st tier supplier understanding of the management needs not outlined in the regulations or guidelines.

***MBD**: It made partial use of MBD practices in the flow down of requirements from the applicant and through to the sub-tier suppliers. Proper use of MBD should span all the tiers in order to obtain its full value. The process defines a component or unit level verification although the guidelines do not drive the developer to this conclusion.*

- Sub-tier supplier PSAC documents are called out by publication number.
- This PSAC outlines supplier requirements responsibilities.
- Documents provided by sub-tier suppliers are inspected by PDQA and DERs using engineering practices defined in the SDP to insure documents conform to DO-178B. Changes fall under the management of the System Change Request (SCR) and System/Software Review Board (SSRB).
- The Contractor DERs will also conduct audits to assure that the sub-tier suppliers adhere to the applicable regulations, policies, plans, standards, and agreements.
- SQA provides oversight of sub-tier suppliers.
- Oversight of the sub-tier supplier DERs are assigned specific names within the Contractor organization DERs.
- The Contractor DERs will audit a sampling of artifacts produced by the sub-tier supplier. This includes oversight of the corporation's foreign developers.
- The document references DO-178B, DO-248B, DO-254, ARP-4754.
- The document provides a high level software architecture and a high level list of systems functions allocated to major software blocks. Textual outline coupled with an architecture figure.
- Traceability to FAA issue papers is provided.

- The SRDD is developed to include both the high-level and low-level software requirements. The software requirements in the SRDD are explicitly traced to the appropriate OEM SCD and Contractor SRS system requirements. Software requirements contained in the SRDD consist of both traditional textual requirements as well as requirements expressed in requirements models. Models are used for functionality that is algorithmic in nature as well as for combinational logic. The requirements models are developed using the MATLAB/Simulink/Stateflow tool suite.
- Contractor will write high level textual requirements applicable to the software functionality allocated. Models will then be created based on the textual requirements. The models, which are the low level software requirements, are the final items that engineers create and edit prior to machine creation of the executable object code. The models are in machine readable format and are used as input into an autocode generator. The output of the autocode generator is then compiled/linked into an executable image. This executable is then tested with a suite of software requirements-based tests. The model based development process is shown in Figure 8.

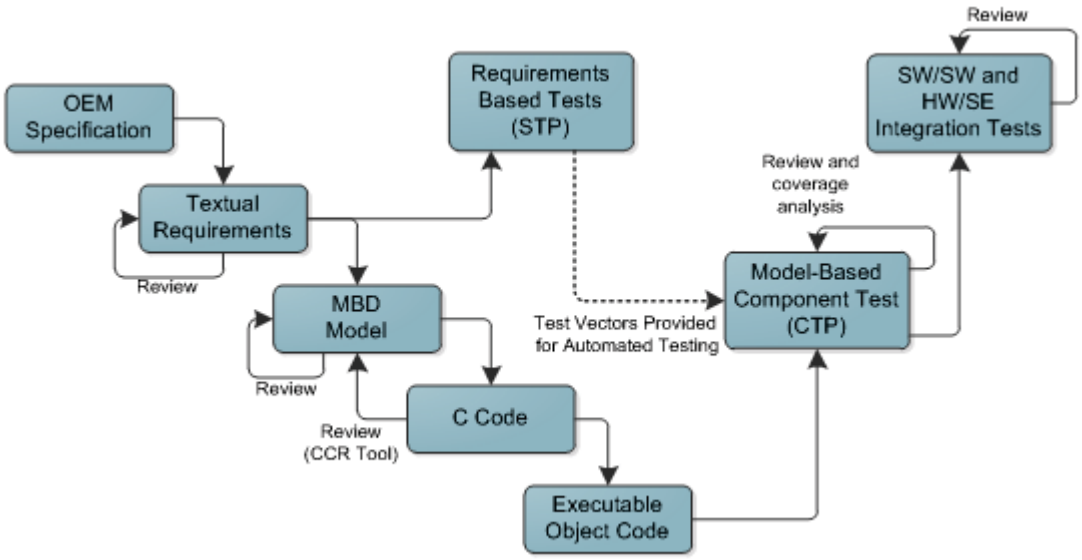


Figure 8. Textually Driven Model Based Development

- The OEM model-based development process differs in that the models are created from diagrams in the OEM Specification Control Drawing (SCD), rather than textual requirements. The planned development process is shown in Figure 9 below.

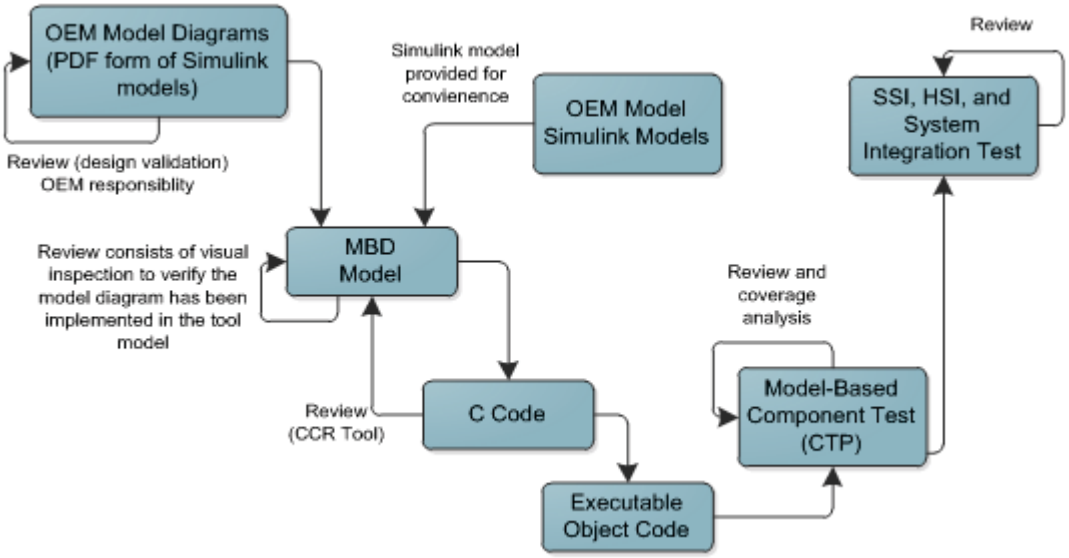


Figure 9. Hardcopy Model Driven Model Based Development

- Software requirements are formally inspected and accepted using the applicable inspection process, applicable requirements standards, and associated checklists. Prior to formal inspection, the SRDD section or model is placed under configuration control. From that point on, changes to the document section or model are controlled through System Change Requests (SCRs) and the System/Software Review Board (SSRB). More detailed information about the software requirements process can be found in the Software Development Plan. For comparison purposes, the hand code development process follows a traditional DO-178B development process. The planned development process is shown in Figure 10.

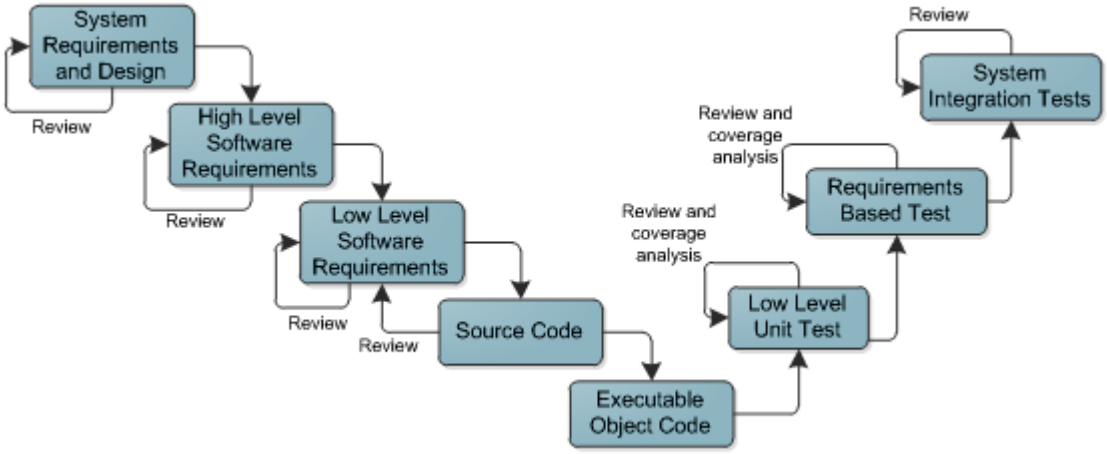


Figure 10. Hand-coded development

- Hand-Generated Code – For functionality that is defined using textual requirements, without the use of models, a software engineer develops the software source code by translating the requirements into the appropriate source code language. After a source code component has

been developed, it is formally inspected and accepted using the applicable inspection process, applicable coding standards, and associated checklists.

- Model-Generated Code – For functionality that is defined in the SRDD using requirements models, C source code is generated using a modeling tool suite. After each source code component is generated, it is verified against the model using a qualified verification tool.
- A System Modeling Tool (SMT) is used to design and manage the time and space partitioning.
- Fig 6-2 and the general process described in the PSAC reflects a hole that should be filled for multitier applications, that is the higher tier requirements flow down should be in the form of a model – not text, nor even a graphic to be captured. It should be an executable low fidelity model of the requirements.
- The PSAC drives verification of model generated code to the component level – With a qualified verification tool. Although it is an approach, this is not required by the regulatory documents and could be a big certification cost driver. Furthermore this approach could introduce risk from the assumption that the function has been validated at the lower level.

4.7.5 Sample Developer PHAC

This PHAC was written for a project in which the 1st tier supplier to the applicant outsourced development of functions to one sub-tier corporation located in Europe. There was also foreign development by the contractor's corporate engineers in a Contractors European office. All hardware components were evaluated as complex critical items for the aircraft. The document outlines oversight of the sub-tier suppliers in terms of PDQA and DER artifact inspections. It provides an example of management of complex systems development in a multitier environment and reflects on the experience of the 1st tier supplier understanding of the management needs not outlined in the regulations or guidelines. It is not as strong in multitier management as is the PSAC.

- The sub-tier supplier PHAC is referenced by document number.
- All PLDs and ASICs used in these designs are considered complex per the definition in section 1.6 of RTCA DO-254 (reference 400).
- The document spends considerable time in the identification of complex components and associated DAL. It identifies lifecycle tools for complex device development.
- The design goals restrict the use of complex COTS devices. A specific allowable list is provided.
- The Contractor has an independent organization with processes to support overall development process assurance, a Product Development Quality Assurance (PDQA) department
- Designated Engineering Representatives (DERs) that have oversight are called out by name.
- Certification Liaison and Process Assurance
    - The Contractor DERs will provide oversight of the lower tier Supplier Quality Assurance plans and activities at key phases of the development and verification process.
    - The Contractor DERs will provide oversight of the Common Partition PLD development activities by both its Supplier and the Contractor in close coordination with the certification authorities and OEM.
    - The contractor's engineers from its European office were involved in requirements based test case procedure development. Hardware process assurance oversight for the

Contractors European engineers will be provided by the European office and Contractors US site PDQA engineers.

- DO-254, DO-178B, ARP-4754, ARP-4761 were referenced.
- Requirements flow down is through a Specification Control Drawing (SCD) and Interface Control Document (ICD). The Software Requirements Specification (SRS) also feeds the requirements.
- Systems functional allocation to hardware is provided in the document in terms of major hardware components and what systems functions are provided by or reside on those components.

4.7.6 INCOSE-TP-2003-002-03.2.1 System Engineering Handbook

The document recognizes that complexity is a major issue but does not provide a means to manage complexity other than rigor in the decision gate review and assessment processes. There is only recognition of a single layer of suppliers. No oversight of suppliers is mentioned. No references to any RTCA or ARP documents are made. INCOSE provides no insight on the topic of this research.

- Only in the supply process activities is a sub-tier supplier mentioned: "Maintain communications with acquirer, sub-suppliers, stakeholders, and other organizations regarding the project."
- Complexity is a major issue. – As system elements are added, the complexity of system interaction grows in a non-linear fashion. Furthermore, conflicting or missing interface standards can make it hard to define data exchanges across system element interfaces.
- Lean Systems Engineering: The application of lean principles, practices and tools to SE to enhance the delivery of value to the system's stakeholders.
- Standards have also grown in number and complexity over time, yet compliance with standards remains one of the keys to interoperability.
- Decision Gates are specified as guidance decision points following a review by qualified experts and stakeholders to establish compliance with a requirement. There is a heavy process in conducting peer reviews, inspections, testing, and conformity audits to insure compliance with requirements.
- Experience in the systems engineer leading a development is valued.

4.8 FAA Issue Papers

Issue papers are generally project specific so do not provide assistance to industry across the board for guidance. So, no issue papers were reviewed.

4.9 Papers

4.9.1 787 Procurement Case Study - Tang and Zimmerman

Under the 787 Boeing instituted a risk sharing approach and tiered supply chain to contracting approximately 50 tier-1 suppliers who also served as integrators of subsystems produced by tier-2 suppliers. These tier-1 suppliers were responsible for delivering complete systems to Boeing. The paper highlights two primary issues with Boeings institution of this multitier network of suppliers that are applicable to any structure with multiple tiers of suppliers; 1) care in selection of tier-1 supplier

experience and capability, and 2) oversight through the multi-levels of the resulting tiered structure. It also brings out several issues with assumptions; 1) assumed alignment in technical and management with the OEM goals and principles, 2) lack of cultural impact understanding, 3) capability and experience of the supplier including the engineering expertise as well as the depth of resources within the supplier. As a paper it does not provide regulatory guidance, however it highlights issues associated with the use of multitier developers and recommends greater level of OEM involvement in tier-1 supplier selection of sub-tier suppliers. It also recommends an oversight working team with visibility across the tiers. These recommendations apply to this study.

Issues

- Technology: Invisibility of development issues with tier-1 suppliers partners to the prime
- Supply: Tier-1 suppliers outsource development tasks to tier-2 partners, which may not have technical know-how, and without Boeing's knowledge.
- Overreliance on tier-1 partners to coordinate their development tasks with their suppliers further down the supply chain.
- Boeing reactive responses:
    - Purchase company at the bottleneck stage
    - Send hundreds of engineers to solve issues with underperforming partners at their sites (tiers-1 through tier-3).

Recommendations

- Greater level of involvement with strategic partner selection and relationship vetting up front. Spend more effort on evaluating each supplier technical ability and management capabilities.
    - Require participation in lower tier vetting of suppliers.
- Establish a cross tier management working team. Appoint individuals at key integration collection points to manage design throughout the lifecycle.

Tiered structure events:

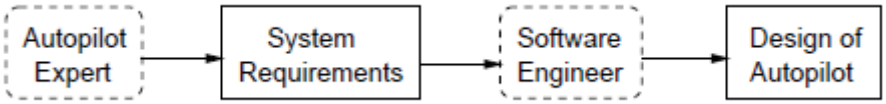
- In one case a tier-1 supplier hired a tier-2 supplier to serve as system integrator without informing Boeing.
- As Boeing outsourced more, communication and coordination between Boeing and its suppliers became critical for managing the progress of the 787 development program. To facilitate the coordination and collaboration among suppliers and Boeing, Boeing implemented a web-based tool called Exostar
    - In several cases due to cultural differences tier-2 and tier-3 suppliers did not enter accurate and timely data into a database system resulting in delays.
- Upon realization that some tier-1 strategic suppliers did not have the necessary know-how to develop the systems or experience in managing tier-2 suppliers Boeing took over the supplier for direct control.
- In some cases the limited resources of a tier-1 supplier were taxed by other delays to the point they were unable to continue providing their critical subsystems without subsidy from Boeing.

- The strategy of relying on suppliers for subassembly proved to be too risky for Boeing in certain circumstances and resulted in Boeing having to perform the work themselves. For instance, Boeing sent hundreds of its engineers to the sites of various tier-1, tier-2, or tier-3 suppliers worldwide to solve various technical problems that appeared to be the root cause of the delay in the 787's development.
- Expecting Tier 1 suppliers to naturally align with Boeing expectations was clearly unrealistic. Engineering design challenges and resolutions clearly required additional unplanned resources and escalated costs for the overall project.
- Computer Network Security Issues: The current configuration of electronics on the Dreamliner puts passenger electronic entertainment on the same computer network as the flight control system. This raises a security concern for terrorist attacks (Zetter 2008).

4.9.2 Use of Safety Cases in Cert and Regulation - Leveson

This paper does not address multitier supplier issues or complexity directly. Neither does it address delegation of design tasks or integration of subsystems and the oversight of these activities, although it does allude to local government oversight through inspections and audits. It does not reference any RTCA papers or ARP documents and procedures. There are however, certain elements identified in the paper that that are applicable to increasing the safety of multitier complex systems.

- The extra communication step between the engineer and the software developer is the source of the most serious problems with software today.



- Both prescriptive and performance based requirements and process management are necessary for complex systems. MBD can address both. It creates the model by which prescriptive coverage can be validated. It creates the model by which performance is validated. It creates the model by which human interaction can be validated. It creates the model by which environmental interactions (traffic, etc) can be validated. It creates the model by which requirements are flowed down without interpretation.
- General issues of the day:
  - Design is directed by those unskilled in the art
  - Control of design is relegated to implementers without system level oversight i.e. no systems engineers
  - As the system oversight is missing the KISS principle fails and results in no one that understands the system – creating high risk for complex and multitier systems.
- Failure to assess properly from an “out of sight, out of mind” phenomenon can develop at each tier. If the representation is not complete the likelihood of recognizing the missing information is not likely to be found. An incomplete problem representation actually impaired performance because the subjects tended to rely on it as a comprehensive and truthful representation—they failed to consider important factors omitted from the specification. This is a big concern for complex systems, multitier systems, and specification interfaces between subsystems.

- System engineering must be in control of the design throughout all phases to insure proper functional and safety design at all tiers.

Notes from the document

- Probabilistic risk assessments, particularly for complex systems cannot be verified. Probabilistic risk assessments are useful to direct the design approach through a fault tree and are useful for shotgun testing to look for missed combinatorial faults but they then must be converted to clinical tests.
- To be most useful, qualitative and verifiable quantitative information must be used, not just probabilistic models of the system.
    - Clinical repeatable qualitative and verifiable artifacts are always necessary: probabilistic artifacts are useful for performance evaluations alone.
    - Models can be used to generate the clinical artifacts but there must be a direct generation of the implementation from the model and a method to show the equivalence of the model and the implementation.
- Local Government Oversight authority is composed of oversight through inspections, surveillance, audits, and witnessing of critical contractor work.
- Address Prescriptive vs Performance based Regulation and Safety Cases
    - FAA and NASA have heavily favored prescriptive although NASA has been somewhat influenced towards a performance based safety case by the nuclear regulatory functions.
    - Prescriptive weaknesses, according to Cullen report
        - Too superficial;
        - Too restrictive or poorly scoped;
        - Too generic;
        - Overly mechanistic;
        - Demonstrated insufficient appreciation of human factors;
        - Were carried out by managers who lack key competences;
            - Failed to consider interactions between people, components and systems.
- Use of Probabilistic Risk Assessment (PRA) such as Fault Tree and Event Tree Analyses.
    - Other high risk industries such as the nuclear submarine community does not allow PRA, instead they require Objective Quality Evidence (OQE)
        - OQE may be qualitative or quantitative, but must be based on observation, measurements or tests that can be verified.
        - Probabilistic risk assessments, particularly for complex systems, cannot be verified.
- Impact of confirmation bias: *Confirmation bias* is a tendency for people to favor information that confirms their preconceptions or hypotheses regardless of whether the information is true. If the goal is to prove the system is safe, they will focus on the evidence that shows it is safe and create an argument for safety. If the goal is to show the system is unsafe, the evidence used and the interpretation of available evidence will be quite different.
- Failure to assess properly from an “out of sight, out of mind” phenomenon. If the representation is not complete the likelihood of recognizing the missing information is not likely

to be found. An incomplete problem representation actually impaired performance because the subjects tended to rely on it as a comprehensive and truthful representation—they failed to consider important factors omitted from the specification. This can be addressed somewhat by changing the goal from proving the system is safe to look for unrecognized fault and hazards.

- Some key points from the Nimrod accident
  - The Safety Case Regime has lost its way. It has led to a culture of 'paper safety' at the expense of real safety. It currently does not represent value for money.
  - The current shortcomings of safety cases in the military environment include: bureaucratic length; their obscure language; a failure to see the wood for the trees; archaeological documentary exercises; routine outsourcing to industry; lack of vital operator input; disproportionality; ignoring of age issues; compliance-only exercises; audits of process only; and prior assumptions of safety and 'shelf-ware'.
  - Safety cases were intended to be an aid to thinking about risk but they have become an end in themselves.
  - Safety cases for 'legacy' aircraft are drawn up on an 'as designed' basis, ignoring the real safety, deterioration, maintenance and other issues inherent in their age.
  - Safety cases are compliance-driven, i.e., written in a manner driven by the need to comply with the requirements of the regulations, rather than being working documents to improve safety controls. Compliance becomes the overriding objective and the argumentation tends to follow the same, repetitive, mechanical format which amounts to no more than a secretarial exercise (and, in some cases, have actually been prepared by secretaries in outside consultant firms). Such safety cases tend also to give the answer that the customer or designer wants, i.e. that the platform is safe.
  - Large amount of money are spent on things that do not improve the safety of the system
- Conclusion Topics
  - To avoid confirmation bias and compliance-only exercises, assurance cases should focus not on showing that the system is safe but in attempting to show that it is unsafe. It is the emphasis and focus on identifying hazards and flaws in the system that provides the "value-added" of system safety engineering. The system engineers have already created arguments for why their design is safe. The effectiveness in finding safety flaws by system safety engineers has usually resulted from the application of an opposite mindset from that of the developers.
  - The process should start early.
  - The assumptions underlying the assurance case should be continually monitored during operations and procedures established to accomplish this goal.
  - The analysis needs to be integrated into system engineering and system documentation so it can be maintained and updated. Safety assurance is not just a one-time activity but must continue through the lifetime of the system, including checking during operations that the assumptions made in the assurance argument remain true for the system components and the system environment.
  - The analysis should consider worst cases, not just the likely or expected case (called a design basis accident in nuclear power plant regulation).

- The analysis needs to include all factors, that is, it must be comprehensive. It should include not just hardware failures and operator errors but also management structure and decision-making.
- To be most useful, qualitative and verifiable quantitative information must be used, not just probabilistic models of the system.

4.9.3 Reliance on Development Assurance Alone for Complex Criticality - CAST

The document does not address multitier supplier development and does not discuss oversight or delegation. It recognizes the ARP and RTCA documents as a means to provide assurance through a development process. The paper takes a position that the regulations and policy are not sufficiently explicit (prescriptive). The greater discussion on the use of diversity implies guidance towards the use of diversity as a means to supplement development assurance. It does not provide guidance towards complex avionics developed in a multitier environment.

- The purpose of this paper is to highlight that development assurance alone is not necessarily sufficient to establish an acceptable level of safety for complex and full-time critical functions implemented in software or complex hardware.
  - The paper presents rationale for the use of mitigation means in the system development to prevent either software or complex electronic hardware development errors from becoming a common point of failure.
- When a failure is caused by a development error in the system, particularly in software or complex electronic hardware, the guidance materials are not clear on the applicability of fail-safe concept and techniques.
  - Thus, the applicant and system designers need to consider the potential effect of such errors in the aircraft-level safety assessment, in order to ensure that their proposed system design and implementation of complex, safety-related systems can be demonstrated to have achieved an acceptable level of safety.
- As the regulations and policy are not sufficiently explicit, this paper explains how the fail-safe concept and design techniques can be interpreted when addressing software-related and complex electronic hardware-related development errors.
  - No clear solutions are suggested. Moreover, this paper does not promote any particular concept.
- New technologies and complexity introduce greater challenges and can introduce new sources of development error. It is generally not practical or maybe even feasible to develop a finite test suite that can conclusively demonstrate the absence of development errors.
- Development process assurance can establish a level of confidence through reliance on methods such as ARP-4754, ARP-4761, DO-178, and DO-254.
- Four basic safety techniques are recognized; fault tolerance, fault detection, fault removal, and fault avoidance.
- There is no quantitative means to assess the acceptable level of safety regarding the mitigation for systematic error. Therefore, the acceptance is based upon engineering

judgment and common understanding of best practices between certification authorities and applicants.

4.9.4 Certification Concerns of IMA Avionics Systems – Bartley and Lingberg

By its nature an IMA system may be made up of multitier suppliers of the individual components and functions. This paper raises many of the concerns relevant to development of complex systems in a multitier environment. It states that the existing regulatory guidance material, though fragmented, provides sufficient guidance to accomplish the necessary safety design and assessments. The concern is that a fragmented supplier development base will exacerbate the issue by inadvertently missing certain aspects of the design and analysis.

- This paper explores some of the issues and concerns surrounding approval of large scale IMA systems.
    - The FAA is concerned that the complexity of these IMA systems and the interaction between their functions is not well understood, especially under failure conditions. Additionally, given the developing business models used by industry, it is likely that large-scale IMA systems will be developed and integrated by multiple companies.
    - From the FAA perspective, IMA systems are not fundamentally different in nature from more traditional, usually simpler, federated systems.
        - What has changed is the complexity of these systems and number of companies developing components of IMA and the increasing possibility of unintended interactions
- Major concerns
    - Lack of integrated and cohesive FAA policy and guidance specific to IMA
        - FAA regulations, policy, and guidance is disbursed across many different sources and documents, may not always be harmonized, and may be confusing.
    - Distributed IMA design responsibility
        - Due to the fragmented nature and scale of IMA there is a danger many necessary design considerations and integration activities may be inadvertently omitted.
        - Specific engineering and design expertise is required to produce the complete IMA
        - Economic incentives and availability of specialized avionics suppliers across the globe may influence distributing the design work to different companies and different countries and cultures.
            - The risk is that no single entity “owns” or “understands” completely all functions in the IMA
        - Additional complications arise through limitations in communication between developers when developers are normally competitors in other areas.

- Unintended operation
  - One obvious difference between IMA systems and simpler federated systems is that failure of the IMA infrastructure will affect all systems that make use of a shared resource. It may be more difficult to determine secondary effects (cascading failures) caused by a failed resource.
  - A data dependency may have multiple links in the chain such that multiple functions are involved.
  - Secondary effects caused by failure of shared resources *may not be immediately obvious* without some level of detailed, cross functional analysis.
- Erroneous assumptions regarding robust partitioning
  - Overconfidence in robust partitioning could result in compromised IMA architecture
  - Dependency between functions is not erased with robust partitioning, data exchanges remain as dependencies that must be taken into account;
    - Data Coupling – The dependence of a software component on data not exclusively under the control of that software component.
    - Control Coupling – The manner or degree by which one software component influences the execution of another software component.
  - Processor stacks, registers and data overlays must be considered.
  - It is false to assume that if the ICD between partitioned systems is not impacted by a change in functional parameters, then the functions using those parameters cannot be impacted.
  - The experts that are required to assess the impact of the change are the designers and analysts of the using system, not the source system.
- Use of TSO for approval of IMA systems
  - With a system as complex as an IMA, there will undoubtedly be some aspects of the IMA system that will come under the purview of the issue papers levied against the aircraft program.

4.9.5 Complexity Concept Causes and Control – McDermid

The paper is focused on the issue of complexity and how to manage and asses the system. The paper provides nothing new or of value but rather proposes some unacceptable means of dealing with assessments for avionics. Not useful to this study.

- Thus we can view complexity as having a number of key facets:
  - Scale - the number of elements in the system;
  - Diversity - the extent to which systems are made up of different elements;
  - Connectivity - the inter-relationships between the components.
- Causes of complexity
  - Intrinsic (due to the nature of the system elements)

        - The paper lists the hardware: processors, ASICS
        - Also interconnectivity and systems of systems
    - Extrinsic (due to the environment of the system)
        - Measurements of success, human desire for achievement
        - Embedded in systems such as aerospace
- Difficulties in assessment of complex systems
    - Shared resources – processors, memory, etc
    - Discontinuous behavior – software is discontinuous
    - Multi-faceted – many properties
    - Hierarchies – understanding of all levels.
    - Emergent behavior – behavior of the whole are not simple combinations of lower level properties
    - Extreme requirements – civil aerospace probability less than $1x10^{-9}$ per hour occurrence requirement
- Coping with complexity
    - Simplicity spelled out as KISS "Keep it simple stupid", basically a value judgment for each requirement is made
        - Simplifying assessments to differences between product families [comment: not acceptable for critical avionics systems]
        - Design for assessment through partitioning
    - Assessment
        - Multi-criteria decision analysis
        - System Modeling – model based assessments
        - Automated analysis
        - Abstraction – purposefully omit details

4.9.6 The Impact of RTCA DO-178C on Software Development - Reddy

The document provides a nice summary of the impact of DO-178C. It is a concise description of the changes made from DO-178B to get to DO-178C. It has no direct value to this study but is recognized as an aid to someone wanting to understand DO-178C structures.

4.9.7 DO-178C and ARP 4754 for UAV SW development using MBD - Erkkinen

This paper takes a look at the changes in DO-178C and supplement DO-331 in regards to the use and processes of MBD. The use of MBD to capture requirements, model the design, and generate code from the model is now clearly acknowledged as an acceptable means to certification by the governing standards. A long standing issue wherein DO-178B provided an uncertainty in mapping objectives to MBD artifacts is now clarified. DO-178C, supplement DO-331, calls out ARP4754A recommendations for MBD requirements capture, modeling, simulation, analysis, and validation. Also noted is that DO-331 defines a design model that is used to not only capture and analyze but to generate embedded code for both hardware and software implementations.

So as it relates to this study this paper provides insight into guideline support for use of MBD as a means, although not stated, by which complex multitier systems requirements can be captured, modeled, tested, and coded. The paper does not outline this system design management approach but establishes that the regulatory documents contain the acknowledgment of MBD that can enable guidelines that raise the bar on multitier development. [This flows into our pre-conceived thoughts that the use of MBD and systems control can be strengthened to address the issues].

- DO-178B lacked guidance on modern development and verification practices such as model-based design, object-oriented technologies, and formal methods, until DO-178C standard was developed. The FAA and EASA worked with aircraft manufacturers, suppliers, and tool vendors to update standards based on modern technologies. Rather than significantly modify the standards, they created technology supplement documents.
    - The impact of the new standards to UAV developers using model-based design is especially significant.
- A general description of MBD design is given where engineers develop and simulate system models comprised of HW and SW using block diagrams. Then they automatically generate, deploy, and verify code on their embedded systems. The outputs of modeling tools generate textual language code in C, C++, Verilog, and VHDL.
- Testing through flight test is expensive. A better way is to test early in the design process using desktop simulation and lab test benches.
    - Test cases based on high level requirements formalize simulation testing. These simulation tests are reused throughout the model based design as the model transitions from a system model to a software model to source code to executable code using code generators and cross-compilers.
        1. Simulation test cases are derived and run on the model using Model-In-the-Loop (MIL) testing.
        2. Source code is verified by compiling and executing it on a host computer using Software-In-the-Loop (SIL) testing.
        3. Executable object code is verified by cross-compiling and executing it on the embedded processor or an instruction set simulator using Processor-In-the-Loop (PIL) testing.
        4. Hardware implementation is verified by synthesizing HDL and executing it on an FPGA using FPGA-In-the-Loop (FIL) testing.
        5. The embedded system is verified and validated using the original plant model using Hardware-In-the-Loop (HIL) testing.
- A requirement based test approach with test reuse for models and code is explicitly described in ARP-4754A and DO-178C supplement DO-331.
- ARP4754A
    - ARP4754A recommends the use of modeling and simulation for several process-integral activities involving requirements capture and requirements validation.

- ARP4754A Table 6 recommends (R) analysis, modeling and simulation (tests) for validating requirements at the highest Development Assurance Levels (A and B). For Level C, modeling is listed as one of several recommendations.
- Also noted in ARP4754A is that a graphical representation or model can be used to capture system requirements. The standard now notes that a model can be reused for software and hardware design.
- If engineers use models to capture requirements, ARP4754A recommends engineers consider the following:
    1. Identify the use of models/modeling
    2. Identify the intended tools and their usage during development
    3. Define modeling standards and libraries

- DO-178C
    - DO-178C calls out ARP4754A, so by implication endorses these processes.
    - The biggest changes for MBD are captured in DO-331 supplement Model-Based Development and Verification
    - A long-standing issue with DO-178B for practitioners of model-based design is the uncertainty in mapping DO-178B objectives to model-based design artifacts. Addressing this mapping was a main goal of the DO-178C Sub-Group (SG-4) focused on model-based design. No single mapping sufficed, so several mappings are provided in DO-331.
        - Some include the concept of a Specification model, which is a model separate from that of the one used for design and code generation.
        - The other concept is a Design model, which serves as the detailed requirements used to generate code. The essence of a Design model is the following:
            1. A model can be used for design (system and/or software) and should be developed using requirements external to the model (for example, a textual document or requirements database).
            2. Source code can be generated directly from the design model (by hand or automatically).
    - One approach noted in the standard is that a model used initially for system design can be elaborated on and reused for software design and code generation. This ties ARP 4754A and DO-178C together quite nicely for UAV system and software developers using model-based design.
    - The test cases for system requirement validation likewise are reused on the model, source code, and executable object code to perform functional testing and collect coverage metrics.

4.9.8 Complying with DO-178C and DO-331 using MBD - Potter

This document is basically the same as the paper on Transitioning to DO-178C and ARP 4754 for UAV SW development using MBD with a few noted differences.

- In the past, some suppliers may have claimed that subsystem development was beyond the scope of ARP4754, even for complex subsystems containing hardware and software, but not anymore. ARP4754A also more clearly refers to DO-178 and DO-254 for item design.
- Model usage in DO-331:
    1. A model can be used for design (of the system, the software, or both) and should be developed using requirements external to the model (e.g., a textual document or requirement database).
    2. Source code can be generated directly from the design model (by hand or automatically).
- DO-331 introduces two important techniques, simulation and model coverage analysis, that may be used with Model-Based Design to satisfy objectives for design models.
    - For some, but not all, objectives for high and low level requirements, DO-331 allows the use of simulation to satisfy objectives in place of traditional reviews and analysis. In fact, simulation can be more effective than reviews in determining correctness, because simulation provides a means of predicting the dynamic behavior of a system.
    - Model coverage analysis is a new technique called out in DO-331, and in fact this analysis is a required activity when using design models. One of the concerns raised by the certification authorities during the development of DO-178C and DO-331 was that past projects using Model-Based Design sometimes had vague requirements associated with very complex models. This raised the concern that unintended functionality could be introduced into the system during the model development process. Model coverage analysis is performed during model simulation and the simulation cases must be based on the requirements from which the model is developed. This is similar to how code coverage is performed; it is done using test cases based on the software requirements, not on the code itself. DO-331 contains examples of the types of model coverage metrics that should be considered for the analysis.
- The factors used to determine if a tool needs to be qualified have not changed from DO-178B to DO-178C. For example, a modeling tool does not need to be qualified as long as the output of the tool (the model) is verified per DO-331 model verification objectives. If an automatic code generator is used, and the generated code (tool output) is reviewed then qualification is not necessary. If, however, the code review is to be eliminated then the code generator must be qualified.
- With Model-Based Design it is possible to also use object-oriented technology and formal methods. For example, an automatic code generator could be used to generate C++ code, or a formal methods tool could be used to prove properties within a model.

4.10 Other Resources

4.10.1 NASASP2010580, NASA System Safety Handbook Volume 1

Although this document is out of the scope of assessing the regulatory guidelines for management and oversight of multitier supplier development of complex systems this document was reviewed for an alternate perspective. The document defines complexity as one of the primary reasons for its purpose, to provide a safety framework with a holistic assessment of the aggregate sources of risk. It does not specifically address multitier supplier network risks; experience, interpretation, boundary issues, etc. However, the purpose of the document is intended for those with oversight responsibilities. The overall framework could easily be applied to multitier suppliers. The document does not reference any ARP or DO documents, but references Mil-STD-882D, Mil-HDBK-217F and a number of NPR documents.

- The document is prefaced with a statement questioning the adequacy of traditional safety analysis tools and processes for identifying and quantifying hazards (FMEA and probabilistic risk assessment methods (PRA). However, the increasing complexity has become an issue and drives the need for a more holistic approach. The handbook takes a more holistic approach in 3 areas:
    1. The handbook takes the position that it is important to consider measures of aggregate safety risk as opposed to focusing on the individual risk. The term aggregate risk, when used in this handbook, refers to the accumulation of risks from individual scenarios that lead to a shortfall in safety performance at a high level.
    2. Second, the handbook stresses the necessity of developing confidence that the controls derived for the purpose of achieving system safety not only handle risks that have been identified and properly characterized but also provide a general, more holistic means for protecting against unidentified or uncharacterized risks.
    3. Third, the handbook strives at all times to treat uncertainties as an integral aspect of risk. Uncertainty analysis finds how the output parameters of the models are related to plausible variations in the input parameters and in the modeling assumptions. The evaluation of uncertainties represents a method of probabilistic thinking wherein the analyst and decision makers recognize possible outcomes other than the outcome perceived to be “most likely.”
        - In line with these considerations, the handbook does not take a hazard-analysis-centric approach to system safety but rather strives to emphasize the most critical scenarios that contribute to the aggregate risk and then identifying the risk drives that cause these scenarios to be critical.
- Volume 1 purpose is to present an overall framework for system safety. Volume 2 provides specific guidance on the conduct of major system safety activities towards development of evidence.
- The document structure is a clear build up of the safety objective with 4 major points; 1) overview of system safety, 2) safety objectives, 3) system safety activities, and 4) RISC informed safety measures.
- Though it is not clearly annunciated there is a discussion of flowing down probabilistic allocations to subsystem elements to the organizational units responsible for the design of these elements (p 60).

The use of tiers does not refer to multitier suppliers, however, but tiered technical flow down of; 1) reliability allocations, 2) recovery from faults, and 3) crewed mission recovery from faults.

- The document identifies several drivers that motivate a change in approaches to safety:
    - The high cost of testing limits the ability to rely on test-fail-fix strategies drives towards reliance on analytical results.
    - Increasing system complexity makes it necessary to go beyond traditional hazard assessments as they are limited in their ability to identify hazardous system interactions. This states a case for modeling and simulation.
    - Development of systems and technologies that operate on the edge of engineering expertise driving a high degree of discipline and oversight.
    - The use of unproven technologies requiring design conservatism to protect against unknown safety risks.
- Scenario development requires systematic analysis of complex interactions, dependencies and combinatorial effects. This states a case for modeling and simulation
- RAA: There is a short statement in (3.2.3) regarding the allocation of requirements to lower levels of the organizational hierarchy. It places oversight responsibility on the organization that is allocating the requirements.
- The Conclusion statement is a very nice statement of what the document is about – organizing the safety aspects under a framework bringing together the results into a single final measure point.

APPENDIX B

Risks and Recommendations from Industry

Objective: Capture safety issues, cost and schedule issues, and recommendations from interviews with avionics and air transport industry experts.

Contents

1 Purpose

This part of the NASA Flight Critical Systems Research (FCSR) study captured safety issues, cost and schedule issues, and recommendations raised by experts in the avionics and air transport industry. We conducted interviews with 19 people who have experience as part of aircraft OEMs, avionics vendors, and the FAA. We looked for a mix of safety, technical, and program management expertise. We were not able to interview anyone in an FAA ACO, which would have been valuable.

Some issues and recommendations were repeated by multiple interviewees, and we extracted these themes into the summary section below. Extracts from the interviews are listed afterwards as supporting material.

We excluded the names of companies, programs, and individuals so this document can be openly shared.

The study objective is "identify effective means to ensure, with a high level of confidence, that computer-based aircraft-level systems are safe and compliant with the letter and intent of regulations and development guidance." The term "effective" also implies that safety mechanisms must be balanced with the time and cost to execute.

2 Summary of Highlights and Repeated Themes

Combined list of **SAFETY ISSUES** in a very rough order of priority:

- The top safety issue for suppliers is their lack systems understanding and experience with designing safety critical functions – how their components interact with the rest of the aircraft. Suppliers do not know assumptions being made by the primes, and misinterpret the requirements.
    - Overseas suppliers have cultural limits on asking questions and taking initiative.
    - Knowledge of how to deal with hazard levels is very tribal – only a few special people know it.
    - The pool of experienced suppliers is small.
- Requirements (and complexity) are increasing exponentially because of interactions between systems – when every system can talk to every other system then there is lots of interaction to specify.
- Primes and suppliers have different expectations for new technology, and the missed requirements cause problems.
- Primes and suppliers are not rigorous enough about defining interfaces – within their own groups and between suppliers.
- There is a loss of systems expertise, and therefore an understanding of safety, as companies outsource work and don't replace experienced engineers that retire.
- Testing for system behavior and "unintended function" is starved (in funding and time) by testing requirements that are not safety related. Testing individual software modules has some value, but does not address system effects. DO-178B originally intended more system bench tests.

- Process steps (docs, reviews, oversight) are given a higher priority in suppliers than a robust design, making systems less safe. This issue is compounded when a supplier has tight budget constraints – design time is cut before the "mandatory" process time.
- It's hard to quantify criticality in chains of partial failures, and only OEMs can do it because they have the systems knowledge.
- ARP-4754A is incomplete for defining systems documentation.
- Reviews are not effective at finding boundary condition problems.

Combined list of **COST and SCHEDULE DRIVERS** in a very rough order of priority:

- The biggest avionics cost driver is large jumps in complexity due to all the possible interactions between systems on open busses.
- The most common cause of budget and schedule overruns is missed expectations for new components.
- Some primes (OEMs and 1st tier suppliers) do not draw adequate boundaries (in contracts) around system pieces and integration – responsibilities are not well defined and their suppliers cannot afford "add-on tasks". These primes also underestimate the time and funding to manage and provide continuing systems support to the suppliers.
- Standards and certifications in one country are not accepted in another (e.g., US / China). This multiplies the cost and time for each country that a system will fly in.
    - Suppliers are being forced to choose what airspace to support.
    - Suppliers are not pursuing TSO's as often. There are too many regulatory bodies with different requirements, so suppliers just get their system certified with an OEM's aircraft.
    - FAA is not taking a more active role in committees with other regulatory bodies (EASA, etc.). This causes two big problems. First, other regulatory bodies are adding process that is not necessary but FAA accepts it anyway. Second, requirements for TSO's and airworthiness certs are diverging between the FAA and other bodies.
- Suppliers hurt themselves when they test beyond what the standards require (particularly DO-178B).
- If requirements tracing and design are done properly, then suppliers do not need to allocate the same amount of time for testing as they do for design.
- TBD's in requirements is a big schedule and cost driver. Avionics requirements take a long time to be set, usually because they are waiting for attention after the fuselage and engines.
- Programs requiring DO-178B compliance are 5x to 10x more expensive than non-DO-178B (based on personal comparison of commercial to military).
    - Time and cost is added for testing detailed requirements when system behavior problems are hidden in corner cases.
    - The time and cost to define, build the test environment, and document tests for every software module is expensive.
- ACO's within the FAA are not consistent – ACO's sometimes drop handoffs of TSO articles between each other because their responsibilities are not clear, ACO's sometimes disagree on cert requirements for systems.
- Suppliers will deliberately underbid engineering efforts by as much as half to win programs, then deal with overruns as they occur.

Combined list of **RECOMMENDATIONS** in a very rough order of priority:

- Primes should train their suppliers.
    - One best practice is bringing suppliers on-site with the prime for several months during design, then hold weekly meetings with suppliers.
    - Directives and processes are only as good as the people / groups that execute them. Therefore, spend more time training and mentoring rather than adding processes.
    - Train overseas suppliers to ask questions and look for functional / safety issues.
- Develop and execute a supplier assessment and oversight process.
- Have a competent experienced team for defining requirements and verification.
- Trade testing on requirements that are not safety related (coverage) for testing "unintended functions".
    - There are already plenty of scripted repeatable tests done under DO-178B.
    - Add "break it test teams" of experienced engineers for each function. Start with a list of test outlines. Set up and run tests manually that are likely to break the system.
- Put conditions in contracts so that missed deadlines for TBD's give schedule and cost relief to the supplier.
- MBD helps system understanding, and reduces requirements confusion.
    - Overall cost and schedule should go down.
    - For MBD to be effective, models must stretch across contractual boundaries. Otherwise, each supplier models his own system in his own way and declares success.
    - Use mature tools on programs. Do not develop tools while developing the avionics systems.
- Primes must allocate time and resources to analyze cascading partial failures. Suppliers cannot because they do not have the systems info.
- (There were no recommendations for maintaining systems expertise in the primes.)

3 Interview Excerpts

These are interesting comments made by interviewees that expand on the themes above.

Lead system engineer interview:

- The FAA was concerned about work being sent to overseas vendors where FAA has no jurisdiction for oversight. At the same time, OEM and 1st tier supplier management did not want limits on who they can use for development. Written corporate plans for supplier assessment and oversight have helped the issue.
- Contractor guidelines for oversight have worked well. Managing oversight through PSAC has not worked as well (primes still dump details in them).
- Don't put oversight details into a PSAC – this adds hard constraints on the software development. However, authors are tempted to do it, and at least one big OEM does it to get more contractual control over suppliers.
- Biggest issue for avionics suppliers: they do not understand how pieces of avionics support the system behavior. Suppliers need someone with system knowledge because it cannot all be written down in a PSAC.
- Rate suppliers by having them do verification or analysis (start easy at first), and comparing their results with the results from an experienced team. Use the rating to decide the oversight required.

- Supplier engineers need interaction on the intent of a function / system. Hold weekly meetings with suppliers.
- The most common issue with requirements and system behavior is engineers given a problem with no interaction on the intent of a function / subsystem. He had multiple examples of failed requirements handoffs to suppliers without continuing support, and no examples of a successful handoff without continuing support.
- Overseas suppliers need to be trained to ask questions and take initiative in looking for functional and safety issues.
- European airlines want different comms protocols than US, so suppliers have to double their code and verify both.
- DO-178B originally written as a guideline promoting system testing on benches with interfaces between modules. Process focused individuals and organizations within corporations since then have pushed coverage testing, which is not addressing where the functional problems occur.
- Coverage testing drives desktop test tools, not system bench tests as 178B intended.
- Some cert authorities require that unused code be removed in the middle of certification. Changing code at that point is senseless because it has not effect on safety, but adds risk by changing baselines.
- Have a competent experienced team.
- There are already plenty of scripted repeatable tests done under 178B. Add "break it test teams" of experienced engineers for each function. Start with a list of test outlines. Set up and run tests manually that are likely to break the system. Do not enforce repeatability because they have a "no excuses" standard. Make escapes personal – "you missed it".
- Different protocols between EU and America is increasing the number of versions of code.
- If using MBD, it is harder for functions like FMS where pilot interaction is involved.
- The original intent of 178B has been dropped, and it is now used to push more unit testing instead of integrated bench testing.
- Cert authorities should not require that unused code be removed while in the middle of certification tests. Removing unused code has no affect on safety, but adds time and cost by changing baselines.
- Train suppliers by bringing them onsite with the primes. Then the suppliers understand the system better.
- Have a systems cert document.
- A good system certification plan is more valuable to a supplier than oversight – oversight cannot replace tester knowledge.

General aviation director interview:

- Had failures with 2nd tier suppliers that did not know how to execute to 178B. Had to "teach them".
- Extra process is being added with intent of being more robust, but not helping – increasing cost.
- Factors that indicate if a sub will work or not: weekly reviews and milestones.
- The pool of experienced suppliers is small.
- FAA guidelines do not emphasize system testing as they should.
- Biggest issue for avionics is getting requirements nailed down early. Avionics is often last to get attention behind fuselage and engines. It also gets a lot of TBD's.
- TBD's in requirements is the biggest schedule and cost driver. Put conditions in contracts so that missed deadlines for TBD's give schedule and cost relief to the supplier.

Scientist interview:

- Unstated assumptions from primes to suppliers are the biggest problem in requirements validation and verification. This is especially true of overseas suppliers that do not know the assumptions around partitioning, realtime performance, or system behavior.
- Requirements and complexity are increasing exponentially because of interactions between systems – lots of interactions to specify when every system can talk to every other system on open busses.
- ARP-4754A is incomplete for defining systems documentation.
- Want supporting facts and analysis that the biggest avionics cost driver is big jumps in complexity (5x increase in software requirements over the last 5 years).
- IMA is more complicated, compared to federated systems, for V&V because it adds partitioning and interaction issues.
- Many suppliers do not understand the design constraints of safety (deterministic execution, hard real time, etc.).
- Suppliers do module testing, but not much system testing. Suppliers should run the tests from which their system or subsystem is derived.
- Generic checklists on supplier experience will not help as much as addressing actual program failures.
- MBD helps system understanding, and reduces requirements confusion. In turn, overall cost and schedule should go down.

Software engineer interview:

- Process steps (docs, reviews, oversight) are given a higher priority in suppliers than a robust design, making the system less safe. This issue is compounded when a supplier has tight budget constraints – design time is cut before the "mandatory" process time.
- Reviews are not effective at finding boundary condition problems.
- His subjective opinion is that programs requiring 178B compliance are 5x to 10x more expensive than non-178B (based on personal comparison of commercial to miliary).
- Suppliers will deliberately underbid engineering efforts by as much as half to win programs, then deal with overruns as they occur. This leads to insufficient design time.

Director for high-integrity systems interview:

- Suppliers lack knowledge or experience with safety and compliance around complex aircraft – how their components interact with the rest of the aircraft. Gave a specific program and 3 vendors (hardware and software), where none were "successful according to the prime's expectations at the start".
- Some 1st tier suppliers write inadequate contracts for 2nd tier suppliers – responsibilities are not well defined and 2nd tier suppliers cannot afford "add-on tasks". These same 1st tier suppliers also underestimate the time and funding to manage subs and provide continuing systems support.
- Some primes and suppliers try to outsource all development to dump all risk on subs. Does not work when subs do not perform.
- 2nd tier suppliers were required to follow 1st tier supplier processes, it did not help when the 2nd tier suppliers did not know what the system should do.
- Overseas suppliers gave mixed results – some did a good job of developing, others would not ask questions, others would demand all information be provided before starting work (no prototypes).

- Do not assume that two groups in the same company have the same skills and experience.
- Do not develop tools (MBD) in parallel.
- Primes must draw boundaries (in contracts) around system pieces and integration.
- Primes have as much trouble coordinating their own teams as coordinating suppliers.
- MBD saved many thousands of hours on flight controls. One secret to using models is drawing the boundary around responsibility for functions.
- Use mature tools on programs. Do not develop tools while developing the avionics systems.
- Properly written contracts are as important as technical integration, and have a big impact on cost and schedule.

DER interview:

- Testing for "unintended function" (funding and time) is starved by testing requirements that are not safety related.
- Requirements-based testing does not look at behavior other than what is required, so abnormal scenarios are not considered. Gave a program-specific anecdote.
- Unnecessary safety requirements increase the cost of planes and plane tickets. Cited a couple of government studies that concluded a $10 increase in plane tickets cause more car-related deaths. Keep this in mind when gauging the value of additional safety costs.
- When an OEM does the PSSA, they should spend a lot of time with suppliers to define the architecture and allocate severity levels. Then suppliers understand better, and quote better.
- OEMs should be proactive about covering problems with suppliers meeting their safety allocations. Less costly to address earlier in design than waiting until testing.
- Trade testing on requirements that are not safety related for testing "unintended functions". This implies testers should be more selective in how they test and document each requirement. A lot of time and cost is being added for testing detailed requirements when system behavior problems are hidden in corner cases.

Lead system engineer interviews:

- Hard to quantify criticality in chains of partial failures.
- Did propose and use a process for analyzing chains of partial failures.
- Primes must allocate time and resources to analyze cascading partial failures. Suppliers cannot because they do not have the systems info.
- Certifications in one country are not accepted in another (e.g., US / China). This multiplies the cost and time for each country that a system will fly in.
- Cost of development is multiplied by the number of countries the aircraft type will fly in – standards and certs vary from country to country.
- Knowledge of how to deal with hazard levels is very tribal. Only a few special people know it.
- 254 is generally frivolous. It can be helpful if developers are worried about counterfeit parts.
- Suppliers hurt themselves in schedule and cost by testing beyond what the standards (particularly 178B) require.
- Testing every software module becomes overly expensive to set up a test environment and document.
- Subs and primes often protect their designs from each other for competition. This makes sharing of information for integration and test much harder. This issue will not go away.
- Most common cause for integration problems and budget and schedule overruns is missed expectations for new components.

- Once a program runs long, resources don't become available at the right time and the schedule problem is aggravated.
- Every aircraft certification is custom. Try to use a previous certification to start with, then tailor it to what has changed in the aircraft.
- Suppliers try to use previously certified systems. This is generally accepted until the supplier "opens the system" or changes a function's contents.
- Getting approvals for revised cert plans to change a function is not too hard to do.
- Very helpful to suppliers if they can re-host software onto new processors without doing full Level A cert.
- Suppliers hurt themselves when they test beyond what the standards require (particularly 178B).
- The least costly approach to testing is to iterate on "system level tests". Test the requirements at a system level. Then add detailed tests for modules not touched by the system tests.
- The time and cost to define, build the test environment, and document tests for every software module is expensive.
- If requirements tracing and design are done properly, then suppliers do not need to allocate the same amount of time for testing as they do for design.
- TSOA's are important for suppliers to deliver spares directly to airlines (instead of the OEMs). The value of TSO's to the OEMs are mixed – valuable to "small airplane" OEMs, but not so much for transport airplane OEMs.
- For MBD to be effective, models must stretch across contractual boundaries. Otherwise, each supplier models his own system in his own way and declares success.

Program manager interview:

- Scope creep is the biggest problem in development programs.
- "Evidence" docs required by safety processes are important to have once the development team is gone.

System and safety engineer interview:

- Directives and processes are ultimately only as good as the people / groups that execute them. Therefore, spend more time training and mentoring rather than adding more processes. Cited a prime.
- A few OEMs have large directives that are enforced on 1st tier suppliers. It adds to cost without helping safety.
- OEMs get involved in 1st tier to 2nd tier efforts when there is a problem with schedule or cost.
- Time and funding is wasted when formal V&V is a big paper exercise by a separate test group that does not understand the system – they do not know what to test for. Then performance problems are found by the OEMs at integration time.
- There is risk in suppliers making last minute changes that break other functions.
- The biggest issues for verification and compliance is time and cost.
- Engineers working for suppliers are becoming just software coders – they do not understand how software is supposed to meet an intended function or safety.
- Mature systems do not suffer as much requirements confusion and TBD's.

DER interview:

- Testing individual software modules has some value, but not great value. The problem is that high levels of abstraction in software force the question: where else does an object have an effect?

Director of certification and chief engineer interview:

- New and novel technology / products are always a problem with subs because everyone is trying to agree on and understand the requirements. Primes have been burned by suppliers bringing tech that does not meet expectations, but suppliers must propose it early to get on the next aircraft type. Gave examples of suppliers for cockpit displays.
- FAA has a strict regulation that says to "stop ship" of a TSOA product that is non-compliant, even if the non-compliance is not safety related.
- Business people like to outsource work, looking to reduce internal overhead. However, they get burned by using subs who claim to have expertise when they do not. They then try to add oversight, which does not work and just adds more cost.
- More layers of suppliers means more opportunities to misinterpret requirements flow down.
- Must train overseas suppliers.
- ACO's within the FAA are not consistent – ACO's sometimes drop handoffs of TSO articles between each other because their responsibilities are not clear, ACO's sometimes disagree on cert requirements for systems.
- FAA is not taking a more active role in committees with other regulatory bodies (EASA, etc. This causes two big problems. First, other regulatory bodies are adding process that is not necessary but FAA accepts it anyway. Second, requirements for TSO's and airworthiness certifications are diverging between the FAA and other bodies. Suppliers are reaching the point where they must choose what airspace to support.
- Suppliers are not pursuing TSO's as often. There are too many regulatory bodies with different requirements, so suppliers just get their system certified with an OEM's aircraft.
- Requests in the EU for more documentation does not mean more safety.

Chief engineer for avionics interview:

- Suppliers are not rigorous enough about defining interfaces within their own groups.
- Primes should be more meticulous with interface definitions.
- Cited the ongoing argument about how to deal with inadequate requirements. Opposes using dissimilar systems – focus on getting correct requirements instead of battling complexity.
- Some OEMs want more integration done by suppliers. This must be clearly captured in quotes and contracts. Primes have had problems with outsourcing integration without clear assignments.
- ARP-4754A gives options, but no guidance (best practices). Should be updated with industry lessons.
- Subs do not look for cascading failures because they do not know all of the aircraft systems. The OEMs must do it.

Hardware designer interview:

- Their biggest schedule delays came from trying new technology for processing or networking.

APPENDIX C

ARP4754A and DO-331

Model Based Design Guideline Adequacy

Objective: Assess ARP4754A and DO-331 effectiveness in providing for Model Based Design (MBD) as an acceptable development methodology.

Contents

Table of Figures

1 Purpose

The purpose of this short paper is to assess ARP4754A and DO-331 for their guidance in the use of Model Based Design (MBD) as an acceptable means to system development. The question posed is; do ARP4754A and DO-331 enable effective use of MBD methodologies as system development methods or do they undervalue systems level MBD application and default to traditional development methods controlled by individual disciplines.

This is a critical topic in that MBD seems to hold the primary promise for managing the growing complexity of the systems and managing multitier supplier networks. Improper perspectives on MBD could defeat its potential values.

There is a concern from its content that ARP4754A does not establish MBD as a systems methodology but rather defers to the approaches defined in DO-331. Then there is a concern from its structure, content, and focus that DO-331 is not a true MBD guideline but rather a DO-178C extension of traditional software management processes over MBD activities that limit the objectives and effectiveness of MBD.

2 Background

Definitions of MBD:

- Model-Based Design (MBD) is a mathematical and visual method of addressing problems associated with designing complex control, signal processing and communication systems. Rather than relying on physical prototypes and textual specifications, model based design uses a system model as an analyzable specification throughout development. It supports system- and component-level design and simulation, automatic code generation, and continuous test and verification. In Model-Based Design, a system model is at the center of the development process, from requirements development, through design, implementation, and testing.
- It is not a software development methodology which focuses on creating and exploiting domain models (that is, abstract representations of the knowledge and activities that govern a particular application domain), rather than on the computing (e.g., algorithmic) concepts. That is Model-Driven Engineering (MDE).

MBD avionics designs have been developed through certification prior to the release of DO-331 and prior to the recognition of ARP4754 as an acceptable means of demonstrating compliance. One of the major realized benefits has been the literal elimination of requirements translation, software design, detailed software design, software verification, and software quality assurance efforts, illustrated in below. This does not mean verification was eliminated but was conducted at a higher level. Where a function is defined through the use of a model at the system requirements and analysis/modeling level the traditional efforts associated with software life-cycle requirements analysis, design and coding should no longer be necessary. Traditional software development processes remain, however, for those

items not defined through a modeling process. Functional verification activities are raised to the system modeling level and are performed earlier in the development cycle.

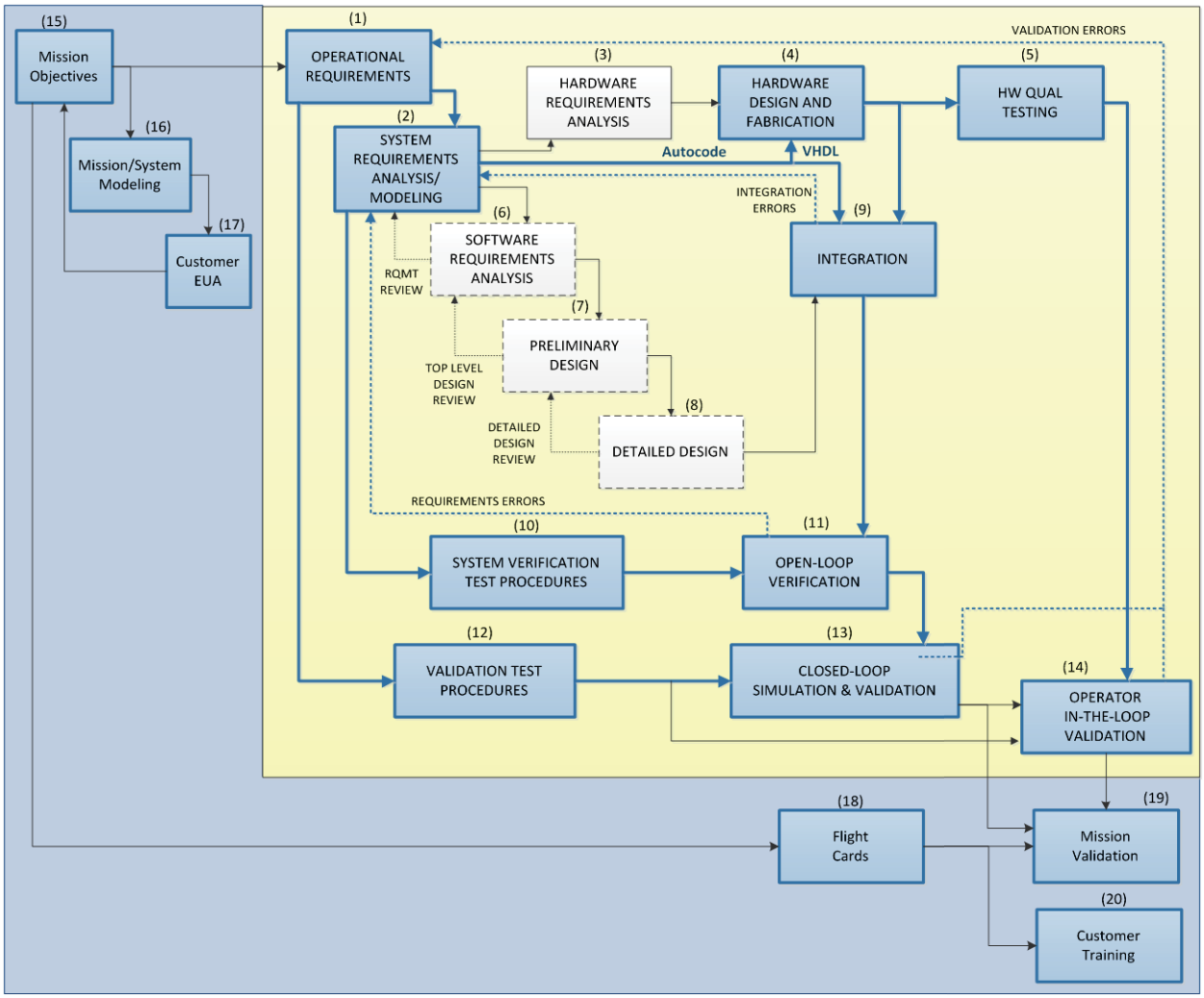


Figure 1. MBD Impact on Development

MBD as a means to develop systems fits as the next step in the progression of methodologies:

- machine code,
  - assemblers,
    - high-order language compilers,
      - graphical language compilers,
        - MBD

Along with each progressive step come the applicable processes, the supporting toolsets, and the verification methods. It is both hard for the regulators and industry to let go of the previously held methodologies and hard to define what equivalent process and toolsets will give the desired safety and productivity at the next step in the progression.

How the guidelines address the step into MBD is the question being raised.

3 ARP 4754A Content Assessment

How ARP4754A views MBD and how and where it delegates activities are of primary concern to the industry as it will shape the focus and work for years to come. There are two possible positions that emerge from an assessment of ARP4754A relative to the applicability of DO-178 to Model Based Design. Unfortunately the guideline is not sufficiently clear as to the writer's intent and there may, at first blush, appear to be a conflict within the guideline. However, when put in full context of ARP4754A one of the possible interpretations of the intended use of DO-178 relative to MBD appears to be consistent. The two interpretations are:

1. For any model that automatically generates code all the processes of DO-178 take over and all aspects of DO-178 in terms of software standard processes must be adhered to.
2. The intent and purposes of verification for certification credit as outlined in DO-178 must be accomplished; however, the other standard software processes and artifacts described in DO-178 do not apply to functions generated through MBD.

The inconsistencies stemming from interpretation #1 lie in the ARP4754A limitation of DO-178 to the item development part of the life-cycle which would eliminate its guidance through the aircraft to system, and system to subsystem modeling. The conflict comes later with the statement that "Models used to capture requirements and then directly used to produce embedded code (Software or HDL) come within the scope of DO-178B/ED-12B and DO-254/ED-80, from the time that certification credit is to be taken until the software or hardware is returned to the system processes for system verification". Placing the model in the scope of DO-178 from the time that certification credit is to be taken until the software is returned to systems verification is a puzzling statement if taken under the view that DO-178 controls all aspects of modeling activities that generate code.

On the other hand it is completely consistent with interpretation #2 that the verification guidelines of proof of: intended function, de-activated code, MCDC, and etc as identified under DO-178 fit under the interpretation that the intention of the statement within ARP4754A submitting to DO-178 for certification phase is that certification proofs outlined in the software guidelines must be accomplished for models that generate embedded code. We would take the side of this interpretation.

3.1 Inadequacy of DO-178C/DO-254 as a means to develop aircraft/systems

ARP4754 acknowledges DO-178C and DO-254 as a means to implement development assurance rigor for software and electronic hardware items but denies their adequacy for mitigation of aircraft/system errors. See ARP4754A pg. 22 last para: "In this context, this ARP4754A/ED-79A regards the activities of DO-178B/ED-12B and DO-254/ED-80 as a means to implement the development assurance rigor for the software and electronic hardware items. These software and electronic hardware related processes are no longer considered to be adequate to mitigate aircraft/system errors without a development assurance process from aircraft level down to item level, as shown in Figure 5." [Figure 5 in ARP4754A]

By implication from this statement DO-178C and DO-254 do not address the system requirements development, application utility, clarity in functional decomposition, requirements translation, modeling, and system functional verification and validation performed outside of the item development.

This view is consistent with the Item design life-cycle assignment for software processes of ARP-4754A section 3.2.

By implication then ARP4754A does not accept DO-178C and DO-254 for Model Based Design efforts leading up to software and hardware item development activities.

These implications are further strengthened by the statement on pg. 23 first para: "The objectives for accomplishment of each IDAL are per DO-178B/ED-12B and DO-254/ED-80 for software and electronic hardware items, respectively." The Functional Development Assurance Level assignments fall under ARP4754A Section 5.2 whereas the Item Development Assurance Level assignments fall under DO-178C and DO-254.

The implication is that DO-178() and DO-331 do not apply to system model based design activities at the functional levels even for those that generate code automatically from the functional model. The Aircraft System Model based development is sufficiently different and generally accomplished at a level above DO-178C authority indicating that an FDAL approach seems to be the only valid method for functional MBD. IDAL per DO-178C is too low a level for MBD.

3.2 Life-cycle applicability

The life-cycle V-diagram, Figure 2, and the definitions in ARP4754A following the [the ARP4754A source Figure 5] in ARP4754A place the applicability of DO-178/331 in the bottom center of the V-diagram. In terms of MBD then it should be clear that DO-178()/331 do not apply to MBD activities outside of the implementation part of the life-cycle. It is at the system implementation stage that DO-178() and DO-331 become applicable, see page 25: "The System Implementation stage of the process model interfaces the system process model described in this document and the DO-178B/ED-12B software and DO-254/ED-80 electronic hardware development process life-cycle guidance documents."

In a traditional approach where requirements are developed, decomposed and allocated to hardware and/or software ARP4754A transitions guidance to DO-178B/DO-254, see pg. 29: "The point where requirements are allocated to hardware and software items is also the point where the guidelines of this document transition to the guidance of DO-178B/ED-12B (for software), DO-254/ED-80 (for electronic hardware), and other existing industry guidelines." However the implications for MBD are left open as MBD paradigms are not addressed by ARP4754A in this context. Does it mean then that in the case of MBD where there is no allocation of functional requirements to software as the requirements are kept in a system model that the guidance of DO-178 is not invoked?

On page 39 where FDAL and IDAL are defined and guideline assignments made ARP-4754A is not completely clear on applicability. It could be interpreted that MBD falls under the FDAL as all behaviors, rules, performance, and requirements are developed in a model format and are validated in a model format. Its output is compiled directly to embedded code and therefore does not invoke an IDAL development phase.

The use of models for requirements capture on pg. 52 of ARP-4754A seems to take a conflicting view of MBD and DO-178() and DO-331 authority. " Models used to capture requirements and then directly used to produce embedded code (Software or HDL) come within the scope of DO-178B/ED-12B and DO-

254/ED-80, from the time that certification credit is to be taken until the software or hardware is returned to the system processes for system verification." Utilizing models to capture requirements is acknowledged, however, there are two implications:

- If the model does not generate embedded code directly then the model is not under the purview of DO-178
- However if the model generates embedded code directly then the model falls under the scope of DO-178.

This is inconsistent with earlier descriptions of life cycle scope of DO-178 being limited to item development. The purpose of the period of time between certification credit until the item is returned for system verification is unclear in this last statement.

3.3 Requirements Development

ARP4754A does not invoke some of the major benefits of MBD for early verification of models and "requirements" Pg 55: "Ideally, requirements should be validated before the design implementation commences. However, in practice, particularly for complex and integrated systems, the validation of requirements may not be possible until the system implementation is available and can be tested in its operational context." ARP4754A does not acknowledge the benefits of MBD bringing early functional verification and validation to the requirements capture phase from the traditional V-diagram verification stages.

ARP4754A also does not reflect differences in MBD activities that would result in a different set of correctness checks, see pg 59. One would expect a significantly different set of correctness checks.

Requirements traceability as described on pg 62 is from a traditional development sense and so does not take into account the paradigm shift from the usage of MBD. Model based designs naturally incorporate traceability through the nature of the model as sub-functions, or blocks as elements of the higher tier model. No additional traceability effort should be required. This changes the mindset of the developer and the regulator from an abstract aloof mechanical process of requirements tracing to requiring a functional and application understanding for proper evaluation. Requirements tracing efforts are traded for functional analysis and understanding.

ARP4754A still contains a mindset of traditional processes supplemented by MBD rather than a fundamental core of MBD supplemented by traditional processes. Pg. 62: c. Modeling: "Models of systems/items may be used to validate the requirements." It needs to be acknowledged that a model may be a complete design and/or the requirements may be in the form of a model.

ARP4754A does recognize modeling as an approved verification method, pg. 68 5.5.5.3 Modeling "Modeling of complex systems typically consists of a combination of computation and test; however, modeling deterministic systems behavior may also be entirely computational. Modeling may be used for system parameter evaluation, to provide early system information, or other purposes."

It is clear that ARP4754 excludes most of the system life-cycle activities from under the guidance of DO-178C/DO-331 as illustrated in Figure 2 below. DO-178C and DO-331 fall into the Item Design portion of the system development life-cycle. However, that brings attention to an apparent missing system MBD

guideline. ARP4754A itself is weak in incorporation of MBD activities throughout. For example sections 4 does not address the impact of utilizing MBD methodologies.

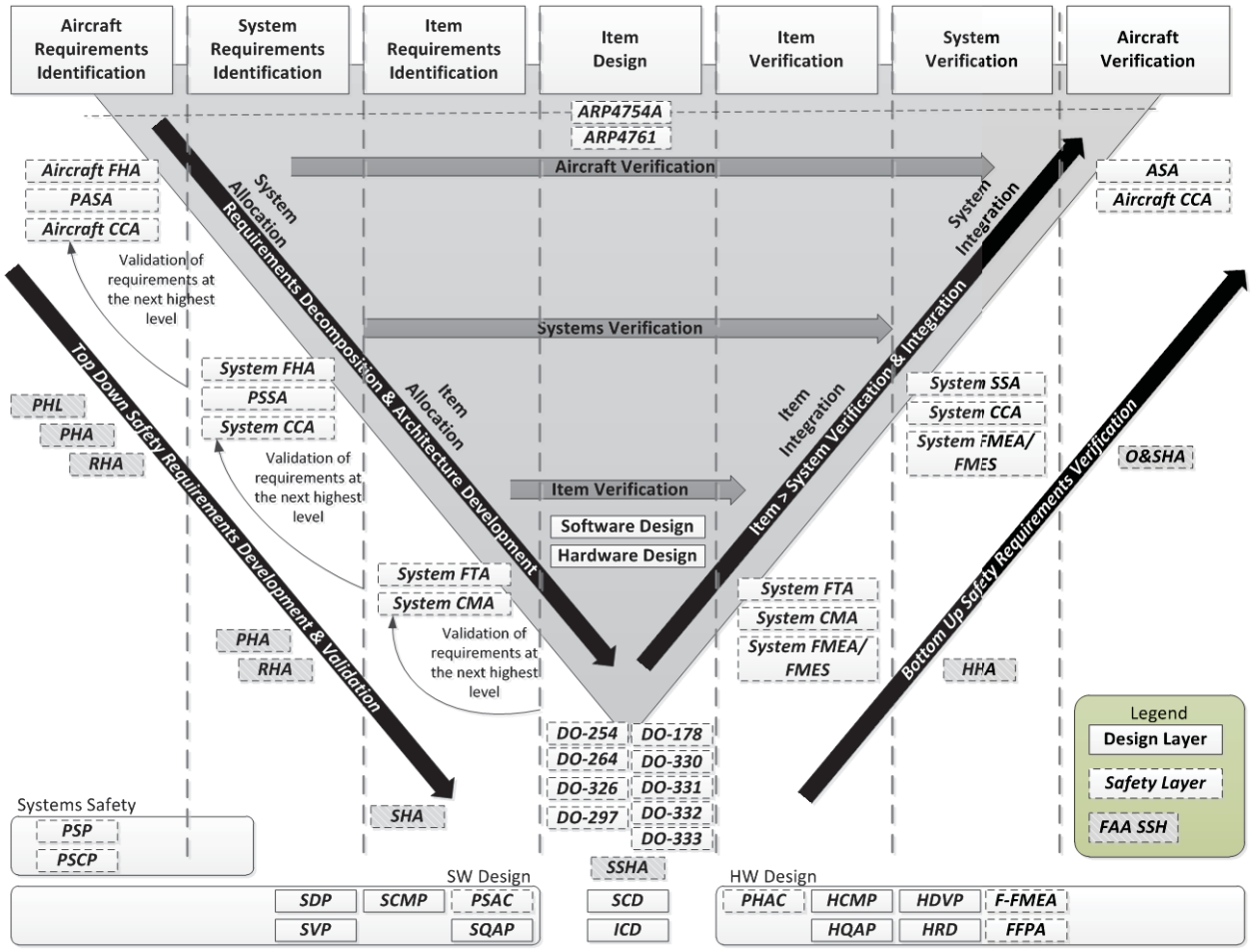


Figure 2. System Development Life-Cycle

4 DO-331 Content and Focus Assessment

As a supplement to DO-178C, DO-331 is espoused as the guideline addressing MBD activities. If it is an MBD guideline then it must address the issues associated with model development, model verification, and should be focused on modeling. It may be that DO-331 is actually limited to a Model Driven Engineering paradigm at the software level and was never intended to address system level modeling activities including those that generate code from the models.

DO-331 structure and content comes under scrutiny as not truly being an MBD guideline but rather a software guideline maintaining traditional software processes over MBD activities. One must ask:

- Why does the table of contents, see Figure 3 below, read like DO-178C? It is all about software life cycle, software planning process, software development process, software verification process, software configuration management process, software quality assurance process, software life cycle data
    - Should it not be: model life cycle, model development planning process, model verification process, model configuration control, and model life cycle data?

Figure 3. DO-331 Contents Outline

- Why does DO-331 refer to “user-modifiable software”, “COTS SW”, “option-selectable software”, etc. in a MBD document? If this is MBD then the term “software” should disappear from these discussions
    - Should it not be “legacy models”, Option-selectable model functions”, reference models, library models, etc.
- Why does DO-331 Figure MB.2-1 not reflect the elimination of traditional software development tasks through the use of MBD activities in comparison with DO-178C Fig 2-1? Some model items are added (see highlighted items in Figure 4 below) but all the DO-178C processes remain. One would expect that MBD would modify software activities and in some cases completely eliminate them. One would expect significant additions of MBD related activities.

Figure 4 illustrates the differences between DO-331 Figure MB.2-1 and DO-178C Fig 2-1. The figures are identical except for the red highlighted items. The implication is that all the detailed software process (planning, requirements development, design, coding, and integration) required by DO-178C for manually generated code remains as process requirements for models and code generated from those models.

Figure 5 below provides a notional diagram that more correctly represents the impact of MBD on the software development process. Functions which are modeled at the system level do not fall under the traditional software development processes. There are, however, functions which are not captured through modeling, such as wrappers and board support software, which do fall under the traditional software processes.

One might conclude that low level software modeling is appropriately covered by DO-331 as fragmented instances of particular low level components of a function. However, DO-331 does not address the system high level modeling of operations and their decomposition down to functional details that generate autocoded systems.

DO-331 contains paragraph after paragraph regarding standard DO-178C software processes that have nothing to do with MBD.

The DO-331 process graphic MB.2-1 with a few model related bullets is just DO-178C regurgitated and does not reflect MBD process reality. At best DO-331 describes a low level application of models within the software discipline silo where models are not passed to software but are developed by software within the silo from textual requirements.

DO-331 clearly does not support requirements development and flow down through modeling mechanisms and the benefits that could be realized from translation layer reduction. It therefore not only does not add value to managing multitier technical accuracy but restricts good practices that would enable multitier and complex system developments through application understanding, removal of translation layers, early verification of concepts and designs, clarity of complex designs, and error removal through modeling and simulation

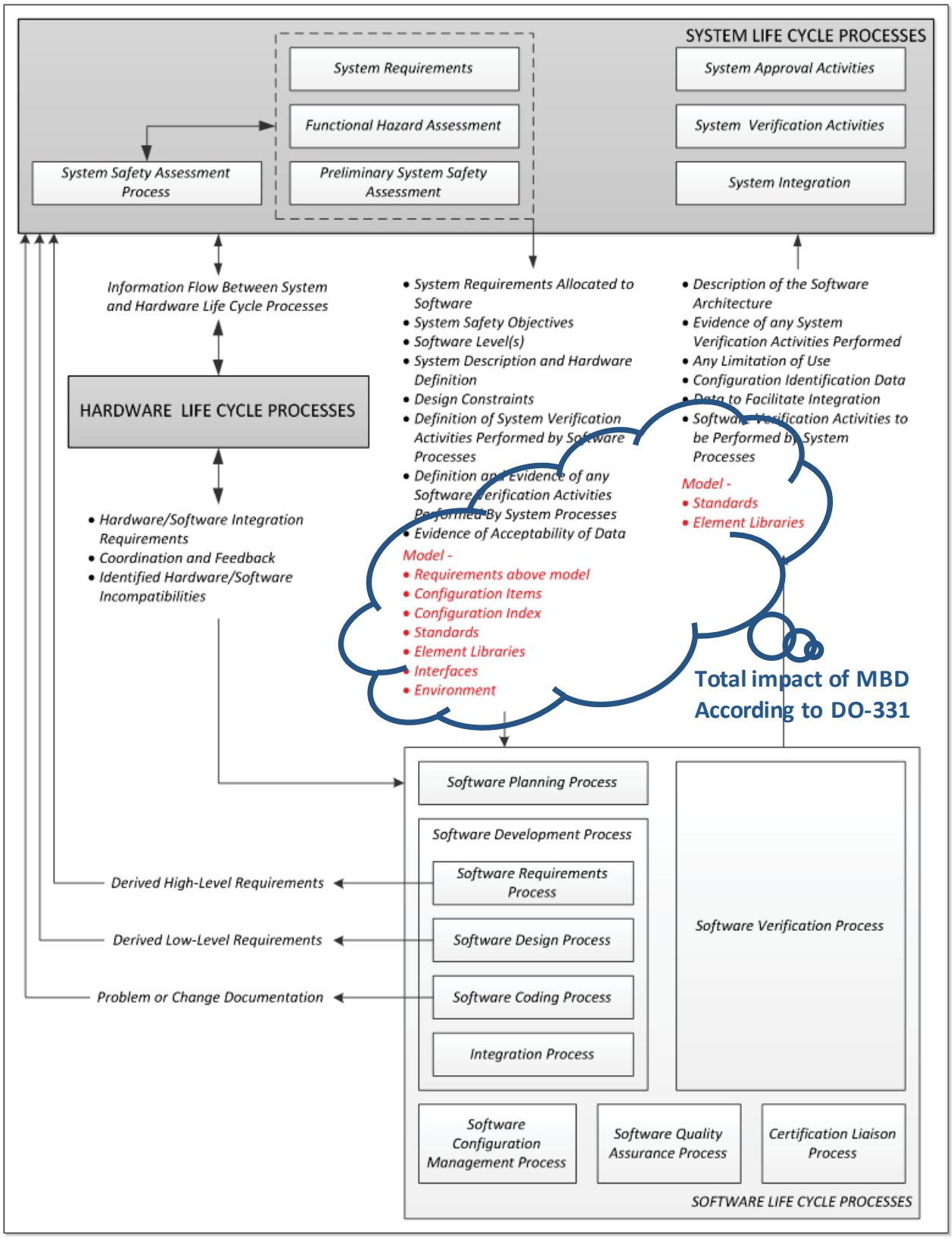


Figure 4. DO-331 MB.2-1

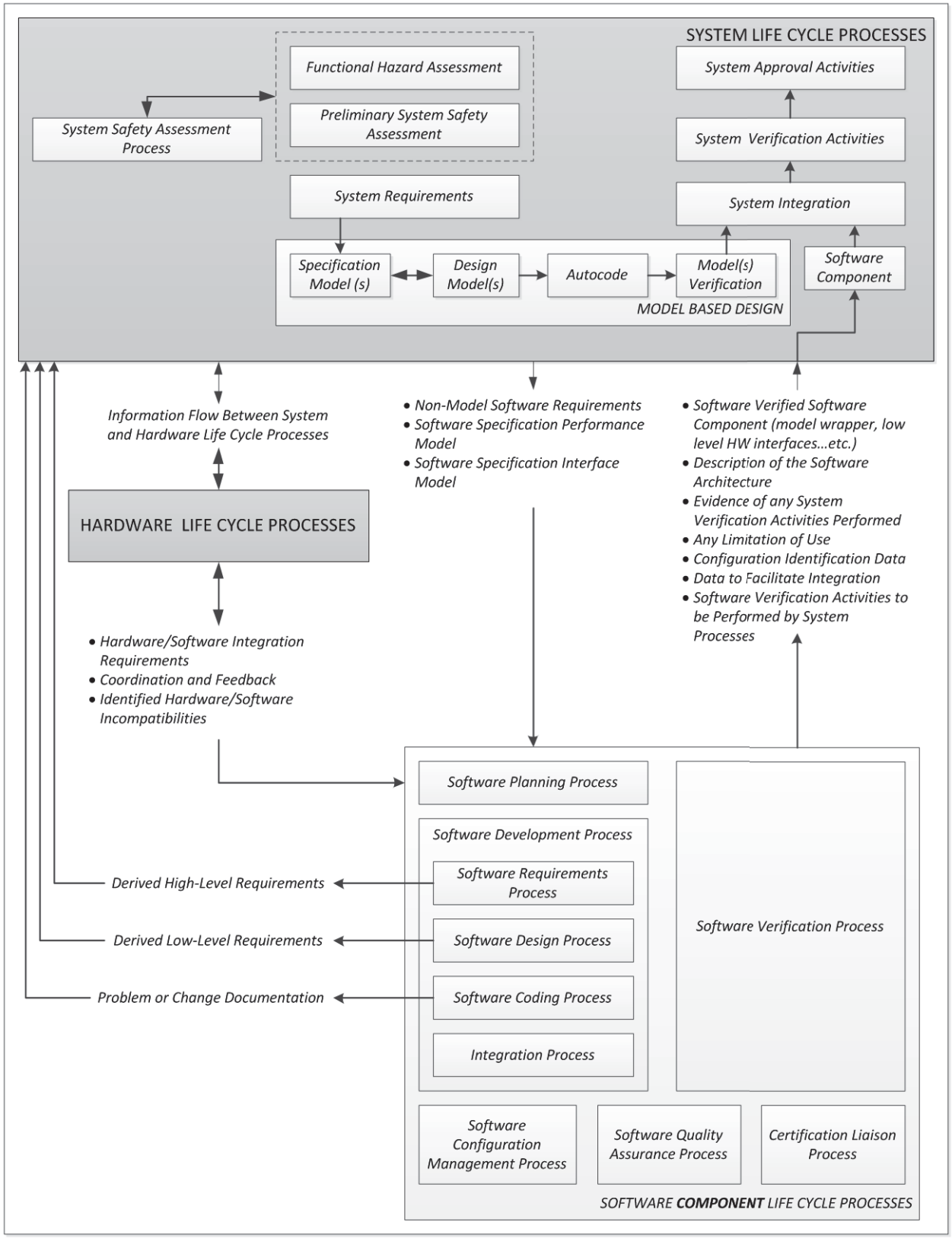


Figure 5. Correct MBD Modeling Process Replacement for MB.2-1

5 Recommendation

DO-331 is nothing more than a DO-178C extension of control to an apparent "Software Model Driven Engineering" process. We conclude DO-331 should not be applied to "Model Based Designs". In its place a Model Based Design guideline with a systems approach needs to be developed under the authority of ARP4754A as a system based modeling guideline. ARP4754A already provides life-cycle distinctions reflecting item development application of DO-178C and DO-331; however, there should be specific descriptions of the boundaries.

Figure 5 provides a notional process that should be supported by a Systems Model Based Design Guideline. The guideline should provide all the model development and management infrastructure processes necessary to effectively conduct system development across tiers in support of this process. All activities are couched under the prime objective of application of MBD principles across all system functional attributes and the processes necessary to develop them. A systems approach to MBD is a mindset guiding all developmental activities. Elimination of non-value added steps, translations, and tasks replaced by MBD activities are key performance goals supporting the prime objective of MBD application across the board.

Figure 6 below describes the mechanisms for flowing down a model based requirement for a "Configuration Item-B" (CI-B) to a lower tier developer. At the prime contractor level a complete model of the overall system is realized containing the environmental interactions and aircraft model, aircraft sensors and effectors, and in this example three interacting "Configuration Items". A "Configuration Item" is an abstract identification of a function or product such as an Autopilot, and FMS, and/or Navigation system, etc. As part of the requirements provided to the lower tier developer robust Interface Models are wrung out at the prime contractor for high integrity and accuracy as they define and parameterize the interfaces between all the elements of the final system and of the current Operational Model. The lower tier developer receives the appropriate interface models and a low fidelity model from the prime contractor as the requirements for the configuration item he is to develop. The low fidelity model's primary purpose is to provide behavioral and performance parameters that the configuration item is to comply with e.g. (resulting roll rate per deg of aileron deflection, handling qualities, navigation accuracies).

The developer modifies and iterates the CI-B Specification Model into a high fidelity Design Model and returns these iterations to the prime contractor for concurrence. When the model reflects the performance objectives it is run through formal verification testing. The formal verification testing must address all the aspects of intended function, conditions, decisions, deactivated functions, and test coverage.

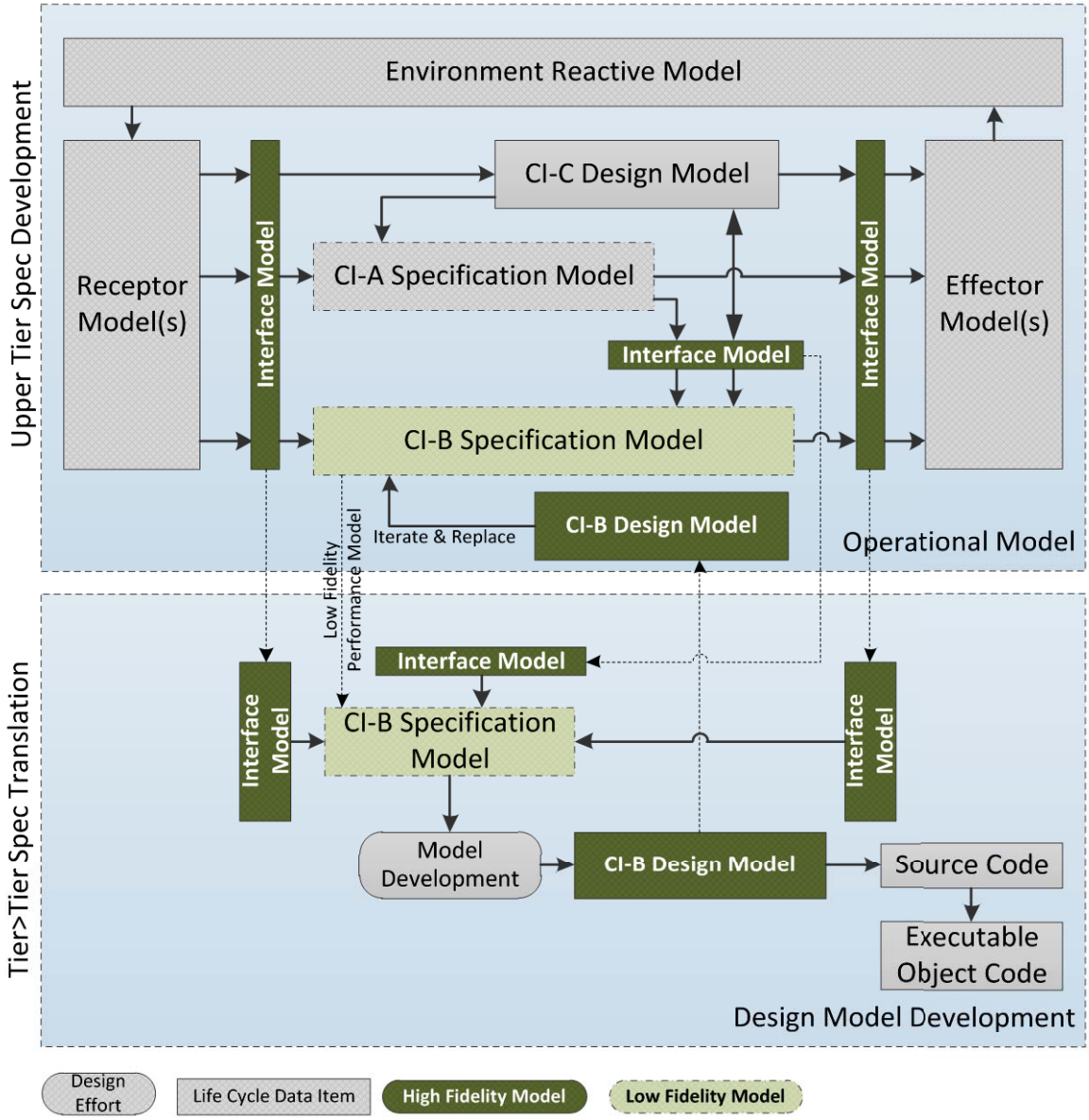


Figure 6. Expected MBD Activities and Capabilities

It is a mistake for industry to attempt to fit system MBD under the current DO-331 software umbrella.

It is clear that as DO-331 cannot address system MBD approaches both from ARP4754A life-cycle description and from DO-331 software process focus that there is a need for a System Model Based Design guideline.

APPENDIX D

Avionics Trends Impacting Guidelines

Objective: Assess trends in avionics that impact regulatory guidelines.

Contents

Table of Figures

1 Purpose

The purpose of this short paper is to assess avionics trends and development methods that have had and will have an impact to regulatory guidelines.

2 Avionics historical trends

A look back at the history of avionics implementations, development methods, and regulatory guideline changes is illustrated in Figure 1.

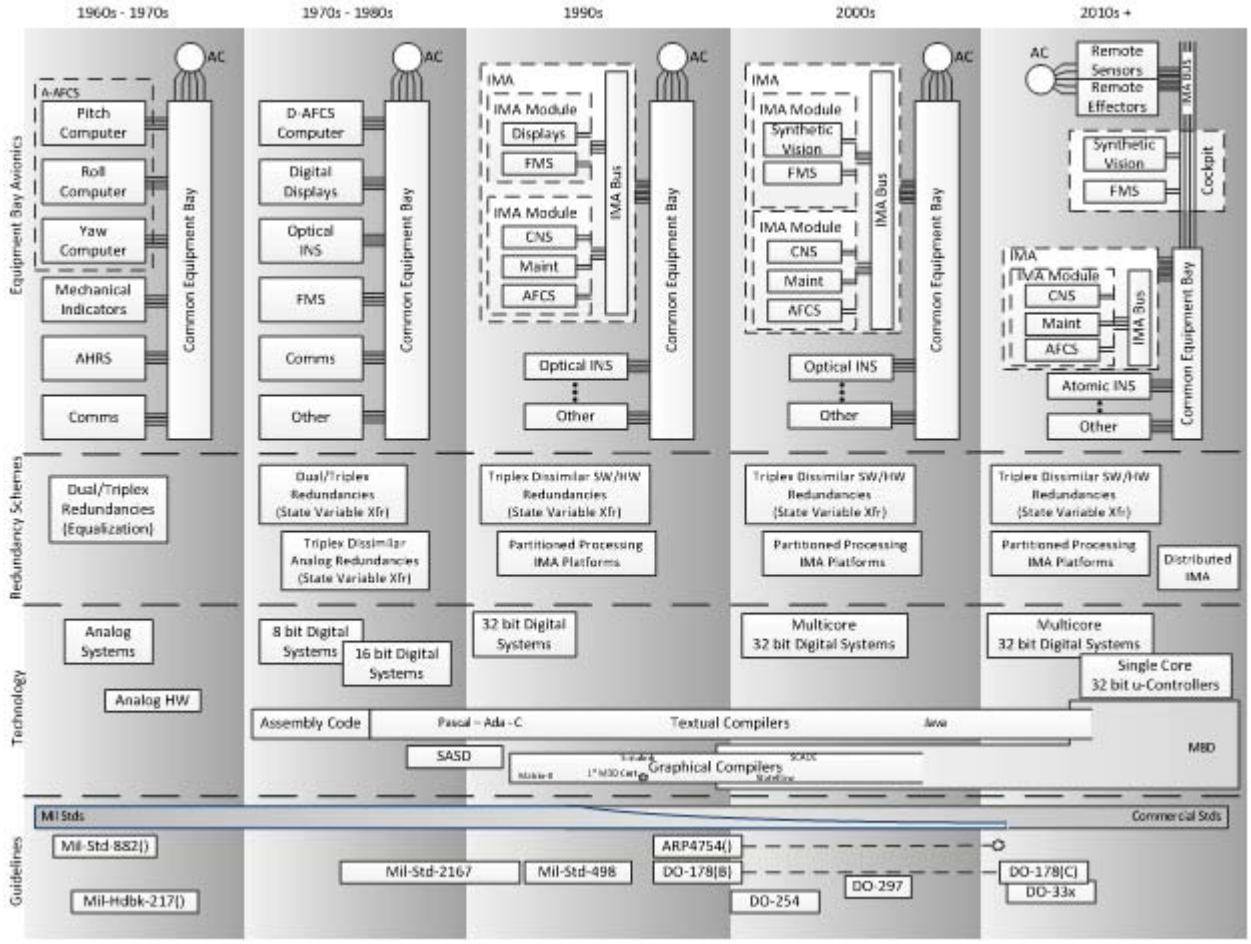


Figure 1. Historical Trends in Avionics

Equipment bay picture: Interestingly the functional partitioning within the equipment bay has hardly changed over the last 50 yrs. Individual computers of a major function such as an autopilot were merged into an overall autopilot function in the switch to digital computing. However, the advent of IMA technology did nothing more than provide temporal and space partitioning so that the individual functions could share the same processing resources. So, functionally the equipment bay remains much

the same in terms of separation of function by purpose as it was 50 yrs ago. There has been little merging of functions one would have expected from IMA architectures.

The direction over the years has been to co-locate and share resources. However, this trend looks like it may reverse. The comparatively low cost and increasing capability of microcontrollers is in competition with the expensive partitioned systems and expensive safety partitioning necessities. With the application of high integrity, high speed and range of bus networks the equipment bay contents will likely change as functions become more distributed throughout the aircraft.

Redundancy approaches: Redundancy approaches have remained constant within the variations of simplex, dual, triplex, quad systems that use equalization or state variable transfer to synchronize computations. Voting techniques and fault identification remain largely the same although processing lock step pairs added some variation demanded by the integrity needs of partitioned resource sharing. IMA demands on temporal separation influenced the emergence of ARNC-653 compliant backplanes. The expected changes coming are in the use of long range high speed buses that span the aircraft lengths. Assurance of integrity on these busses will be critical to a distributed avionics system.

Technology: The major shift in technology application came with the switch from analog to digital processing. Thereafter changes have been capacity and performance enhancements to the digital processing elements. The immediate future shift is likely to go with the high capacity low cost microcontroller replacing the larger resource shared central processing schemes. Further in the future some areas of avionics will look to parallel processing techniques that mimic the human cortex.

In terms of development methodologies software development has moved from machine code to assembly code to textual compilations, and is currently moving more and more towards graphical compilations. MBD will become the overall trend towards conceiving and developing systems because of the significant cost savings and error management.

Guidelines: Guideline source material has shifted from military standards to commercial standards as the investment funding for technology in common avionics has shifted to commercial ventures. At the moment there are two sources of guidelines, EASA and FAA, which are in some form of competition. Current separation of disciplines will become more blurred as MBD takes over the development process from a systems perspective. With the direction towards systems guidelines themselves will need to be developed according to a systems perspective applying systems methodologies to the guideline design.

3 Operational trends that will impact avionics

Expected operational trends and issues that will impact avionics are:

Connected aircraft functions	Turning an aircraft into a network node
	Data for functions coming from other platforms while in-flight (e.g., weather)
	Introduces issues with timeliness of data, security (trusted sources, hacking), bandwidth
Security issues	Aircraft operators and manufacturers have identified many potential economic and safety benefits using e-Enabled technology and software applications
	There are many applications that will require increased aircraft connectivity to non-governmental service providers such as the internet, portable electronic devices, and commercial-off-the-shelf technologies that have not been certified and accredited for secure operations by a government authority
	Prior to the availability of e-Enabled technologies, legacy aircraft used federated architectures with limited wired or wireless connectivity to non-governmental service providers
	Legacy aircraft are now being modified to add Wi-Fi, Electronic Flight Bags, wireless Field Loadable Software, real-time aircraft health monitoring and reporting and Passenger Information and Entertainment Systems. These designs can introduce cyber security vulnerabilities beyond the scope of current airworthiness regulations and traditional systems safety assessment methods typically used to show compliance with the airworthiness requirements located in Title 14 CFR
	UAVs in NAS - maintaining separation, collision avoidance, cooperative flight
	Overhaul of air traffic control systems – using digital messaging instead of voice

4 Implementation technology trends

Expected implementation trends and issues that will impact avionics are:

Continuing increase in functional complexity	Evidenced in software lines of code • B777: 4.0 x 10^6 • B787: 6.5 x 10^6 • F35: 5.7 x 10^6
	Functions will become more interconnected
	No big initiatives by customers and OEMs to reduce functionality and complexity – keep adding features
CPU and memory physical limits	The Von Neumann bottleneck is continually getting worse • Memory latency relative to CPU speed is now 56,000 times slower than in 1985 • CPU "Hubble Radius" (physical size reachable in one CPU clock tick, round trip) – Is just 1.5" at today's typical 2 GHz CPU clock speed – Even with infinitely fast logic, a processor larger than that will incur wait states – Memory (including cache) latency now consuming half of processor throughput
	Caches can help, but don't improve worst case
	Multiple cores make the problem worse
Execution time prediction is difficult	CPU manufacturers can no longer offer cycle-accurate models of their products
	DRAM controllers now do out-of-order memory accesses (to optimize page operations)
Communication trends	Higher data rates • Need shorter media lengths for higher bit rates (e.g. 15m @ 1GB) or multiple media in a cable • Need more tightly controlled parameters (e.g., receiver thresholds, path impedances, …)
	Serial links provide (low pin count, no clock), even at card level (e.g., Serial RapidIO and PCI Express)
	N type links between cards in a box (e.g., Ethernet)
	More use of adapted COTS standards, versus avionics unique networks

5 Architectural impacts

Three aspects; behavioral, physical, and logical play against each other in the design of any system as illustrated in Figure 2.

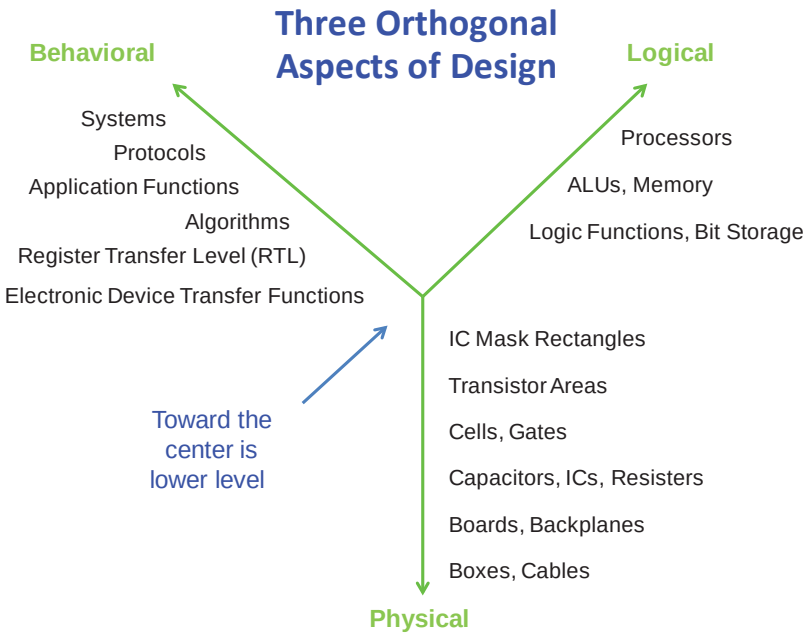


Figure 2. Three Orthogonal Aspects of Design

Trends in any of the outer to inner areas will impact the overall design trends in aircraft avionics.

Expected architectural trends and issues that will impact avionics are:

Near term trends	Higher degree of Behavioral integration
	Somewhat lower degree of Logical integration (e.g., multicore vs multitasking)
	Degree of Physical integration is mixed • Serial links provide looser coupling • Trend toward cards from different suppliers in the same box increases physical integration
Far term trends	Higher degree of Behavioral integration
	Much lower degree of Logical integration • One partition per SoC having a simple CPU, all the memory that the partition needs, and serial connections to other processors – Solution to the von Neumann bottleneck

	– Solves the problem of a low criticality partition executing a halt-and-catch fire instruction (e.g., the Intel F00F bug) that stops the execution of higher criticality partitions – Simple CPU makes accurate worst-case execution time predictions feasible • No pipeline stalls or bubbles, removes many hidden caches (e.g., branch target cache, virtual registers) – Provides protection for software intellectual property
Lower degree of Physical integration (physical distribution)	Solves the heat density problem e.g., multicore processors are at the limit of conduction cooling, can't crowd
	Solves the "Porcupine Problem" (electronics shrink to the point where there's not enough accessible surface area for all the electrical power, signaling, and cooling connections)
	Makes better use of available space throughout the aircraft

6 Design and verification tool trends

Expected design and verification tool trends and issues that will impact avionics are:

Increasing use and confidence in MBD	Avionics formal methods modeling tools lag behind other modeling methods
	Increasing sophistication of modeling tools
	Increasing computational power allows for more complicated models
	Increasing need to integrate models from different disciplines • Electrical, mechanical, software, thermal,…
	Some models need to be increasingly accurate (e.g., electrical signal path impedance modeling for high-speed signals)
	As integrated circuit design tools become more sophisticated, it may become less costly to design (semi-)custom integrated circuits
	With the increase in the number of disciplines doing modeling, the integration of models between disciplines, and the number of suppliers, one can expect a heavy burden of housekeeping that could use the help of an integration framework .

7 Impact on multi-tier regulations and verification

Potential guideline impact on multi-tier regulations and verification:

Impact on regulations	Off-board interactions and security will complicate every function – a lot. Not only will there be new requirements to protect the system from external security threats, there may need to be security requirements to protect the intellectual property of one supplier from another (e.g., software and data).
	Regulations will need to address systems more comprehensively and precisely – data sources, network and bus performance, timing, verification of data sources, distributed functions
Verification	More complex and precise descriptions of the interface between the multitier suppliers will need to be verified. In some scenarios, such as the near-term plan by some aircraft companies to have multiple cards from different suppliers in the same box, will create failure coupling paths between products of different suppliers that do not exist in federated systems or in a single-supplier IMA. For example, a card supplier may have to worry about heat, EMI, and even exploding components coming from another supplier's card.
	Suppliers will need to share their models and/or data. This can be a simple single-discipline sharing, such as requiring all suppliers that have equipment through which a signal passes to provide the input-to-output delay, in order to calculate end-to-end latency; or, it can be a complex interdisciplinary sharing, such as ensuring that heat propagation and power supply voltage fluctuations don't cause a processor to slow down to the point where it's software misses deadlines. This may cause proprietary data concerns. Compliance to COTS high-speed data network physical layer standards may need to be more stringently enforced than the COTS bodies do themselves. COTS interoperability needs only to be good enough to be economically viable. Whereas, in avionics, strict compliance may be safety critical. Given that an excessive error rate may be safety critical and can be caused by any combination of marginal driver strength, the summation of all impedance reflections along the signal path, or marginal receiver threshold, all the parameters must be precisely tested to be well away from their error threshold by all suppliers whose equipment can affect these parameters. This can be difficult when a signal is allowed to be as small as 200mV high and 0.32 ns wide (1000BASE-CX Ethernet). Similarly, it cannot be assumed that the Bit Error Ratio (BER) *requirement* stated in a standard is the actual BER that a COTS device will deliver; it must be tested

	A disturbing trend is the number of “counterfeit” parts that make it into legitimate testing “sold out the back door”. Combating this may require strict provenances or acceptance testing at handoff points in a multitier supplier hierarchy.

APPENDIX E

Certification Process in Practice

Objective: Show the airworthiness certification process in practice, with an avionics and supplier slant. Also show when the regulatory guidelines are used.

Contents

Table of Figures

1 Purpose

This part of the study outlined how the airworthiness certification process is really implemented by industry, and pays attention to contractor and supplier interactions. It gives a context for when the regulatory documents apply.

2 Caveats

This is NOT PRECISE – each project establishes its own objectives and parameters (one process does not fit all). This means no project will go through safety and certification the same way, nor will OEMs be the same (each has own process and names for analyses done by suppliers).

We stopped at Type Inspection Authorization because the rest of the TC process is directed by FAA, and OEM and suppliers should be "done". This means the diagram skips certification flight tests, continued airworthiness, Final TCBM, production certification, and airworthiness certification.

3 Certification Process

Figure 1 below is color-coded to show generally when suppliers participate in the certification process. The bubbles in the figure are explained in the following section. Figure 2 below highlights when the regulatory documents are typically used.

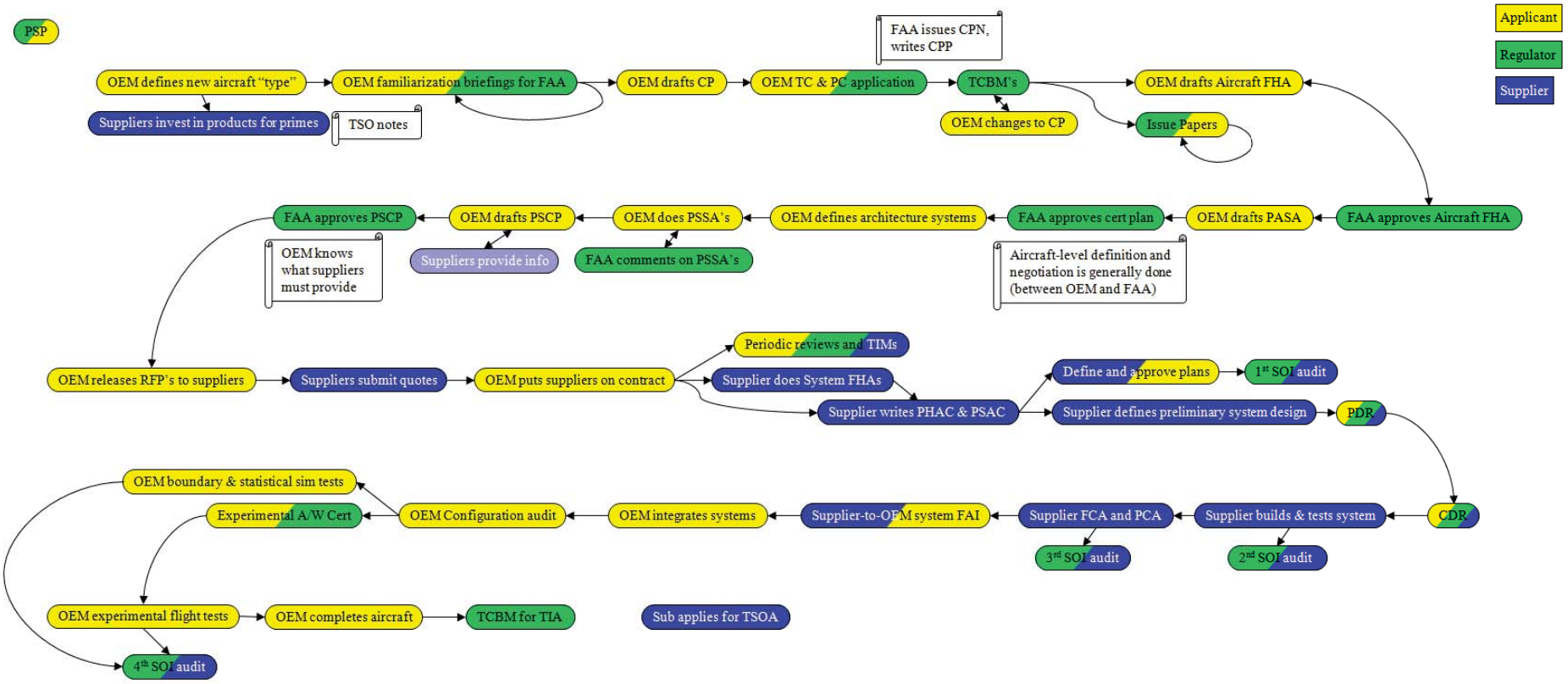


Figure 1. Certification process in practice, and generally when suppliers participate

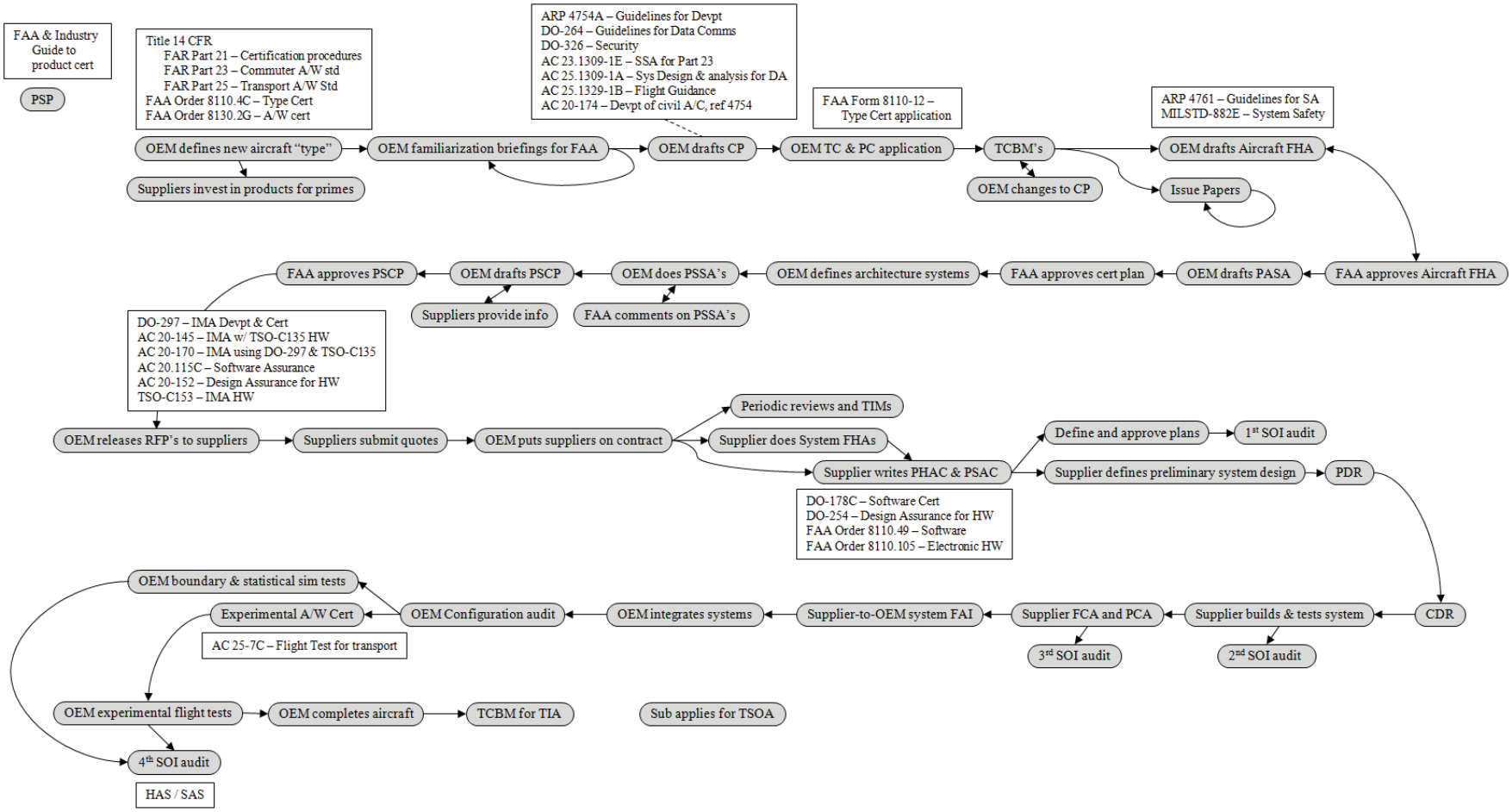


Figure 2. When are regulatory documents used in the certification process

4 Descriptions of the Steps in Certification Process

PSP – Partnership for Safety Plan

- Draft, agree, and sign a PSP.
- PSP = signed agreement how the FAA and Applicant will conduct product cert, set expectations and deliverables, set methodology for exchanging information.
- PSP is an umbrella for the OEM, under which there are project specific cert plans (PSCP's).
- Defines Training and meetings required by FAA. Identify FARs, policies, and procedures that will normally apply to the OEM (how will the OEM talk with the FAA).

OEM defines new aircraft "type"

- Define the mission / concept of operations. Include the operation sequence: steps for airline ops, pre-flight, pilots and aircraft, maintenance.
- Define operational requirements: range, speed, ceiling, fuel economy, cargo, number of passengers, number of pilots, etc.
  - This defines the aircraft type.
  - Describe the operational environment (NAS, European airspace, …).
- Hold workshops with subs for ideas. Consider functions, size/weight/power, safety, new technologies, ….
- Define the system block diagram for the aircraft.
  - Define prelim system boundaries. These boundaries will match the OEM's internal teams.
  - Make a preliminary list of TSO's wanted in the systems.
- Define function list for aircraft – taxi, navigate, altitude hold, …
- Define Preliminary Hazard List (PHL) from operation sequence, system diagram, and function list. Most of this will come from experience.
- If OEM has enough info from re-using existing components, he may define aircraft-level safety reqts (eg., redundancy).
- Airbus calls this the "platform phase".

Suppliers invest in products for primes.

- Usually marketing products with primes for the next major aircraft sale.
  - Suppliers have very few upcoming programs on which to compete. Means suppliers have to invest a lot of money to get on aircraft.
  - Primes like to keep a few suppliers around for price competition.
- Suppliers develop technology and processes to improve performance, safety, or reduce cost of certification.
- Suppliers pursue TSO's and TSOA's for some key products.
  - TSO's are good for clearly defined, re-usable products – TCAS, EGI, GPS, ….
  - Suppliers like to sell products with Technical Standard Order Authorizations (TSOA's) because a supplier can make minor changes with less re-certification cost. Hopefully, they sell the same product to multiple primes without multiple verifications.

- Primes are often interested in products with TSOA's because it means some verification has already been done, and it will save some certification costs at the aircraft level.

TSO notes.

- Technical Standard Order = minimum operating performance standard (MOPS) for a system, material, or part. Written and approved by FAA, usually with RTCA committees drafting the requirements. Usually includes requirements for reliability (supporting fault severity levels).
- TSO Authorization (TSOA) = approval by the FAA that a system or component meets a TSO.
- Reasons for TSO's:
  - Good way to compartmentalize (and do once) safety and verification.
  - Reduces costs on primes (less verification). More potential sales for suppliers. In theory, TSO's help interoperability.
  - Smaller airplane OEMs (smaller than regional airliners) ask for TSOA systems which they can drop into an aircraft. Big airplane OEMs ask for TSO functions more than TSOA boxes.
- Risks around TSO's:
  - Suppliers are "self regulating" when evaluating if a product change is within the TSO scope.
  - A TSOA does not mean an installation is approved – the OEM / consumer must install the system properly.
- Suppliers apply for TSOA's at the beginning of an OEM aircraft development because the product must be certified as part of an aircraft (use the test results for the TSOA). Primes charge suppliers a fee for using the primes' test results in the suppliers' TSOA's.

OEM familiarization briefings with FAA.

- "Ice breaker" for the concept aircraft. Big suppliers may be invited if new systems or technology is involved.
- Review operational requirements, system block diagram, function list, preliminary hazard list (PHL), aircraft safety requirements if any from legacy systems, high level schedule, major suppliers.
- If there is any new technology or new functions, show it now to the FAA (eg., 3D displays, 1 pilot, …). Give the FAA time to think about how to cert.
- FAA gives informal guidance: points to watch, position papers to read, features it thinks are good, … OEM gets an informal action item list to make updates.

OEM drafts CP (Certification Plan).

- At application time, complete CP expected for simple projects; partial CP for complex projects. Need to have enough info for FAA to determine OEM's knowledge and capability.
- CP includes:
  - Description of the design with sketches, schematics, CFR parts, components with TSO's.
  - Proposed certification basis (regulation paragraphs, exemptions, special conditions, equivalent level of safety findings), description of how compliance will be shown (analyses, ground test, flight test, …), list of docs that will be submitted to show

compliance and a compliance checklist, list of test articles for generating compliance data.
    - Project schedule, identification of DERs and their authority.
- Keep the CP current throughout the project.
- If the CP does not assure FAA of applicant's understanding, then FAA rejects the TC application.

OEM TC (Type Certification) and PC (Production Certification) application.

- This is the official start of the certification process. OEM provides an application package which includes the CP.
- Most OEMs apply for PC (from MIDO) at the same time as the TC (from FAA). PC cannot be approved until after the TC.
- FAA issues a Certification Project Notification (CPN), identifies the cert team, schedules the Prelim Type Cert Board Mtg (PTCBM).

TCBM's (Type Certification Board Meetings).

- One or more meetings triggered by the TC application.
- Review the application, review the certification basis, review and refine the CP.

Issue papers.

- FAA may write Issue Papers for difficult issues, like how to use model-based design in a project, or how to verify a new technology.
- FAA and OEM negotiate how to answer the issue papers. Normally, modifications to the CP and PSCP are results of issue papers.
- Issue papers can be written all the way up through PSSA's and the PSCP draft. They need to be resolved before approving the PSCP.

OEM drafts Aircraft FHA (Fault Hazard Analysis).

- Complete/update the PHL, and assign severity levels to the hazards in PHL.
- Identify the block and function failure conditions that can cause the hazards in PHL – use the aircraft block diagram and function list. Pay attention to new blocks and functions. This is normally done by systems or safety engineers.
- Assign severity levels to the failure conditions.
- Initial Common Cause Analysis (CCA) of faults in FHA.
- Look for integrated system hazards if know enough about the architecture - combinations of non-catastrophic failure conditions that can be catastrophic.

FAA review and approve Aircraft FHA.

- FAA does an analysis and formal review, providing action items. For major items, FAA can add issue papers.
- Once approved, the Aircraft FHA is a control point. Up to this point, the OEM has had some leeway on the level of analysis. Once Aircraft FHA approved, the aircraft definition and "negotiation" for certification requirements is done. It won't change much unless a mistake is discovered later. The Aircraft FHA drives safety requirements to all the subsys and suppliers.

OEM drafts PASA (Preliminary Aircraft Safety Assessment).

- Outlines a plan for the critical issues in the Aircraft FHA. Include issue papers, unacceptable risks, mitigations of the risks.

FAA approves cert basis.

- And also the CP?
- 8110.4c Fig 2-1 shows TCBM for CP coincident with PSCP gateway.
- Done at a TCBM. OEM officially tracking critical issues.

OEM starts defining architecture.

- Adding detail to the aircraft block diagram and function list.

OEM does PSSA's (Preliminary System Safety Assessments).

- Draw a fault tree for each hazard in Aircraft FHA.
- Define systems contributing to fault trees. Allocate severity numbers, integrity budget, and availability budget to each system.
- Review and negotiate fault trees and allocations with suppliers.
- Suppliers usually recommend mitigations at this point. Mitigations noted in PSSA and added as safety requirements on systems, like redundancy and separation.

FAA comments on PSSA's.

- May write issue papers.

OEM drafts PSCP (Project Specific Certification Plan).

- "Plans generated by one contractor are rarely efficient or effective for another. Each plan is unique to the corporate personality and management system." SSH Ch5.
- PSCP includes:
  - CP and FAA's Certification Project Plan (CPP).
  - Systems overview (hardware and software), TSO's.
  - Plan for qualification of systems, plans to answer issue papers, OEM's integration plan, flight test plan, certification compliance matrix.
  - Schedule of milestones, delegation of responsibilities to representatives
- OEM will ask selected suppliers to provide information for the PSCP. The suppliers help on the hope of getting the development and production work – ties into RFP.

FAA approves PSCP.

- Done at a TCBM. This is a control point. It specifies what the OEM and suppliers must do during design, integration, and test for certification.
- The OEM now knows what the suppliers must provide, and can start releasing RFP's to suppliers.

OEM releases RFP's to suppliers.

- In practice, an OEM will be selecting suppliers from the beginning of the effort. This is the latest point at which they will select suppliers, usually for a competitive item.
- Important that prime plan time and resources for himself to cover detailed management of suppliers. Define how the sub will be managed (risk and opportunity logs, etc.)

- Important for supplier to note any subs the suppliers will use (affected by DO-178C).
- Important to include details in contract for responsibilities and handling of changes. Include who is responsible for integration.
- The system boundaries that the OEM picks will match his own organization, and forces suppliers to propose similar scope (not mixing functions).
- Flow down for system: operational requirements, PSSA and associated mitigation requirements, safety requirements, TSO's, pieces of PSCP that apply to the supplier (required standards and processes).

Suppliers submit quotes.

- Suppliers will run trade studies beforehand to have improved technology or product to quote. Usually done on the suppliers' funding.
- Suppliers will be getting bids from their subs. The level of oversight the suppliers enforce on subs is a function of how they assess the subs' capabilities. Interviewees commented that suppliers have problems with assessing subs:
  - Suppliers often overestimate subs' capabilities; suppliers are in a hurry to pick subs because the suppliers have a time limit on quoting; does the supplier have an available evaluator qualified to assess? (experts are often busy).
  - Can an evaluator assess a sub's culture and attitude as well as capability?

OEM puts suppliers on contract.

- This may be spread out earlier in the process based on the OEM's need for information or a requested lead time.

Periodic reviews and TIMs (technical information meetings).

- In parallel to the rest of the suppliers' work.
- OEM does much of his oversight during reviews of suppliers. Likewise for suppliers to their subs.
  - Reviews are often tilted toward admin and functions instead of safety and human factors.
  - OEM does reviews with one supplier at a time – don't mix supplier meetings to protect intellectual property.
- OEM does reviews with FAA separately. May have a supplier available to answer questions.

Supplier does System FHA's.

- Fault tree analysis of system, then select mitigations of risks and set safety requirements. Used to justify design assurance level, and used in PHAC and PSAC.
- Allocate integrity and availability budgets for the system down to subsystems.
- Common Cause Analysis (CCA) of faults within the system, and look for integrated subsystem hazards.

Supplier writes PHAC (Plan for Hardware Aspects of Certification) and PSAC (Plan for Software Aspects of Certification).

- Done in parallel with System FHA's, but includes risk mitigations and safety requirements from the System FHA's.

- Include proof of compliance with requirements from the OEM's PSCP. Specifies what artifacts are needed for certification.
- Sometimes a supplier will write his own PSCP that references the PHAC and PSAC. In practice, system aspects of certification are in the supplier's PSCP.

Define and approve plans.

- Given the supplier PSCP, suppliers write plans for: software devp't, hardware devp't, verification, quality assurance, and configuration mgt. Approved by OEM.

SOI (Stages of Involvement) audits.

- FAA auditing the first tier suppliers (normally do not look at the subs to suppliers).
- 1st audit – FAA audits the plans of suppliers.
- 2nd audit – FAA looking for evidence that supplier followed plans (reviews, …). Implies the suppliers is developing designs and has sufficient evidence (~50% done).
- 3rd audit – latter half of verification, FAA looking for evidence that the supplier has complied with his verification plan.
- 4th audit – after experimental flight tests, FAA doing a wrap-up / close-out of action items from previous SOI's.

Supplier defines preliminary design.

- Systems and safety engineers flow down functional and safety requirements to hardware and software.
- Write Design Requirement Specs for subsystems / components, which capture the functional and safety requirements.
- Create compliance matrix (or plan) that says how each requirement will be verified, eg., inspection, analysis, lab test, ….
  - Certification requirements – 14CFR regs, airworthiness orders and guidelines (4754, 254, 178C), TSO's.
  - Functional requirements – must demonstrate traceability from system requirements to modules to verification test.
- Write system integration and test plan that defines the tests in the verification matrix, includes: function tests, environments to test in, reliability tests (long-term tests).
- Define software architecture, functions, state flow, sequence diagrams, ….
- Define hardware components and draft the schematics.
- Human factors assessments as applicable.

PDR.

- OEM holds PDR with each supplier separately to protect intellectual property. Main purpose is to keep OEM confident that suppliers know what they are doing.
  - Most OEM's audit a few functions or systems (conformity inspections), and deep dive to check that suppliers are being thorough.
- OEM holds its PDR with invitation to FAA. Main purpose is to maintain FAA confidence that the aircraft will be safe.

- Typical content of a PDR:
  - Review functional flow, storage, control and timing, software structures, security, development tools, test tools, documentation, resources.
  - For each configuration item, assess if meeting requirements (function, performance, safety), risk, compatibility with interfaces (and HF), reliability, manufacturability, maintenance.
- After review, hardware engineers add tests to test plan for hardware items not covered by the system tests. Same for software.
  - OEM test plan usually refers to the supplier test plans.
- Supplier starts developing test equipment (want it earlier for testing hardware and software as it is finished). Should know enough about interfaces (e.g., busses) to start picking COTS equipment.

CDR.

- For big programs, CDR may be broken into incremental meetings.
- OEM holds CDR with each supplier separately (protect intellectual property).
  - By CDR, suppliers have completed their subsystem hazard assessments (SSHA's).
  - By CDR, each supplier should know that his design will meet the severity levels.
- OEM updates PSSA's given supplier data.
- OEM holds its CDR with invitation to FAA.
  - Review allocated design assurance levels to components.
  - For each configuration item, determine that detailed design satisfies requirements (function, performance, safety), is compatible with other configuration items, assess risk (technical, cost, schedule), assess producibility and maintenance.

Supplier builds and tests system.

- Level of oversight requested by FAA done back at OEM's PSCP. If the OEM has any additional oversight, it will be specified in the supplier's PSCP/PHAC/PSAC. Supplier chooses oversight of his subs.
- Finish test equipment and qualify if necessary.
- Define test procedures as hardware is built and code is written.
- Integrate and test system.
- Run functional tests in the system test plan, and check off the compliance matrix. Usually have witnesses from the prime, maybe even the FAA. Write test reports.
- (In parallel for a long time, but done before certification) Run environmental and reliability tests. Write test reports.

Supplier FCA (Functional Configuration Audit) and PCA (Physical Configuration Audit).

- Supplier's internal "official" review of the test data. Necessary to get permission to put a system on OEM test bench or in a grounded airplane.
- Final resolution of action items.

Supplier-to-OEM System FAI (First Article Inspection).

- OEM reviews supplier's FCA, PCA. Includes reviewing supplier's test results. OEM may give a waiver for non-critical action items to move into flight test.
- OEM blesses the system, and accepts delivery of 1st prototype. Expects to use it in flight test.

OEM integrates systems.

- Follow integration test plan. Often use sims first, SIL's second, iron bird third. OEM's QA will be internal oversight.
- If the OEM wants to take credit for compliance testing during integration, they invite FAA oversight (eg., conformity inspection of test facility or SIL or …). OEM may request supplier support.

OEM configuration audit.

- "Official" review of the compliance matrices and test data, and official list of all the part numbers going into flight tests. FAA or a DER will be present.
- Final resolution of action items, or get waivers.
- OEM reviews the system safety assessment (SSA) output.
- Draft TSO compliance matrices – contain the requirements in the TSO's and MOP's and point to where the requirements were verified. Asserts that systems are verified.
- Supplier's provide SAS (software accomplishments summary) and HAS (hardware accomplishments summary) – summary of what has been done for verification and lists problem reports.
- Complete compliance matrices for the CFRs and cert basis.

OEM boundary and statistical sim tests.

- Run sim tests in lieu of on-aircraft tests that are too expensive or dangerous to fly. Example, 10,000 monte carlo simulation runs for autolanding used for cert credit.
- Parallel to the experimental flight tests. Normally use a SIL which has been inspected for conformity. May also use a collection of simulation tools from earlier.

Experimental A/W (airworthiness) cert.

- OEM applies for cert. Review flight test plan (in PSCP) with FAA. If FAA is content, grants experimental cert.

OEM experimental flight tests.

- Fly tests with 1st prototype aircraft and test pilots. Lots of data collection. FAA pilots invited to participate at the end of the flight tests.
- Write and deliver flight test report to FAA. Used for certification credit.
- The aircraft is complete enough to fly, but is probably lacking interior finishing.

OEM complete aircraft.

- Finish interior. Test lighting, oxygen, seats, …
- OEM has started setting up production lines to build the interior.
- Must close all non-compliances before applying for TIA.

TCBM for TIA (Type Inspection Authorization).

- “Preflight TCBM”. FAA reviews the results of the OEM’s flight tests, OEM’s compliance reports, reliability test results (from OEM and suppliers).
- If FAA is satisfied, they authorize type inspection flight tests.

Supplier applies for TSOA.

- After FAA has completed their flight tests, supplier uses test results to get box “stamped”.3

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01- 11 - 2014	Contractor Report	

4. TITLE AND SUBTITLE

Regulatory Compliance in Multi-tier Supplier Networks

5a. CONTRACT NUMBER

NNL13AA04B

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Goossen, Emray R.; Buster, Duke A.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

534723.02.02.07.30

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

NASA Langley Research Center
Hampton, Virginia 23681

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)

NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

NASA/CR-2014-218550

12. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Unlimited
Subject Category 62
Availability: NASA CASI (443) 757-5802

13. SUPPLEMENTARY NOTES

Langley Technical Monitor: Wilfredo Torres-Pomaoles

14. ABSTRACT

Over the years, avionics systems have increased in complexity to the point where 1st tier suppliers to an aircraft OEM find it financially beneficial to outsource designs of subsystems to 2nd tier and at times to 3rd tier suppliers. Combined with challenging schedule and budgetary pressures, the environment in which safety-critical systems are being developed introduces new hurdles for regulatory agencies and industry. This new environment of both complex systems and tiered development has raised concerns in the ability of the designers to ensure safety considerations are fully addressed throughout the tier levels. This has also raised questions about the sufficiency of current regulatory guidance to ensure: proper flow down of safety awareness, avionics application understanding at the lower tiers, OEM and 1st tier oversight practices, and capabilities of lower tier suppliers. Therefore, NASA established a research project to address Regulatory Compliance in a Multi-tier Supplier Network.

15. SUBJECT TERMS

Avionics; Complexity; Compliance; Guidelines; Life-cycle; Model-based development; Outsourcing; Risk; Safety; Suppliers

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
					19b. TELEPHONE NUMBER *(Include area code)*
U	U	U	UU	183	(443) 757-5802