Orbital CS
Carretera de Artica 29, 3ª Planta
31013 ARTICA (Navarra)
Tel. +34 848 47 31 81

FEASIBILITY ANALYSIS OF INNOVATIVE PRACTICES IN VIRTUAL TESTING METHODS FOR AIRCRAFT CERTIFICATION

Project: FAVIT

Grant Agreement nº: 864475

D2.1.Identification of Challenges of New Virtual Testing Methods in the Current Aircraft Certification

DUE DATE OF DELIVERABLE: 31/03/2021

ACTUAL SUBMISSION DATE: 25/06/2021

START DATE OF THE PROJECT: 01/10/2019

PROJECT DURATION: 30 months

DISSEMINATION LEVEL: PU (Public)

This project has received funding from the Clean Sky 2 Joint Undertaking (JU) under grant agreement No 864475.
The JU receives support from the European Union's Horizon 2020 research and innovation programme and the Clean Sky 2 JU members other than the Union.

Orbital CS
Carretera de Artica 29, 3ª Planta
31013 ARTICA (Navarra)
Tel. +34 848 47 31 81

Document Change Log

Iss./Rev.	Date	Section / Page	Change Description
D2.1_v1	03/06/2021	All	Version submitted
D2.1_v2	18/06/2021	4.1.3, 5.3	dSPACE comments included

This project has received funding from the Clean Sky 2 Joint Undertaking (JU) under grant agreement No 864475.
The JU receives support from the European Union's Horizon 2020 research and innovation programme and the Clean Sky 2 JU members other than the Union.

Contents

LIST OF TABLES

EXECUTIVE SUMMARY

FAVIT's main objective is to deliver a set of knowledge-based proposals for the improvement of aerospace standards and guidelines for the system suppliers and aircraft manufacturers. FAVIT will analyse the current aerospace standards and guidelines to identify how the design and verification processes can be enhanced to accelerate the processes using the state-of-the-art technologies based in virtual testing.

The purpose of this deliverable is to identify the challenges that lay ahead for the incorporation of a new certification process that would incorporate significant use of Virtual Testing Technologies (VTTs).

The contents of this document are partly derived from analyses of several existing standards documents that are used in the aerospace industry today (see ***[D01.a]***).

The current industry preference is to use Integrated Modular Avionics (IMA) systems for airborne systems. Therefore, a supplementary analysis of the document RTCA DO-297 – *Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations* ***[RTCA DO-297]*** has also been performed, the results of which are presented in this document.

Several challenges have been identified in the pursuit of using VTTs for the certification of airborne systems:

- Demonstration of equivalence between a Virtual Test Environment (VTE) and a real environment
- The technological challenges of implementing a VTE
- Updates to current standards
- Standardization of the conclusions of this report

The conclusions of this document are three-fold:

- How to match a VTE to the Design Assurance Level (DAL) of the component under test
- Adopt a requirements/design philosophy that would not only promote portability between a target environment and a VTE, but also reduce the amount of testing needed in a real environment.
- Guidelines (standards) for the use of VTTs are needed

REFERENCED DOCUMENTS

[D01.a]	*Gap Analysis*
[RTCA DO-297]	*Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations November 2008*
[RTCA DO-178/C]	*Software Considerations in Airborne Systems and Equipment Certification, December 2011*
[RTCA DO-254]	*Design Assurance Guidelines for Airborne Electronic Hardware, April 2009*
[D100.3.6.1_a]	*Virtual Testing Methods Definition, December 2017*
[CAST-32A]	*Certification Authorities Software Team (CAST) Position Paper Multi-core Processors, November 2016*

1 INTRODUCTION

1.1 PURPOSE

Airborne systems comprise different aircraft functions that are typically assigned a Design Assurance Level (DAL). Those functions may be based in hardware, software, or a combination of the two. The DAL is categorized from A (the highest level) to E with A being the most safety-critical. The higher the DAL of a function, the more data is needed as evidence to support the certification of that function for use in an aircraft.

The development and verification of software and hardware aircraft functions with a DAL of A or B are typically performed on a fully-representative test rig using real avionics equipment, sometimes known as aircraft zero (A/C0). The results of the verification process are used to form part of the certification data. It is also common that functions with lower DALs are heavily tested in a real environment because it is often the only such environment available.

This can be problematic because of the following reasons:

- Such test rigs are expensive to build and maintain
- Therefore, they are not readily available due to high demand.
- They are not usually available during earlier phases of the project so individual suppliers of hardware or software must use alternative (simulated) test environments to progress through their development lifecycle

The purpose of this document is to identify the challenges that may lie ahead in the consideration of using Virtual Testing Technologies (VTTs) for the certification of airborne systems.

The main problem with using VTTs to validate/verify aircraft functions is how to ensure that those functions will demonstrate the same behaviour in a real aircraft environment as they do in a Virtual Testing Environment (VTE) and so avoid the need to repeat VTE testing in a real testing environment.

It is assumed that the reader is familiar VTTs as described in ***[D100.3.6.1_a]***.

1.2 CONTENTS

The Identification of the challenges in the application of VTTs to certifiable airborne systems is largely based on the analyses of several existing standards documents used by the industry to see if and how VTTs are considered.

The *Instituto Nacional de Técnica Aerospacial* (INTA) certification authority has also provided some input to this document.

Document ***[D01.a]*** is a previous analysis of three standards documents for the absence of VTT considerations. The reader is encouraged to be familiar with that document.

Section 2 of this document shall present a brief summary of ***[D01.a]***.

Section 3 is a summary of a similar analysis performed on the ***[RTCA DO-297]*** document. A fully-detailed analysis of ***[RTCA DO-297]*** is provided in ***Annex A***.

Section A.3 identifies various challenges that have arisen when considering the use of VTTs in the certification process of airborne systems.

Section 5 presents the conclusions of this report.

1.3 DOCUMENT HIERARCHIES

There are relationships between the documents that have been analysed. Whether the avionics system under development is a federated one or an Integrated Modular Avionics (IMA) one:

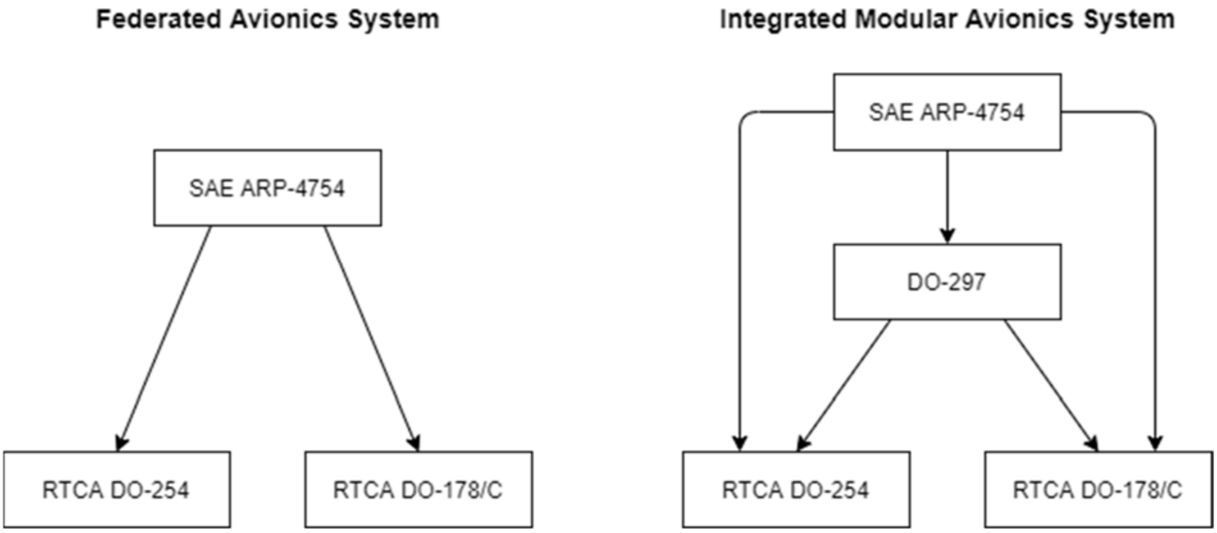

Figure 1 - Document Hierarchies

SAE ARP-4754 serves as a parent document to both ***DO-254*** and ***DO-178/C*** which deal with the specifics of hardware and software certification respectively. In the case of an IMA system, ***DO-297*** also serves as input to the afore-mentioned two documents.

2 PREVIOUS GAP ANALYSES

The previous gap analysis was performed on the following documents:

- **SAE ARP-4754**
  "Certification Considerations for Highly-Integrated or Complex Aircraft Systems."
- **RTCA DO-254**
  "Design Assurance Guidelines for Airborne Electronic Hardware."
- **RTCA-DO178/C**
  "Software Considerations in Airborne Systems and Equipment Certification"

For the complete analysis of these, see document ***[D01.a]***.

Here is a summary of the contents of those documents and the conclusions of the analysis.

2.1 SUMMARY OF CONTENTS

2.1.1 SAE ARP-4754

This is a top-level guide to the overall development process for certification of the whole avionics system of an aircraft.

The specific certification of hardware and software systems are delegated to RTCA DO254 and RTCA DO178/C respectively.

The document introduces the concept of Item Development Assurance Levels (IDALs). These identify the criticality of a failure of a software or hardware function. Level A being the most catastrophic and level E having no safety impact.

The consequence being that functions with a higher IDAL must be subjected to more rigorous testing and certification criteria.

2.1.2 RTCA DO-254

This document is used as a guide to the hardware development process for a certifiable airborne system.

The document will be used to help define project standards and procedures that will influence the development of requirements, design and testing methodologies throughout the hardware engineering lifecycle.

Hardware functions are also assigned a Design Assurance Level (DAL) which is akin to the above-mentioned IDAL.

2.1.3 RTCA DO-178/C

This document is used as a guide to the software development process for a certifiable airborne system.

The document will be used to help define project standards and procedures that will influence the development of requirements, design and testing methodologies throughout the software engineering lifecycle.

Software functions are also assigned a Design Assurance Level (DAL) which is akin to the above-mentioned IDAL.

2.2 SUMMARY OF CONCLUSIONS

For each of the three documents analysed, various “gaps” in the consideration of VTTs were identified. These are either ambiguities in the existing contents of the documents or the absence of VTT considerations at key points in the document.

2.2.1 SAE ARP-4754

The following “gaps” were identified:

1. The requirements validation section mentions “modelling validation” which would be applicable to a Model-In-The-Loop (MIL) Virtual Testing Environment (VTE), but it lacks any detail about this could be used.
2. The requirements verification section states (somewhat ambiguously) that modelling can be used for “other purposes”, but it does not elaborate on this.
3. Only modelling is mentioned as a validation/verification method. There is no mention of other VTTs such as Software-In-The-Loop (SIL), Hardware-In-The-Loop (HIL) or Virtual Processor-In-The-Loop (VPIL).

2.2.2 RTCA DO-254

The gaps identified in this document are:

- Why is there no consideration of defining a test environment during the planning process?
- Modelling (and therefore MIL Virtual Testing) could be used during requirements and design elaboration but there is no mention of this.

- There is a lack of discussion about what “other verification methods” could be used when the “intended operational environment” is not available
- The use of models in simulations is mentioned as part of the “analysis” verification activity

2.2.3 RTCA DO-178/C

Six gaps were identified in the analysis of this document:

- The software integration process objective is to use the target computing platform, but the test activity of this process allows other test environments. This seems contradictory.
- Ambiguity in the meaning of the word “compatible” when demonstrating that the software is compatible with the target computer
- It is unclear if “target computing environment” means only the LRU being tested or a full A/C0 type environment
- “Correct operation of the software” needs to be defined in relation to the testing objectives
- There is no cohesion between test objectives, test activities and the test environment
- There is no consideration of test environments in relation to DALs

3 SUMMARY OF DO-297 ANALYSIS

Integrated Modular Avionics (IMA) is now commonplace within the industry. In modern commercial avionics it has mostly replaced federated avionics systems. Because of this an analysis of ***[RTCA DO-297]*** *"Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations"* has been performed.

For a complete analysis of ***[RTCA DO-297]*** see ***Annex A. Analysis of DO-297***.

What follows below is a summary of that analysis.

3.1 SUMMARY OF CONTENTS

[RTCA DO-297] is a guide to the incremental acceptance of Integrated Modular Avionics (IMA) systems. The main point being that since IMA *is modular* it allows different components of the system to follow a different development path. "*Acceptance*" meaning that the data (or evidence) generated by the development process is sufficient to be certified for use on an aircraft.

The document defines three major components:

- IMA Platform
- Hosted Applications
- IMA System

The document defines six incremental acceptance tasks that each deal with different development activities which, in total, cover the acceptance of all three of the above components.

The IMA Platform contains all the modules needed to build a target environment that can host applications on the target hardware. This includes any hardware modules, low-level software (drivers), Operating System (OS) software, Board Support Package (BSP) software and application interface software. The platform is independent of aircraft functionality and can be certified by itself.

Hosted applications can be either dedicated hardware components or software partitions executing on the IMA platform. Applications can be aircraft-specific or more generic and reusable between aircraft projects.

The IMA System is the combination of the platform and the applications. For a specific aircraft, the IMA system must be certified.

The goal of incremental acceptance is to avoid the need to re-certify the entire IMA System when a change is introduced. That change may be an update to an application, a new application, or even a different aircraft.

If an application changes it can be re-tested and the IMA System can be certified without re-testing the IMA Platform.

If any part of the IMA System is re-used on a different aircraft, the goal is to re-use as much of the certification evidence from the original aircraft as possible. Thus, avoiding the certification effort on the new aircraft.

3.2 SUMMARY OF CONCLUSIONS

Four points of interest arose from the analysis of ***[RTCA DO-297]***.

1. There is no consideration of VTEs in the definition of the incremental acceptance tasks.
   Some of the incremental acceptance tasks could be done without real target hardware in a VTE
2. The categorization of platform-dependent and platform independent modules of the IMA platform could be encouraged.
   Some modules of the platform could be hardware-independent (e.g. scheduler, application interface, generic fault management logic) which would allow them to be tested in a VTE.
3. The term “re-use of acceptance data” could be applied to application testing in a VTE
   Only re-use between different aircraft is considered. If non-platform-dependent components can be functionally tested in a VTE then why not re-use this acceptance data?
4. The document could promote the use of data signal concentrators in the IMA platform
   The platform could provide data signal concentrators to act as application-level drivers for different types of hardware interfaces. All other applications that need such data would use the standard OS interfaces. This would allow a VTE to simulate the required data. Testing of an application’s interaction with the real hardware may not be necessary.

It should also be noted the ***[RTCA DO-297]*** does not consider different DALs when discussing the incremental acceptance development processes.

4 IDENTIFICATION OF CHALLENGES

The industry standard documents analysed do not provide much guidance for the use of VTEs in the certification process. Current practice relies heavily on real target environments for the verification process, especially so (if not exclusively so) for DALs A and B.

The problem with VTEs is how to assure that the real target environment is sufficiently well reproduced so that any verification data obtained would equate to real data obtained from the real environment. The higher the DAL, the more important this becomes. ******

To date, the standards do not offer guidance in how to achieve this equivalence between the two environments, nor how to demonstrate such an equivalence.

This is perhaps the biggest challenge.

Another challenge is the construction of VTEs which is a technological challenge. The fidelity of a VTE to the real environment is dependent on the technology available and the inherent cost of creating the environment. After all, if a VTE is more expensive and time-consuming to construct than an AC/0 test rig, then there would be no benefit in using a VTE.

These challenges, and others, are discussed in the following sub-sections.

***** INTA have also identified the need to assess to what DAL the use of VTTs may be applied.***

4.1 DEMONSTRATION OF EQUIVALENCE

Any VTE that claims to represent a real environment must be able to support that claim. To do this there are essentially two options:

- Analysis of the VTE/Real environment
- Repetition of results

4.1.1 Analysis

This would involve an initial analysis of the characteristics of each environment with particular emphasis on those which have a direct interaction with the aircraft function(s) to be tested in that environment. For example, if a host computer simulation of the IMA platform was being used to host a particular application, the interactions of that application with the IMA platform would be of special interest to the analysis of the VTE.

If external equipment was being simulated in the VTE, the execution rates and refresh periods of any I/O data associated with them would have to be analysed to show that they accurately represent the real environment.

The list could go on. Depending on the extent of simulation that the VTE provides.

The difficulty here is to determine what level of analysis would be sufficient for the functions under test and the DALs that each of them carry.

4.1.2 Repetition of Results

Demonstration that a VTE is representative of the real environment could be achieved by repeating a series of tests in the VTE that have already been performed in the real environment. The scope of such a demonstration could be limited to the testing of a particular function, or a fully-representative virtual aircraft.

This of course would necessitate that the real environment already exists and has been used for verification activities. As mentioned in the introduction, one motive for using VTEs is to eliminate the need to have a real environment and often the real environment is not available during development phases of the project.

So what use would this be? The main reason why VTEs would be used after the real environment has already performed the verification is for ongoing maintenance work. Such as modifications, additions, or if a phased approach to delivering a fully functional system has been adopted.

Regarding the re-use aspects of ***[RTCA DO-297]***, once a VTE has been demonstrated to be valid for a particular aircraft, it could potentially be used during development of an IMA System for another aircraft, if the IMA platform would be the same on each aircraft.

4.1.3 Summary

To demonstrate that a VTE is representative of the real environment is sufficiently large a topic that it would warrant its own set of guidelines.

Such a document would have to consider all aspects of the two different environments from electrical power supplies, environmental considerations (e.g. CPU temperature), anomalous behaviour of each computing platform and how any VTE's host computer operating system might influence the behaviour of any simulations.

Moreover, the document would have to define what level of fidelity models need to achieve to be "representative" or even "equivalent" of the real environment (see chapter 4.2). It can be assumed that the required fidelity varies depending on the DAL as well as on the test object and test objectives. For example, some functions may allow for larger I/O deviations or have lower real-time constraints than in other IMA systems. It must be noted that there will always be differences between a modelled/simulated and a real environment, but the effort to achieve representativeness should correlated with the intended function

If a system was to be developed from the beginning with VTE use in mind, there may well be the need to consider this when elaborating the requirements and design of the system. In other words, make the system "*VTE friendly*". Exactly how to do this could also be part of this new guideline document (or not, see ***section 4.3***).

4.2 TECHNOLOGICAL CHALLENGES OF VTES

How to represent the real platform in a VTE? Is there existing COTS technology available to be able to represent the real environment?

It is possible to use real avionics equipment in a VTE. A Hardware-In-The-Loop (HIL) VTE could include one or more real avionics computing units. Of course, the more real equipment that is "in-the-loop" the closer one gets to actually having a real environment and so the argument for using a VTE over a real environment diminishes somewhat.

How accurate are any processor simulations used in the VTE? For a Virtual Processor In-the-loop (VPIL) VTE, there must be some assurance as to how accurately the CPU simulation represents the real CPU. Such an assurance may have to be provided by manufacturer of the CPU simulation which could prove difficult to obtain.

4.2.1 Multi-Core Considerations

Most (perhaps all) certified avionics systems in use today do not use multi-core processors. Or if they do use them, the processor is used in a single-core mode.

The reason being that multiple cores have the potential to introduce uncertainty into the behaviour of the CPU and/or any software executing on it.

So why use multicore CPUs at all? The main reasons are performance and obsolescence. It is increasingly more difficult to find manufacturers of high-performance single-core CPUs.

None of the standards documents so far analysed have any specific considerations for multi-core CPUs in their guidelines but there are documents that address this topic.

The Certification Authorities Software Team (CAST) have a paper on the use of multicore CPUs for DAL A, B, and C software functions ***[CAST-32A]***. It is beyond the scope of this document to discuss that paper in any detail.

If multiple cores are used, there is also the need to consider which aircraft functions would execute in which processor core and how to ensure partitioning of these functions. For instance, would it be necessary to certify the whole platform to the DAL of the highest function, rather than certify each function (or core) to a different DAL? **

So, the challenge here is how to incorporate a paper such as ***[CAST-32A]*** into the development lifecycle. This means:

- Identify system requirements to deal with multicore characteristics
- Translate those into constraint-type software requirements
- Use those requirements to make design decisions (low-level requirements) just for multicore
- Identify how to test those requirements and design decisions

For software development, the first step in being able certify the system for use with multi-core CPUs is to have a certified operating system and board support package (BSP) for using multiple CPU cores. If the supplier of the operating system does not provide this, it would have to be certified by one of the partners of the aircraft project.

***** INTA have also identified the need to consider multi-core processor aspects and partitioning of functions (by processor core).***

4.3 UPDATES TO CURRENT STANDARDS

As demonstrated in earlier sections, the use of VTTs is not really considered by the existing standards. For DAL A and DAL B the recommendation is to use target platform testing only in the verification process.

There is a real need to identify to what degree verification data from a VTE can be used in the certification process.

This will be dependent on to what extent the VTE can be demonstrated to be representative of the real environment (***section 4.1***), and the DAL of the component being developed.

The previous gap analysis document ***[D01.a]*** postulated that a new document would be needed to specifically address the use of VTTs and their applicability to the certification of airborne systems.

That sentiment is echoed here. The topic is too large not to have its own set of guidelines. The current guidelines only briefly mention "non-target platforms" and there do exist ambiguities as to how and where their use is acceptable.

That document also suggested that the VTEs themselves could be given a DAL-style rating to reflect their equivalence to the real environment. So if the VTE were DAL B, then DAL B software could be verified in that VTE, for example.

4.3.1 Requirements Considerations

Whether it be in a new document or updating the current documents, some guidance on considering the use of VTEs during the elaboration of requirements would be useful.

Such guidance may encourage the developer to categorize requirements under platform-specific and non-platform-specific, for example.

The concept of "architectural/design requirements" could be introduced to dictate certain aspects of the design that will make components of the software more platform independent. For example, using standard interfaces only; robustness against timing/overrun anomalies; buffering of data to avoid "glitches".

Further investigation would be needed to identify what other requirements considerations for using VTEs would be useful. **

***** INTA have also identified the need to assess if high-level requirements would need to be modified to accept the use of VTEs.***

4.3.2 Design Considerations

Similar to the above, guidance for the design of the system for use with VTEs would be needed.

Apart from any design constraints imposed by architectural requirements (see above), there can be a design philosophy to minimize platform dependencies.

So far the use of VTEs has been focused on having a VTE that represents the real environment as accurately as possible, and how to demonstrate that.

Another approach is to minimize the need for such accurate representation by developing software that is less dependent on the target platform. This would be a requirements/design philosophy to truly isolate the platform-dependent parts, and make the rest of the software essentially portable across different platforms.

This would more easily allow more parts of the software to be tested on a host computer, for example, without having to consider how well that computer was simulating the target platform.

Of course, there are some components of the system that cannot be independent of the underlying target platform, the idea here is to minimize that number of components and hence maximize the usefulness of VTE testing of the other components.

INTA have also identified the need to assess if low-level requirements would need to be modified to accept the use of VTEs.

4.4 STANDARDIZATION OF CONCLUSIONS

The identified challenges and conclusions raised by this document would need to be incorporated into current practices and accepted by certification authorities. How to do this is itself a great challenge and will be further discussed below (***section 5.3***).

5 CONCLUSIONS

5.1 VIRTUAL TESTING ENVIRONMENTS

There is certainly a place for using VTTs in the development process for acquiring certification data.

The real question is to what extent VTTs can be used instead of the real environment.

This ultimately depends on how representative of the real system a VTE would be. In all probability it would not be possible to precisely reproduce a real aircraft platform in a VTE, and if it were technologically and economically possible, it may be very difficult to demonstrate that the two environments are totally equivalent to the satisfaction of all parties involved.

Further study of this topic would be needed to explore the all the difficulties involved.

Perhaps a more pragmatic question would be how best to use VTEs in the context of the DALs because the higher the DAL of the component being verified, the more important the equivalence of the VTE and the real environment becomes.

So, to make VTEs really useful, the VTE itself must be matched to the DAL of the component under test. The higher the DAL to which this can be done, the more prolific the use of VTEs would be.

5.2 REQUIREMENTS/DESIGN PHILOSOPHY

This is both a conclusion and a challenge, as covered by ***sections 4.3.1*** and ***4.3.2***.

The main motivation for using VTEs is to reduce the need to test on an A/C0 type test rig (***section 1.1***). Another way to reduce the need for A/C0 testing can be achieved by designing the system to be less dependent on the real environment.

Of course, the very nature of avionics/airborne systems carries a high level of responsibility with regards to aircraft safety, so there will always be some critical components of a system that must be tested to the highest possible levels.

Some of those critical components will have to be highly-dependent on the real target environment and it may not be possible to test them in a VTE (for example some modules of an IMA platform).

The philosophy here would be to reduce the number of those components to a minimum and design robust interfaces between them and other components so that those other components may be tested in a VTE.

So, a design philosophy is needed that would isolate those critical, hardware-dependent components of the system from other components by using standard interfaces that can be implemented in VTEs. The concept of IMA goes some way to doing this at the application level but the IMA platform is often closely associated with the underlying hardware.

Section 3.2 discusses the idea of making an IMA platform less inter-twined with the hardware to reduce the amount of real target testing of an IMA system to a minimum.

IMA applications can also be designed to be more "self-sufficient" in the event of possible IMA platform failures. So a failure that may only arise on the real target platform** has no consequence at the application level, for example. This could allow the complete testing of IMA applications in a VTE.

** *Due to behavioural characteristics of the real target hardware that may not be reproducible in a VTE.* or at least this would require a level of effort that surpasses the economic benefits of using VTEs for creating certification credit

5.3 STANDARDS

There is a lack of consideration of VTTs in the current standards.

There is a need to have serious guidelines for VTT use in the current standards, or perhaps create a new set of documents that are specifically focused on the certification of airborne systems using VTTs.

This may be an unrealistic goal, however. So, is there another way to incorporate the acceptance of the use of VTTs into the certification process?

[CAST-32A] has already been mentioned in regards to multi-core processors. This paper was a collaboration between the Federal Aviation Administration (FAA) and the European Aviation Safety Agency (EASA) (***see https://en.wikipedia.org/wiki/CAST-32A#cite_note-4***).

There are also other papers produced by the FAA under the general category of Advisory Circulars which deal with a multitude of topics in the airworthiness/certification arena.

Rather than update or add to the current industry standards, it may be possible to create an Advisory Circular (or an equivalent paper) that deals with the use of VTTs.

Such a paper would have to be accepted by the relevant certification authorities (most prominently the FAA itself and the EASA) as a valid input to the development process of airborne systems.

Regardless of the selected approach, acceptance by certification authorities will be a necessity to spread the application of VTEs in the industry and hence contribute to a more efficient and sustainable development and certification process.

6 ACRONYMS & ABBREVIATIONS

AC/0	Aircraft Zero (testing rig)
AFDX	Avionics Full-Duplex Switched Ethernet
API	Application Programming Interface
ARINC	Aeronautical Radio, Incorporated
ARP	Aerospace Recommended Practice
CAST	Certification Authority Software Team
CSCI	Computer Software Configuration Item
DAL	Design Assurance Level
EASA	European Aviation Safety Agency
FAA	Federal Aviation Authority
HIL	Hardware In-The-Loop virtual testing methodology
HLR	High-Level Requirement
IDAL	Item Development Assurance Level
INTA	Instituto Nacional de Técnica Aerospacial
I/O	Input/Output
IMA	Integrated Modular Avionics
LLR	Low-Level Requirement
MIL	Model In-The-Loop virtual testing methodology
RTCA DO	Radio Technical Commission for Aeronautics DOcument
SAE	SAE International (formerly Society for Automotive Engineers)
SIL	Software In-The-Loop virtual testing methodology
VPIL	Virtual Processor In-The-Loop virtual testing methodology
VTE(s)	Virtual Testing Environment(s)
VTT(s)	Virtual Testing Technology(ies)

End of Document.

ANNEX A.

Here is the analysis of the document ***[RTCA DO-297]***.

A.1 ANALYSIS OF DO-297

Throughout this section, references to other sections shall take the form:

- ***Section x.y.z*** – Meaning a reference to the external document under discussion
- ***Section x.y.z*** – Meaning a reference to this document

A.1.1 Definitions

Some key terms used in ***[RTCA DO-297]*** need to be understood to effectively discuss the contents of the document:

- **Acceptance**
  Means that the development data for a module, application, platform or system has been accepted by a certification authority for use on an aircraft system.
- **Component**
  A self-contained hardware, software, database item, or combination thereof that is configuration controlled. It does not provide an aircraft function by itself (i.e. it must be integrated with the IMA system to be functional).
- **Application**
  Software and/or specific hardware with a defined set of interfaces that, when integrated with an IMA Platform, performs a function.
- **IMA Platform**
  A module or group of modules that can support at least one application. The platform itself has no aircraft functionality. It can be certified alone without applications.
- **Core Software**
  The Operating System (OS). It comprises one or more modules.
- **Module**
  A module can be accepted stand-alone or part of the IMA system. It can contain sub-modules and can be hardware, software or a combination of both. It provides resources to the IMA system. And can be located with the IMA platform or external in another part of the aircraft. Core software is a module. Core hardware also.
- **IMA System**
  IMA platform plus a set of applications.
- **Resource**
  Any object used by one or more applications. It can be physical (hardware) or logical (information).
- **Re-usable**
  Means that the design data for previously accepted modules can be used for acceptance in other systems.

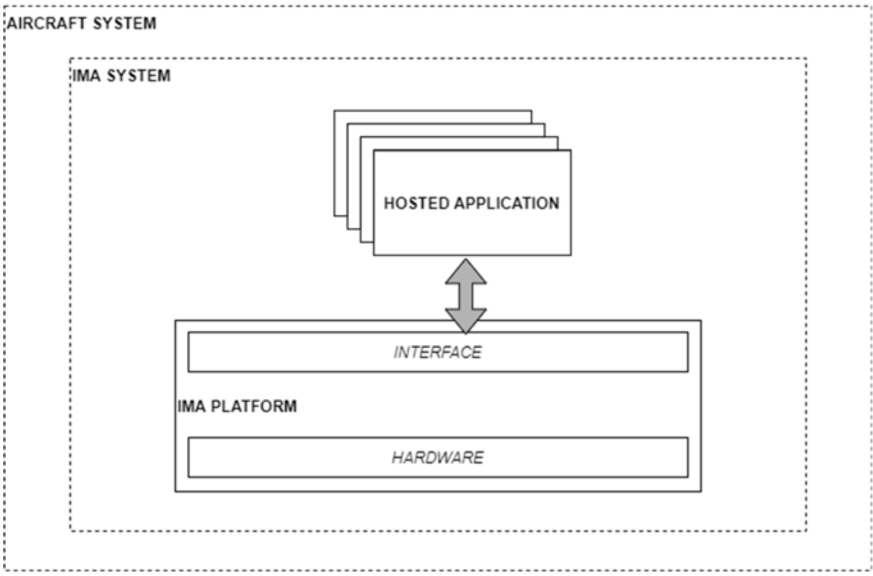

Figure 2 - IMA System Context

A.1.2 Incremental Acceptance and Re-use

[RTCA DO-297] is focused on the incremental acceptance of an IMA System for airborne systems.

Incremental acceptance means being able to certify separate parts of an IMA system rather than the system as a whole as would be the case for a federated avionics system.

In practice this could mean that a previously accepted IMA System which hosts a new application can gain acceptance by using the development data of the new application only.

Similarly, and already accepted application may be re-used on a different IMA Platform to form a new IMA System without the need to re-test that application as a standalone module.

A.1.3 Incremental Acceptance Tasks

Section 1.1 of the document introduces 6 tasks involved in the incremental acceptance process:

1. Module acceptance
2. Application software or hardware acceptance
3. IMA System acceptance
4. Aircraft integration of an IMA System - including V&V&V
5. Change of modules or applications
6. Re-use of modules or applications

These tasks are further explained in subsequent parts of the document and will be summarized below.

A.1.4 IMA Development Process

The overall development process comprises three sub-processes for the development of the three general components of an IMA System.

In general, the specific details of software or hardware development for an avionics system are not specified by the document, instead references are made to ***[RTCA DO-178/C]*** and ***[RTCA DO-254]*** respectively. However, there are important points to consider:

A.1.4.1 IMA Platform Development Process

This process can be done independently of any aircraft-specific functions. The idea being that an IMA platform can be re-used across different aircraft avionics systems. For a complete IMA platform to be truly re-usable, the target hardware for the platform across aircraft would also have to be the same. To date, this is not a common practice in the industry.

Since the IMA platform can comprise several modules, it is possible that some of the platform's modules may be truly re-usable, even across aircraft with different hardware (e.g. the OS-Application interface, some parts of the core software, possibly some Health Management (HM)/Fault Management (FM) software modules).

A.1.4.2 Hosted Application Development Process

The document only really mentions that this process should take consideration of the IMA Platform resources needed by the application.

A.1.4.3 IMA System Development Process

The IMA System here is discussed primarily in terms of aircraft functions and platform resources. So with a sufficiently flexible IMA Platform, one could suppose that the specification of the IMA System can be covered by some sort of system configuration. Ideally this would a dynamic configuration that can be loaded on start-up so that the IMA Platform itself would be re-usable between different systems.*****

The following tasks mentioned for this process are largely concerned with the development, integration and testing of applications with the IMA Platform.

***** *This has been used in existing IMA systems via XML configurations (e.g. A400M, VxWorks 653)*

A.1.5 Certification Process

Section 4.1 presents an overview of the certification process for incremental acceptance of IMA systems by elaborating on the contents of the six tasks identified in ***section 1.1*** (see ***section A.1.4***) and to which components of an IMA system those tasks apply.

The following table summarises this information:

Task	Description	Applies to the Acceptance of:
1	Module acceptance	- IMA Platform. *Individual modules of the platform can gain incremental acceptance to comprise the platform or the platform as a whole can gain acceptance.*
2	Application software or hardware acceptance	- Application
3	IMA System acceptance	- IMA System. *Off-aircraft integration of the platform and applications.*
4	Aircraft integration of an IMA System - including V&V&V	- IMA System. *On-aircraft integration of the platform and applications.*
5	Change of modules or applications	- IMA Platform Module. - Application.
6	Re-use of modules or applications	- IMA Platform Module. - Application.

Table 1 - Incremental Acceptance Tasks

[RTCA DO-297] describes several objectives for each of the tasks but the area of interest for this document is the necessary Validation and Verification (V&V) data to gain acceptance for each task (where applicable). This shall be summarized in the following sub-sections.

A.1.5.1 Module Acceptance

(***Section 4.2***)

Module acceptance can be applied to various modules of the IMA Platform or treating the IMA platform as one whole module. The objective is to provide documented evidence of acceptance/compliance (development data) to support the acceptance of an IMA System for the same aircraft and possible re-use of the IMA platform in other aircraft.

The module acceptance task follows a typical development lifecycle plan including V&V activities for module integration and software verification of a module, which defers to ***[RTCA DO-178/C]***.

A.1.5.1.1 Acceptance Data

Defined as being *"evidence of the completeness, correctness and compliance of the module with its requirements".*

This includes:

- Module V&V plan
- Software verification cases, procedures and results (as per ***[RTCA DO-178/C]***)
- Traceability data
- Environmental testing data
- Module integration V&V cases and procedures:
    - Review and analysis procedures
    - Test cases
    - Test cases *(including the test environment)*
- Module integration V&V results

A.1.5.2 Application Acceptance

(***Section 4.3***)

The main objective of application acceptance is described as "*to demonstrate that the application complies with the applicable regulations and requirements allocated by IMA system design, performs within module limitations, and provides the characteristics and performance as specified.*"

Another goal is to provide acceptance data for later use in the IMA system integration and re-use tasks.

A.1.5.2.1 Acceptance Data

Here, the document refers to ***[RTCA DO-178/C]*** (for software) and ***[RTCA DO-254]*** (for hardware). It indicates that the acceptance data for an application would typically be compliant with those documents.

For a more IMA-specific set of acceptance data, more information may be needed to show compliance with the IMA platform (for example, interface specifications, usage analysis).

For application re-use in other IMA systems there is a more elaborate list of acceptance data activities, including:

- Justification for re-use of the application
- List of data to be provided to certification applicant to support certification and re-use
- Credit being claimed for the application (full, partial, none) and how users can achieve full credit (for their IMA system)
- Development of data to support re-use: e.g. interface definitions, failure conditions, user guide, and environmental qualification.

A.1.5.3 IMA System Acceptance

(***Section 4.4***)

This task is to demonstrate that the modules of the IMA platform together with the hosted applications continue to function correctly and without adversely affecting each other.

The task may be performed on or off-aircraft. One goal for off-aircraft V&V activities is to provide acceptance data that can be applied to the overall certification effort.

It is not specified what “off-aircraft” testing means in terms of VTTs. Does it mean real target hardware (HIL) or can it also mean a simulated IMA platform (SIL)?

A.1.5.3.1 Acceptance Data

The acceptance data comprises:

- IMA System Certification Plan
- IMA System V&V Plan
- IMA System Accomplishment Summary

None of these goes into any detail of the environment used to gain acceptance data. So the question of how representative of the real aircraft hardware any “off-aircraft” testing must be is not addressed. Indeed, the contents of each of these activities does not mention “off-aircraft” testing at all.

A.1.5.4 Aircraft Integration of an IMA System

Includes installation, integration and V&V activities in an “on-aircraft” environment. Both ground testing and flight testing would be performed. It is not mentioned whether or not a real aircraft must be used for ground testing or if an aircraft-zero (A/C 0) test environment is acceptable.

It does seem clear that real equipment must be used throughout. So there is no scope for using VTTs during this process.

A.1.5.4.1 Acceptance Data

The same three acceptance data artefacts are produced for this activity, but in the context of the IMA System being used on a real aircraft. The V&V activities would involve real aircraft crew during some of the testing.

A.1.5.5 Change of Modules or Applications

A change to an IMA system could mean:

- The addition/deletion of a new module, application or hardware.
- A modification to an existing module, application or hardware component
- A change to the infrastructure of the aircraft platform (e.g. the AFDX network)

A principle goal of IMA and actually one of the reasons for using IMA is to be able to avoid re-certifying the entire IMA system when a change is introduced. Only the changed component and perhaps any directly-interacting components would need to be re-certified.

A.1.5.5.1 Acceptance Data

The following items comprise the acceptance data for a change to an already accepted IMA system:

- Change Impact Analysis
- Change Management Plan
- V&V Plan
- Modified lifecycle data
- Updated accomplishment summary
- Maintenance and change history records

None of these mention anything to do with the test environment, so whether or not VTTs could be used as part of the V&V plan and to what assurance level would be project-specific (and specific to the change itself) and depend on the original lifecycle data for the IMA system, one would assume.

A.1.5.6 Re-use of Modules or Applications

The goal here is not to re-test an IMA system for use on another aircraft, but to re-use the previously-accepted lifecycle data for acceptance on the new aircraft. Therefore, a large part of this activity is assessing the suitability of that previous data for certifying the IMA system on a different aircraft.

This task will be much easier if the two aircraft have identical target computing platforms. If this is not the case then some V&V activities will have to be performed again.

For the re-use of module or application software only previous acceptance data can be used if the software has been shown to have no adverse effects on the safety, performance or functionality of the new aircraft’s operational capability.

Some integration of the IMA system with the new aircraft must be performed but depending on the initial analysis it could mean that not full integration testing is necessary.

One thing which is not clear in this section is whether or not the term “re-use” could be applied when installing an IMA System from a VTT environment onto a real aircraft. Previous discussion of the IMA System process does involve one task that includes on-aircraft testing so the assumption is that an IMA system cannot be taken directly from a VTT environment and used on an aircraft without on-aircraft testing.

A.1.6 Integral Process for IMA Development

Section 5 of the document serves as a template for what needs to be done for each of the activities involved in the certification (and acceptance) of an IMA System. This section is extensive but of particular interest to this document are the *Environmental Qualification Testing* (***section 5.2.6***), *Validation* (***section 5.3***), and Verification (***section 5.4***).

A.1.6.1 Environmental Qualification Testing

This section is of interest only because it seems to be exclusively considering the real aircraft environment. So no discussion of alternative VT environments is presented whatsoever.

A.1.6.2 Validation

The validation activity is concerned with the allocation of IMA Platform, Application and IMA System requirements and ensuring that those requirements are correct and complete.

Of note is the possibility to have an IMA Platform based on generic requirements and then subsequently apply that platform to a specific aircraft. This may give rise to separating IMA Platform modules into “re-usable” and platform-specific (or aircraft-specific). In this scenario, it may be reasonable to pursue the verification of the “re-usable” modules in a non-aircraft test environment, possibly a VTT environment.

A.1.6.3 Verification

Here is the only place in ***[RTCA DO-297]*** where testing in a non-target platform environment is discussed in a positive manner.

“Verification may initially be performed in a simulated representative target computer and environment…however the [verification] activity cannot be completed without verification on the target platform.”

This statement does not state whether or not such non-target verification can actually be used to acquire acceptance data. The inference is that this would be a development/debugging activity to promote a more error-free verification activity on the target platform.

“… it is recognized that initial application verification process described by DO-178/ED-12 may be performed in a “host” computer environment…”

“In this case partial acceptance credit may be granted for completion of those processes, if the developer can substantiate that those verification procedures and results are valid for the target computer and environment."

This allows the potential for the use of VTTs to gain acceptance for applications. It does depend on the developer being able to demonstrate that the VTT accurately represents the real target platform and no further guidance is given as to how this can be accomplished. Nor does it discuss to what DAL host environment testing may be used. This may be considered to be in the scope of other documents such as ***[RTCA DO-178/C]***.

A.1.7 DAL Considerations

The document does not make any consideration of specific Design Assurance Levels (DALs) for any part of an IMA System.

The development data needed to certify a component for a specific DAL would appear to be delegated to documents such as ***[RTCA DO-178/C]***.

Section 4.4 when discussing IMA System acceptance does state: "*The level of certification credit obtained for the particular off-aircraft V&V should be coordinated in advance with the certification authority*". Implying that there is the potential for having acceptance data of differing DALs.

A.1.8 Virtual Testing considerations

[RTCA DO-297] within itself does not discuss the use of VTTs in connection to the IMA development process with the exception of that discussed above (***section A.1.6.3***).

Because the document defers the details of the development process to those documents which have already been analysed in the context of VTT ([include Ref]), the conclusions reached by that analysis are also applicable here. It could also be argued that such VTT considerations are beyond the scope of ***[RTCA DO-297]***.

Nevertheless, the very nature of IMA systems also presents certain opportunities to apply VTTs to each of the three development processes and most of the six incremental acceptance tasks summarized above. This will be discussed in the following chapter.

A.2 CONSIDERATION OF VTTS TO DO 297

This chapter will identify possible development activities mentioned in ***[RTCA DO-297]*** that may not need to be performed on a fully integrated aircraft or even on the target hardware platform of an IMA System. It will also identify if there are any aspects of incremental acceptance guidance where VTTs could be used as the principle means of verification.

In order to be consistent with ***[RTCA DO-297]***, the analysis will first identify the six tasks of incremental acceptance (***section A.1.2***) to which VTT may be applied.

It is perhaps not justified to say that ***[RTCA DO-297]*** has "gaps" as such in the consideration of VTTs in V&V activities. This is because the document does refer to the other standards documents as a guide for how to do the V&V processes.

However, since the document is a development guide for an IMA system, there are perhaps missed opportunities to include the use of VTTs when considering the concepts of incremental acceptance of IMA platform modules and IMA software applications and the potential for re-use not only in other aircraft but also in Virtual Testing environments.

A.2.1 Incremental Acceptance Tasks and VTT

Can any of the tasks identified in ***[RTCA DO-297]*** be performed in a Virtual Test environment?

The following table identifies in which tasks of the incremental acceptance guidelines VTT could be used and how:

Task	Description	VTT Use
1	Module acceptance	- IMA Platform. *Identify non-hardware dependent modules of the platform (e.g. application interface, scheduling logic, fault management logic) that can be tested in a SIL environment.*
2	Application software or hardware acceptance	- Application *Using a SIL environment with a host-based OS simulation using the non-hardware dependent modules of the platform in a host-based build*
3	IMA System acceptance	- IMA System. *HIL with real target hardware can be used together with simulations of external equipment. An IMA configuration can be used for a HIL test environment (e.g. map communication channels for host-based simulations).*
4	Aircraft integration of an IMA System - including V&V	- IMA System. *Not applicable to VTT*
5	Change of modules or applications	- IMA Platform Module. *For non-hardware dependent modules (e.g. fault management logic, scheduling logic, application interfaces), a SIL or HIL environment can be used to test changes in specific modules.* - Application. *As per task 2. If the application has changed due to external equipment changes then the VTT environment will also need updating.*
6	Re-use of modules or applications	- IMA Platform Module. - Application. *For the platform and applications, re-use should be considered not only in the context of other aircraft systems, but for VTT environments.*

Table 2 - Incremental Acceptance Tasks and VTT

DO-297: GAP001

When defining the scope of the incremental acceptance tasks, some consideration of VTT environments could be added.

What remains to be determined is how to apply the use of VTTs to the verification process for different DALs and this would be project-specific and depend upon the supporting documents ***[RTCA DO-178/C]*** and ***[RTCA DO-254]*** which have already undergone VTT analysis.

A.2.2 IMA Platform - Independent Modules

The Module Acceptance task of ***[RTCA DO-297]*** does not really specify the physical platform for the activity.

Ultimately, an IMA platform must be compatible with the underlying hardware and any supporting software (e.g. Board Support Package (BSP), drivers, etc.). This means that some of the modules of the platform must be specific to the target hardware and non-reusable on other hardware platforms (or VTT environments).

There will be modules of the core software, however, that can be designed to be independent of the underlying hardware. For example, tasking/scheduling, HM/FM logic, application interfaces, configuration tables could all be designed in a way as to make them re-usable in a VTT SIL environment with simulations providing the “hardware data” as needed. This would allow verification of the core software’s functionality to be performed with VTTs and subsequent integration testing of the real interfaces to be done with the real target platform.

So ***[RTCA DO-297]*** could include an emphasis on isolating key modules of the IMA Platform itself from the target platform hardware, which would be more of a design activity.

DO-297: GAP002

The IMA platform development process could encourage the modules to be designed into two categories: target platform-dependent and independent (re-usable in VTTs).

A.2.3 Re-use of Host-Based IMA Software Application Testing

Since an IMA application does not have to interact directly with underlying hardware, it would seem to be possible that an application compiled for a VTT platform (i.e. SIL) would be sufficiently representative of the application running on the target platform*****, and that VTT could be used to provide valid development data.

***** *Provided there is a valid representation of the IMA Platform’s OS and any necessary simulated data inputs to the application.*

That being said, the value of testing of applications in VTT environment was only briefly mentioned in the document (***section A.1.6.3***). There are places in the document that do emphasize real target platform testing and so by inference, it can be considered that testing on other platforms is a possibility.

An application that is dependent only upon the established IMA platform API could be tested to a very thorough level and such test evidence must be of some value to the acceptance of that application. This would be another application of the term "re-use" that is so often cited in ***[RTCA DO-297]***.

DO-297: GAP003

Why is there no significant consideration of "re-use" of acceptance data between VTTs and the target platform? Only re-use between different aircraft is considered.

A.2.4 IMA Signal Concentrators

One key idea of IMA is that hosted software applications interact with the IMA platform through an established API. It is possible for the core software (together with the BSP) to provide direct access for an application to hardware device data through its own set of customized APIs.

When testing applications in a SIL VTT environment, direct access to hardware may not be available so some sort of simulation would be needed for any direct-access APIs. If several applications required such direct-access then the interfaces that each application uses would have to be re-tested on the real IMA platform.

To this end, a dedicated application or schedulable module of the IMA platform could be used as a data signal concentrator. Thus providing hardware access to an application via the standardized API. This would potentially remove the need for real-target testing of hardware interfaces with real applications.

Signal concentrator modules/applications could be delivered with an IMA Platform so that an IMA system which is re-used between aircraft would (potentially) not need re-testing of those hardware data channels at application integration level.

So ***[RTCA DO-297]*** could include sections to encourage the use of signal concentrators for access to specific hardware data such as analogue/discrete signals, MIL-1553 data, AFDX data, etc. which would better promote the use of VTTs when testing applications.

Alternatively, for a VTT environment, those APEX channels used for hardware data could be mapped to external simulations by simply changing the IMA configuration and omitting a signal concentrator module/application from the software build when testing in a VTT SIL environment.

Such signal concentrators do not need to be concerned only with low-level hardware data but can also serve as the unique interface to external equipment. For example, there could be a signal concentrator module/application that deals exclusively with driving the graphical displays based on messages from other applications. Thus eliminating the need for specific application testing with the real graphics equipment.

To summarise, if signal concentrators are used in place of customized hardware APIs then it further isolates applications from the IMA Platform and thus facilitates VTT SIL testing of applications in a host-PC environment.

DO-297: GAP004

The IMA Platform process could promote the use of data signal concentrator modules/applications to facilitate platform-independence of applications which may allow re-use of VTT based application verification data.

A.3 CONCLUSIONS AND RECOMMENDATIONS

The major conclusion of this report is that ***[RTCA DO-297]*** has such an emphasis on re-use of IMA components across different aircraft systems but it could just as easily have also considered VTT environments in its re-use agenda. There is almost no consideration of VTT environments in the document.

Perhaps the document itself considers VTT to be out of scope for its own guidelines. In which case a supplementary annex could be created to deal specifically with VTT considerations when developing an IMA system.

The document provides extensive lists of what should be done for the different tasks of an incremental acceptance process but it does not give real guidance on design concepts and philosophies that would really promote re-usability across a wide range of hardware platforms (including VTT environments). It could go into more detail about how to decompose an IMA platform into re-usable and non-re-usable modules, for example (***section A.2.2***).

In the experience of this author, different aircraft projects almost never have the same underlying hardware. So the idea of re-use for an IMA Platform between different aircraft is unrealistic unless there is a top-level mandate from the aircraft manufacturer to use the same hardware across projects.

However, if VTTs can be used to gain acceptance data at some level then this would reduce the amount of on-aircraft retesting needed between projects. The same VTT acceptance data could potentially be re-used directly between different aircraft projects for those verification activities that test platform-independent components of an IMA System.

Also, there could be a greater emphasis on the use of signal-concentrator applications or modules which could make each user application even more independent of the IMA platform, and hence more re-usable and easier to test more completely in a VTT environment (***section A.2.4***).

The document has no mention of different V&V requirements for different DALs. This is understandable because the supporting documents deal with those issues (albeit to a limited degree). As noted already in the analysis of those documents ***[D01.a]***, there is no consideration of DALs and non-target platform environments. So any use of VTTs for specifically testing IMA systems would still have to resolve the issue of assigning the value of VTT results to the level of assuredness of the component being tested. This would most probably need to be done in collaboration with the certification authority.

A.3.1 Summary of Identified Gaps

The following table presents a summary of any gaps found during the analysis of ***[RTCA DO-297]***:

Reference	Page	Brief
[RTCA DO-297]	20	Consideration of VTT environments in the definition of the incremental acceptance tasks.
[RTCA DO-297]	21	Identify target platform-dependent and independent IMA platform modules. This aspect can be considered in the scope of A653 definition.
[RTCA DO-297]	21	Apply "re-use" of acceptance data to application testing with VTTs.
[RTCA DO-297]	22	Promote the use of data signal concentrators in the IMA Platform. This aspect can be considered in the scope of A653 definition.

Table 3 – DO 297 Identified Gaps

A.3.2 Recommended Enhancements to DO 297

By implication, the above "gap" tables will serve as recommended points to be addressed for the document which could result in subsequent document enhancements.

Due to the nature of the document under review, it is not particularly obvious where such enhancements should be incorporated. The four identified "gaps" are not really specific omissions at specific points in the document. Rather they are philosophies of IMA design which could reverberate throughout the document. So a potential enhancement to ***[RTCA DO-297]*** would be to incorporate those four considerations in all of the sections to which they apply, otherwise create a supplementary annex exclusively for discussing the use of VTTs in IMA development.