Certification Authorities Software Team (CAST)

Position Paper
CAST-33

Compliance to RTCA DO-254/ EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware", for COTS Intellectual Property Used in Programmable Logic Devices and Application Specific Integrated Circuits

COMPLETED August 2014 (Rev 0)

NOTE: **This position paper has been coordinated among representatives from certification authorities in North and South America, Europe, and Asia. However, it does not constitute official policy or guidance from any of the authorities. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

Table of Contents

NOTE: **This position paper has been coordinated among representatives from certification authorities in North and South America, Europe, and Asia. However, <u>it does not constitute official policy or guidance from any of the authorities</u>. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

Compliance to RTCA DO-254/ EUROCAE ED-80, *"Design Assurance Guidance for Airborne Electronic Hardware",* for COTS Intellectual Properties Used in Programmable Logic Devices.

1 Purpose

The purpose of this paper is to explore how material in RTCA DO-254/ EUROCAE ED-80 (hereafter referred to as DO-254/ED-80), can be adapted to be used as an acceptable means of compliance for Programmable Logic Devices (PLDs) and Application Specific Integrated Circuits (ASICs) implementing a third party Commercial Off-The-Shelf (COTS) Intellectual Properties (IP). The primary material in RTCA DO-254/ EUROCAE ED-80 that is proposed for adaptation to COTS IP is contained in Section 11.1.4, "Upgrading a Design Baseline" and 11.2, "Commercial Off-The-Shelf (COTS) Components Usage."

> ***Note**: The terms "IP" and "IP core" are used interchangeably throughout the white paper without distinction.*

2 Background

DO-254/ED-80 is a design assurance document that provides acceptable means for approval of airborne electronic hardware such as ASICs and PLD[1] by international certification authorities. For the purpose of this paper, these devices are hereafter referred to as Airborne Electronic Hardware (AEH).

The premise behind DO-254/ED-80 is that of a design assurance process. The notion of design assurance should be understood throughout this document in a wider scope as development assurance, in accordance to more recent avionics guidance material (system and software domains). If the developer of an application specific AEH device follows the guidance provided by DO-254/ED-80, then the potential for hardware design errors has been reduced in a consistent and verifiable manner during both the design and certification processes. The likelihood that design errors exist in the end item PLD or ASIC increases as the design assurance level decreases.

---

[1] *PLDs include, but are not limited to, Field Programmable Gate Arrays (FPGA), Erasable Programmable Logic Devices (EPLD), Generic Array Logic (GAL), Programmable Array Logic (PAL) and Programmable Logic Array (PLA) devices.*

For airborne applications in civil aviation, the digital logic implemented in AEH devices has been historically developed by the OEM and/or their suppliers for the specific purpose of the airborne application. With such arrangement, the AEH processes and data are owned by the OEM and suppliers, and are therefore available to support the compliance demonstration. When third party COTS IPs are used, however, the required data and process artifacts may not exist or may not be fully available.

> ***Note**: The design assurance process defined in DO-254/ED-80 does not address the possibility of errors in the requirements from which the device was designed.*

DO-254/ED-80 does not directly address a design assurance method for AEH devices utilizing third party COTS IPs. Section 11.2 addresses general COTS component usage, and Section 11.3 addresses using product service experience to substantiate design assurance for COTS components. Neither section, however, directly discusses the use of COTS IP cores in AEH devices. Additionally, no industry standard for using COTS IP has been recognized by the international certification authorities as an acceptable means of showing compliance to the applicable airworthiness regulations. However, the use of COTS IP in AEH devices which perform non-trivial functions is becoming widespread. Therefore, it is imperative that the certification authorities explore possible methods of compliance for use of COTS IP in AEH devices.

This CAST paper proposes using existing DO-254/ED-80 objectives that can be adapted to COTS IP cores intended for use in these devices. The goal of this CAST paper is to provide a certification authority position on use of COTS IP in airborne systems and equipment.

3 Certification Authorities Software Team (CAST) Position

3.1 Definition of COTS IP Cores

For the purpose of this CAST paper, COTS IP cores will be classified in one of the following three categories:

- Soft IP core.
- Firm IP core.
- Hard IP core.

Sections §3.1.1, §3.1.2, §3.1.3 of this paper provide the definition and additional information about these three categories of COTS IP. Figure 1 shows a 'simplified' design flow of a PLD, FPGA, or ASIC, and where Soft IP, Firm IP, and Hard IP are located in the design cycle.

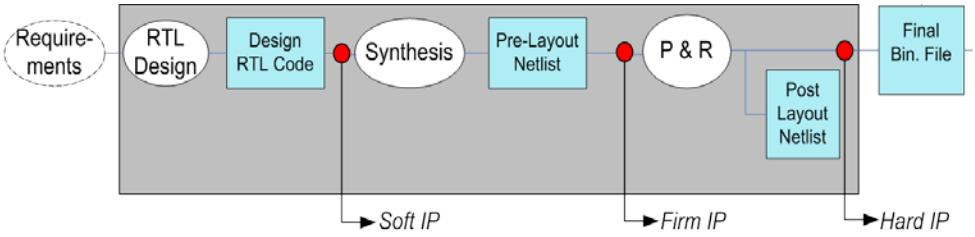


Figure 1 – Position of COTS IP within a 'simplified' design representation flow

The key stakeholders are identified as the IP Provider and the IP User.

3.1.1 Definition of Soft IP Cores

Soft IP cores are the category of IP core that comes to the user with the most life-cycle data. This data generally include register transfer level (RTL) descriptions in languages such as Verilog or VHDL. This allows a detailed analysis and optimization (and eventually customization) of the soft IP cores for the intended application. Soft IP cores still need to be synthesized, placed and routed (P & R) in the target AEH device.

3.1.2 Definition of Firm IP Cores

Firm IP cores are next in the decreasing level of design description, specified in technology-independent netlist level format. This allows the IP provider to hide the critical IP details and yet allow the IP user to perform some limited amount of analysis and optimization during placement, routing, and technology-dependent mapping of the IP block. Firm IP cores still need to be placed and routed in the AEH device.

Firm IP cores are generally considered to be technology dependent even though the netlist level format could be generic.

3.1.3 Definition of Hard IP Cores

Hard IP cores have the least design description and life-cycle data, specified in technology-dependent physical layout format using industry standard languages such as stream, polygon, or GDSII format. Hard IP cores can be thought of as a "black box" that, due to the lack of knowledge about the internal detailed design, they cannot be fully analyzed and/or co-optimized. Hard IP cores come with a detailed specification of integration requirements in terms of clock, testing, power consumption, interfaces and a host of other parameters. Hard IP cores are embedded in the PLD/ASIC at the silicon level.

3.1.4 Definition of IP Provider

The IP Provider develops and sells IP Cores that are not necessarily intended for civil aviation airborne applications.

3.1.5 Definition of IP User

The IP User acquires the right to use the IP and integrates the IP core with some application specific logic, in the AEH device. Typically, the IP User is the one who takes a direct role in supporting the AEH compliance demonstration with airworthiness requirements.

3.2 Using DO-254/ED-80 Objectives for AEH Devices Implementing COTS IP Cores

This CAST paper proposes how the objectives of DO-254/ED-80 can be adapted to IP cores, so that they can be used in airborne equipment (including safety critical applications) that must comply with applicable airworthiness regulations. The IP User may need additional data and/or generate data through additional activities in order to satisfy the objectives of DO-254/ED-80.

3.2.1 DO-254/ED-80 Applicability to COTS IP Cores

DO-254/ED-80, Section 11.2, addresses the subject of COTS components usage. Although widespread use of complex COTS IP cores in programmable AEH devices was not envisioned during the initial drafting and publication of DO-254/ED-80, it is also true that COTS IP cores are a subset of COTS components in general and raise the same concerns regarding showing compliance when used in civil aviation products. Therefore,

this paper explores how considerations in Section 11.2 of DO-254/ED-80 may be applied to AEH devices that have been designed using COTS IP cores.

The information in DO-254/ED-80, section 11.1, "Use of Previously Developed Hardware," is also relevant to the subject of COTS IP cores. COTS IP cores may be treated as previously developed components. Given this as a starting point, existing life cycle data regarding the IP may be used as a method of showing compliance to the applicable DO-254/ED-80 objectives. Alternatively, the appropriate life cycle data may need to be generated to satisfy these objectives.

3.2.2 Design Assurance Level Considerations

There are five AEH Design Assurance Levels (DAL), Level A through Level E, respectively corresponding to the five classes of failure conditions: catastrophic, hazardous/severe-major, major, minor, and no effect. Please refer to DO-254/ED-80, Table 2-1, for additional information.

The expected life cycle data for the IP should be modulated according to the DAL of the design in which the IP core is implemented. In particular, the guidance material contained in Appendices A and B of DO-254/ED-80 should be considered when a COTS IP Core is integrated into an AEH device.

3.3 Soft IPs

3.3.1 Soft IP Assessment and Strategy

This section focuses on COTS Soft IP assessment and strategy to gain design assurance at the IP level, the integration of the COTS IP into the target device is addressed in paragraph 3.7 of this paper.

3.3.1.1 IP Assessment Process

Applying the guidance in DO-254/ED-80, Section 11.1 "Use of Previously Developed Hardware" and specifically §11.1.4, "Upgrading a Design Baseline" to COTS IP cores results in different approaches that can be proposed:

1. The IP core is developed and verified according to a structured approach that satisfies the DO-254/ED-80 objectives.

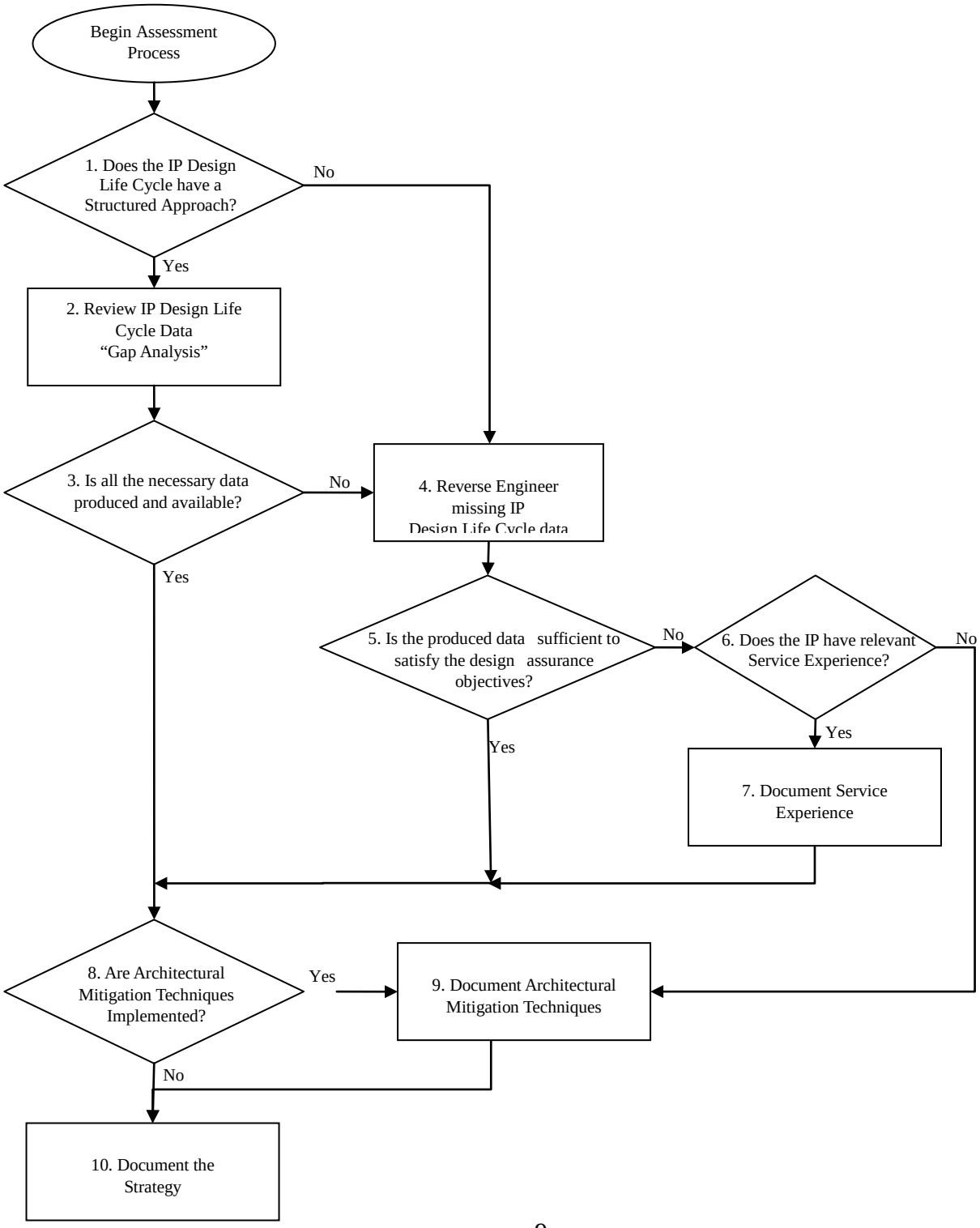
2. ‘Reverse engineering’ is applied to the IP core to provide the required data, using the “upgrading a design baseline” approach and considerations defined in DO-254/ED-80.
3. The IP core has relevant Service Experience as discussed in DO-254/ED-80 Section 11.1.3, which can be used to complement the design assurance.

These methods are not mutually exclusive. Combinations of these methods should also be considered, especially if one method by itself is lacking full satisfaction of the objectives of DO-254/ED-80.

In addition to these approaches at IP core level, architectural mitigation techniques at an upper level of the design architecture could be used. In each case it is up to the IP User to present and justify the proposed strategy to the certification authority. Architectural mitigation techniques are not included in the above list of approaches because those methods are only used at the device-level for design assurance. Architectural mitigation techniques, on the other hand, may be used at the system or function level to account for what could be eventually seen as a complementary means to cover specific “holes” in the design assurance process at the device level. The architecture mitigation is only a complementary approach and isn’t to be used as the only means, therefore, this option is set apart from the three approaches described in the numbered list above.

A flowchart describing the assessment process for soft IP is presented in Figure 2. A description of each step in the process is given after the figure.

Figure 2: Soft IP Assessment Process Flowchart



NOTE: **This position paper has been coordinated among representatives from certification authorities in North and South America, Europe, and Asia. However, <u>it does not constitute official policy or guidance from any of the authorities</u>. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

Step 1: Does the IP Design Life Cycle have a structured approach?

If the IP core has been designed according to a structured approach, based on requirements capture and the data is available to demonstrate this, then the IP design life cycle and produced data should be reviewed (step 2) in order to decide if the structured approach and associated data can demonstrate satisfaction of DO-254/ED-80 objectives.

See Section 3.3.2 of this paper for more information.

Step 2: Review IP Design Life Cycle Data "Gap Analysis"

The IP development life cycle process and associated data should be reviewed. Here "data" is considered to be any artifact that can be submitted to the certification authorities, also including internal (proprietary) data that could be made available for a review. No certification credit should be expected from data unless it can either be submitted to the certification authorities or made available during reviews.

During this review, the IP user should perform an assessment on the available life cycle data for their satisfaction of DO-254/ED-80 objectives, the result should be documented in the PHAC.

The DAL of the device should be considered by the IP User for this assessment. That is, a DAL for the hardware device that will utilize the COTS IP should be assigned, and the Design Life Cycle data for the IP should match that as defined by DO-254/ED-80 for an AEH device that is designed without the use of an IP core.

Step 3: Is all the necessary data produced and available?

After completion of the life cycle review the applicant should evaluate if all the data necessary for DO-254/ED-80 objective's satisfaction is available.

Step 4: Reverse engineer missing IP Design Life Cycle data

If an assessment of a structured approach is not possible or sufficient data is not available, then reverse engineering activities should be performed to satisfy the DO-254/ED-80 objectives according to the assigned DAL. (See Section 3.3.3 of this paper).

The DAL should be considered by the IP User for this assessment.

Step 5: Is all the necessary data complete?

To answer this question, the IP User should perform an assessment on IP provider produced data with reverse-engineered life cycle data. The IP User should ensure their satisfaction of DO-254/ED-80 objectives and document the results in the Certification Data Package. When the regenerated data cannot fully satisfy the DO-254/ED-80

objectives or when the IP User is able to augment its design assurance, the IP User may choose the approach of Service Experience which may complement the achieved design assurance.

The results of this assessment and the approach chosen by the IP User should be documented in the certification data package.

The DAL of the device should be considered by the IP User for this assessment.

Step 6: Does the Soft IP have relevant Service Experience?

The concept of service experience is discussed in DO-254/ED-80 Section 11.1.3. If the IP has relevant service experience, then it may be possible that it can be used in order to receive some complementary certification credit and to compensate for any shortcomings that occurred during the reverse engineering of the required data.

> ***Note****: If only limited service experience is available, it should still be documented to complement the main approach selected.*
>
> ***Note****: Consider Previously Developed Hardware (PDH) principles to assess the usage in the application and design environment, as described in DO-254/ED-80 Section 11.1. Most COTS IPs are not simple functions and, therefore, it is likely that service history of the IP will not cover all executable paths in the IP.*
>
> ***Note****: As the Soft IP by definition does not contain any layout data, each instantiation of the IP may lead to a completely different layout. Service experience may therefore have some limits in the certification credit that can be attributed to it.*

Step 7: Document Service Experience

If the service experience approach is being taken, then the evidence required by this approach should be collated and documented – see Section 3.3.3.3 of this document.

Step 8: Are Architectural Mitigation techniques implemented?

Review whether architectural mitigation techniques are necessary to mitigate any deficit in the level of assurance and review their implementation.

> ***Note****: It is recommended that the IP User always considers using architectural mitigation techniques to complement other approaches. If architectural mitigation techniques are used to mitigate design errors, this should be claimed and presented for certification credit. For level A and B functions, section 3.1. of Appendix B of DO-254/ED-80 should be used.*

Step 9: Document Architectural Mitigation techniques

If architectural mitigation techniques are going to be used, the method and rationale should be documented in the certification data package.

Step 10: Document the strategy

The strategy and the conclusions of the IP assessment should be documented in the certification data package.

Table 1 and Table 2 list all data that should be considered for a soft IP.

3.3.2 Strategy Based on Soft IP Design Life Cycle Processes

3.3.2.1 Purpose

With this strategy, the IP core is developed from the outset using a structured and well-defined design life cycle process, complying with the hardware design life cycle and supporting processes described in DO-254/ED-80. The IP User is then able to directly reference the relevant life cycle data – supplied as part of the IP core package – that is used to satisfy DO-254 objectives.

To satisfy the objectives of DO-254/ED-80, the IP Provider should have all appropriate processes and procedures in place, including configuration management (see section 7.0 of DO-254/ED-80) and process assurance (see section 8.0 of DO-254/ED-80).

The IP Provider's processes and procedures should be made available to the IP User and the certification authority, such that satisfaction of the objectives of DO-254/ED-80 can be assessed.

The assessment will be performed through data-oriented and objectives-oriented approaches. The IP Provider's development process may be considered as acceptable provided that it satisfies the objectives defined in Table 1, and produces the data described in Table 2.

3.3.2.2 Soft IP Design Life Cycle

Prior to the design of a new IP core, the design life cycle and supporting processes should be defined, with particular emphasis placed on the transition criteria between the main processes.

3.3.2.2.1 Soft IP Life Cycle Design Processes

The IP supplier's design life cycle processes should address the following:

1) The requirements capture process should identify and record the IP requirements. This includes those requirements imposed by the IP architecture, IP controllability and configuration, environmental, safety and performance requirements.
2) The conceptual design process goal is to produce a high-level design description that can be assessed to determine the potential to meet the requirements. This may be accomplished using such items as functional block diagrams, and/or design and architecture descriptions.
3) The detailed design process objective is to produce the low-level design data using the requirements identified and data produced during the upstream processes. This is typically the HDL code (for soft IP) and the constraint file containing at least the necessary constraints (including timing) to fulfil the requirements. If the IP is being developed to DAL A or B, then the detailed design data should be traced to the requirements.

***Note**: The implementation process should use the detailed design data to produce the hardware item that fulfils the requirements. The implementation process is out of scope of the IP design life cycle since, by definition, the IP still needs to be placed and routed in the PLD/ASIC by the IP User.*

3.3.2.2.2 Supporting Processes

The IP Provider's design supporting processes should address the following:

1) The validation process is intended to ensure that the requirements are correct and complete. These objectives may be satisfied through a combination of activities such as reviews, simulation, prototyping, modelling, analysis, service experience, engineering assessment, or the development and execution of tests.
2) The verification process provides evidence that the hardware implementation meets the requirements. These objectives may be satisfied through a combination of methods such as reviews, simulation, analyses, and the development and execution of tests. In addition, when implementing DAL A and DAL B functions, one or more of the methods described in DO-254/ED-80, Appendix B, should be selected. Alternatively, another method could be proposed as far as it would provide an equivalent level of design assurance. Among the methods described by the appendix

B, elemental analysis is the most common for the design of IP cores. A typical approach taken for this analysis is to use HDL code coverage data to demonstrate that the verification test cases have achieved full coverage of the code, with any shortfalls justified.

3) The configuration management process is intended to provide the ability to consistently replicate the configuration item, regenerate the information if necessary, and modify the configuration item in a controlled manner if modification is necessary. It covers configuration and design tools identification, baseline establishment, problem reporting, problem tracking, problem corrective action, change control, release, archive, and retrieval.
4) Process assurance ensures that the life cycle process objectives are met and activities have been completed. It covers review reports, audit reports and records of deviation.

Some of the Design Life Cycle processes activities related to the IP are generic and may be performed by the IP Provider, whereas other activities can only be done by the IP User while considering the specific application context. Typically, generic activities include design activities, part of validation activities and verification activities down through RTL simulation. Application specific activities are validation of the IP requirements in the use context, post-layout and physical verification, and all supporting activities needed to integrate the IP in the device.

In both generic and specific context, verification activities should be performed with independence (i.e., independently of the design activities) for IP used in DAL A and B functions. For independence concept and examples of acceptable means see DO-254/ED-80 Appendix C (definition of “independence”) and Appendix A.

3.3.2.2.3 Data To Be Provided

Table 1 and Table 2 provide a reference for the set of data that should be provided or made available to the IP User or certification authorities when requested. Table 1 contains data that are related to the life cycle and Table 2 contains data related to the IP itself (requirements, development, production, and verification data). Numbering within the table is associated to DO-254/ED-80, Table A-1, Hardware Life Cycle Data.

It is acceptable that the IP Provider provides a different combination of documents, assuming that the objectives defined in column 3 are satisfied.

The requested amount of data should be modulated according to the DAL, as described in and DO-254/ED-80, Appendix 1, Table A-1.

IP Users may need to modify the data delivered by the IP Provider, in order to make them relevant for the specific IP use case. Typically, if the IP User selects a target device that is not the same as the one used by the IP Provider to generate data, the User may have to produce the equivalent data for its target. In any case, the final step of the verification process will be done by the IP User once the IP has been integrated in the real hardware.

The IP Provider may supply individual DO-254/ED-80 set of plans (such as the Plan for Hardware Aspects of Certification, the Hardware Development Plan and the Validation and Verification Plan) and standards (such as hardware requirement standards or coding standards), or a single 'IP Design Assurance Plan', as part of the 'certification package'. If a single plan is supplied, it should cover the objectives of the individual plans and standards that are applicable to the IP core.

In that case, the IP package should contain an “IP Design Assurance Plan” describing the structured process that produced the IP delivered data items mentioned in Table 2.

The applicant and its suppliers (IP User and/or Provider) should ensure that the certification authorities have the opportunity to access and/or review the mentioned plans and standards when requested.

Table 1 – Soft IP Plans and Standards

DO-254/ ED-80 DATA SECTION	*IP LIFE CYCLE DATA*	*DESCRIPTION*	*PROVIDED TO (USER OR CERT. AUTHORITY)*
10.1	IP Design Assurance Plan	A document describing the following points: • IP core overview • Safety aspects • Design life cycle description • Design, validation and verification environment and activities • Design team organization • Independence aspects (for DAL A and B) • Configuration Management process description	To be submitted to the certification authority by the IP User
10.2	IP Standards	Design Standards (Guidance for documentation and design rules), Requirements Standards (Guidance for writing and naming requirements), Validation and Verification Standards, and Configuration Management and Hardware Archive Standards: If the IP package does not contain these documents, the IP Provider should still reference them in the IP Design Assurance Plan	Data available upon request (Normally provided to the IP User)

Table 2 - IP Core Design Life Cycle Data Available

DO-254/ ED-80 DATA SECTION	*IP LIFE CYCLE DATA*	*DESCRIPTION*	*PROVIDED TO (USER OR CERT AUTHORITY)*
10.3	IP Design Data	The specifications, documents and drawings that define the IP.	
10.3.1	IP Requirements	The IP design has to be defined using identified requirements. One element of specification becomes one requirement and all the requirements are identified with a unique and formal Identification number. Requirements may concern functional and non- functional aspects, normal and abnormal conditions.	Data available upon request (Normally provided to the IP User)
10.3.2	IP Design Representation Data		
10.3.2.1	Conceptual Design Data	A high-level description of the IP architecture (block diagram, Finite State Machine, HW and SW interfaces, protocols, chronograms…).	Data available upon request (Normally provided to the IP user)

DO-254/ ED-80 DATA SECTION	IP LIFE CYCLE DATA	DESCRIPTION	PROVIDED TO (USER OR CERT AUTHORITY)
10.3.2.2	Detailed Design Data	HDL source code (RTL description) Constraint files (for both synthesis and place and route processes) Note : additional data that can be of interest if the same tools and target are used: Synthesis Script and Reports Static Timing Analysis Script and Reports Place and Route Script and Reports Bit stream implementation data	Data available upon request (Normally provided to the IP User)
10.3.2.2.1	IP Configuration Index Document	List of all HDL and constraint files versions and relevant documentation of IP, including integration test benches Configuration script for HDL options if possible for this IP. Also any Open PRs raised by the IP Provider (=errata) IP programming procedures and tools for IP integration	Data available upon request (Normally provided to the IP User)
10.3.2.2.4	IP user Manual	Description of programmable parameters, interfaces with SW and HW, memory mapping, and register descriptions among others.	Data available upon request (Normally provided to the IP User)
10.4	Validation And Verification Data	*See Appendix C of DO-254/ED-80for Validation and Verification definitions.*	
10.4.1	IP Traceability Data	Establishes a correlation between the requirements, detailed design, implementation (hard IP), and validation and verification data.	Data available upon request (Normally provided to the IP User)
10.4.2	IP Review and Analysis Procedures	Define the process and criteria for conducting reviews and analyses.	Data available upon request (Normally provided to the IP User)
10.4.3	IP Review and Analysis Results	Establishes the review and analysis results, including the code coverage report for the elemental analysis (depending on DAL)	Data available upon request (Normally provided to the IP User)

DO-254/ ED-80 DATA SECTION	IP LIFE CYCLE DATA	DESCRIPTION	PROVIDED TO (USER OR CERT AUTHORITY)
10.4.4	IP Test Procedures	Define the methods, environment and instructions for conducting both functional and environmental (hard IP) qualification testing. Test Benches (Compilation Script) Test Bench Manual (How to launch the simulation) Acceptance Test Criteria	Data available upon request (Normally provided to the IP User)
10.4.5	IP Test Results	Test results including: • Test execution date • Test results and witness • Code coverage results (DAL A and B)	Data available upon request (Normally provided to the IP User)
10.6	Problem Reports	Identify and record the IP design problems and their solutions	Data available upon request (Normally provided to the IP User)
10.7	IP Configuration Management Records	Set of data covering: • Baseline • Change history records • Problem reports • Design tools identification • Archive and release records	Data available upon request
10.8	IP Process Assurance Records	Set of data covering: • Review reports • Audit reports • Records of deviation after the first official release	Data available upon request
10.9	IP Accomplishment Summary	Documents compliance to the IP Design Assurance Plan	To be submitted to the certification authority by the IP User

***Note**: See the Hardware Control categories 1 (HC1) and 2 (HC2) for each deliverable in DO-254/ED-80 Appendix A. HC1 is more rigorous than HC2, basically in that the Change Control, changes having to be formally recorded, approved and traced.*

As described in the Soft IP Assessment Process in paragraph 3.3.1 of this paper, only part of this data may be available for the IP. In such a case, missing data should be re-generated to increase the IP core implementation visibility, including extensive testing and analysis.

3.3.2.3 Modulation According to DAL

DO-254/ED-80, Appendix A, Table A.1 indicates the data depending on the DAL the IP User should submit or make available to the certification aAuthorities.

Ultimately, it is the responsibility of the applicant to ensure that the data is provided and to ensure that the data mentioned in this table satisfies the objectives or must be complemented with additional requests from certification authorities (such as applicable Certification Review Items (CRI), Issue Papers (IP) or project specific discussions).

3.3.3 Strategy Based on Soft IP 'Reverse Engineering'

For the context of this paper, the term 'reverse engineering' refers to the process used to generate hardware life cycle data that are deficient or missing in order to satisfy the design assurance objectives of DO-254/ED-80.

The intention of the 'reverse engineering' approach in this paper is to produce the necessary data to support approval.

3.3.3.1 Purpose and Scope

The strategy described in this section applies when an IP core already exists, but with life cycle data that is determined to be deficient for satisfying the design assurance objectives associated with the target application. For example:

- Re-use of an 'in-house' IP design that was generated prior to the application of a DO-254/ED-80 development process.
- Re-use of an 'in-house' IP design that was developed for a lower DAL than the new application.
- Use of third party IP that has not been developed using a DO-254/ED-80 process.

The reverse engineering approach relies on the process to generate missing or deficient life cycle data for DO-254/ED-80 objectives referred in Table 2 according to the DAL assigned to the device (see DO-254/ED-80 Appendix A Table A-1).

Section §11.1.4 "Upgrading a Design Baseline" of DO-254/ED-80 should be used when following a reverse engineering approach.

If reverse engineering of an IP core is proposed, the IP User should describe the processes to be used and justify the strategy to be followed in the PHAC (as "use of previously developed hardware") as part of the Planning life cycle process defined in DO-254/ED-80.

The applicant should start discussions with the certification authority early in the certification process regarding their strategy for ensuring the satisfaction of DO-254/ED-80 objectives using the reverse engineering techniques.

The reverse engineering approach is only applicable for Soft IP when the IP HDL RTL code is available.

3.3.3.2 Recommended Development Approach for Reverse Engineering IP

3.3.3.2.1 Minimum Input Data

As a minimum, the HDL RTL code for the IP core should be available, allowing the IP function to be fully understood, which is essential for a reverse engineering approach to be successful.

The following sections identify how the DO-254/ED-80 life cycle processes apply to IP reverse engineering. A description of each step in the process is given below.

3.3.3.2.2 Planning

The IP User should identify the IP core(s) that will be reverse engineered and summarize the gap analysis and proposed development approach in the PHAC (or equivalent document).

3.3.3.2.3 Requirements Capture

For an IP core that is to be integrated into a PLD/ASIC device, the device level requirements should already include a subset of requirements that correspond to the primary functions implemented by the IP. The rationale here is that, if the IP has been selected for use, then it must already represent some existing requirements to which the IP complies. However, it is possible that the IP either deviates slightly from the existing requirements or it includes additional functionality that may be unused in the target device. In these cases, the IP User may choose to modify the IP detailed design data as necessary to address the issue(s), at the appropriate point in the life cycle.

> ***Note:*** *As the reverse engineering approach is being used, IP Users are able to modify an existing IP as, by definition, there is no existing certification data package for which credit would be altered (unless any credit is also being taken for service experience).*

The IP requirements should be adapted to correctly and completely specify the IP functionality.

If the IP User plans to utilize the IP without any changes, the following approaches could be proposed:

1) The user should decide whether the target system can accommodate any deviations from existing requirements and modify the system architecture and device requirements accordingly.
2) Where the IP has additional functionality, the conceptual design process (see paragraph 3.4.4.2.4) may identify derived requirements that need to be fed back and added to the device level requirements.

3.3.3.2.4 Conceptual Design

Conceptual design life cycle data is likely to be deficient or missing for an IP core. The supporting data that is supplied with the IP may range from a simple data sheet to more comprehensive documentation. In some cases, there may be no supporting documentation at all. In these cases, the IP User will need to generate conceptual design data – typically as part of the target device conceptual design document – based on the documentation supplied and/or analysis of the HDL code.

> ***Note:*** *Conceptual design data is only necessary for DAL A and B designs (per Appendix A of DO-254/ED-80). Nevertheless regenerating the conceptual design data is not the approach covered in DO-254/ED-80 which proposes a top-down approach while reverse engineering is more corresponding to a bottom-up flow. Therefore, generating the conceptual design data is considered as a necessary step when preforming reverse engineering on HDL design, and subsequently establishing traceability between requirements and conceptual design data is considered essential activity to guarantee that the IP design fulfills the requirements.*

For DAL A, B and C, traceability between the device requirements and the conceptual design – including the section(s) applicable to the IP – needs to be generated and reviewed. Performing both a 'top-down' and a 'bottom-up' review contribute to identify any missing design functionality and any functionality that exists without parent requirement(s). Discrepancies between requirements and conceptual design could be resolved utilizing the following means:

1) The omissions are fed back to the requirements capture process and captured as derived requirements.

   > ***Note:*** *This will ensure that the unused functions are verified as part of requirements-based testing. For all other derived requirements, they will need to be validated to ensure that there is no impact on system safety.*

2) The conceptual design is modified (which will then result in a modification to the HDL code).

3) Architectural mitigation techniques are employed such that it can be demonstrated (by analysis) that unused functions will not be inadvertently activated/used in the target device.

3.3.3.2.5 Detailed Design

The IP HDL code should be reviewed against an appropriate coding standard. This may be a standard provided by the IP Provider or an existing standard that the IP User has for in-house designs. The latter approach should only be used where there is consistency between the standard and the IP code. It should not be necessary to re-write large amounts of HDL code to meet the standard. In some circumstances, it may be necessary to reverse engineer a HDL coding standard – based on the general content and style of the IP code – which can then be applied to ensure consistency throughout the IP HDL code.

For DAL A and B, traceability between the conceptual design and the HDL code – including the file(s) applicable to the IP – needs to be generated and reviewed. Performing both a 'top-down' and a 'bottom-up' reviews contribute to identify missing code and any code that exists without adequate conceptual design. For the latter example, either the omissions need to be fed back to the conceptual design process or the HDL code should be modified.

For all other device life cycle data, the IP HDL code will need to be subjected to configuration management objectives consistent with the DAL. When IP constraints file are delivered by the IP Provider, this file has to be reviewed to ensure the consistency of the IP core design with its intended requirements.

3.3.3.2.6 Implementation

As the Soft IP is delivered to the IP User before the design implementation, no implementation data is available at the Soft IP block level. Soft IP constraints will be integrated into the device constraints file and used as input to implementation activity (see Section 3.7 'Integration of the IP within its target AEH device').

3.3.3.2.7 Validation

No specific activity is required for the IP block, as any IP-related derived requirements (see paragraph 3.3.2.2.2) should be reviewed along with other device-related derived requirements. This will include the validation of any derived requirements captured as a result of unused function(s) within the IP.

3.3.3.2.8 Verification

Where the IP is supplied without a set of tests, there is no specific activity that is required for the IP block. Instead test cases developed against the set of device level requirements should include verification of the subset of IP requirements applicable to the IP function(s).

Where the IP is supplied with an HDL test bench that the IP User adopts for certification credit, this IP test bench should be integrated with the device level test bench and documented in a verification procedure.

For all DALs, traceability between the device requirements and the test cases – including the requirements and tests applicable to the IP – needs to be generated and reviewed.

For DALs A and B, where advanced verification methods may also be applied, the selected method should be modified accordingly to include the IP. For example, code coverage performed as part of Elemental Analysis may indicate that there are deficiencies in the test bench supplied with the IP. Therefore, additional test cases would need to be developed until the required coverage is achieved or unintended functions are removed.

3.3.3.2.9 Production Transition

The production transition activities for AEH should be included in the final definition of the device data (e.g., a Configuration Index) and the compliance statement in the HAS.

The device Configuration Index data should include a section dedicated to 'previously developed hardware', where the IP usage should be indicated including version/revision.

The Hardware Accomplishment Summary should document any deviations or additions to the development approach proposed in the PHAC for use of the IP.

3.3.3.3 IP Service Experience

3.3.3.3.1 Purpose

Product Service Experience is discussed in DO-254/ED-80 section 11.3. When the IP is a COTS component, typically, design life cycle data is not fully available and reverse engineering activity may need to be complemented by relevant IP service experience credit. Therefore, to use this approach, the applicant should ensure that the IP core design is mature and free of errors up to a level equivalent to the case if the component would have been designed using the standard design assurance guidance of DO-254/ED-80.

> ***Note 1****: As soon as design changes are applied to the IP, service experience of Soft IP becomes problematic to use as certification credit.*

***Note 2**: the IP service experience approach requires a level of rigor and detail that may be difficult to accomplish for COTS IPs. However, this requirement cannot be reduced if this approach is used to show that the IP core design is mature.*

Service experience relates to data collected from any previous or current usage of the IP. Data from non-airborne applications (e.g., the automotive field) may be used, if it can be shown that the data is relevant to the proposed usage. The challenge is to assess that usage domain (configuration, parameters used in generics instantiation, etc.) of the previously used COTS IP is relevant to the IP User case.

When providing relevant service experience data, the IP User could follow applicable guidance for service experience of COTS device in order to obtain appropriate data to gain some certification credit.

Service experience should not be used as the only certification justification for a Soft IP.

3.3.3.3.2 Data To Be Provided

The IP User's proposal to use service history as a means to provide complementary design assurance for the COTS IP core should address the following:

1) Problem (also called errata) recording and tracking process: the IP Provider should explain the process in place to collect problems during service, and describe how the reported problems are recorded, tracked and analysed. The process should also include a formal means of notifying existing IP Users of any new Problem Reports that affect the IP core.
   Throughout the development and service life of the equipment using the COTS IP, the IP User should have a continuous access to IP errata. Errata should be analysed and assessed for their impact on the resulting device intended function and mitigated when necessary.

1) Identification of the targeted PLD/ASIC device, previous applications, installations and environments to the target application, configurations parameters (generics, etc…).

2) Data used to determine appropriateness of use and usage limitations may be available in specifications, data sheets, application notes, service bulletins, user correspondence and errata notices. These sources of information may also describe the functions associated with the IP core, and their controllability (activation/deactivation mechanism). In this way, the airborne intended use can be correlated to previous uses. The demonstration should be coherent with the safety objective of the intended function to which COTS IP contributes. IP Providers are encouraged to gather and provide data about their IP service experience in safety-critical, high-integrity or high dependability domains, as it supports certification strategy (see Figure 2).

3) The IP User or IP Provider should provide evidence of sufficient service experience and widespread use. Widespread use means previous usage in one or several of the following domains demonstrating a significant probability of locating erroneous or unexpected behaviours:

   - Aviation, Space, Military.
   - Other safety applications (e.g., nuclear, railways, medical, etc.).
   - Other high integrity applications (e.g., automotive, banking, etc.).
   - Other applications (e.g., telecommunications, computers, etc.).

   Service experience credit can only be granted when the Soft IP design configuration is exactly the same as the Soft IP used during the service experience period of time. Nevertheless, the implementation and Place & Route will output different physical representation of the IP. As a consequence, operating hours accumulated or widespread number of years during the current or previous development should be considered as a complementary credit to the reverse engineering or DO-254 development process.

   Note that if other applications are used as evidence, the work to demonstrate a significant probability to detect design errors may be very high. It is always the responsibility of the IP User to ensure this service experience data is acceptable (e.g., relevance, demonstration, etc.).

3.4 Firm IP

A Firm IP is a portion of structural or physical netlist that could be linked to a specific device technology (e.g., PLD, FPGA, ASIC). This allows the IP Provider to not disclose the critical IP details and the IP User does not get access to its source code.

It is generally possible to configure a Firm IP for its specific usage with or without modification of the physical implementation. The IP User or system integrator can usually perform some limited amount of analysis, and the IP User can still perform optimization during placement, routing, and technology-dependent mapping of the IP functional blocks. Detailed design data for Firm IP (e.g., HDL code, traceability, etc.) mentioned in Table 2 may not be available. This has an impact for the IP User, and possibly the system integrator, and can jeopardize:

1) The usability for DAL A and B functions, if the IP is seen as a “black box”.
2) The satisfaction of DO-254/ED-80 objectives and Appendix B at AEH device level for DAL A and B, especially code coverage since HDL code may not be available.

3) The capability to perform reverse engineering and regenerate data, especially for DAL A and B functions.

4) The ability to use architectural mitigation at device level.

Service experience is not relevant for Firm IP cores, as the IP isn't reproducible in the same exact configuration and layout from one implementation to another.

Due to these limitations, IP users attempting to implement a Firm IP core into in a safety-related airborne application will likely experience many difficulties when attempting to show compliance for that AEH device, unless the data listed in Table 2 is available. Depending on the amount of data made available by the IP Provider, it may not be possible for the IP User to demonstrate compliance to airworthiness requirements for the airborne system or satisfaction of DO-254/ED-80 objectives for the hardware device.

3.5 Hard IP

A Hard IP is a fixed portion of a device that has completed the complete design process (conceptual, detailed design and implementation) resulting in a completed fixed layout. By definition, data related to the detailed design (HDL code, traceability, code coverage etc.) shown in the Table 2 is generally not available. Depending on the device, it is sometimes possible to configure a Hard IP for its specific use in a device. However, physical implementation will remain identical in any instantiation of the IP in a target device.

Because of these considerations, and provided that the IP Provider is offering a structured configuration management and errata process equivalent to COTS devices, a Hard IP can be considered similar to a COTS hardware device.

When selecting a Hard IP for an airborne application, the IP User should follow guidance related to 'Usage of COTS devices' that is applicable to the product, in order to obtain appropriate design assurance of the device implementing the Hard IP.

In order to provide a general background, the main topics to be addressed when intending to use a Hard IP could be summarized as follows:

- Knowledge of the Hard IP

  The IP User should have some access to design data (conceptual data, datasheet, controllability and monitoring features, etc.) to allow the IP User to evaluate if the IP is consistent with the device requirements into which it is integrated, and so correctly and completely fulfils its intended function.
  Intended IP requirements should then be captured and further verified at IP level using the available data (datasheet, user manual, etc.).

  Because the IP User has access to those design data, the IP User is so able to define the IP usage domain and assess its compatibility with respect to top-level device

safety and system aspects. This usage domain can be translated into requirements so that configuration is kept under IP User control and that the process ensures that it is completely and correctly verified.

- IP Errata analysis
  The IP User should have a continuous access to Hard IP errata. Errata should be analysed by the IP User for their impact on the resulting device and mitigated when necessary.

- IP service experience
  Because of the limited access to design data, the IP User of a Hard IP should present an amount of service experience appropriate to the DAL of the airborne function it performs or to which it contributes. The service experience can be taken from widespread usage of the IP but needs to be quantified in hours and/or number of different applications in which the IP is implemented.

  The collection of the IP service experience should be documented in the PHAC of the top-level device or separate IP documentation.

- COTS IP configuration management process: When using Hard IP, the IP User should document its IP configuration management process to gain assurance of the appropriate usage of the IP in an airborne application.

***Note**: This section focused on COTS Hard IP assessment and configuration management process to gain some development assurance at IP level. The integration of the COTS IP into the target device is addressed in paragraph 3.7 of this paper.*

Finally, the approach related to the use of COTS Hard IP should then be described in the Plan for Hardware Aspects of Certification (as "COTS components usage") and should address as well the guidance and requirements applicable to the product where the device is implemented.

3.6 Architecture Mitigation Considerations

Architectural mitigation techniques at different integration levels of the COTS IP core (i.e., hardware device, board, LRU, or system level) can be used to mitigate the possible existence of design errors in the IP core. Note that for a COTS IP core that has not been developed using a design assurance process, reverse-engineered, or has not been exhaustively tested, the existence of design errors may neither be proven nor excluded.

Architectural mitigation should at least be implemented when the IP lacks or has deficiencies in the design assurance process or data, or when an IP error could cause a Catastrophic failure condition without any other contributing faults occurring.

The following activities could be performed and documented to show the effectiveness of the proposed mitigation techniques:

1) Identify failure conditions of the COTS IP core as implemented in the target hardware device.
2) Identify all implemented upper level functions.
3) For all functions identified in 2) above:
    - Establish correlations between these functions and the IP core's functions.
    - Perform an analysis if a design error in the IP core is critical (i.e. potentially exhibiting a failure condition that could impact an upper level failure condition) and provide the associated rationale for that
4) For those failure conditions that cannot be mitigated at IP level provide other means of failure mitigation at higher levels.
5) The system development and safety assessment processes should ensure that the architectural mitigation techniques are implemented correctly.

These activities should be documented in the certification data package.

3.7 Integration of the IP within its Target AEH Device

In order to properly implement the IP into its AEH device, the IP User should perform the following integration activities.

3.7.1 Integration activities at requirements level

The IP User should establish traceability between IP requirements and upper level requirements (i.e., device or board level, depending of the IP level on integration with regards to the AEH device) and perform IP requirements validation activities per DO-254 / ED-80.

Activation and configuration of IP functions should be captured into device level requirements, as well as deactivation mechanisms for unused IP functions. This specific requirement capture of IP usage at device level is then ensuring the basis for verification of the IP usage domain at device level.

If there are unused IP functions, the method used to deactivate those functions should be captured in to device level requirements and be further tested.

3.7.2 Integration activities at IP design and verification level

Regarding design level aspects, the IP User should perform additional activities :

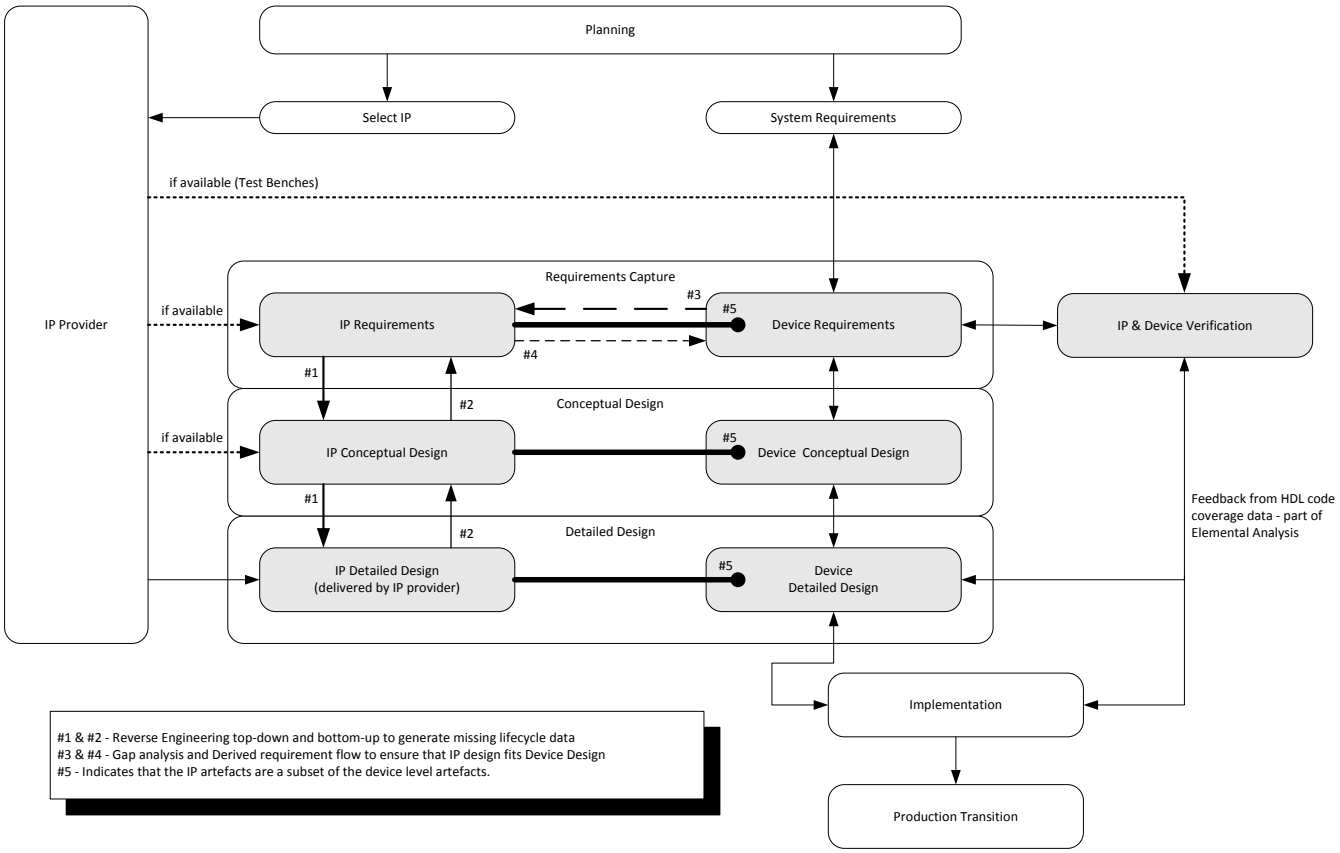
- For Soft IP:
    - In addition to the integration of IP HDL code into the AEH HDL code, the IP User should integrate IP timing constraints into AEH timing constraints file. The IP User should review the IP timing constraints and check their compatibility with AEH device timing constraints. The review should additionally verify the proper matching and compatibility of IP constraints file with the device level constraints.
    - The IP User should verify all IP requirements at implementation level after place and route. This will typically consist on post-layout simulations and physical testing.
    - The IP User should perform Static Timing Analysis using the integrated device and reviewed the timing constraints file to ensure that all requirements are met for any timing conditions within specifications as well as for any batch of the device (taking into account temperature, voltage and dispersion of transistor performance in a range guaranteed by the target device manufacturer).
- For Firm IP, no guidance is provided in this paper, see conclusion of paragraph 3.4
- For Hard IP :
  The IP routed block should be implemented within AEH device layout as a block and the IP User should comply with interface routing requirements recommended by the IP Provider, for instance with respect to timing constraints of input signals and adapting to outputs signals characteristics.

3.7.3 Integration activities at integration testing level

To complete the verification aspects, integration testing should include the verification of the IP integration into the AEH device. Specific test cases exercising the IP interface signals with the AEH device and proper deactivation of the unused functions may be developed for the specific design integration. These tests should be complementary to the IP verification test cases and verify the IP in its target application.

Finally the verification of the AEH device requirements should cover 'by design' the used IP functions and activation/deactivation mechanisms of IP functions.

Figure 3: Integration of IP Core into DO-254 Development Process



4 Summary

Certification experience in IP assessment shows that different approaches can be proposed for usage of IP cores in airborne electronic hardware and that these depend on the design level at which the IP is delivered (Soft, Firm or Hard) and on the accessibility to the design data.

In addition to these approaches at the IP level to gain design assurance, architectural mitigation techniques within the device or at the board or system may be used, and service experience may complement the certification credit already gained by available or reverse-engineered design data.

When choosing to use an IP within an airborne electronic hardware, the IP User should choose the most appropriate approach(es) to ensure that the IP will satisfy the design assurance objectives. This paper provides information on the approaches that can be used, and the data that should be obtained or generated. It provides certification authority position on the use of COTS IP in an AEH device intended for use in an airborne system.

5 Reference Documents

a. RTCA DO-254 and EUROCAE ED-80, April 2000, Design Assurance Guidance for Airborne Electronic Hardware, www.rtca.org , www.eurocae.org .

***Note**: Even though both DO-254/ED-80 and ED-80 are valid references, the term DO-254 is mostly used in the document for better understanding.*

b. AC 20-152, June 2005, Advisory Circular Document DO-254/ED-80 Design Assurance Guidance for Airborne Electronic Hardware, www.faa.gov .

c. CAST 27 paper, rev 0 June 2006, Clarification on the use of DO-254/ED-80 Design Assurance Guidance for Airborne Electronic Hardware www.faa.gov .

d. CAST 28 paper, rev 0 December 2006, Certification Authorities Software Team (CAST) position paper: Frequently Asked Questions (FAQ) on the use of DO-254/ED-80 Design Assurance Guidance for Airborne Electronic Hardware, www.faa.gov .

e. FAA Change Order 8110.105 change 1, September 2008, SIMPLE AND COMPLEX ELECTRONIC HARDWARE APPROVAL GUIDANCE www.faa.gov .

List of Acronyms

ASIC	Application Specific Integrated Circuit
BIST	Built-In Self Test (also referred as BIT or BITE)
BIT	Built-In Test
BITE	Built-In Test Equipment
CAST	Certification Authorities Software Team
CEH	Complex Electronic Hardware
COTS	Commercial Off-The-Shelf
CRI	Certification Review Item
DAL	Design Assurance Level
EASA	European Aviation Safety Agency
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FPGA	Field Programmable Gate Array
HAS	Hardware Accomplishment Summary
HDL	Hardware Description Language
IP	Intellectual Property
PHAC	Plan for Hardware Aspects of Certification
PLD	Programmable Logic Device
PR	Problem Report
RTCA	RTCA, Incorporated (formerly, Radio Technical Commission for Aeronautics)
RTL	Register Transfer Level
SoC	System on Chip
SSA	System Safety Assessment
STA	Static Timing Analysis

NOTE: **This position paper has been coordinated among representatives from certification authorities in North and South America, Europe, and Asia. However, it does not constitute official policy or guidance from any of the authorities. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**