A PRACTICAL APPROACH FOR AIRCRAFT SYSTEMS REQUIREMENTS VERIFICATION IN COMPLIANCE WITH ARP4754

Nicole Cardili, Leonardo Helicopters, Samarate, Italy
Filippo Simonetti, Leonardo Helicopters, Samarate, Italy
Valerio Zanetti, Leonardo Helicopters, Samarate, Italy
Maurizio Parolini, Leonardo Helicopters, Samarate, Italy

Abstract

This paper illustrates a verification process compliant with ARP4754 guidelines to achieve the System level requirement Verification. The system verification process described has been developed and applied for the civil certification of the Fly-By-Wire Flight Control System (FCS) of the AW609 tiltrotor by Leonardo Helicopters and reviewed by the Federal Aviation Administration (FAA). The verification process proposed is based on the FuSE approach and is highly interconnected with the Validation FuSE process: it has been achieved by integrating the certification requests with the pre-existing process while minimizing disruptions on the ongoing development process.

Fly-By-Wire FCS is a fitting example of complex system, since it is required to provide safety-critical functions continuously throughout the mission, and it is deeply interconnected with most of the aircraft systems, e.g. hydraulics, drive system, powerplant, avionics, etc. The verification process proposed considers also the verification of all the other areas.

1. NOTATION

The following acronyms will be used throughout the paper:

ARP	Aerospace Recommended Practice
AVS	Air Vehicle Specification
AWPC	Agusta Westland Philadelphia Corp.
CLAW	Control Law
CM	Configuration Management
DAL	Design Assurance Level
DOORS	Dynamic Object-Oriented Requirements System
ERF	European Rotorcraft Forum
ECR	Engineering Change Request
FAA	Federal Aviation Administration
FBW	Fly by Wire
FCS	Flight Control System
FHA	Functional Hazard Assessment
FuSE	Function-Based Systems Engineering
IBM	International Business Machines
IRS	Interface Requirement Specification
LHD	Leonardo Helicopters Division
PLM	Product Lifecycle Management
PR	Problem Report
PSSA	Preliminary System Safety Assessment
REDMAN	Redundancy Management
RMT	Requirements Management Tool
SAP	System Applications and Products in Data Processing
SCD	Source Control Drawing
SME	Subject Matter Expert
SSS	System / Subsystem Specification
TRR	Test Readiness Review

2. INTRODUCTION

The work presented herein is a follow-up of a previous research on an original approach for tailoring and applying of ARP4754 guidelines (Ref. 3). While the prior work was focused on Validation activities, the current paper extends the framework to include Verification.

According to the guideline as per ARP4754 (Ref. 1), verification process should begin after the completion of the validation process. Furthermore, if the project was already in an advanced stage of development when compliance to ARP4754 became mandatory, the identified process should comply to certification guidelines and should also fit to the already existing process, reusing as much previously produced material as possible.

This paper proposes a method for applying SAE ARP 4754 guidelines (Ref. 1) to system requirements verification, suitable for any aircraft complex system. The proposed method can be used either to establish a new process or to tailor a preexisting one, maximizing the result and minimizing costs and effort. The verification methodology proposed is integrated with the validation process described in Ref. 3 and is therefore based on the Function-based Systems Engineering (FuSE) method introduced in Ref. 2.

Consequently, the suggested verification process is divided into three main phases: prepare for verification, perform verification, and manage verification results. This paper provides methodological solutions and guidance for each phase, as summarized in Table 1, addressing various aspects of the verification process.

Table 1 - Process solutions for each verification phase

Prepare for verification	**Perform verification**	**Management verification results**
Process definition with FuSE approach	Verification by Functions	Verification summary Structure
Digital development environment setup (in accordance with validation environment)	Verification evidence from other level (reusage of verification activities from item level, aircraft level, etc.)	Verification knowledge management
Validation Matrix	Verification evidence from other aircraft system activities (reusage of verification activities from avionics, hydraulics, etc.)	
Verification Matrix structure		
Testing verification environment setup		

3. PREPARE FOR VERIFICATION

3.1. Process definition with FuSE approach

When the FuSE validation process is adopted, the most effective and efficient verification methodology is also based on the FuSE approach.

In the AW609 FCS validation and verification example, the FuSE approach was applied to both validation and verification activities.

The verification carried out function-by-function, instead of requirement-by-requirement, offers several advantages.

Verifying the function means to verify the implementation of each single requirement in the function. Since they all pertain to the same functionality it grants:

1. Better overall understanding of the System functionality
2. Reuse the knowledge about the function gained during validation activities to identify all the possible test cases
3. Increase confidence in the completeness of the verification performed
4. Simulation and testing scenarios that trigger function-level behaviors, allowing multiple functional requirements to be verified simultaneously. These verification evidence can be traced directly to the function.

For complex systems, the functions can be further decomposed into subfunctions during the validation phase (see Ref. 3 for further details about function and subfunction decomposition during validation phase). Verification can then be conducted either at subfunction or function level, depending on the level of complexity of the functionality being addressed.

3.2. Digital development environment setup

In the context of system requirements V&V, the digital development environment consists of the set of tools, databases, and their customizations (including embedded workflows) used to perform and support process activities. At a minimum, the environment should provide the capabilities to store requirements and verification evidence, support change control and signature processes, involving the Certification Authority or its delegates and allowing data sharing with the technical specialists who receive or refine requirements.

To meet these needs, the environment should include:

1. A Requirements Management Tool (RMT), with modules and traceability between requirements, functions, and verification items.
2. A version-controlled database to collect supporting evidence in various formats: test procedures, analysis documents, review meeting minutes, etc.
3. A tool to issue official documentation and support the signature process.

For the AW609 FCS case, the three tools adopted were respectively IBM DOORS, Serena Dimensions, and SAP (Figure 1).

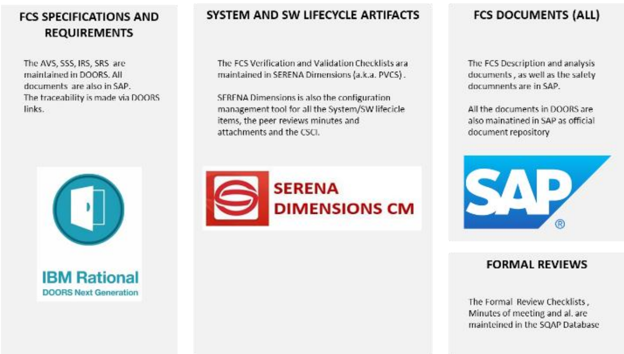

Figure 1 - Development Environment Elements

The AW609 Fly-by-Wire FCS V&V activities had additional needs for the environment due to the highly interconnected system, hence requirements validation and verification activities heavily depend on information exchanges with other technical areas. This translates in the necessity for the digital environment to support cross-team collaboration. The solution adopted was to finely configure the environment, especially the requirements management tool. This was achieved by the following means:

1. Mapping of all data required to RMT structure elements and other tools, to define a module and inter-module links structure compliant with ARP guideline.

2. Defining views in each tool and RMT module aligned with the deliverables required by ARP4754 and agreed with the Authority.

3. Definition of a change control workflow, with each step mapped to a tool and to a user profile.

4. Defining detailed user profiles and permissions, aligned with workflow roles.

3.3. Validation and Verification Matrix

During the Verification Process, two main streams must be monitored:

1. The validity of the function and requirements to be verified
2. Verification activities progress.

According to guidelines as per ARP4754, a requirement can be verified only if it has been already validated. It's essential to track the actual status of each requirement during verification activities (e.g., if the requirement is still under work, or if the requirement is valid or not). Only requirements completed, reviewed and fully validated, make sense to be verified to reduce rework. It is also important that all the other requirements pertaining to the same function are all valid and reviewed to avoid verification effort while is not confirmed if the function is complete and correct.

Once the requirement is reviewed and valid, its verification status must be tracked. The verification status needs to consider the progress of the verification, the status of the verification item used to verify the requirement and the scoring of the result run on the actual system under test (the latter applicable only in case of verification by testing).

This leads to consider a requirement verified only when an independent review along the verification item has been successfully conducted, and the verification result on target is the one expected. In case the verification is perform via analysis, it's important to retrieve and to review all the analysis before considering a requirement fully verified. The categorization of each requirement, along with the verification method chosen, can speed up the process: possibly, requirement with similar categorization can be verified with the same verification method and verification item. To keep track of all this information, the Verification Matrix can be set with the following attributes, as suggested in ARP4754- (Ref. 1):

- Unique Requirement ID
- Validation status of the requirement
- Requirement categorization (including pertaining FCS function and in case of integration/interface requirement the other applicable area)
- Verification Methods used (Test, Analysis, inspections, etc..)
- Verification Conclusion (Verified, Not Verified)
- Verification evidence collection
- Verification result

3.4. Testing verification environment setup

To support integration and formal V&V activities, a dedicated test environment is necessary.

Due to the nature of systems requirements, the verification cannot rely solely on software test on target (this type of verification ca be delegated to software verification).

The system verification, especially for integration requirements or end to end requirements, requires to be tested in an environment that closely replicates the Aircraft itself.

Since Aircraft availability maybe be limited or nonexistent during early project phases, an initial investment on a laboratory testing environment can be highly beneficial. It enables early testing even when the Aircraft is not yet produced (for example in a new project) or if the aircraft is overbooked for other activities. Along, the lab testing can be an expensive investment, but eventually will reduce the testing cost compared to testing on the aircraft itself.

The laboratory testing environment should replicate the aircraft environment as closely as possible. This means that it should be an integrated laboratory testing, that includes different benches (Avionics, Flight Control Systems, Hydraulics, Cockpit, etc..).

The testing environment should include as much environments as possible. A complete testing bench, with the cockpit can be used not only for system end to end or integration tests, but also from pilots for simulated flight test. The integrated bench can be used for initial pilot training, before using the aircraft, and to test corner case or risk conditions in a complete safe environment.

To do that, the testing environment must be representative of the aircraft.

4. PERFORM VERIFICATON

4.1. Verification by Functions

As explained in §3.1, the FuSE approach gives a methodology to subdivide the verification work along functions and subfunctions. The subfunctions are the elementary blocks for the system validation activities as well as for the system verification activities.

Following the decomposition described in Ref. 3 in subfunction and in RedMan (Redundancy Management) and Claw (Control Laws), the verification activities can be likewise decomposed to assigned to each specific discipline specialist the corresponding subfunctions.

Testing all the requirements of the same functionality together helps in reducing costs and allow to achieve a greater confidence on the verification coverage. The verification activities must be organized following ARP4754- (Ref. 1) independency rules:

- Requirement Originator and Requirement Reviewer (during Validation phase)
- Requirement Originator and Test Procedure Originator
- Test Procedure Originator and Test Procedure Checklist Reviewer.

The verification process and methods must be captured in the Verification Plan, as suggested by the ARP4754.

4.2. Verification evidence from other level

The main efforts of verification process are producing and running verification evidences (like test, analysis, ecc) and scoring the verification results.

To increment efficiency and reduce time and costs effort, the knowledge and especially the verification items must be shared between different level form the same areas (for example system and software as displayed in Figure 2).

System verification can take credit from verification activities carried out at other system/sub-system levels, leveraging by appropriate traceability. To be compliant with ARP4754, each verification item must satisfy the applicable verification checklist included in an approved verification plan.

This shared verification held to reduce time and costs for both system and software verification process and grant greater confidence of the integrated system.

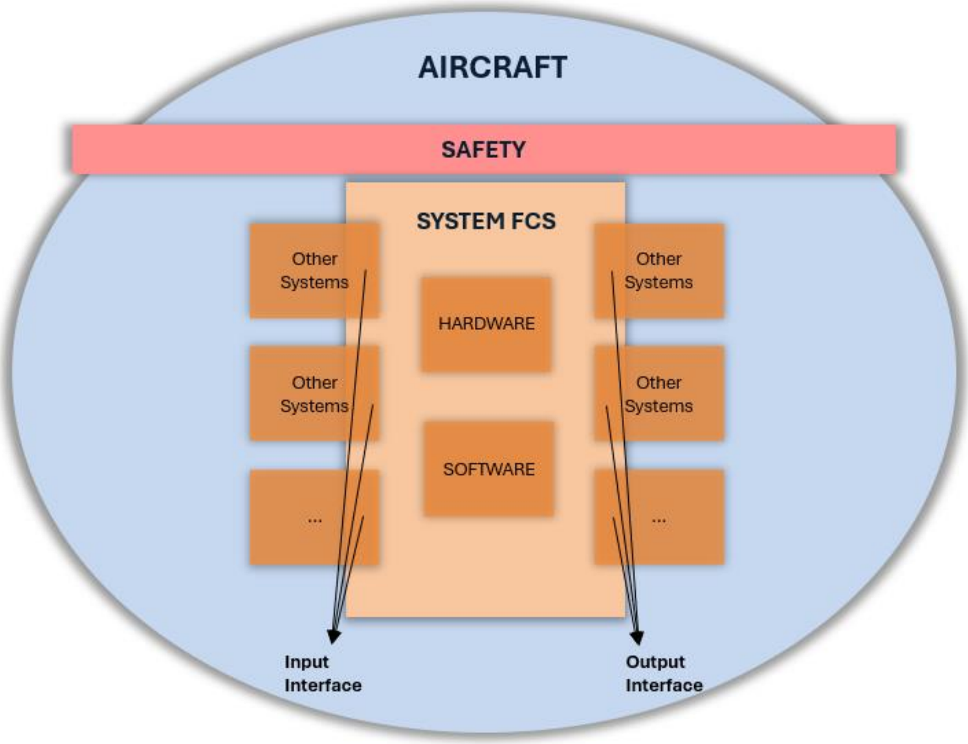

Figure 2 – System and Sub-System Integration

4.3. Verification evidence from other aircraft system activities

Another verification evidence sharing is between other aircraft activities.

To make sure that the verification evidence is applicable and fully verify the system requirement, the verification item must be checked against the requirement and the verification checklist.

Moreover, using the same verification items grants the correctness of integrated system implementation.

Sharing verification items allows to reduce the verification effort both at system level and globally to the program.

5. MANAGEMENT VERIFICATION RESULTS

5.1. Verification Summary structure

As per ARP4754- (Ref. 1) the verification summary is a report that mainly contains:

- Verification matrix
- Collection and description of any significant deviation from the verification plan
- Collection of all the problem report system and, in case of safety impact, a description and assessment of the problem report and impacts
- Identification of all the supporting data used

In the presented approach to system requirements verification, it has been agreed with the Certification Authority to capture this kind of report – as well as the validation summary – in a final System Certification Summary.

5.2. Verification knowledge management

During verification process of AW609 FCS, several strategies have been adopted to manage the knowledge acquired gradually. All the material, from test procedure and script, partial results, analysis, has been stored, even if drafts. All the material retrieved was recorded in case useful for requirements with the same category or pertinent to the same subfunction.

The verification item used, the checklist and the scoring with the result along with the verification method used has been captured per each requirement in the verification Matrix.

The Validation and Verification results have been collected in a single document to increase readability and ease access to information about system V&V for certification authority.

6. CONCLUSIONS

The proposed solutions were fully applied for the certification process of AW609 onboard systems and approved by the Certification Authority. The main point proposed are:

1. A validation and verification process with function-based approach. This held to see the system as multiple functions, hence as a subset of requirement to be analyzed as a whole, and not as isolated requirements. To help the activities, is necessary to decompose the top-level function (suggested by ARP4754) into adequate subfunctions.
2. Definition of process, tool customization and verification approach to reduce efforts and cost.

Sharing of verification evidence and knowledge between different aircraft areas and between different level in the same areas contributes to increase the knowledge itself and to grant a better confidence on the system developed while reducing global effort.

Despite the methods described above and in Ref.3 was tailored for the first issue of ARP4754 and ARP4761, the authors believe that this work defines an approach that can be compliant also to the latest standards revisions.

Author contact:

Nicole Cardili, nicole.cardili@leonardo.com

Filippo Simonetti, filippo.simonetti@leonardo.com

Valerio Zanetti, valerio.zanetti@leonardo.com

Maurizio Parolini, maurizio.parolini@leonardo.com

7. REFERENCES

1. “Aerospace Recommended Practice (ARP) 4754 Certification Considerations for Highly-Integrated Or Complex Aircraft Systems” Society of Automotive Engineers (SAE), 1996-11-01

2. Hutcheson, R. S., McAdams, D. A., Stone, R. B., and Tumer, I. Y., “Function-Based Systems Engineering (Fuse),” International Conference On Engineering Design, Paris, France, August, ICED’07/470

3. Turco L, Zanetti V, Cardili N, Parolini M, “A Practical Approach for Aircraft Systems Requirements Validation in Compliance with ARP4754”, 2024 European Rotorcraft Forum