DOT/FAA/TC-20/6

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

Final Report for System-Level Assurance of Airborne Electronic Hardware (AEH)

March 2020

Final Report

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DOT/FAA/TC-20/6		

4. Title and Subtitle	5. Report Date
FINAL REPORT FOR SYSTEM-LEVEL ASSURANCE OF AIRBORNE ELECTRONIC HARDWARE	March 2020
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Guy A. Berthon, Laurence H. Mutuel, Cyril Marchand.	D4

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Thales ATM 10950 El Monte, Suite 110 Overland Park, KS 66211	11. Contract or Grant No. DTFACT-13-D-00008

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Federal Aviation Administration William J. Hughes Technical Center Aviation Research Division Atlantic City International Airport, NJ 08405	Final Report
	14. Sponsoring Agency Code AIR-130

15. Supplementary Notes

The FAA William J. Hughes Technical Center Aviation Research Division Technical Monitor was Manuel A. Rios, PhD.

16. Abstract

Industry standards SAE ARP4754A, Guidelines for Development of Civil Aircraft and Systems, and RTCA DO-254, Design Assurance Guidance for Airborne Electronic Hardware (AEH), are now extensively used and recognized by certification authorities as acceptable means of compliance with airworthiness standards. They recommend a process-oriented structured development assurance for systems and AEH, respectively.

The particular issue with commercial off-the-shelf (COTS) components is that they are not developed to the above standards, and their development data remain proprietary and, therefore, are not available for review to the levels expected by those standards. Circuit board assemblies (CBAs), as another particular type of AEH, do not reach a level of complexity that would require such a structured development process to be fully deployed; a verification testing approach is deemed sufficient to provide assurance.

The purpose of this research was to assess feasibility and provide recommendations of how AEH, CBAs, and COTS components could be assured at system level (i.e., going beyond DO-254 or beside ARP4754A guidance documents), although remaining acceptable in terms of providing evidence of development assurance.

The initial conclusions of this research are twofold: First, DO-254 or related material already provides guidance on handling COTS component assurance; second, ARP4754A, though well suited for a system-level approach, neither specifically targets COTS nor provides sufficient guidelines to support COTS assurance, regardless of their level of integration, inherent complexity, or allocated development assurance level.

These considerations naturally lead toward recommending a system-wide, manifold approach rather than a more limited system-level assurance process. This approach is referred to as a systemic approach and is examined in this report.

17. Key Words	18. Distribution Statement
DO-254, Airborne electronic hardware (AEH), Commercial off-the-shelf (COTS), Circuit board assemblies (CBA), Model, Attribute, Property, ARP4754A, Overarching properties	This document is available to the U.S. public through the National Technical Information Service (NTIS), Springfield, Virginia 22161. This document is also available from the FAA William J. Hughes Technical Center at actlibrary.tc.faa.gov

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	49	

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AEH	Airborne electronic hardware
ASIC	Application-specific integrated circuit
CBA	Circuit board assembly
CEH	Complex Electronic Hardware
CM	Certification memorandum
COTS	Commercial off-the-shelf
CPS	Complex physical system
CPU	Central/Core Processing Unit
DAL	Development/Design Assurance Level
DAS	Development assurance strategy
EASA	European Aviation Safety Agency
ECMP	Electronic component management process
ECMR	Electronic component management report
FPGA	Field programmable gate arrays
IC	Integrated circuit
IP	Intellectual property
LRU	Line replaceable unit
MAP	Model-attribute-property (approach)
OEM	Original equipment manufacturer
PDH	Previously developed hardware
PLD	Programmable logic device
PSE	Product service experience
SEH	Simple electronic hardware
SOC	System on chip
SOW	Statement of work
SSA	System safety analysis
TRL	Technology readiness level

EXECUTIVE SUMMARY

Current FAA guidance recognizes SAE ARP4754A, Guidelines for Development of Civil Aircraft and Systems, and RTCA DO-254, Design Assurance Guidance for Airborne Electronic Hardware (AEH), as acceptable means for establishing a development assurance process for systems and AEH, respectively. No FAA guidance addresses line replaceable units, circuit board assemblies (CBAs), integrated circuits (IC) technology, or commercial off-the-shelf (COTS) components in an explicit manner. DO-254 is potentially applicable to all of these AEH types. The European Aviation Safety Agency (EASA) developed and is currently using additional guidance for these AEH types that can be found in EASA certification memorandum CM-SWCEH-001.

This report examines a system-oriented approach that is deemed able to create a framework for assuring AEH toward airworthiness certification. Such an approach, based on a model-attributes-properties (MAP) approach, seems particularly suited for COTS AEH and CBA, but could be equally extended to any other unit of equipment, custom micro-coded application specific ICs, or programmable logic devices. However, for a newly developed AEH per DO-254, life-cycle data are available as produced from a structured process; therefore, this systemwide approach might be useful only as an alternative. In addition, this approach could be extended to assure previously developed hardware that was not developed to DO-254.

This report shows that, based on airworthiness standards applicable to the equipment (e.g., Title 14 Code of Federal Regulations Part 25/29.1301, 14 CFR 25/29.1309), some attributes and overall objectives could be derived; if instantiated for COTS or CBA, the report will help identify activities that, when performed, will contribute to meeting these overall objectives.

Any new AEH technology generally causes new interpretative or guidance material to be developed to support assurance (i.e., to help assess and demonstrate compliance with airworthiness standards). These considerations, together with the gap in guidance material and particular issues with COTS AEH, suggested that a systemwide approach would be best suited to provide common ground to address those types of AEH. This approach should be independent from the description of the details of COTS AEH's constitutive elements. MAP is then proposed to support this approach and is further described in this report.

The concept of model is always proposed as a means to provide a representation of a system, in particular for a complex physical system. This model can then be used to gain a better understanding of the system behavior, possibly virtually act on it, and observe its behavior and potential misbehaviors. In addition, successive models can be derived to various levels of abstraction, ultimately leading to the actual physical device. However, a model in the case of a COTS component can only be built using limited data available from its supplier's datasheet. Though a model would be useful in supporting assurance for COTS or CBA AEH, it must be complemented by identification of additional elements within this proposed systemwide approach. The use of a model, providing it is representative of the actual physical device, is the first step toward providing assurance.

The concept of attribute is used in this report to delineate the aspects, outlines, or elements that a physical object and any component (e.g. COTS or CBA AEH) should feature and be perceived as possessing to ensure it performs its intended functions, is both fit-for-purpose and safe-for-use,

adequately behaves under operating and environmental conditions, and will continue to do so over its lifetime. This is a second major step in providing assurance whenever these attributes are shown to belong to the physical object as designed, built, and used.

The concept of property is also used in this report to express any relationship established between those attributes defined above, either combined in pairs, triplets, or more complex n-tuples. Properties are based on overall principles that generally govern the existence, necessity, and persistence of physical objects. These properties establish statements of consistency between attributes and, when instantiated for a particular type of object, they must be shown to be true; this demonstration will then constitute a third major step in providing assurance.

A commonly accepted definition for the term “assurance” is: “the planned and systematic actions necessary to provide adequate confidence and evidence that a product or process satisfies given requirements.” This report elaborates on how similar assurance can be provided on the basis of this new systemwide approach based on the MAP approach. DO-254 guideline documents and related interpretative material should certainly remain in use as they recommend sound objectives, in particular for an electronic component management process. However, complementary activities are suggested in this report to further support meeting assurance objectives. This approach in terms of activities supporting objectives remains consistent with the common practices in assuring development of any type of AEH.

Appendix A provides further examples of instantiation of attributes to COTS AEH.

Appendix B illustrates application of the MAP approach to COTS and CBA AEH.

1. INTRODUCTION

1.1 PURPOSE

This research has been undertaken in response to Statement of Work (SOW) DTFACT-13-D-00008, Delivery Order 06 Software and Electronics Section—System-Level Assurance of Airborne Electronic Hardware, from Contracting Officer Representative FAA William J. Hughes Technical Center, June 2015. The SOW requested to create a framework for system-level assurance of airborne electronic hardware (AEH) items in the following categories: 1) line replaceable units (LRUs); 2) circuit board assembly (CBA); 3) integrated circuits (IC) technology such as hybrids and multi-chip modules; and 4) commercial off-the-shelf (COTS) components.

1.2 BACKGROUND

1.2.1 General

Modern systems designed for airborne applications in commercial transport aircraft frequently incorporate complex AEH items and components that may or may not have been developed by the AEH manufacturer to the most recent standard for safety assurance and airworthiness approval. For these components, safety assurance must be demonstrated both in terms of proper functioning of each component in isolation and proper behavior within the context of the system being assessed for approval. Certain units of equipment, items, devices, and components raise special concerns when LRU, CBA, and COTS components have previously been developed by an organization other than the AEH manufacturer's. These may be treated as non-DO-254 [1] assured components, but guidelines for approval in that circumstance would be less comprehensive and less acceptable than those for the fully compliant DO-254 process.

1.2.2 LRUs and CBAs

Until recently, there were no specific expectations from either FAA or EASA on the hardware development assurance activities, as they would apply to LRUs or CBAs. As of March 2012, guidelines for development assurance of LRUs and CBAs were issued by EASA via certification memorandum (CM) SWCEH-001 [2], which included a specific section on assurance of LRUs and CBAs. These guidelines provided guidance based on DO-254 minimum requirements, namely objectives that would be similar to those required for simple hardware in association with a set of lifecycle data that would be minimal.

Over the past few years, development assurance for LRUs and CBAs has been handled either under aerospace equipment suppliers' in-house practices, or through system development assurance generally handled at aircraft installation level. To the authors' knowledge and to date, no evidence of safety issues exists that would be related to not applying a DO-254-like development process (i.e., a structured development process with documented evidence of activities toward established objectives). LRU and CBA development assurance could therefore be addressed using relevant provisions of DO-254, but would possibly need some clarifications on their proper implementation. In addition, DO-254 already provides guidance on how to handle relationships between system-level ARP4754A-like development assurance and AEH-level [3].

1.2.3 Commercial Off-the-Shelf

Considerations related to the assurance of COTS are mainly those expressed in DO-254 section 11.2, COTS components usage, and section 11.3, Product service experience (PSE), in which only the following directions are provided on assuring COTS components:

- "COTS components are used extensively in hardware designs and typically COTS components design data are not available for review. The certification process does not specifically address individual components, modules, or subassemblies because these are covered as part of the specific aircraft function being certified. As such, the use of COTS components will be verified through the overall design process, including the supporting processes, as defined in DO-254. Use of an electronic component management process (ECMP), in conjunction with the design process, provides the basis for COTS AEH usage."
- PSE may be used to substantiate design assurance for previously developed hardware (PDH) and for COTS components. Service experience relates to data collected from any previous or current usage of the component. Data from non-airborne applications is not excluded.
  Note: Wide and successful use of an item in service may provide confidence that the item's design is mature and free of errors and that the manufacturing quality of the item is demonstrated.

DO-254 sections 11.2 (COTS) and 11.3 (PSE) seemingly recognize that a process-oriented approach reflected in DO-254 does not apply to COTS because the necessary artifacts (i.e., design data) are not available for review, and only limited descriptive data are available for system design. These statements would also suggest that arguments other than process-oriented approaches are possible. However, it is still unclear what the statement "verified through the overall design process" means within the context of the current DO-254 guidance. If it is interpreted as "verified through the overall (i.e., system-level) design process," this statement would suggest that the process-oriented approach could be replaced by a system-oriented approach. Note also that "system-level" remains to be defined as multiple levels could be involved.

In other words, the question remains as to what extent verification done at an upper level of both description (the as-designed AEH) and implementation (the as-built AEH) would provide sufficient confidence in the verification at a lower level of description or implementation.

Note that verification at the lower level of description or implementation may then not necessarily need to be performed. This assumes that the principle of a two-way causation is verified, both upward causation (i.e., 100% predictability of the whole by its parts) and downward causation (i.e., 100% determinability of the parts by the whole). A good example of a COTS component for which such a two-way causation principle would be satisfied is a Core Processing Unit (CPU) example further discussed in section 2.1.3.

A COTS component is generally a black box for which a detailed description of the individual hardware elements inside the device is neither available nor are specific design data produced during its development by original equipment manufacturer (OEM) accessible.

Using some limited description of the COTS AEH behavior and interfaces available from its datasheets, only inputs can be controlled and output can be observed (i.e., a system-level approach can be applied at least at the next level up of description and implementation).

Other arguments could be devised; for example, a product-oriented approach is still possible in the context of DO-254 for simple electronic hardware (SEH). Such a product-oriented approach would be limited only to 1) establish the intended function in which the COTS component is destined to be involved, 2) perform COTS technical suitability analysis based on available description and other artifacts, and 3) ultimately verify the COTS component as implemented within the surrounding AEH versus the target intended purpose.

Considerations on COTS intellectual property (IP) as a specific case of COTS components are provided in FAA Order 8110.105 [4] section 4.9 and EASA CM SWCEH-001 [2] section 8.4.4. COTS IP issues are investigated under a different research effort and will therefore not be covered in this report.

1.3 DEFINITIONS

The following definitions are used in this report:

Airworthiness	Ability of an aeronautical product to satisfy applicable rules and regulations, to conform to its approved design, and to be in condition for safe operation. [Based on ICAO, FAA and EASA definitions] The condition of an item, which can be an aircraft, aircraft system or component, in which that item operates in a safe manner to accomplish its intended function. [Source: DO-254 [1]]
Assurance	The result of planned and systematic actions necessary to provide adequate confidence and evidence that a product or process satisfies given requirements. [Source: DO-254]
Assumption	Statements, principles, and/or premises offered without proof. [Source: ARP4754A [3]]
Assurance case	A reasoned and compelling argument, supported by a body of evidence, that a system, service, or organization will operate as intended for a defined application in a defined environment. [Source: Goal Structuring Notation Community [5]]

Attributes	All features, outlines, or elements that have to be considered as defined and made sure to belong to a [Complex] Physical System, which will be built. [Source: proposed in this report]
Complex	Composed of parts, surrounding, encompassing; or braided together, entwined, and interwoven. [Source: freely adapted from The Free Dictionary]
Complexity	An attribute of functions, systems/items, which makes their operation, failure modes, or failure effects difficult to comprehend without the aid of analytical methods. [Source: ARP4754A]
COTS component	Component, IC, or subsystem developed by a supplier for multiple customers, whose design and configuration is controlled by the supplier's or an industry specification. [Source: DO-254]
Continued airworthy operation	All dispositions, procedures, or built-in devices deployed over the entire lifetime of a unit of equipment with the aim to maintain its compliance with airworthiness standards/certification specifications. Continued airworthy operation requires handling of failures, malfunctions, and defects. [Source: proposed in this report]
Complex AEH (CEH)	When an item cannot be classified as simple, it should be classified as complex. [Source: DO-254]
Complex COTS IC's, controllers and microcontrollers	The definition of CEH versus SEH also applies: When an item cannot be classified as simple, it should be classified as complex. [Source: DO-254]

COTS controller	Any digital or hybrid electronic device that does not execute software in a specific core, therefore having no CPU, and implements peripheral hardware elements that may be: - Simple (e.g., UART, A/D, D/A) or - Complex (e.g., an I/O bus controller). [Source: EASA CM SWCEH-001, [2]]
COTS IP	Any commercially available electronic function designed to be reused as a portion of a device that may be classified in the following three categories: soft IP, firm IP, or hard IP. [Source: EASA CM SWCEH-001]
COTS microcontroller	Any digital or hybrid electronic device that executes software in a specific core area known as a CPU, and implements peripheral hardware elements that may be: - Simple (e.g., UART, A/D, D/A) or - Complex (e.g., an I/O bus controller). [Source: EASA CM SWCEH-001]
Defined intended function (DIF)	All actions, transformations, or behaviors expected to be performed by a particular unit of equipment or system at any level of their hierarchical structure. Intended function can generally be first captured in a requirements specification then ultimately designed, implemented, and verified. [Source: proposed in this report]
Fit-for-purpose behavior	All usages, missions, or services fulfilled by a particular unit of equipment or system when either used standing alone or within another system. The fit-for-purpose behavior may vary depending on what the user is allowed, expected, or intended to do, but must be documented into some form (e.g., scenarios, expected usage, or interface). [Source: proposed in this report]

Function	An action or activity performed by a product, person, or process that produces results for which this product, person, or process is specially fitted or exists. [Summary definition freely adapted from The Free Dictionary]
Highly-complex COTS microcontroller	Any COTS microcontroller having any of the following characteristics: - More than one core CPUs are embedded and they use the same bus (which is not strictly separated or using the same single port memory). - Several complex peripherals in the microcontroller are dependent on each other and exchange data. - Several internal busses are integrated and are used in a dynamic way (for example a dynamic bus switch matrix). [Source: EASA CM SWCEH-001]
Integrated Circuit	A circuit (also IC, microcircuit, microchip, silicon chip, or chip) consisting of elements inseparably associated and formed in-situ on or within a single substrate to perform an electronic function. [Based on EASA CM SWCEH-001]
[Intended] Function	Intended behavior of a product based on a defined set of requirements regardless of implementation. [Source: ARP4754A]
[Intended] Purpose	All foreseen usages or services assumed to be provided at some level of operation (e.g., a COTS component is selected for specific use at CBA level). An intended purpose varies depending on what the user is allowed to do. [Source: proposed in this report]
Model	The representation, either graphical, descriptive, or by any other means, of a complex physical system (CPS) behavior, structure, and/or interactions. [Source: proposed in this report]

Operating and environmental conditions	All functional, environmental, or operational conditions, either external, internal, or at the interfaces, to which the particular unit of equipment or system—at any level—should be faced with and be able to handle properly, including for normal, abnormal, or emergency situations. [Source: proposed in this report]
Properties	All relationships established between "attributes" that are based on overall principles that govern the existence, necessity, and persistence of objects. [Source: proposed in this report]
Proper and safe functioning	All capabilities, architectures, and structures as-required, as-designed, and ultimately as-built into a particular unit of equipment or system that will allow the unit of equipment or system to meet the safety objectives assigned to it, both in terms of functional and dysfunctional behaviors. [Source: proposed in this report]
Purpose	An aim or goal achieved by something for a particular reason appropriate to a situation. [Summary definition freely adapted from The Free Dictionary]
Simple AEH (SEH)	A hardware device is identified as simple if a comprehensive combination of deterministic tests and analyses appropriate to the Development/Design Assurance Level (DAL) can ensure correct functional performance under all foreseeable operating conditions with no anomalous behavior. [Source: DO-254]
Simple COTS	The definition of SEH also applies. In addition: Ability to verify by test on the physical device all requirements in all configurations is a prerequisite for the classification of a device as simple. [Source: EASA CM SWCEH-001]

Technically suitable implementation	All physical characteristics and performances of hardware, software, or any other items to the necessary detailed level of construction of the unit of equipment or system that will contribute to the adequate realization of such an “as-designed” then “as-implemented” and/or “as-built” unit of equipment or system. [Source: proposed in this report]
Requirement	An identifiable element of a function specification that can be validated and against which an implementation can be verified. [Source: ARP4754A]
Safety Net	Mitigations and protections at the appropriate level of aircraft and system design to help ensure continuous safe flight and landing. […] The safety net can include passive monitoring functions, active fault avoidance functions, and control functions for recovery of system operations. [Source: DOT/FAA/AR-11/2,[6]]
System	A collection or combination of elements or parts, organized and interrelated in a pattern or structure to accomplish or produce a characteristic set of behaviors known as its “functions” or “purpose” in relationship with an overall environment. [Based on ARP4754A and DO-254]
System[ic] [Approach]	Refer to something that is “systemwide” (i.e., affecting or relating to a group or system as a whole instead of its individual members or parts). Not to be confused with “systematic,” which means “methodical.” [Summary definition freely adapted from The Free Dictionary]
Validation	The determination that the requirements for a product are correct and complete (i.e., are we building the right aircraft/system/function/item). [Source: ARP4754A]
Verification	The evaluation of an implementation of requirements to determine that they have been met (i.e., answer to did we build the aircraft/system/function/item right). [Source: ARP4754A]

2. DISCUSSION

2.1 GENERAL

Any unit of equipment destined for installation on an aeronautical product should be shown to support the product's compliance with the applicable airworthiness regulations. When considering LRU, CBA, or COTS AEH, the applicable airworthiness requirements should be captured as overall objectives that should be met to satisfy the AEH aspects of certification.

2.1.1 LRU and CBAs

For LRUs and CBAs newly developed by avionics suppliers, DO-254 guidance could be used as providing a minimum set of activities that would then result in a minimum set of data commensurate with the simplicity of the AEH. DO-254 also provides guidance for reused LRUs and CBAs when understood as PDH. In addition, DO-254 does not preclude LRUs and CBAs to be considered as COTS items; however, this approach is deemed acceptable for DAL C or lower. COTS LRUs and COTS CBAs to DAL A or B would raise few more concerns in terms of intended functions and safety features, particularly if they incorporate complex AEH.

2.1.2 Commercial Off-the-Shelf

DO-254 does address COTS components with a minimal set of guidance in section 11.2. The suggestion that COTS could be addressed in the context of the current ARP4754A does not fit with what is understood as system-level assurance. ARP4754A is more focused on higher levels of system integration and complexity. COTS components may also feature high levels of integration and complexity, but still cannot be considered in the same manner as avionic systems such as cockpit displays, flight controls, and integrated modular avionics. However, future revision of ARP4754A might incorporate considerations on COTS to some level (e.g., COTS units of equipment, CBAs, and other COTS items).

Assurance for COTS components cannot completely discard DO-254 or any related interpretative material, such as the one generally found in FAA's issue papers or EASA certification review items (partly based on EASA CM SWCEH-001). In addition, assuring COTS at the system level does not mean an exclusive use of ARP4754A in lieu of DO-254. The authors' first assessment of such an issue would naturally guide the reader toward a multiple-view system approach rather than a single system-level assurance process.

Whereas system design can implement such features as monitoring, redundancy, or partitioning that will help detect, correct, or mitigate design errors, the target error types are those that might occur at the interface of the COTS components themselves because they are embedded in the system. Error types deep inside a COTS component are generally not known in detail and, therefore, cannot be mitigated by straightforward mechanisms. Appropriate mitigation would only be possible if internal safety mechanisms, OEM-recommended workarounds, or other safety barriers were already available within the COTS component itself.

The concept of a safety net has also been suggested by various authors. A safety net can be designed only if the size of its "mesh" is commensurate with the item it is designed to catch. Because error types within a COTS component are generally not known in detail, the safety net

cannot be tailored to them, except if designed to some coarse grain. However, it is common practice at the system level to design architectures intended to meet safety objectives and mitigate global failures assumed at the interfaces of the various items. Architecture mitigations, safety nets, and safety barriers are common in designing safety-critical systems.

The maturity of a COTS component is usually assessed via errata analysis of pending and new errata, and plotting their profile or rate of occurrence over time. COTS component service experience in both airborne and non-airborne applications is also gathered when available. COTS maturity is therefore not really a system-level related property. This report argues that COTS maturity can be used as an element within an overall approach to COTS assurance. For the user, to master the COTS component would allow reaching an acceptable maturity level. For example, skilled ability to properly configure a COTS component is essential. The recommendation from this research, therefore, is to combine all the above elements of COTS component's maturity assessment.

In the context of maturity, the more a COTS component is used in various applications, the more errata can be revealed or discovered and be solved to gain both service history and design maturity on that COTS component. However, it is not guaranteed that all potential errors, when not revealed, are fully eliminated. Whenever an AEH item, and a COTS component in particular, is used in different operating contexts and environments, it is expected that residual errors are revealed and corrected to some extent.

COTS components, such as COTS IP, will be more and more deeply embedded in complex or highly complex AEH constructions whether they are application-specific integrated circuits (ASICs), programmable logic devices (PLDs), field programmable gate arrays (FPGAs), systems-on-chip (SOC), or CBAs. Systems have hierarchical structures, featuring multiple layers of integration. This statement justifies the question of the system level to be considered for the COTS component's assurance. However, in general, multiple intermediate levels exist from the COTS AEH item level up to the system level being considered; therefore, assurance that could be provided at the system level would be too remote to be adequate in providing acceptable assurance at the COTS AEH component level. Even the layer immediately surrounding the COTS component has a limited capability to provide such assurance. This consideration further supports the authors' recommendation for a global systemwide approach, rather than a system-level-only assurance for COTS components.

Few additional question items quite relevant to COTS components need be addressed:

- How is a COTS component determined (selected and implemented) to perform the required function and to fit with the intended purpose?
- How can one ensure that a COTS component performs the intended function (it may be by itself or within the AEH in which it's been involved)?
- How is a COTS component technically suitable in terms of characteristics, performance, safety, interface, and other abilities (e.g., reliability, availability, maintainability)?
- How can a COTS component be assessed to properly function without anomalous behavior under all foreseeable operating and environmental conditions?
- How are operating conditions, including functional interfaces and environmental conditions, compatible with the COTS component's features?

- How can a COTS component maintain its characteristics and performance over its operating life, including through design or manufacturing changes or obsolescence?

These questions could easily be translated into overall objectives for the assurance of COTS components. Additionally, they can be shown traceable to general FAA airworthiness standards or EASA certification specifications, as developed in this report.

The direction taken for this research was to examine how assurance of COTS components could meet such objectives based on activities and artifacts, and how mastering the COTS component's miscellaneous data could support such activities. A COTS component is generally a black box that can only be viewed as an interface between the inside structure and functions, and its outside conditions and surroundings. It is only when the inside matches the outside and can be shown to fit correctly that it can be said that this black box serves the intended purpose for the system design.

A canonic example of a COTS component in which assurance has been deemed feasible and acceptable at the system (software) level, and even outside the use of DO-254, is the case of pure COTS microprocessors. It is recognized that assurance of microprocessors and of the CPU part of microcontrollers can be based on the application of DO-178B to the software they host, including testing of the software on the target. The rationale behind this is that the interface between the COTS CPU and the system software is entirely determined by the CPU instruction set (designed to such end) and that software code is bound to using this instruction set, possibly using all possible configuration settings, sequences constructs, including for software errors handling. This is a perfect example of the two-way causation principle by which the software behavior is fully predictable on the basis of the instruction set that is used for programming, and only on this instruction set, and the behavior of the COTS microprocessor is fully determined by the sequence of software code, which has been subjected to adequate verifications.

3. APPROACH

The approach taken in this report goes beyond a strict system-level assurance that would cover the AEH by addressing the system embedding it, but rather it exhibits a more systemic nature, in the sense of combining multiple views of the AEH as a potentially complex system within another system.

3.1 GENERAL FRAMEWORK

This section is dedicated to the description of the general framework for this research in terms of goals and objectives. It consequently focuses on Title 14 of the Code of Federal Regulations (CFR) Part 25 [7] and/or 29 [8], and on EASA Certification Specifications CS-25 [9] and/or CS-29 [10], as it relates to objectives and assurance activities.

3.1.1 Links with Certification Basics

14 CFR 25.1301 and 25.1309 (and CS 25.1301/1309) express requirements that must be satisfied by any unit of equipment, including software and AEH items, planned for aircraft installation. For equipment covered by a technical standard order (TSO), 14 CFR 25.1301/25.1309 or 29.1301/29.1309 would only apply when the unit is intended to be installed on an aircraft. They

should nevertheless be taken into account early on in the process and prior to installation, so these sections apply. Key terms are highlighted below:

- 14 CFR 25/29.1301 (CS 25/29.1301) Function and installation states that each item of installed equipment must:

  - Be of a kind and design appropriate to its intended function; […].
  - Be labeled […].
  - Be installed according to limitations specified for that equipment.
  - Function properly when installed (no longer in CS-25, [9]).

- CS 25.1309 Equipment, systems and installations states that (a) the aircraft equipment and systems must be designed and installed so that:

  - Those required for type certification or by operating rules, or whose improper functioning would reduce safety, perform as intended under the aircraft operating and environmental conditions.
  - Other equipment and systems are not a source of danger in themselves and do not adversely affect the proper functioning of those covered by subparagraph (a)(1).

  And that (b) the aircraft systems and associated components, considered separately and in relation to other systems, must be designed so that:

  - Any catastrophic failure condition (i) is extremely improbable; and (ii) does not result from a single failure; and
  - Any hazardous failure condition is extremely remote; and
  - Any major failure condition is remote.

- 14 CFR 25/29.1309 Equipment, systems, and installations states that the equipment, systems, and installations whose functioning is required by this subchapter, must be designed to ensure that they perform their intended functions under any foreseeable operating condition.
- 14 CFR 25/29.1309 Equipment, systems, and installations states that the airplane/rotorcraft systems and associated components, considered separately and in relation to other systems, must be designed so that:

  - The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane/rotorcraft is extremely improbable, and
  - The occurrence of any other failure conditions which would reduce the capability of the airplane or rotorcraft or the ability of the crew to cope with adverse operating conditions is improbable. […].

- 14 CFR 25.1529 Instructions for continued airworthiness requires the applicant to prepare these instructions.

DO-254 section 11.1 for previously developed hardware, section 11.2 for commercial off-the-shelf components, and section 11.3 for product service experience provide the following additional objectives:

- 11.1.2. Change of Aircraft Installation, 11.1.3. Verification of hardware interfaces should be conducted where previously developed hardware is used with different interfacing hardware.
- 11.2.1 (3). There is service experience supporting the successful operation of the component.
- 11.2.1 (6). The components have been selected on the basis of technical suitability of the intended application, such as component temperature range, power or voltage rating, or that additional testing or other means has been used to establish these.
- 11.2.1 (7). The component performance and reliability are monitored on a continuous basis, with feedback to component manufacturers concerning areas that need improvement.
- 11.3 Product Service Experience (PSE). Service experience may be used to substantiate design assurance for previously developed hardware and for COTS components.

3.1.2 Objectives or Attributes

From the regulatory and guidance material referenced in the previous paragraph, a derivation is performed in terms of objectives to be met or be alternatively seen as attributes that should be shown to belong to any equipment or item, whether those attributes are directly shown as built-in or demonstrated via other means/activities, see table 1, “Derivation of objectives/attributes from certification requirements”.

These objectives could equally be derived from the various aspects that can be perceived as belonging to every implemented physical system or unit of equipment, namely: performing its intended functions, being fit-for-purpose and safe-for-flight, behaving adequately in operating environment, and continuing to do so over time.

Table 1. Derivation of objectives/attributes from certification requirements

Origin	CS-25/29 & FAR 25/29 DO-254/ED-80 extracts		Objectives/ Attributes
CS 25.1309(a)(1) FAR 2x.1309(a) 2x.1301(a)(1)	"perform as intended" "perform their intended functions" "[…] appropriate to its intended function "	O1/A1	Has a known defined intended function, which it performs
2x.1301(a)(4) DO-254 §11.1.2 DO-254 §11.1.3	"function properly when installed" "the use in a new aircraft installation of hardware […]" "used with different interfacing hardware"	O2/A2	Exhibits Fit-for-purpose behaviors and interfaces (note 1)
CS 25.1309(a)(2) FAR 25/29 & CS 29.1309(b)(1)(2)	"do not adversely affect the proper functioning" "[*ensure*] the continued safe flight and landing" "ability […] to cope with adverse operating conditions"	O3/A3	Features proper and safe functioning when installed
FAR/CS 25/29.1301(a)(1) DO-254 §11.2	"Be of kind and design appropriate to […]" "technical suitability of the intended application"	O4/A4	Implements suitable technical characteristics & performance
CS 25.1309(a)(1) FAR 25.1309(a) CS 29.1309(a)	"[…] under the aircraft operating & environmental conditions." "[…] under any foreseeable operating condition."	O5/A5	Able to operate under operating and environmental conditions
FAR/CS 25/29.1529 DO-254 §11.1, §11.2.1 (3) & (7) and DO-254 11.3	"Instructions for Continued Airworthiness" "service experience supporting the successful operation" "performance and reliability monitored on a continuous basis" "Service experience may be used to substantiate design assurance […] for COTS"	O6/A6	Continue to operate [Airworthy] for its determined lifetime

Note 1: There is a difference between "defined intended function" under objective/attribute O1/A1 and the ultimate behavior for which such function must be designed (i.e., be fit-for-purpose under objective/attribute O2/A2). The objective/attribute O2/A2 may include functional aspects and interface constraints, expected behavior, and robustness aspects.

3.1.3 Rationales and Instantiations

Everything that exists manifests itself under various aspects that can be called "attributes." In a broad sense, these attributes encompass:

- First, a determination of the substance in terms of matter and energy. Physical objects are made of, or implemented via, some suitable characteristics and materials. When properly fed with energy, they will provide adequate and proper functioning.
- To some extent, a physical object must be considered in both space and time. Its structure and outline in space are important. What is happening at its interface with environment and operating conditions is of real significance, together with its lifetime operating usage.
- Last, a physical object must be known to perform defined intended functions that must ultimately fit the expected purpose for which it has been designed. In addition, the object is interacting with many other objects within an encompassing system.

The following sections then consider all six objectives or attributes and provide a rationale for each with a method for instantiation for a particular type of AEH (e.g., CBA, COTS).

3.1.3.1 Objective/Attribute 1: Has a Known Defined Intended Function, Which it Performs

The rationale for this objective/attribute is based on the fact that the intended function of an AEH may depend on its type. For a COTS AEH, it can only be established on the basis of available device data (e.g., its datasheet). For a CBA, the intended function is generally captured (i.e., specified) as requirements.

3.1.3.2 Objective/Attribute 2: Exhibits Fit-for-Purpose Behaviors and Interfaces

The rationale for this objective/attribute is that an AEH is expected to fit with the next upper level of integration of both hardware and software (if any). Therefore, traceability to requirements for a CBA or a matching assessment for COTS AEH must be documented with requirements allocated at the next level of integration.

3.1.3.3 Objective/Attribute 3: Features Proper and Safe Functioning When Installed

The rationale for this objective/attribute is that both the functional behavior and potential dysfunctional behavior of an AEH should be analyzed at the adequate level to show that allocated safety objectives are met regardless of the configuration, including the case of inadvertent alteration of configuration settings for a COTS component.

3.1.3.4 Objective/Attribute 4: Implements Suitable Technical Characteristics and Performance

The rationale for this objective/attribute is that all characteristics and performance of an AEH that are contributing functionally, environmentally, or for any safety reason in the design of the next integration level of hardware or software must be considered. Limitations should be shown compatible with the overall design.

3.1.3.5 Objective/Attribute 5: Able to Operate Within Operating and Environmental Conditions

The rationale for this objective/attribute is that the functional verification and environmental qualification is generally performed at the level of the overall unit of equipment (e.g., LRU). This includes verifications versus operating conditions, interfaces, environmental conditions, and robustness to normal/abnormal conditions.

3.1.3.6 Objective/Attribute 6: Continue to Operate (Airworthy) for its Determined Lifetime

The rationale for this objective/attribute is that an AEH, both initially implemented and during its whole operating life, should be tracked for in-service reliability, failures, and defects. Configuration management should also be continued via problems reporting and change impact analyses.

3.2 A SYSTEMIC APPROACH

This section describes the overall/intermediate goals and requirements with the enablers that must be put forward to allow for a streamlined process or assurance roadmap for AEH at any level of hierarchy in terms of satisfactory activities supported by evidence.

3.2.1 Systems Complexity

Several principles should be considered to create a framework for a system-level assurance of AEH. A system approach is recommended as particularly suited for COTS AEH. As part of the proposed approach, this section further discusses key principles.

First, because a system approach addresses systems, the COTS component itself and the embedding AEH have to be considered as systems. With the exception of simple CBAs and simple COTS components, which by definition can be assured by verification testing, COTS components are generally complex. Therefore, they should be approached in a way similar to that used for complex systems (i.e., a complex COTS component should be treated as a system by itself).

Complex systems are generally described as exhibiting emergent properties as a result of interactions between their various constitutive elements. This is summarized in the axiom “the whole is more than the sum its parts.” This is usually complemented by its antipodal principle “the whole is also less than its parts.” In other words, the system, seen as encompassing its parts, constrains them (e.g., multiple agents communicating through a data bus, which has a limited bandwidth, will somehow constrain the performance capability of each individual agent).

Additionally, a COTS component should be considered as a system by itself, embedded within a system. For example, a CBA is contained within another system (e.g., unit of equipment). The encompassing system either imposes additional limitations on the functionalities, or might reveal behavior of the subsumed system(s) that were not initially considered.

The definitions of system and complex system would suggest that the pair (complex, system) could be seen as a tautology, as both terms may define a composition of interrelated parts. However, the term complexity implies a more in-depth emphasis toward a stronger imbrication of parts.

For CPSs, uncontrolled emergent properties are not desired as systems are built to feature deterministic functions. The only emergent properties needed are the functions these CPSs are intended to perform and for which they are built. In other words, CPSs should always feature a stable structure and repeatable functions (i.e., the same conditions lead to the same behavior). Non-linearity that could stir up emergent properties is assumed to be strictly limited to that necessary to perform the intended functions. It is worth mentioning that a CPS should neither feature any adaptive behavior nor randomly defined structures, nor be self-organizing.

A clear definition of complexity, either direct or indirect, is not available, and is often subject to misunderstanding even within the industry community. Measurement of complexity is also subject to questioning. Metrics for measuring complexity generally refer to a concept from information theory stated as "The quantity of information that is missing—or uncertainty—on the system (i.e., the quantity of information that would be needed to design the system)." The use of such definition and attributes do not help finding solutions to master CPSs. These words are more problem-related terms reflecting the inevitable black-box approach to CPSs. Complex systems are to some extent open systems. In reality, a system cannot be disconnected from its context and some dependencies are always involved in the definition of complex systems.

Conversely, a simple device is defined, designed, and implemented or built to implement a specific portion of the hardware design at the CBA level. Because of simplicity, the quantity of design information that is then embedded is generally limited and easily manageable. Therefore, a verification activity should be able to show that such information is actually built into the device and, consequently, that functional performance will be ensured when such information can be retrieved.

Common mind traps associated with complex COTS AEH include the following binary questions: "Is the COTS component simple or not? Or is it complex/highly complex?" The way to escape from such traps is to understand complexity more as a continuum than a mere on/off choice.

3.2.2 A Systemic Approach

A systemic approach to complexity could consist of:

- Collecting available knowledge on each of the individual parts or subsystems of the complex system (e.g., CPU cores, GPU, data buses, I/O units).
- Identifying limitations (performance of the whole is less than the sum of individual performances) and managing the configuration and persistent stability.
- Looking for the distinctions and interdependencies between multiple parts and their hierarchical inner structure.
- Recognizing the value of multiple complementary views toward the actual intended functions and behaviors, and accepting contentions between parts.
- Avoiding reductionism to look at only one or a few items independently from others, but accepting autonomy of some.
- Having a global approach (e.g., I/O, data flow, hardware/software interface, intended functions, resources usage, and hierarchical integration).

Because a complete knowledge of a CPS is impossible, a certain degree of uncertainty must be accepted, assessed, and mitigated as necessary. Intuitively, some COTS AEH are more complex than others (e.g., multi-core processors versus single-core). Nonetheless, just as no clear general definition of complexity exists and, above all, no single theory of complexity is elicited, no single measure of complexity is consequently achievable. Literature abounds with proposals to measure complexity; unfortunately, none is as generic as expected. This may only mean that no single measurement is possible or even that a combination of all measures may not be satisfactory.

Another approach to complexity refers to complexity profile, which is based on miscellaneous criteria for assessing products, projects, or organizations, and allows for risk mitigation. The complexity

profile helps only in addressing the level of efforts, costs, delays, and product, project, or organizational risks. Guidelines can be derived as follows:

- Step 1: Identification and profiling
    - Identifying the complexity factors
    - Quoting and ranking complexity factors
    - Evaluating risks on most critical factors
- Step 2: Risk-mitigation analysis
- Step 3: Decisions and action plan

Examples of complexity factors used in a complexity profile may include reliability, safety, security, robustness, functional performance, environmental conditions, observability, controllability, and verification. Other technical factors can be considered, such as technology readiness level (TRL), human factors, prototyping, systems integration, quality assurance, maintainability, sourcing, and obsolescence. Finally, non-technical factors include cost, schedule, organization, sub-contracting and partnership, training, and procurement.

3.2.3 Links With Objectives/Attributes

The previously derived objectives/attributes O1/A1 through O6/A6 can be understood as elements of a systemic approach for units of equipment—CBA AEH or COTS AEH—as they provide multiple views of the CPS:

- Objective/attribute O1/A1, intended function, provides the functional view of the unit of equipment (COTS component as a system). This viewpoint is therefore dealing with "what" the COTS component is intended to do on its own perspective.

- Objective/attribute O2/A2, fit for purpose, considers an overview of the unit of equipment (COTS component as a system). This viewpoint is therefore dealing with the COTS component's goals (answering the question of "why?").

- Objective/attribute O3/A3, proper functioning, provides a kind of mechanistic view of the unit of equipment (COTS component as a system). This viewpoint is therefore dealing with "how" the COTS component is structured to provide correct and safe behavior.

- Objective/attribute O4/A4, technical suitability, considers the detailed technical view of the unit of equipment (COTS component as a system). This viewpoint questions the identity of this object in terms of characteristics (answering the question of "who?").

- Objective/attribute O5/A5, operating conditions, provides a view from the environment surrounding the unit of equipment (COTS component as a system within a system). This viewpoint addresses "where" the COTS component is operated.

- Objective/attribute O6/A6, continued airworthiness, considers the evolutionary view of the unit of equipment (COTS component as a system). This viewpoint is covering the

questions of what will happen to this COTS component over its operating life (close to answering a "when?" question).

3.3 A SYSTEM MODEL

This section describes the representations of the related artifacts most suitable to allow for a better understanding of an AEH within its environment. These representations may be used to devise the most adequate model to support AEH assurance argumentation.

3.3.1 The Concept of Model

Whenever a systemic paradigm is envisioned as a way to master a system approach on a physical object, the concept of a model is always provided as a means to represent the system. This representation, or model, is particularly needed when the system proves to be complex (i.e., as information is missing on its internal structure).

This model can be used in simulations to gain a better knowledge or understanding of the system's mechanisms, therefore enabling deducing or predicting its behavior under specific conditions or environments. Simulation allows acting on the model and observing unexpected behaviors or unsafe misbehaviors. Simulation is used in this way for both functional and dysfunctional assessments.

Simulation can also be used to support designing: models represent design alternatives that could be assessed successively, starting with known design constructions. The models represent increments toward the expected construction. The models are then exercised in simulation until the desired behaviors can be observed and match how they ought to be. Simulation used in this way is a powerful design technique.

A model cannot represent all aspects of a physical device: a particular model is always built to help characterize a set of behaviors toward specific goals. For example, a functional model is built to assess normal behaviors, and possibly abnormal behaviors. However, abnormal behaviors are significantly different from normal cases (e.g., degraded modes), and another model may be required.

Additionally, a model cannot represent all levels of details for all parts of a system. Whenever complexity is increased, parts can only be defined by their interactions or relationships. The model will only constrain its parts to their relevant effects within the system (i.e., the expectation is that the principle of downward causation can be relied on).

A model for a specific portion in a system can be used for integration with other portions, providing that such integration scales properly (i.e., only limited known properties and linear interactions between those portions exist). In other words, the expectation is that the principle of upward causation can be relied on.

3.3.2 Application to Development

What do developers want to do in constructing CPS in general, and using COTS AEH in particular?

1. They want to "operate" them (i.e., they would like to make sure and predict what will happen when they are operated in a real-world situation, including when embedded within another

system or subjected to another environment). This is similar to a deductive approach of physical laws: Whenever known inputs or initial conditions are applied to a CPS, it is assumed by the laws of physics, or at least based on some transfer function, that the system will produce known outputs or final conditions.

2. They want to "design" them (i.e., they would like to obtain some expected behavior or specific outputs). To this end, the goal of "design" is to determine what specific inputs must be applied and within which overall situations and environment. This is similar to an inductive approach of physical laws: Whenever an output or final conditions are expected for some purpose, the "design" goal is to determine, based on physical law, or at least using an inverse transfer function, what inputs/external conditions should be established.

3. They want to "verify" them (i.e., they would like to ensure that the CPS behavior, or its transfer function, actually performs as intended and meets all adequate objectives; e.g., is suitably implemented, fit for purpose, safe for use, and able to continue to operate properly when installed). This is similar to verifiability of physical laws: Whenever both inputs and outputs, or initial and final conditions, are supposed to fit the law, a comparison can be made between the actual behaviors and the expected ones.

3.3.3 Application to COTS AEH

A first assumption is that COTS components are physical objects to be considered as CPS. As such, they are non-adaptive, non-random, and non-self-organizing. The representation level closest to the physical object is a model (e.g., a bit stream for an FPGA, the implementation net lists for an ASIC, or its datasheet for a COTS component). Unfortunately, data available in a COTS component's datasheet are limited. Because missing information on a COTS component makes it complex, the ability to build a model for that COTS component is then limited.

Matching the COTS component's model with the model of the overarching system can be supported by the concept of "usage domain/domain of use" of the COTS component. The usage domain defines the limitations in the use of the COTS component, based on the identification of used/unused functions, elements (resources), or interfaces necessary for its use at the system level.

Another model can also be considered for the COTS AEH's assurance process, not the COTS component. Such a model could be useful in representing the COTS component within its assurance context and in illustrating its relationships with the objectives previously discussed.

Figures 1 and 2 show the COTS AEH's model and its assurance model using the objectives/attributes previously derived and discussed.

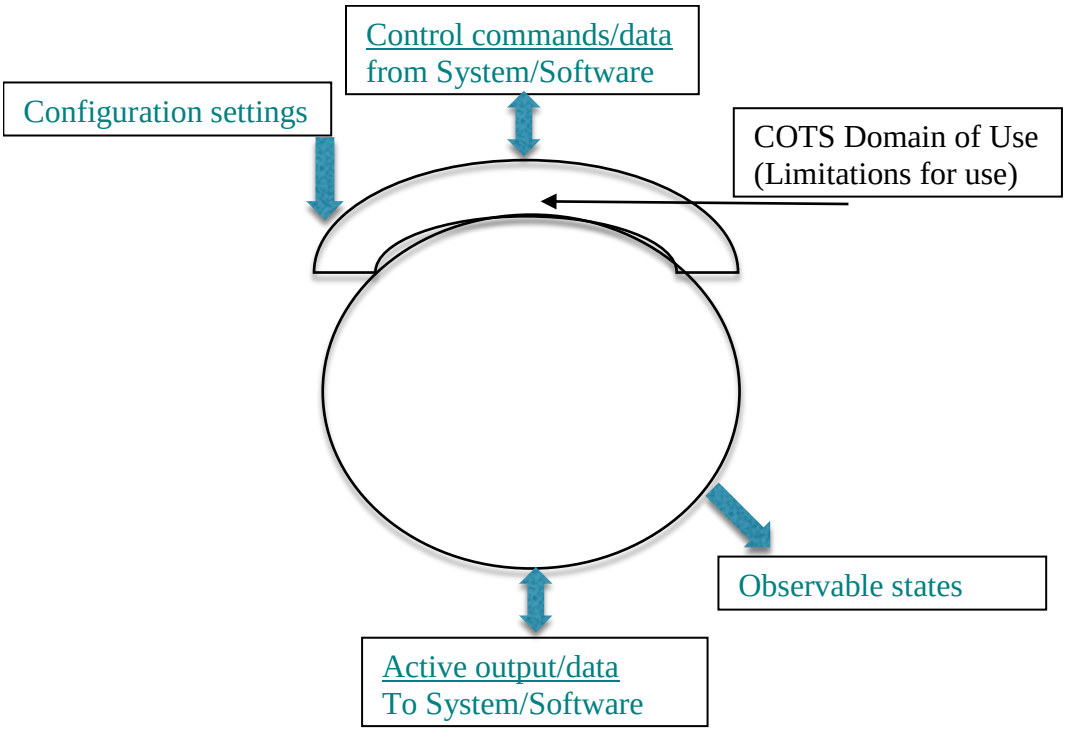

Figure 1. COTS AEH component model showing the usage domain

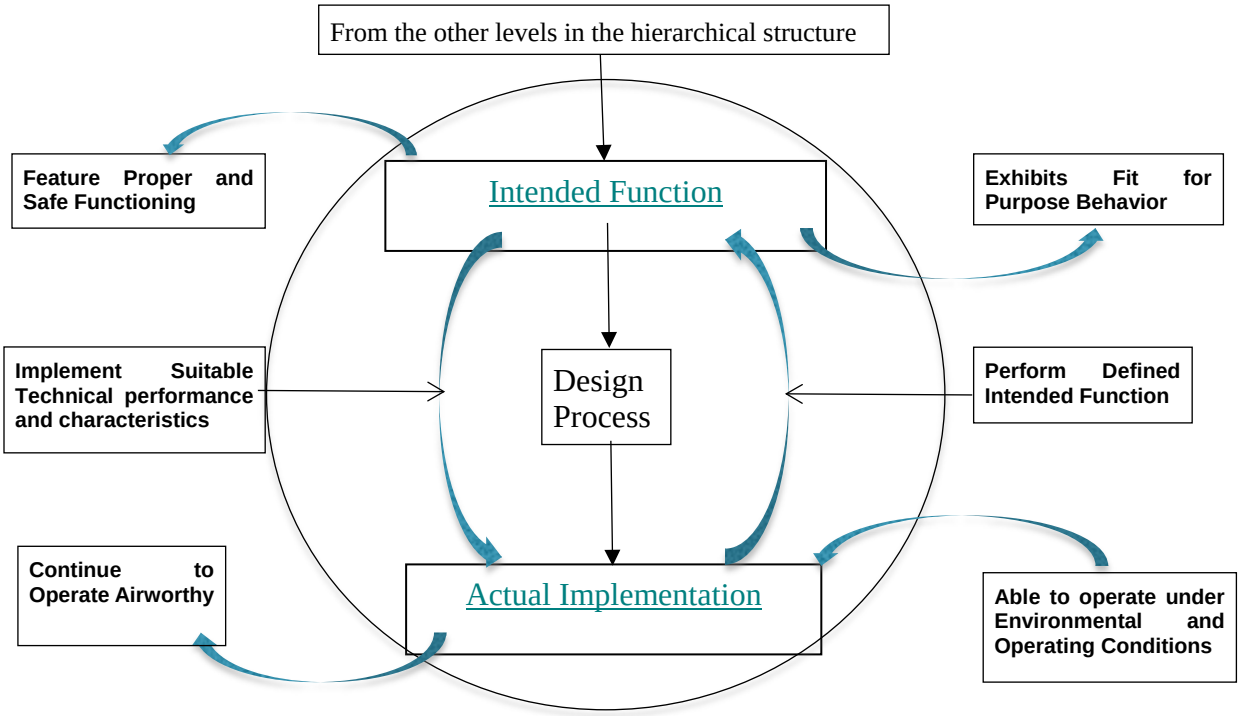

Figure 2. COTS AEH assurance model showing the objectives/attributes

3.4 ASSURANCE PROCESS

This section describes the incorporation of the proposed assurance process within a development process logic and deployment scheme within which the related development assurance objectives can be achieved on the basis of a model-attribute-property (MAP) approach.

3.4.1 MAP

When attributes of a CPS have been defined (see table 1 in section 3.1.2), relationships between those attributes can be established using the suggested property concept. Properties are derived from overall principles or general statements that are assumed to be universally true. Identity, causality, and continuity are such principles that can be selected and are discussed in following sections. Note that quite a few other overall principles could have been selected, including suitability, unity, totality, stability, maturity, capability, observability, and controllability, or more detailed abilities, such as safety, reliability, integrity, availability, maintainability, and quality. However, three principles are addressed in sections 3.4.1.1, 3.4.1.2, and 3.4.1.3 to show how properties can be generated.

3.4.1.1 The Principle of Identity

Something necessarily exists or is nothing at all. This principle expresses the mere existence of a CPS in terms of its material and functionality. From this identity principle, and expressed by using a combination of, either two, or four attributes taken from table 1 in section 3.1.2, leads to these two possible properties:

- Identity: The CPS implements suitable technical characteristics and performance to feature proper, correct, and safe functioning; and, with four attributes combined:
- Identity: A technically suitable implementation of the CPS as designed with respect to its defined intended function is ensuring proper and safe functioning under its operating and environmental conditions.

3.4.1.2 The Principle of Causality

Everything has a reason or is intended for something. This principle expresses the purpose of a CPS in terms of its intended function and its expected purpose. From this causality principle, and expressed by using a combination of either two or four attributes taken from table 1 in section 3.1.2, leading to the two possible properties:

- Causality: The CPS characteristics are designed to its known defined intended function to fit its expected purpose; and, with four attributes combined.
- Causality: The defined intended function of the CPS, as implemented with suitable technical characteristics and performance, fits its expected purpose on a continued basis for its determined lifetime.

3.4.1.3 The Principle of Continuity

Anything is deemed to persist and remain self-consistent. This principle expresses the extent to which a CPS continues to exist in space and persist over time. From this continuity principle, and expressed

by using a combination of either two or four attributes taken from table 1 in section 3.1.2, leading to the two possible properties:

- Continuity: The CPS is verifiable to operate within its environmental and operating conditions and continue to do so for its whole lifetime; and, with four attributes combined.
- Continuity: The CPS operates within its environmental and operating conditions and is fit for its expected purpose while proper and safe functioning is continuously maintained for its lifetime.

Going forward, considering at least the four first attributes, combined in pairs, this leads to up to six properties, which can be expressed as shown in table 2:

Table 2. Combination of four attributes in pairs leading to six properties

Pairs	Properties
A1 and A2	The defined intended function is adequately captured from the expected purpose, desired behavior, and interface needs (kind of validity property; comparable to some intended OP).
A1 and A3	The defined intended function is established to achieve proper and safe functioning when installed (kind of safety—intrinsic property).
A1 and A4	The defined intended function is correctly designed into a technically suitable implementation (kind of conformity property; comparable to necessity plus correctness OP).
A2 and A3	The expected purpose, behavior, and interface requirements must be achieved properly and safely (kind of safety—extrinsic property).
A2 and A4	A suitable technical implementation is consistent with the expected purpose, behavior, and interface requirements (kind of suitability—for-purpose property).
A3 and A4	A suitable technical implementation ensures proper and safe functioning when installed (kind of suitability-for-safety property).

3.4.2 What Assurance Process?

For a complex AEH fully developed to DO-254, a structured development assurance process is normally deployed to ensure intended function and safe behavior within the operating environment. This approach of a structured development process must be reduced tremendously for a COTS component because development data are not accessible and the only process achievable is:

- The capture of requirements at the upper level of the design hierarchy (e.g., the CBA) that reflect the intended purpose of the function that will be further designed incorporating the COTS component.
- The identification of the COTS component functions, interfaces, and other features from the datasheet, user manual, or errata that would define the specific capabilities but also constraints imposed by the COTS component itself.

- The assessment of the matching of upper-level requirements allocated to the COTS component as the intended purpose, with the capabilities and constraints of the COTS component as the intended function identified above.

Then at the upper level of AEH design (LRU or CBA), the process is continued by:

- Completing the AEH design at the CBA level
- Verifying the AEH design versus the CBA upper-level requirements
- Verifying the implementation versus its requirements and interfaces

For a CBA, a reduced assurance process is generally deployed because, when complex AEH items are addressed by appropriate strategies, the remaining AEH on the CBA can be considered as simple AEH. Refer to appendix B for an example of objectives and activities for a CBA.

3.4.3 Advanced Assurance Process

Using the MAP approach previously described, an assurance approach can be built as follows:

The definition of assurance provided in section 3.4.3 references "given requirements." This term might deserve a complete explanation. It is understood as all requirements, not only technical requirements pertaining to the product, but also non-technical, safety, and certification requirements to which compliance must be established for a product or process.

As previously discussed, attributes must be, to some extent, adequately perceived as instantiated and built into the final product by the designer/developer. It is the manufacturer's responsibility to make sure that the specific attributes will actually belong to their product. To this end, a qualification[1] process is generally deployed. Moreover, for use by airworthiness authorities, evidence of design/development assurance must be acceptable with respect to rules, regulations, and all related expectations. To this end, a certification[2] process is normally deployed.

A first step toward CPS system design and development assurance can then be made when:

1. Attributes, as instantiated, are shown to belong to the product within its embedding system.
2. Related evidence of that showing, as a result of activities, is made available for assessment.

Properties can therefore be seen as statements that must be verified to be true on the basis of activities within a process, with supporting evidence. Knowing that a CPS can be dealt with only by using successive models, those models must be assessed for representativeness versus reality over the product's development, and related evidence must be provided. All evidence mentioned above should be documented and verified (i.e., reviewed for adequacy to the product and to processes-related actions and activities). This may require additional guidance for the assessment of completion, acceptance, and approval of all evidence.

[1] Qualification etymology: From Latin "qualitas" (qualities) and "fiare" (to make), i.e. "to make qualities".

[2] Certification etymology: From Latin "certus" (certain) and "fiare" (to make), i.e. "to make [sure] certain".

In summary, a consistent chain made of representative models—adequate attributes—satisfactory properties, with their related evidence of validity and verification of these evidences (i.e., a second look at evidence), are all that could provide a complete framework for assurance of compliance with certification requirements.

The development assurance strategy (DAS) process would then follow the steps below:

1. Establish a descriptive model of the specific CPS.
2. Assess and show representativeness of that model.
3. Capture all relevant attributes of the specific CPS.
4. Provide evidence that attributes belong to the CPS.
5. Establish properties gathering consistent attributes.
6. Provide evidence that instantiated properties are true.

3.5 SUPPORTING RATIONALE

This section describes additional rationales and justifications complementary to the previous sections. This section therefore concentrates on the rationale behind the achievement of an acceptable level of assurance using the MAP approach.

As previously addressed, whenever a two-way causation principle is satisfied for a COTS AEH component as a system within a system, a system-level approach would provide an acceptable basis for COTS component assurance. However, several other cases exist for which this principle cannot be claimed as valid, starting with new technology of COTS microcontrollers with built-in complex peripherals. The question is then which rationale can be found to support the global systemic approach based on objectives and activities as described and discussed in the preceding sections for which the authors claim that it is able to provide adequate assurance for COTS components.

3.5.1 Attributes and Properties

The approach using objectives/attributes O1/A1 to O6/A6 is deemed adequate because it allows addressing all questions that can be asked on a system or any unit of equipment, namely: who, what, how, why, where, and when. These questions were addressed in section 3.2.3.

The whole set of attributes is generally captured via requirements' specifications. At this stage, akin to a validation process, consistency between these attributes can be assessed using the approach described for properties.

3.5.2 Matching at Interface

A COTS component, just as any CPS, is known only at its interfaces and via quite a few details in a model description of it (datasheet or user manual). Matching at those interfaces, between the inner COTS structure and its outer environment, is what matters the most.

Moreover, a COTS component is selected to fulfill some intended functions, but in general it covers more than the necessary functions; therefore, it should be correctly configured in such a way that the unnecessary functions are properly deactivated and that others are properly restricted in use.

3.5.3 Design Process Integration

When a complex COTS component is involved in a CBA design, it should be considered as a system within a system. In addition, requirements' capture (top-down view), design description (bottom-up view), and implementation verification (transverse view) are essential in the process.

In other words, a CPS always features a hierarchical construct into multiple levels or layers of integration. The actual levels at which a COTS AEH is attached should be clearly delineated. The MAP approach could then be applied at each and every layer of the system breakdown.

3.6 PUTTING IT ALL TOGETHER

This section describes the necessary effort and work scheme consistent with the complexity of the approach to assure AEH via a systemwide (or systemic) approach. This section concentrates on miscellaneous artifacts part of the ECMP.

3.6.1 Assurance Data for COTS Components

DO-254 section 11.2 COTS guidance suggests that an ECMP should be followed. However, there is no specific list of life-cycle data recognized by the certification community to adequately address all issues related to COTS component assurance.

EASA CM SWCEH-001 recommends that related guidance on activities for COTS components assurance should be documented in an ECMP. Dedicated electronic component management report (ECMR) for COTS components provided as a result of ECMP execution have proven effective in both analyzing, documenting and ultimately showing mastering of COTS components' complexity. Both ECMP and ECMR(s) can be used to show evidence of COTS assurance.

3.6.2 Acceptability of COTS Data

A general criterion for acceptability of data supporting assurance is when all objectives or attributes, namely those previously defined as O1/A1 to O6/A6, are shown to be achieved on the basis of results gained from activities that have been performed. Therefore, compliance statements in hardware accomplishment summaries can be used to record completion of activities and acceptability of results.

In addition, the ECMP as suggested by DO-254 has proven its effectiveness in gaining acceptable TRLs for brand new COTS components, which feature either new integrated functionalities and/or new technologies.

3.6.3 Electronic Component Management Plan

The ECMP provides evidence of assurance of adequate mastering of all AEH components, including but not limited to, COTS AEH components. The ECMP plan that is generally used in the industrial context of management of all aspects of a component, from initial procurement to continuous monitoring.

The ECMP covers all aspects of the AEH components' management process, not only COTS AEH. The ECMP is mainly used for industrial purposes. In the part dedicated to COTS planned compliance, the ECMP assesses overall risks, planned assurance activities, and expected results.

The following is an example of a documented ECMP plan outline:

1 INTRODUCTION

2 REFERENCE DOCUMENTS

3 ECMP PROCESS (Included For Certification)

4 COMPONENT APPLICATION

4.1 Analyses (De-rating, Thermal, Structural)

4.x Reliability, Safety

4.y Electro-Magnetic Compatibility, Radio Frequency Interferences

4.z Single Event Effects, Electro-Static Discharges

4.t Application to PLDs Certification

4.u Application to ASICs Certification

4.v Application to Complex COTS

5 COMPONENT PROCUREMENT

6 MANUFACTURING AND ASSEMBLY

7 DATA COLLECTION AND ANALYSIS

8 OBSOLESCENCE MANAGEMENT

9 APPENDICES

Note: The ECMP is generally required by the applicant from the AEH suppliers of any unit of equipment incorporating COTS component. The ECMP is typically made available for review by the applicant. The ECMP may incorporate industrial proprietary data for supplier's in-house use only in how all procured components are handled within its company.

An ECMR is used to document evidence that objectives are achieved via assurance activities on COTS components. It is particularly useful for complex or highly complex COTS components to DAL A, B, or C, as the whole set of assurance activities and resulting evidence should be documented. An ECMR gathers the results of the ECMP execution mainly with respect to COTS assurance activities. An ECMR records evidences of analyses performed and of data collected

from COTS suppliers and identifies risks mitigations and compliance shown to certification objectives as applicable.

The following is an example of an ECMR outline:

1. INTRODUCTION

2. REFERENCE DOCUMENTS

3. ECMR SUMMARY OBJECTIVES

4. HARDWARE DESCRIPTION

5. COTS(s) AEH DESCRIPTION

6. INTEGRATION IN H/W PROCESS

7. COMPLIANCE WITH ECMP

7.1. Compliance with ED-80/DO254 section 11.2

7.2. Compliance with Certification Objectives

7.3 Compliance with Interpretative Material

8. SERVICE EXPERIENCE ANALYSIS

4. CONCLUSIONS

Complex Physical Systems (CPSs) in general and any unit of equipment in particular—line replaceable units (LRUs), circuit board assemblies (CBAs), commercial off the shelf (COTS)—must be designed, built, and shown to perform their intended functions and be suitable for use to meet expected system behaviors within specific operating and environmental conditions, such as the airborne ones. In addition, such systems must be built to an acceptable level of design and safety assurance, and continue to do so during their operating lifetime.

This report established a general theory on what complex physical systems (CPSs) as artificial constructs are made of, and how an assurance target can be achieved. This theory involved the concepts of models, attributes, and properties, gathered within a model-attribute-property (MAP) approach. Then, it discussed the relationships between these concepts and their application to products and processes to support the associated assurance activities and evidence that are generally expected to demonstrate that a CPS is technically acceptable and approved for installation on aircraft.

Models are representations of real things (i.e., a reality that will eventually exist but that must be dealt with during its development via some kind of manageable artifact). A successive chain of consistent models, also designated as tiers, are used in most product development projects, going from a higher level of abstraction down to lower abstraction levels.

Attributes are the whole set of features or elements that are perceived as belonging to the model of the CPS intended to be built. Attributes can be understood as the overall aspects that a CPS will exhibit within its context. Intended functions, when known and defined, are an example of such attributes. This report proposed a more complete set of attributes: A1 to A6.

Properties are relationships established between attributes, either combined in pairs, triplets, or more complex n-tuples. Properties can also be traced to general principles that govern the possibility of actual elements to exist and persist for some reason. They express consistency between attributes and must be satisfied when instantiated on a CPS.

Attributes can have different types: either generic (templates for multiple products) or specific (instantiations for a particular product within a project). Examples for the various types of representation for the A1 (intended function) attribute are: requirement specifications, design description, physical implementation, programming file (bit stream or executable code), and net list.

Properties can be instantiated as statements to be assessed and verified as true at some point. They can be structured into a hierarchy of substatements, possibly along multiple axes or dimensions (e.g., product-, process- or tool-oriented axes). They ultimately are decomposed into more specific objectives, activities, and data, including evidence of supporting contribution in the achievement of assurance goals, with recognized tailoring to the target complexity and criticality (e.g., a modulation versus assurance level, novelty, or any other significant aspect).

4.1 FINDINGS

This report proposed a MAP approach for assurance of CPS in general and airborne electronic hardware (AEH) in particular (CBA, COTS). The approach to models is discussed and a complete set of attributes is derived (O1/A1 through O6/A6). Properties, seen as combining attributes, are also derived, and a more complete set of properties is listed.

This approach results in a DAS that could be deployed on the basis of these attributes, which must be shown to belong to the CPS intended to be built and based on properties shown to be true. Additionally, properties could be used as part of the DAS with the ultimate usage to show compliance with certification requirements when activities are performed and data produced.

This MAP approach shows that a product-oriented approach could be used at least for COTS AEH as an alternative to a process-oriented approach, which is not achievable for COTS AEH. LRU and CBA, when considered as simple units, could also be supported by such a product-oriented approach.

The MAP approach can also be understood as a structured way to gather, organize, and assess data available with an AEH (COTS AEH in particular) to make sure that such data are necessary and sufficient to cover all attributes and assess all properties in the MAP approach.

Finally, this MAP approach, applied to COTS AEH devices and CBA AEH items, seems to properly meet the intent of this research for an alternate assurance approach because it has been shown to be easily achieved, at least for COTS components and CBA.

4.2 RECOMMENDATIONS

Recommendation: This report has shown that returning to a more product-oriented approach compared to a (complex) process(s)-oriented approach is achievable. A revisited meaning of the term assurance is also shown as being necessary (i.e., show compliance on the basis of true and adequate ideas via a first, second, and third look at models, attributes, and properties, respectively), provided by the proposed MAP approach to assurance and instantiation, and review on the related MAP artifacts.

Recommendation: Objectives, also referred to as attributes 1–6 in the report, adequately capture the essence of certification requirements from Title 14 Code of Federal Regulations Part 25/29 for equipment and systems. These objectives/attributes could be used to show compliance with certification requirements when instantiated for a particular type of equipment (LRU, CBA, COTS) and shown to belong to a particular item of such type via specific activities.

Recommendation: Multiple views are always necessary to describe COTS components as for CPSs in general. Multiple activities may be recommended to address COTS component assurance while cautioning against being too prescriptive on the expected activities.

Recommendation: A distinction should be made between assessing COTS component simplicity/complexity and the route to compliance, which is selected versus development assurance level (DAL), including activities selected as part of the DAS.

Recommendation: There is no commonly accepted/ generic definition or measurement method for complexity. The available definition of simple AEH available in DO-254 appendix C, glossary of terms, should be used to derive any assessment of COTS component complexity.

Recommendation: The MAP approach described and shown in this report is deemed to provide the expected general framework for assurance of CBA and COTS components, but could also be extended to other AEH items, possibly software items or systems. This MAP approach could also be used to help understand the applicable related industry standards whenever these standards are objective oriented and suggest activities to be performed to meet the objectives.

Recommendation: Use all five to six attributes, including: operating and environmental conditions and continued airworthy operation in addition to the four attributes; and consequently use more properties (i.e., more combinations of two or three attributes among five or six, leading to 10, 15, up to 20 properties [3 among 6]).

Recommendation: DO-254 section 11.2 does provide useful guidance on handling COTS. Assurance and this DO-254 guidance should be used as a basis. Then the MAP approach could be used as the overall assurance framework for COTS, as shown in appendix A.

Recommendation: CBAs, when all other complex components are addressed, are generally considered as simple AEH; therefore, it is not necessary to apply in its entirety a structured development process in accordance with the guidance of DO-254. However, DO-254 should still be applied using a minimum set of activities and produced data. The MAP approach could also be used as a general assurance framework for CBA, as shown in appendix B of this report.

4.3 FURTHER RESEARCH

4.3.1 In Terms of Objectives for AEH

This report addressed the derivation of top-level objectives designated as attributes from sections 1301 and 1309 of 14 CFR 25/29 [7,8] and/or CS-25/CS-29 [9,10], and DO-254 [1]. Objectives/attributes must be shown to belong to any unit of equipment or hardware item.

To expand the approach proposed in this report to more general CPSs, including developmental systems, a derivation of the various modes or instantiations of the attributes would be of significant interest. Related properties could then also be instantiated to further support a development assurance strategy, including modulation of activities versus DAL.

Future research beyond this report on assurance issues for COTS components and CBAs could describe a more product-oriented process. This process would consist of addressing the objectives/attributes as they can be instantiated for a COTS AEH, and in providing both rationales and activities to be considered with respect to objectives.

4.3.2 In Terms of Additional Properties

This report addressed a newly proposed approach to assurance of COTS AEH and CBA AEH based on a MAP concept that, when instantiated for a particular hardware item (COTS component or CBA), could support an acceptable level of assurance.

A derivation of all possible properties and for any DAL would be even more beneficial in future development of this research. In particular, establishing criteria for the assessment of properties in terms of their truth could be accomplished using all combinations of attributes and their instantiations in pairs, leading up to 15 properties (all combinations of instantiated pairs of six attributes).

4.3.3 In Terms of Extension to Other Items

The current report concentrated on a systemwide assurance for AEH, but limited to CBAs and COTS components. Future research beyond this report could address other types of AEH, such as custom micro-coded devices, programmable logic devices, system on chip, and multicore processors. Moreover, the MAP approach could be applied to other units of equipment and possibly software systems.

Finally, an examination of current industry standards for development assurance (DO-254, DO-178C, and ARP-4754A [3]) versus such a MAP-based assurance approach could help pave the way to provide means to assess any newly proposed industry standard or certification material in line with such an approach.

5. REFERENCES.

1. RTCA. (2000, April). Advisory Circular 20-152. *Design Assurance Guidance for Airborne Electronic Hardware.* (RTCA, DO-254).

2. EASA Report. (2012). European Aviation Safety Agency Certification Memorandum, Development Assurance of Airborne Electronic Hardware. (CM-SWCEH-001).

3. SAE Report. (2010). Guidelines for Development of Civil Aircraft and Systems. (ARP4754A).

4. FAA Order 8110.105. Simple and Complex Electronic Hardware Approval Guidance. Change 1. (2008).

5. Origin Consulting (York) Limited, (2011). GSN Community Standard Version 1.

6. FAA Report. (2011), DOT/FAA/AR-11/2, Handbook for the Selection and Evaluation of Microprocessors for Airborne Systems

7. Airworthiness Standards: Transport Category Airplanes 14 CFR Part 25, (2019)

8. Airworthiness Standards: Transport Category Rotorcraft, 14 Part 29, (2019)

9. EASA Report. (2017). Certification Specifications for Large Aeroplanes. (CS-25)

10. EASA Report. (2017). Certification Specifications for Large Rotorcraft. (CS-29).

APPENDIX A—OBJECTIVES FOR COTS AEH ASSURANCE

Table A-1 instantiates for commercial off-the-shelf (COTS) airborne electronic hardware (AEH) the objectives/attributes that were established in this report via rationales for each and suggested activities grouped versus objectives/attributes.

Table A-1. Objectives/attributes instantiated for COTS AEH in terms of activities

	Overall Objectives/Attributes	Rationale for Instantiation of Objectives/Attributes to COTS	Activities for Instantiation of Objectives/Attributes to COTS
O1/A1	Has a known defined intended function, which it performs. (based on: FAR/CS 25/29.1301(a)(1) and on CS 25.1309(a)(1), FAR 25/29.1309(a) or CS-29.1309(a))	A COTS is selected to perform all or part of an intended function allocated from the next level up of H/W design. Consequently the COTS description should be adequately documented, including determined for simplicity or complexity. In addition, as part of the COTS may not be used, COTS usage must be clearly defined. Moreover, all data necessary to show adequate mastery of COTS must be established as part of a process and documented.	- Assessment of COTS characteristics and determination of simplicity vs complexity - Electronic component management (Available COTS device & design data) - Determination of the COTS usage domain limitations
O2/A2	Exhibits fit-for-purpose behaviors and interfaces. (based on FAR/CS 25/29.1301(a)(4) and on DO-254 11.1.2 & 11.1.3)	A COTS is a black or grey box, hence everything is happening at, or close to, its boundaries with the next level up of H/W design. Consequently the COTS must be shown to fit properly at AEH boundaries in terms of Interfaces, used functions and for handling of failures.	- Identification of safety requirements allocated to the COTS and safety means - Validation of the COTS usage domain limitations - Definition of H/W–H/W and H/W–S/W interfaces
O3/A3	Features proper and safe functioning when installed. (based on: FAR 25/29 & CS 29.1309(b)(1)(2), and CS 25.1309(a)(2)	A COTS may be involved in one or more functional failure paths (FFPs). Quite a few failure conditions can be emphasized: inadvertent alteration of critical configuration settings, un-mitigated errata that may have safety impact and failures in detection, and handling of potential failures or defects.	- Functional failures paths analysis within the COTS used configuration - Capture and assessment of relevant errata and their impact on safety (pre-TC) - Identification of critical failures situations: errors in settings, un-mitigated errata, etc.

Table A-1. Objectives/attributes instantiated for COTS AEH in terms of activities (continued)

	Overall Objectives/Attributes	Rationale for Instantiation of Objectives/Attributes to COTS	Activities for Instantiation of Objectives/Attributes to COTS
O4/A4	Implements suitable technical characteristics & performance. (based on: FAR/CS 25/29.1301(a)(1) and on DO-254 §11.2)	When implemented, a COTS must be verified to feature acceptable reliability and technical suitability in terms of: functional usage performance, technical characteristics & performance within limits, and interfaces and configuration.	- Verification of COTS Usage Domain versus functional requirements - Verification of technical suitability in general, incl. configuration management - Verification of H/W-H/W and H/W-S/W Interfaces
O5/A5	Able to operate under operating and environmental conditions. (based on: CS 25.1309(a)(1), FAR 25.1309(a) or CS 29.1309(a))	In general both functional verification to operating conditions, environmental qualification to environment and acceptance testing of the production H/W, are performed at the level of the overall unit of equipment (i.e. LRU), which incorporate all the AEH and the COTS AEH in particular.	Functional verification (at LRU level) Environmental qualification (LRU level) Acceptance testing (at LRU level) (particularly for safety mechanisms)
O6/A6	Continue to operate [Airworthy] for its determined lifetime. (based on: FAR/CS 25/29.1529 and DO-254 11.1, 11.2.1(3)(7), and 11.3)	A COTS must be shown to be able to maintain adequate behavior post TC. Both newly issued errata and change notices must be assessed for impact on safety, and continuing operation in service must be monitored. New occurrence of failures and defects must be analyzed and assessed for safety.	Assessment of relevant errata and impact on safety (post-TC) Identification of the effects of COTS Failures (post-TC) ED-80/DO-254 11.1 for Chande impact analysis (CIA). (post-TC) ED-80/DO-254 11.3 for product service experience (PSE) (post-TC)

LRU = Line replaceable unit

A development/design assurance level (DAL) is allocated to AEH from the system safety analysis, including to COTS AEH components that are not developed to ED-80/DO-254; therefore, life-cycle data are not available for review; consequently, a COTS AEH may not be able to be shown to meet any DAL. It is then clear, though surprising, that COTS would have no DAL per se, except the DAL that is allocated to the AEH in which the COTS is embedded. The following rules[3] could be adopted to tailor assurance activities to DAL for a COTS AEH:

[3] The generally agreed way is: the higher the DAL, the more activities and related results are required to show that the COTS AEH really meets/features its corresponding objectives/attributes and that assurance is achieved.

DAL D: No specific activity required. Assurance provided via in-house industry processes.

DAL C: One assurance activity for COTS AEH at the unit of equipment or system level.

DAL B: One additional assurance activity for COTS AEH, but not as many as for DAL A.

DAL A: Another assurance activity or more in-depth assurance activity than the one for DAL B.

Table A-2 suggests a modulation in terms of activities versus DALs for a COTS AEH, based on the instantiations for the first four objectives/attributes. There is no particular justification to modulate versus DAL objectives/attributes O5/A5 and O6/A6 because they have significance only at the level of a full unit of equipment or line replaceable unit (LRU), not at the level of a COTS AEH.

Table A-2. Suggested modulation of objectives/activities versus DAL for COTS AEH

	DAL A	DAL B	DAL C	DAL D
A1 Defined Intended Function	3 activities: - Assessment of COTS characteristics and determination of simplicity vs complexity - Electronic component management (Available COTS device & design data) - Determination of the COTS usage domain limitations	2 activities: - Assessment of COTS characteristics and determination of simplicity versus complexity - Electronic component management (Available COTS device data)	1 activity: Determination of COTS simplicity/complexity per DO-254 §1.6 and all COTS addressed under DO-254 11.2.1 (1) to (5).	In-house process (i.e. not necessarily per DO-254)
A2 Fit-for-Purpose Behavior	3 activities: - Identification of safety requirements allocated to the COTS and safety means - Validation of the COTS usage domain limitations - Definition of H/W–H/W and H/W–S/W interfaces	2 activities: - Identification of safety requirements allocated to the COTS & safety means, - Definition of H/W–H/W and H/W–S/W interfaces.	1 activity: Assurance at the upper level of AEH design for allocation of safety requirements and definition of H/W–H/W and H/W–S/W Interfaces	In-house process (i.e. not necessarily per DO-254)
A3 Proper, and Safe Functioning	3 activities: - Functional failures paths analysis within the COTS used configuration, - Capture and assessment of relevant errata and their impact on safety (pre-TC), - Identification of critical failures situations: errors in settings, un-mitigated errata, etc.	2 activities: - Functional failures paths analysis within the COTS used configuration, - Capture & assessment of relevant errata and their impact on safety (pre-TC).	1 activity:. Considerations on overall performance and reliability for all COTS per DO-254 11.2.1(7)	In-house process (i.e. not necessarily per DO-254)
A4 Suitable Technical Implementation	3 activities: - Verification of COTS usage domain versus functional requirements - Verification of technical suitability in general, incl. configuration management - Verification of H/W-H/W and H/W-S/W Interfaces	2 activities: - Verification of technical suitability in general, including configuration management - Verification of H/W-H/W and H/W-S/W interfaces	1 activity: Considerations on overall technical suitability for all COTS per ED-80/DO-254 11.2.1 (6)	In-house process (i.e. not necessarily per DO-254)

APPENDIX B—PROPERTIES-BASED ASSURANCE FOR COTS AND CBA AEH

B.1. APPLICATION TO COMMERCIAL OFF-THE-SHELF AIRBORNE ELECTRONIC HARDWARE

The following examines how the development assurance strategy (DAS) as proposed in this report can be applied to commercial off-the-shelf (COTS) airborne electronic hardware (AEH). A COTS component is essentially a black box that can be viewed only as an interface between its inside structure and functions, and its outside conditions and surroundings. When matching between the inside and the outside can be shown to fit correctly, it could be said that such a black box would serve the expected purpose for the system design.

DO-254/ED-80 11.2 on COTS AEH recognizes that a process approach to design and development assurance does not apply to COTS because the necessary artifacts (i.e., design and process data) are not available for review, and only a limited amount of descriptive data are available for system design.

This clearly suggests that COTS really needs an alternate or complementary process or approach to what is currently available in general DO-254/ED-80 guidance. COTS AEH can then be selected as good candidates to quickly test a model-attribute-property-based assurance approach without the need to refer to the whole set of objectives, activities, and data recommended by DO-254/ED-80 for developmental hardware items.

Models: A model in the case of a COTS component can only be built using limited data on its behavior and interfaces available from the supplier's datasheet. Only inputs can be controlled and outputs can be observed (i.e., a system-level approach can be applied at least at the next level up of description and implementation).

What data are available for COTS? In general they are very limited, as shown below:

- Datasheet: block diagram, descriptions, configurations
- User manual, installation and application manuals
- Errata sheets for both datasheets and user manuals

For the representativeness of a COTS AEH datasheet as a model, does the datasheet really and completely reflect the actual device content, interfaces, and behaviors? Researchers could rely only on the COTS supplier itself and its visibility and prominence on the market, and its long-term recognition. Alternatively, a huge effort would be necessary to characterize the COTS AEH device versus its datasheet. However, current industry practices include initial relationships with COTS AEH providers and continuing suppliers overseeing and surveillance as part of their quality system procedures and processes. During such exchanges, more accurate models are built.

Attributes: Attributes for COTS AEH and their instantiations in terms of rationale and activities have been addressed in appendix A, with a modulation versus Development/Design Assurance Level (DAL) for at least the four first attributes.

Properties: To simplify the exercise, a broader property can be established based on all six attributes that would look like a totality property and which could be expressed as follows:

Totality property: “Technically suitable characteristics and performance are implemented in a complex physical system (CPS) to perform its known defined intended function, and is featuring proper and safe functioning under its operating and environmental conditions, and will continue to operate correctly for its determined lifetime, while exhibiting fit-for-purpose behavior.”

B.2. APPLICATION TO CIRCUIT BOARD ASSEMBLIES

The following examines how the DAS proposed in this report can be applied to AEH types, such as circuit board assemblies (CBAs). CBAs are generally developmental items (i.e., for which all necessary development data are available).

As such, DO-254/ED-80 can be applied at any level of AEH (i.e., line replaceable units [LRUs] or CBAs), but it does not specifically expand on the necessary activities or life-cycle data expected in support of development assurance of LRUs or CBAs, except if they were considered as simple.

CBA AEH is then also a good candidate to quickly test a properties-based assurance approach without the need to refer to the whole set of objectives, activities, and life-cycle data expected by DO-254/ED-80 for the development of hardware items within a fully structured process.

When a CBA is assessed as simple electronic hardware (SEH), a reduced set of data (i.e., the minimum required by DO-254/ED-80) is deemed sufficient to support SEH assurance.

Models: A CBA is developed; therefore, its design is known in the form of design representations (block diagrams, electrical schematics) to the necessary level of detail. Descriptions of miscellaneous behaviors of the CBA are also available through text or additional diagrams.

Attributes: Table B-1 provides instantiations, possibly into various modes, of the so-called attributes as they could be understood, achievable, or available for a CBA AEH item.

Table B-1. Example for Instantiations of attributes for CBA

	Attributes	Application to a CBA	Rationale
A1	Has a known defined intended function, which it performs	Capture of functional requirements specification and architecture design description.	The intended function is first established via technical requirements specification, then via the design description, and ultimately implemented and verified.
A2	exhibits fit-for-purpose behavior and matching with Interfaces	Validation of functional requirements, safety requirements and definition of Interfaces.	A fit-for-purpose behavior is assessed at the boundary of the CBA with overall environment, i.e., allocated requirements (safety, functional, and interfaces.
A3	Features proper, correct & safe Functioning when implemented	Dysfunctional and behavioral analyses, e.g., functional failure modes effects / failure path analysis (FMEA or FFPA).	Proper, correct and safe functioning is ensued first via architecture design, then via both functional (e.g. deterministic behavior) and dysfunctional analyses.
A4	Implement suitable Technical Characteristics and Performance	Design description & schematic drawings, constraints, characteristics and performance.	It is the responsibility of the designer to implement suitable characteristics and performance. However those must be appropriate to the intended function.
A5	Able to operate within Operating & Environmental conditions	Functional and behavioral verification, including robustness analyses and testing and environmental qualification testing.	Operating conditions as interfaces are addressed under A2. Verification of all aspects (functional, environmental and robustness) is done by analysis or test.
A6	Continue to operate Airworthy for its entire Life time	Reliability, availability, maintainability and safety (RAMS) and other “ities” follow-up.	All those aspects (ities) for continued airworthiness are closely related to the CBA design itself, with many other aspects.

Properties: Similar to the same approach for COTS AEH, a broad property based on all six attributes in table B-1 that look like a truly total property, can be expressed as follows:

Totality property: “Technically suitable CPS characteristics and performance as implemented to perform its known defined intended function, is featuring proper and safe functioning under its operating and environmental conditions, and will continue to operate correctly for its determined lifetime, while exhibiting fit-for-purpose behaviors and matching interfaces.”

Modulation versus DALs: Similar to the modulation of activities versus DALs for a COTS AEH, the instantiations of the six attributes as derived above can be modulated versus the allocated DAL, see table B-2, "Proposed Modulation of Attributes versus DAL for a CBA".

Table B-2. Proposed Modulation of Attributes versus DAL for a CBA

CBA	DAL A	DAL B	DAL C	DAL D
A1 Defined Intended Function And A2 Fit-for-Purpose Behavior	Capture of functional requirements specification and architecture design description. Validation of functional requirements, safety requirements and definition of interfaces.	Capture of Functional Requirements Specification and Architecture Design Description.	Capture of functional requirements	System-level assurance only
A3 Proper, and Safe Functioning And A4 Suitable Technical Implementation	Dysfunctional and behavioral analyses, e.g., functional failure modes effects/failure path analysis (FMEA or FFPA). Design description & schematic drawings, constraints, characteristics and performance.	Dysfunctional and Behavioral Analyses. E.g. Functional Failure Modes Effects / Failure Path Analysis (FMEA or FFPA).	1 activity: failure modes & effects analysis (FMEA)	System-level assurance only
A5 Operating & Environmental Conditions And A6 Continued Airworthy Operation	Functional and behavioral verification, including robustness analyses and testing and environmental qualification testing. Reliability, availability, maintainability and safety (RAMS) and other "ities" follow-up.	2 activities: Functional and behavioral verification, including robustness analyses and testing and environmental qualification testing.	1 activity: environmental qualification testing	System-level assurance only

The totality property then becomes (for a CBA to DAL A): "A CBA when implemented to perform its specified requirements while matching with its interfaces will be analyzed for potential safety impacts and will be qualified to operate properly within its environment, and ultimately feature expected in-service reliability."