A Structured Assurance Case for Commercial Off-The-Shelf (COTS) Airborne Electronic Hardware (AEH)

Guy André Berthon (RESSAC Group @ IRT Saint Exupéry). *[guy-a.berthon@fr.thalesgroup.com]*

Introduction

A properties-ready assurance approach for COTS Airborne Electronic Hardware (AEH) was already proposed and discussed in a FAA Software and Digital Systems (SDS) research on system-level assurance for AEH. This approach was coined as the Model-Attributes-Properties (MAP) approach in research paper [TC-AEH] DOT/FAA/TC-xx/xx "Final Report for System-Level Assurance of Airborne Electronic Hardware (AEH)". May 2017.

The purpose of the FAA SDS task 006 research was to provide recommendations of how COTS AEH devices in particular could be assured at system-level, i.e. going beyond DO-254, possibly using or not ARP4754A guidance. This research concluded that neither DO-254 nor ARP4754A were deemed fully adequate to completely and correctly support COTS AEH assurance, hence recommended a more system-wide or systemic approach rather than a mere system-level process. Refer to this FAA SDS research report for more details.

The intent of the present paper is to show how an Assurance Case could be derived for COTS AEH on the basis of previous results obtained by the research referred to above. To this end we intend to use the principles and notation proposed by John Rushby in report SRI-CSL-15-01 (July 2015), Interpretation and Evaluation of Assurance Cases. In this report a Claims, Arguments, and Evidence (CAE) notation in a text form was used which is deemed sufficiently simple and easy to use for building a small assurance case for COTS AEH. The underlying principles for this Assurance Case for COTS AEH are sufficiently general and could be extended to any other item, e.g. complex AEH, software, item, unit, system, etc. providing that the case is made with appropriate argumentation, i.e. a set of claims, reasoning and evidences.

Abstract extract from the above mentioned SRI report:

"Assurance cases are a method for providing assurance for a system by giving an argument to justify a claim about the system, based on evidence about its design, development, and tested behavior. In comparison with assurance based on guidelines or standards […], the chief novelty in assurance cases is provision of an explicit argument. In principle, this can allow assurance cases to be more finely tuned to the specific circumstances of the system, and more agile than guidelines in adapting to new techniques and applications."

Summary of the FAA SDS research:

A concept of "Attribute":

Any item of equipment can be considered from a multi-viewpoint perspective also referred to as a set of Attributes[1] representing all aspects that should be shown to belong to such item.

The concept of Attribute was then used to delineate the main aspects, outlines or elements, that any physical object, hence any item of equipment, should feature and be perceived as featuring in order to ensure that: It has a known [defined] intended functions, is both fit-for-purpose and is safe-for-use; plus: it adequately behaves under operating and environmental conditions, and will continue to do so over its entire lifetime. When those attributes, once instantiated, are shown to belong to the item, as designed, built and used; this is a main contributor to provide assurance. This paper shows how attributes can be used part of an assurance case.

The set of attributes was structured into a manageable number of 6 that were also related to airworthiness standards and/or certification specifications. They were established as follows:

Origin	CS-25/29 & FAR 25/29 extracts		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 "	A1	Performs a Known [Defined] Intended Function.
2x.1301(a)(4)	"function properly when installed"	A2	Exhibits Fit-for-Purpose Behaviors at its Interfaces (see note).
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"	A3	Features proper and safe Functioning when installed.
FAR/CS 25/29.1301(a)(1)	"Be of kind and design appropriate to […]" "*technical suitability of [to] the intended application*" (source: DO-254 §11.2.1 (6)).	A4	Implements suitable Technical Performance and Characteristics.
CS 25.1309(a)(1) FAR 25.1309(a) CS 29.1309(a)	"[…] under the aircraft operating & environmental conditions." "[…] under any foreseeable operating condition."	A5	Sustains Operating and Environmental conditions.
FAR/CS 25/29.1529	"Instructions for Continued Airworthiness"	A6	Continue to operate [Airworthy] for its determined Life Time.

Note: There is a difference between the known defined intended function (in attribute A1) and the fit-for-purpose behavior (in attribute A2). A2 includes nominal functional aspects already expressed by A1, but also operational aspects that can be desired, expected or derived behaviors; and possibly other aspects such as additional behaviors revealed by alternate use, misuse or abuse.

[1] "By attribute, I mean that which the intellect perceives as constituting the essence of substance." Ethics, part I, definitions. Benedictus [Bento] de Spinoza (1632-1677).

A Properties approach:

Once Attributes were defined, Properties were established in the form of relationships stated between Attributes, this based on overall principles that generally govern the mere existence, purpose and persistence of objects. All Properties e.g.: Validity, Conformity, Suitability, Safety, etc. should be ultimately assessed as true. In a first attempt, only the first 4 Attributes (A1 to A4) were used for application to COTS AEH because A5, "able to operate under Operating and Environmental conditions" and A6, "Continue to operate [Airworthy] for its determined Life Time", are generally associated with a full unit of equipment. Hence, only 6 Properties were generated and expressed as combinations of Attributes in pairs as follows:

Pairs	Properties
A1 & A2 (VALIDITY)	**The Defined Intended Function is adequate with the expected purpose, desired behavior and interface needs.** (kind of VALIDITY Property comparable to INTENT OP)
A1 & A3 (SAFETY-Int.)	**The Defined Intended Function is established to achieve proper and safe functioning once installed.** (kind of SAFETY–Intrinsic Property).
A1 & A4 (CONFORMITY)	**The Defined Intended Function is correctly designed into a technically suitable implementation.** (kind of CONFORMITY Property ~ CORRECTNESS+ACCEPTABILITY)
A2 & A3 (SAFETY-Ext.)	**The expected purpose, behavior and interface requirements must be satisfied properly and safely.** (kind of SAFETY-Extrinsic Property).
A2 & A4 (SUITABILITY-P)	**A suitable technical implementation is consistent with the expected purpose, behavior & interface requirements.** (kind of SUITABILITY–for Purpose Property).
A3 & A4 (SUITABILITY-S)	**A suitable technical implementation ensures proper and safe functioning once installed and operated.** (kind of SUITABILITY-for-Safety Property).

Note: When using all 6 Attributes, 15 Properties (2 among 6) could be expressed quite easily. Going forward to combining Attributes in triplets will lead to 20 Properties (3 among 6) but statements for 20 Properties are difficult to express and may not bring additional value for the targeted assurance case.

Once instantiated, Properties can be assessed and verified true for assuring any item. They can be structured into a hierarchy of sub-statements, possibly along with multiple axes (e.g., product-, activity- or tool-oriented), down to more specific product data, activities results and tools data, all supporting trustable evidence in achieving the sought compliance. This makes those properties good candidates as Claims or Sub-Claims in a structured assurance case.

Building an assurance case for COTS AEH:

An Assurance case notation: Based on SRI J. Rushby's paper, the idea is to "make the case" to justify an item, system or product by stating the main Claim that it must satisfy. Then the construction of the case is made of a hierarchy of argument steps, each of which justifies a Claim or Sub-claim, possibly on the basis of further Sub-claims, and ultimately on the basis of Evidence(s). As J. Rushby noticed, any such argumentation is more inductive than deductive, i.e. Evidence strongly suggests but does not formally imply the top-level Claim.

C: Main Claim
AS: Argumentation Step (Sub-claims strongly suggest truth of main Claim)
SC: Sub-claims
RS: Reasoning steps (Sub-claims are supported by further Sub-claims)
SC: [Sub-]Sub-Claims
ES: Evidence Steps (Sub-claims are supported by a set of evidence(s))
E: Evidences

Application to COTS AEH:

CLAIM: COTS AEH is assured to meet airworthiness requirements in certification specifications.
Strategy: Use a six-Property approach.
AS: All six Properties: Validity, Safety-I, Conformity, Safety-E, Suitability-for-Purpose and Suitability-for-Safety are satisfied. Means: One Sub Claim for each Property.
SC#1: The Defined Intended Function is adequate with the expected purpose, desired behavior & interface needs. Strategy: Consistent pairs of Attributes.
SC#2: The Defined Intended Function is established to achieve proper and safe functioning once installed. Means: Strategy: Consistent pairs of Attributes.
SC#3: The Defined Intended Function is correctly designed into a technically suitable implementation. Means: Strategy: Consistent pairs of Attributes.
SC#4: The expected purpose, behavior and interface requirements must be satisfied properly and safely. Means: Strategy: Consistent pairs of Attributes..
SC#5: A suitable technical implementation is consistent with the expected purpose, behavior & interface requirements. Strategy: Consistent pairs of Attributes.
SC#6: A suitable technical implementation ensures proper and safe functioning once installed and operated. Strategy: Consistent pairs of Attributes.
END AS
END CLAIM

Then each Sub-Claim can be further expanded down into Sub-Sub-Claims via a Reasoning Step down to Evidences Steps, then actual Evidences. Note that the following described assurance case is a generic one for COTS AEH types of items. Instantiations should be provided for a specific COTS AEH, on the basis of actual evidences. SC#1 is then shown expanded below:

SC#1: VALIDITY. The Defined Intended Function is adequate with the expected purpose, desired behavior and interface needs. Strategy: Show consistent pairs of the following two Attributes.
RS#1: The two Attributes: “Defined Intended Function” and “Expected purpose and Behavior” are assessed to be consistent with each other. Means: An additional SC#1.3 is stated.
SC#1.1: Performs a Known Defined Intended Function. Strategy: Instantiate a documented Defined Intended Function
ES#1.1: The COTS AEH is selected to perform all or part of an intended function allocated from the next level up of H/W design
E#1.1.1: Assessment of COTS characteristics and determination of Simplicity vs Complexity,
E#1.1.2: Electronic Component Management and Report (Available COTS device datasheet & design data if available),
E#1.1.3: Determination of the COTS Usage Domain limitations. Used/Unused functions.
END ES#1.1
END SC#1.1
SC#1.2: Exhibits Fit-for-Purpose Behaviors and Interfaces. Strategy: Instantiate a documented Fit-for-Purpose Behaviors and Interfaces
ES#1.2: The COTS AEH must fit properly at boundaries in terms of Interfaces, allocated functions and for handling of failures.
E#1.2.1: Definition of H/W–H/W and H/W–S/W Interfaces requirements and interface descriptions,
E#1.2.2: Identification of System Requirements allocated to the functions in which the COTS AEH is involved
E#1.2.3: Identification of safety requirements allocated to the COTS and safety features,
END ES#1.2
END SC#1.2
SC#1.3: Consistency is ensured. Strategy: Matching Validation Review
ES#1.3 & E#1.3: Matching Validation Technical review report
END ES#1.3
END SC#1.3
END RS#1
END SC#1

The other SCs: SC#2, SC#3, SC#4, SC#5 and SC#6 could be expanded in a similar manner. But, the whole Assurance Case might look a bit complicated due mainly to the fact that there will be some repetitions as Evidences associated with each and every Attribute will appear at least three time, e.g.: A1 is involved in SC#1, SC#2 & SC#3; A2 is involved in SC#1, SC#4 & SC#5; A3 is involved in SC#2, SC#4 & SC#6; and A4 is involved in SC#3, SC#5 & SC#6.

Anyway, the number of evidences supporting claims can be limited to 12 related to Attributes plus 6 related to Properties (one per property). A summarized list of evidences is suggested in the table below. In addition, depending on the allocated DAL, the number of evidences could be adapted, leading to a fully graduated assurance case commensurate with the DAL.

Evidence data supporting attributes as sub-sub-claims are listed below, incl. w.r.t. DAL:

[SUB]SUB-CLAIMS	EVIDENCES FOR DAL A COTS AEH ASSURANCE CASE	EVIDENCES FOR DAL B COTS AEH	EVIDENCES FOR DAL C COTS AEH	EVIDENCES FOR DAL D COTS
A1 Performs a Known Defined Intended Function.	**3 Evidences:** **- Assessment of COTS AEH characteristics & determination of Simplicity/Complexity,** **- Electronic Component Management report (Available COTS device & design data),** **- Determination of the COTS Usage Domain limitations.**	**2 Evidences:** **- Assessment of COTS characteristics & determination of Simplicity /Complexity,** **- Electronic Component Management (Available COTS device data),**	**1 Evidence:** **Determination of COTS Simplicity/Complexity, e.g. per DO-254 §1.6 and all COTS addressed under, e.g. DO-254 11.2.1 (1) to (5).**	**In-house process (i.e. not necessarily per DO-254)**
A2 Exhibits Fit-for-Purpose Behaviors and Interfaces.	**3 Evidences:** **- Definition of H/W–H/W and H/W–S/W Interfaces,** **- Identification of system requirements allocated to the COTS,** **- Identification of safety requirements allocated to the COTS.**	**2 Evidences:** **- Identification of system requirements allocated to the COTS,** **- Definition of H/W–H/W and H/W–S/W Interfaces.**	**1 Evidence::** **Assurance at the upper level of AEH design for allocation of system 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 Features proper and safe Functioning when installed.	**3 Evidences:** **- Identification of Functional failures paths in which the COTS AEH is involved as configured,** **- Capture and assessment of relevant errata and their impact on safety,** **- Identification of critical failures situations: wrong settings, un-mitigated errata, etc.**	**2 Evidences:** **- Identification of Functional failures paths in which the COTS AEH is involved,** **- Capture & assessment of relevant errata and their impact on safety.**	**1 Evidence:.** **Considerations on overall performance and reliability for all COTS, e.g. per DO-254 11.2.1(7)**	**In-house process (i.e. not necessarily per DO-254)**
A4 Implements suitable Technical Characteristics & Performance.	**3 Evidences:** **- Verification results from COTS Usage Domain versus functional requirements,** **- Verification results from technical suitability in general, incl. configuration management,** **- Verification results from H/W-H/W and H/W-S/W Interfaces.**	**2 Evidences:** **- Verification results from technical suitability in general, incl. configuration management,** **- Verification results from H/W-H/W and H/W-S/W Interfaces.**	**1 Evidence:** **Considerations on overall technical suitability for all COTS, e.g. per ED-80/DO-254 11.2.1 (6).**	**In-house process (i.e. not necessarily per DO-254)**

Evidence reports supporting Properties seen as Sub-Claims are expressed as follows:

SUB-CLAIMS	GENERIC PROPERTIES	EVIDENCES FOR A COTS AEH ASSURANCE CASE	A	B	C	D
SC#1: Property (A1 & A2) (VALIDITY)	**The Defined Intended Function is adequate with the expected purpose, desired behavior and interface needs.**	**Matching validation report from analysis between system requirements allocated to the hardware functions in which the COTS AEH is involved, and the COTS AEH selected capacities from datasheet).**	**X**	**X**		
SC#2: Property (A1 & A3) (SAFETY-Intrinsic)	**The Defined Intended Function is established to achieve proper and safe functioning once installed.**	**Functional Failures Modes & Effects Analysis FFMEA report. Top-down FFMEA conducted w.r.t. the allocated safety objectives at the functional boundaries of COTS AEH and AEH in which the COTS is incorporated.**	**X**	**X**		
SC#1: Property (A1 & A4) (CONFORMITY)	**The Defined Intended Function is correctly designed into a technically suitable implementation.**	**Verification report as a result of reviews, analyses and tests showing conformity of the actually implemented COTS AEH (configured, activated & installed) to the COTS AEH selected capacities from datasheet).**	**X**	**X**	**X**	
SC#1: Property (A2 & A3) (SAFETY-Extrinsic)	**The expected purpose, behavior and interface requirements must be achieved properly and safely.**	**Functional Failure Path Analysis (FFPA) report. End-to-end FFPA identifying Functional Failure Paths (FFP) in which the COTS AEH is involved and showing proper fit and consistency with the encompassing AEH.**	**X**	**X**	**X**	
SC#1: Property (A2 & A4) (SUITABILITY-for Purpose)	**A suitable technical implementation is consistent with the expected purpose, behavior and interface.**	**Hardware Design Validation report as a result of assessment of the actually implemented COTS AEH (configured, activated & installed), versus the encompassing AEH incorporating the COTS AEH.**	**X**			
SC#1: Property (A3 & A4) (SUITABILITY-for Safety)	**A suitable technical implementation ensures proper and safe functioning once installed and operated.**	**Failure Modes and Effects Analysis (FMEA) as a result of a piece-parts FMEA conducted using detailed failure modes, failure rates (when available), and errata items from the COTS AEH supplier.**	**X**			

Note: For a DAL D no evidence is required to formally support any of the six properties. The only expected evidences are those supporting attributes themselves (refer to the previous table). Using the two tables means that the assurance case is simplified depending on the assigned DAL.

References:

[TC-AEH] Guy Berthon, Laurence Mutuel, Cyril Marchand “Final Report for System-Level Assurance of Airborne Electronic Hardware (AEH)”. DOT/FAA/TC-xx/xx. May 2017. https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/media/TC-AEH.pdf

[] John Rushby. The Interpretation and Evaluation of Assurance Cases. Technical Report SRI-CSL-15-01. July 2015. http://www.csl.sri.com/users/rushby/abstracts/assurance-cases15