WP403 (v1.0) September 8, 2011

Practical Use of FPGAs and IP in DO-254 Compliant Systems

By: Dagan White, Xilinx, Inc.
and Todd R. White, FAA DER - Qualtech Consulting, Inc.

There exists little doubt that a fully compliant DO-254 process is required for custom FPGA designs and for the custom intellectual property (IP) that resides within them, but how can a designer use commercially available IP within a DO-254 compliant system? Here is where ambiguities enter the DO-254 process. This white paper addresses where and when to use DO-254 and DO-178 in FPGA designs and recommends practical means for employing widely used commercial off the shelf (COTS) IP in custom FPGA designs that target avionics applications.

This white paper is meant to open discussion on these topics, but it is not to be construed as official guidance regarding DO-254 application to IP cores or systems on chips. Similar topics are the subject of the joint US and European DO-254 User Group papers, which are directed to influence policy making in both of these subject areas. The methods that are presented in this white paper should be discussed with the appropriate avionics certification personnel prior to application on any avionics program.

Purpose, Scope, and Audience

This white paper highlights ambiguities in the interpretation of DO-254 with regard to FPGA developments, including various types of IP, e.g., COTS IP, with recommendations for practical approaches for addressing these issues. It does not describe basic DO-254 compliant processes—rather it covers the broader issues related to the application of DO-254 to IP for FPGA designs. The target audience is certification authorities, designated engineering representatives (DERs), designers, managers, and IP developers.

State of DO-254 and Its Interpretation

FPGA designs typically combine a COTS device with both custom and COTS IP. The combination of these items can ultimately result in shades of gray when considering how an end device complies with DO-254. Confusion exists as to how and when guidance should be applied to the various types of IP.

Guidance documents are being published to clarify the issues, and they are being published in greater frequency as time progresses. With each new publication, the intent is to increase the level of understanding and guidance for the application of DO-254 to programmable logic devices (PLDs) and beyond.

RTCA/DO-254 is the product of a joint RTCA Special Committee and EUROCAE working group. The goal of this guidance is to establish clear objectives that ensure development of safe and robust avionics equipment. This guidance is intended to be applied across line replaceable units, circuit card assemblies, integrated circuits, and PLDs.

FAA Advisory Circular (AC) 20-152 [Ref 1] officially recognized DO-254 as an acceptable means of compliance for ensuring that a custom micro-coded component, such as an ASIC, FPGA, or PLD, meets intended functional and safety standards for airborne applications. The AC also states that DO-254 is "a means" but not the "only means" of compliance.

FAA Order 8110.105 Chg 1 [Ref 2] was then published to explain how FAA certification staff can use and apply DO-254 when working on certification projects. This order also provides guidance to the designer, yet gray areas still exist regarding the application of DO-254 in FPGA development. Although DO-254 addresses design assurance of hardware up to and including the line replaceable unit (LRU), the FAA has chosen to only apply it to custom complex micro-coded devices (ASICs, FPGAs, and PLDs). The application of DO-254 has thus diverged from its initial intent, and with this, confusion regarding application of DO-254 to FPGAs has increased. The limited application of DO-254 is changing with the introduction of further guidance from the European Aviation Safety Agency (EASA) [Ref 3], which also requires the application of DO-254 at the board and LRU level. This guidance additionally introduces further clarification regarding application of DO-254 to FPGAs, graphics processors, and microprocessors. Even with this latest guidance, however, questions about FPGAs and IP still abound.

FPGAs are being used to implement increasingly complex functions, and it is necessary to employ rigor during the design process to ensure end-product safety. However, in the context of system design that hosts the FPGA, the rigor of the design process must be balanced and can be used to mitigate or manage functions hosted within the system. Likewise, it is important to consider how low-level IP elements are managed within the customized FPGA design.

Definitions

Custom micro-coded component is the term given to ASICs, FPGAs, and PLDs intended for avionics applications [Ref 1]. However, COTS devices are not custom-coded, nor is COTS IP, which refers to commercially available logic blocks or cores that are included in device silicon or vendor libraries [Ref 2].

Design assurance refers to the methods used to substantiate that a design is free of errors [Ref 4]. Service history, extensive testing and analysis, architectural mitigation, reverse engineering, and/or fully compliant DO-254 design all contribute to means of assurance. Avionics developers might need to apply a combination of these techniques to "demonstrate that the intended function is free from anomalous behavior, satisfies applicable regulations, and meets airworthiness requirements” [Ref 2].

Hard IP is hard-wired and not modifiable by the end user. Examples of hard IP include integrated Endpoint blocks for PCIe or embedded processors in FPGAs.

Firm IP describes IP delivered as a net list. Firm IP is not modifiable by the end user, but these IP cores must be placed and routed with the rest of the end-user design.

Soft IP refers to IP delivered as HDL code. Soft IP is modifiable by the end user and is synthesized, placed, and routed along with the rest of the end-user design.

Fully compliant with DO-254 refers to the ability to show evidence of compliance with all DO-254 objectives applicable to a particular design assurance level (DAL). The distinction is made in contrast to the case of COTS IP use, where it might not be possible or feasible to show evidence of compliance with all required objectives.

DO-254 Interpretations - The COTS Status of FPGAs

DO-254 defines COTS devices as components, integrated circuits, or subsystems that are developed by a supplier for multiple customers, whose design and configuration are controlled by the specification from the suppliers or industry. FAA Order 8110.105 [Ref 2] clarifies this definition by stating that COTS IP includes commercially available vendor library IP that can be used in custom FPGA designs. The COTS IP can also be embedded within the device as delivered from the vendor.

The Certification Authorities Software Team (CAST) position relative to COTS IP is also reflected in FAA Order 8110.105 [Ref 2]. The CAST position is as follows:

"Since the use of a COTS IP can greatly impact the performance and functionality of a custom micro-coded component, the rigor of the development processes for a COTS IP implemented in a custom micro-coded device for use in airborne systems or equipment should be commensurate with its intended use and should satisfy applicable functional and safety-related requirements."

"Moreover, the guidance in section 11.2 of DO-254/ED-80 may not be sufficient for design assurance of a COTS IP implemented in a custom micro-coded device that support safety critical applications such as Level A or B aircraft functions. As a result, life cycle data (i.e., verification, testing, and analysis) of a COTS IP may need to be developed or augmented to demonstrate its intended function, satisfy applicable regulations, and meet airworthiness requirements."

When vendor-delivered hard, firm, or soft IP is used in the custom FPGA design, confusion arises as to whether the IP can be considered COTS, and if so, what is sufficient to satisfy functional and safety-related requirements for its intended use. To mitigate this, some vendors offer a DO-254 compliant version of the COTS IP. In this case, the compliance evidence is provided to the integrator via license. In other cases, this information is not made available and other means need to be employed. This scenario is especially problematic for DAL A and B, due to the inability to satisfy the detail design, elemental analysis (coverage), and related verification objectives.

Figure 1 shows five different scenarios, asking whether the blank device or its standard subcomponents can be considered a COTS device or whether a fully compliant DO-254 life cycle process must be followed by the vendor before use in avionics applications. This is not to say that COTS are not governed under DO-254, but only whether a fully compliant DO-254 life cycle process is specifically required for that type of vendor-delivered IP or component.

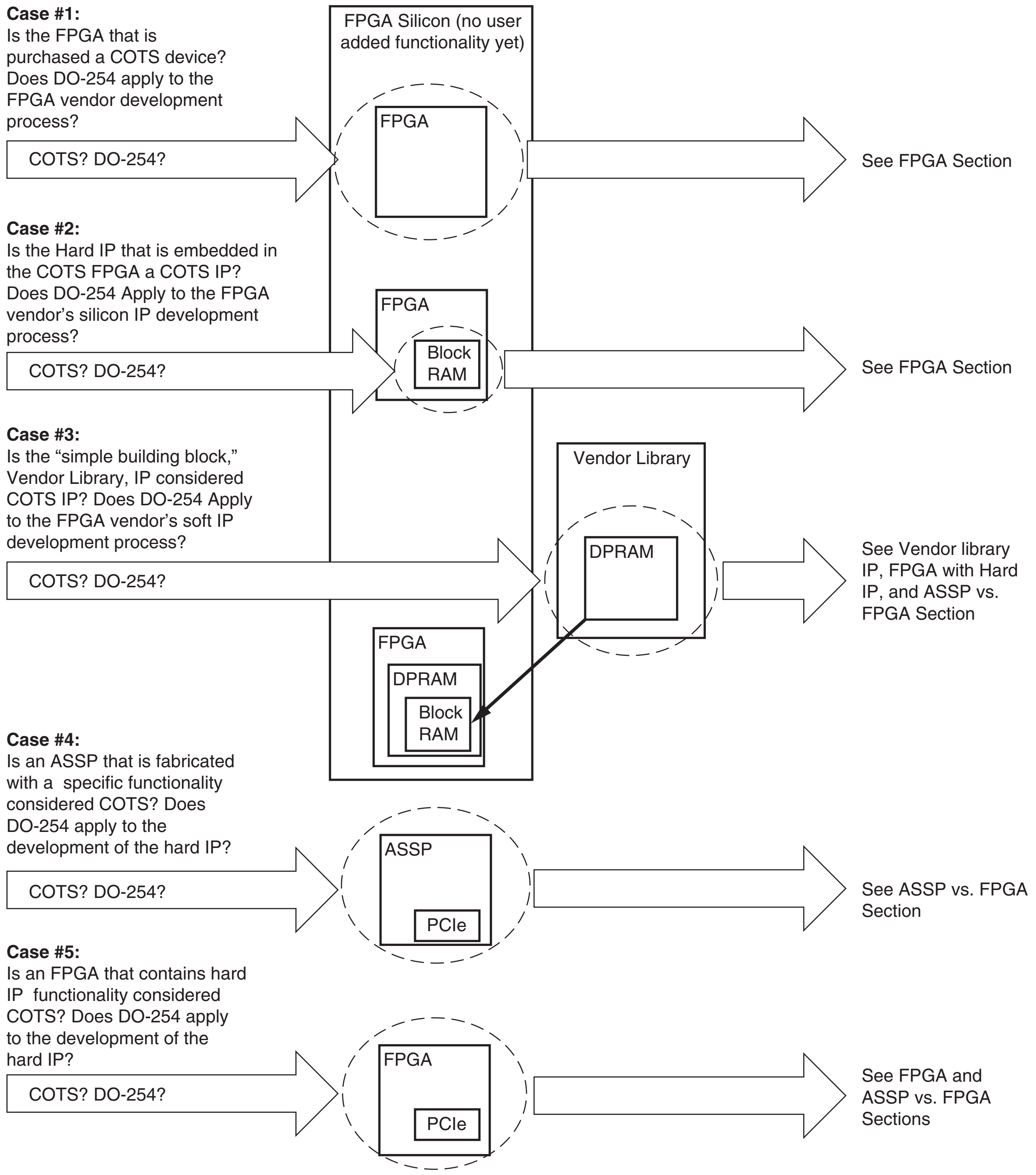
Case #1:
Is the FPGA that is purchased a COTS device? Does DO-254 apply to the FPGA vendor development process?
COTS? DO-254?
FPGA Silicon (no user added functionality yet)
FPGA
See FPGA Section
Case #2:
Is the Hard IP that is embedded in the COTS FPGA a COTS IP? Does DO-254 Apply to the FPGA vendor's silicon IP development process?
COTS? DO-254?
FPGA
Block RAM
See FPGA Section
Case #3:
Is the "simple building block," Vendor Library, IP considered COTS IP? Does DO-254 Apply to the FPGA vendor's soft IP development process?
COTS? DO-254?
Vendor Library
DPRAM
See Vendor library IP, FPGA with Hard IP, and ASSP vs. FPGA Section
FPGA
DPRAM
Block RAM
Case #4:
Is an ASSP that is fabricated with a specific functionality considered COTS? Does DO-254 apply to the development of the hard IP?
COTS? DO-254?
ASSP
PCIe
See ASSP vs. FPGA Section
Case #5:
Is an FPGA that contains hard IP functionality considered COTS? Does DO-254 apply to the development of the hard IP?
COTS? DO-254?
FPGA
PCIe
See FPGA and ASSP vs. FPGA Sections
WP403_01_083111

Figure 1: **FPGA as COTS Device**

Note: None of the components in Figure 1 implements custom functionality.

FPGA

Cases 1 and 5 question whether the FPGA itself can be considered a COTS device. In case 1, the user-configurable logic of the FPGA should be considered to be a COTS device. FPGAs are manufactured at very high volume for use across many applications and industries. For the cases where hard IP is embedded in the FPGA (as in cases 2 and 5) see FPGA Hard IP.

FPGA with Hard IP

Cases 2 and 5 show hard IP embedded in an FPGA. Case 2 differs from case 5 only in the complexity of the embedded IP and in the context of viewing the IP as stand-alone versus part of a COTS device. This type of IP is not modifiable by the user, who generates custom application content. Although the IP is not customizable, it can be configurable, making hard IP very similar to, if not the same as, COTS integrated circuits. These blocks are not custom micro-coded components, but rather they are standard products—no different than stand-alone COTS devices such as analog-to-digital converters or programmable clock management devices, which require configuration.

The examples shown in Figure 1, block RAM and an integrated Endpoint for PCI Express, are common in mainstream FPGAs. These types of IP are key to an FPGA vendor's target market and are widely employed at high-volume across many end-products and markets. As such, these blocks can be classified and handled as COTS devices.

Vendor Library IP

As a part of the design package, an FPGA vendor delivers a library of building-block IP to the customer. This IP can range from simple logic functions such as wide ANDs, multiplexers, etc., to more complex functions such as those that configure a block RAM hard IP to create a dual-port RAM (case 3 in Figure 1).

Vendor library IP is delivered as a mix of both soft (synthesizable) or firm (netlist level) IP. If the vendor IP is delivered in fully soft, synthesizable form (i.e., as HDL), the end-user actually has the opportunity to modify the HDL code. Therefore, DO-254 should be fully applied.

In the case of firm IP, where a pre-synthesized netlist is delivered, the IP is typically verified by the FPGA vendor for use as is across a broad range of markets and applications. The IP might be configurable, but the output of the configuration tool is a pre-synthesized netlist. This type of IP can be considered COTS based on the extent of its usage. It needs to be clearly understood, however, that simply creating a netlist from source code, such as in the case of firm IP, does not in itself give an IP vendor a way around DO-254.

When a firm IP is treated as a COTS device, its use within the custom application must still satisfy DO-254 objectives. Assuming that a compliance data package or source code is not provided, it is not possible to comply with the elemental analysis requirement of a firm IP block (which is an issue in DAL A and B applications). It is, however, possible to verify its use in accordance with data sheet specifications and that all ports and boundary conditions are exercised. Requirements definition and requirements-based simulation and testing are possible when verifying the IP at the port level within a custom design. A developer can also employ architectural mitigation techniques to address any perceived failure mechanisms. Regardless of the methods used, the final approach must justify that COTS IP meets an appropriate level of safety within the custom design. All COTS IP must be substantiated within the integrator's design activity. See COTS IP and Design Assurance.

Low-level primitives, such as memories and clocking elements, should be treated as COTS devices, and verified as part of the overall system verification. They typically do not have source code because they are hard elements in the FPGA fabric. See COTS IP and Design Assurance.

Note: The distinction between firm and hard IP is that the user must still place and route firm IP.

ASSP versus FPGA

ASICs can be developed for a single mission, used across a handful of applications, or widespread commercial availability (the latter being referred to as ASSPs). If a device is an ASSP, then it can be treated as a COTS device under DO-254, assuming the service history is sufficient to support a case for equivalent level of safety relative to the COTS device. But what volume qualifies an ASIC/ASSP for COTS status? While the volume of devices sold into various applications can be obtained, estimating the exact number operating hours is nearly impossible. Ultimately, a program working with the certification authorities have to make a compelling case as to why a COTS IP is acceptable (see COTS IP and Design Assurance).

Given that an ASSP with an integrated Endpoint block for PCIe (case 4) is essentially identical to an FPGA with an integrated Endpoint block for PCIe (less the end-user application) as depicted in case 5, an FPGA and its hard IP as delivered from the device vendor can be classified as a COTS device using the same justification as an ASSP. In this example, a compliant DO-254 life cycle process is only applied to the use of the IP block as a COTS device, not its generation. See FPGA with Hard IP.

COTS IP and Design Assurance

A fully compliant DO-254 process, or an equivalent alternate means of compliance, is always applied at the custom application level. When COTS IP is employed in an FPGA design, it must be identified and verified within the custom application, and this is a typical part of the FPGA development process. In this case, a combination of methods are typically used to demonstrate that the IP complies with the regulations.

Service Experience

After the COTS status of an FPGA IP has been determined, the issue of design assurance arises. DO-254 states that service experience (operational hours) can be used to substantiate design assurance of a COTS device, also stating that data from non-airborne applications is acceptable.

Some interpretations, however, place a service-experience threshold in the millions of operational hours in avionics or high-reliability applications only. Even stricter interpretations require that the service experience be in safety applications (defined as space, airborne, military, nuclear, and medical), and if greater than a million hours cannot be substantiated in these applications, then ten million or more hours in other high-reliability applications must be substantiated.

Excepting the case of a high-volume avionics developer with prior experience shipping a particular COTS device in its own systems, it is virtually impossible for any vendor to prove the number of operational hours for a given device. Without this data from the vendor, an avionics developer cannot substantiate service history as a means of design assurance. With these strict interpretations, it seems unlikely that any device could prove a case for an equivalent level of safety based on service experience alone (forcing that other methods be used). The operating hours requirement in a particular configuration and in an avionics application is very stringent and might prohibit newly developed commercial devices from ever being deployed in avionics applications without architectural mitigation or extensive testing. Clear and reasonable methods are needed to allow use of COTS devices/IP based on service experience.

The user must take a step back to assess the situation from a macro perspective. What is the nature of device/IP under consideration? How does it fit into the system? And in terms of service experience, what evidence is necessary to demonstrate that an IP is free of unintended functions?

Considerations in lieu of detailed operational hour statistics include:

- How long has the device/IP been available?
- Is the device under strict configuration control, with a problem report history?
- How many devices have been sold, or in how many systems/projects has the IP been used?
- Does relevant device errata exist to the show past updates and that the manufacturer is able to revise and control the device or IP?
- What types of end-products use these devices/IPs, and how would the reliability affect that type of end-product?
- How long has the vendor been in business, and what is their financial standing (if public)?
- Are supplier management processes in place and has the manufacturer been audited?

Much of the information regarding volume of devices, their end applications, and customers is often considered to be proprietary by many vendors. System developers must be prepared to enter into nondisclosure agreements (NDAs) to receive any information regarding service history. Xilinx provides service history justification for devices/IP upon request, and requests can be sent through the Xilinx sales to the avionics team.

Combining the answers to the service history questions, the user can logically deduce whether or not an IP has been employed successfully. Mean time between failure (MTBF) calculations are the responsibility of system developers and should be based on the same criteria used for custom IP. These calculations must be based on device vendor reliability reports, such as the *Xilinx Device Reliability Report* [Ref 5], in conjunction with the IP resource utilization, which is stated in vendor IP data sheets.

Beyond Service Experience

Service experience alone as an alternate means of compliance can be a difficult case to get through a Certification Authority under current interpretations. Arguments against using service experience as the sole means for demonstrating design assurance include but are not limited to the following:

- The IP is not used or configured in the same way across all applications
- The service history is reduced with every new revision of the IP (even in the case of a revision to support a new version of development tool or a new device series)

However, service history can be used effectively in conjunction with other means, including satisfaction of the "achievable" DO-254 objectives. For DAL C and D applications, alternate means of compliance is not an issue since the avionics developer is able to comply with all of the required DO-254 objectives. The difficulty enters for DAL A and B applications, where objective evidence of compliance is missing (as is the case for COTS IP, where the artifacts are not offered or licensed by the vendor or a third-party provider). In this case, a combination of partial DO-254 compliance and alternate means of compliance can be proposed to the certification authority.

When sufficient service experience cannot be substantiated, the FAA [Ref 2] provides alternative methods for establishing design assurance:

- Reverse engineering
- Extensive testing and analysis
- Architectural mitigation

These methods can be used in lieu of service experience, or they can be used in conjunction with it.

Reverse engineering is normally perceived as deconstructing and/or analyzing the workings of a system in an effort to replicate its functionality. In DO-254 context, reverse engineering refers to development and verification of the application from the source code backward. All of the objectives, activities and life cycle data are the same. The difference is the order in which they are satisfied.

In the case where source code for COTS IP cannot be obtained (the typical case), reverse engineering to generate the required life cycle data from known information about the COTS IP can be difficult and ultimately lead to complete redevelopment of the IP to satisfy all of the DO-254 objectives. This situation leads to new, custom IP that does not gain the same level of broad industry review, scrutiny, and testing as the original COTS IP. Because alternatives to regenerating IP do exist, even for DAL A and B systems, regenerating the IP should be the last resort.

To mitigate this risk, Xilinx is reverse engineering its own IP, or working with IP vendors and a third party to reverse engineer the IP vendors' IP (with their permission), to make the IP DO-254 compliant (since it was not originally designed to the specification). In this case, the source code can be encrypted/obfuscated, yet the IP can be licensed with a complete package of compliance artifacts.

Extensive testing and analysis of COTS IP is another method of design assurance. The goal of extensive testing and analysis is to demonstrate requirements-based test coverage, which traces COTS IP performance to the design requirements. This testing and analysis performed by a system developer builds on the testing already done by the COTS IP supplier and customers. COTS IP is used across many industries and products, which increases the likelihood of finding errors that could exist even in the best engineered IP, whether that IP was developed under a DO-254 process or not.

Moreover, extensive verification is in fact common (and required) during COTS IP integration. System developers typically conduct black-box simulation and hardware-level verification of IP in the custom design as a part of the DO-254 processes.

Lastly, FAA Order 8110.105 [Ref 2] proposes using architectural mitigations at the device, board, LRU, or system level to detect and/or mitigate undesirable behavior of the IP within the system. System- and device-level architectural strategies can be the most effective way to handle areas of concern for high-reliability systems. For instance, watchdog timers and parity checks are often used in a wide range of applications. SEU monitoring of configuration memory CRC checking is another example of commonly employed architectural mitigation. Depending on the design function and architecture, many more mitigation techniques can be employed in higher-level custom IP.

In the case where it is not possible to obtain the compliance artifacts from the vendor or a third-party provider, combining these methods might make it possible for the developer to employ COTS IP in level A and B applications. Conceptual and detailed design of custom IP can be completed down to the COTS IP level, treating any COTS IP as a black box. Requirements can be allocated to the COTS IP, and these requirements can be verified through black-box simulation and board-level testing, including corner cases. Architectural mitigation can be used to enhance robustness as appropriate. Service history can then be used in conjunction with the extensive black-box testing and architectural mitigation to substantiate the equivalent level of safety for the COTS IP in level A and B applications in lieu of code coverage and detailed vendor life cycle data. These methods of employing COTS IP are consistent with the guidance provided in sections 11.2 and 11.3 of DO-254 [Ref 4]. However, a fully compliant DO-254 process, or equivalent alternate means of compliance, must be applied at the custom application level that incorporates the COTS IP.

Custom IP as an Alternative Route

The requirements of design assurance to meet DO-254 can push some programs to decide to just design their own IP, rather than manage the COTS IP through the alternative means of certification. However, there are some questions that arise with this approach:

- Is an internally developed IP (for example, a TEMAC) going to be more robust than its COTS equivalent used by a broad market? Is it plausible for broadly focused avionics design engineers to develop more robust specialized IP solutions than the specialists within an FPGA or ASSP device company? Xilinx utilizes specialized IP teams for each family of IP (memory, DSP, transceivers, etc.), and these developers have deep insight into the device-level hardware.
- Does the industry want each integrator to develop custom IP or modify COTS source code destined for its avionics application, or is it preferable to use COTS IP with alternate means of compliance?

The risks of developing custom IP solely as means of achieving DO-254 design assurance should be considered in contrast to using equivalent COTS IP with the methods of reverse engineering, extensive testing and analysis, and architectural mitigation.

Decoding Use of DO-254 and DO-178 in FPGAs

The inherent qualities of FPGAs allow for great flexibility in systems design. FPGAs have relatively quick and inexpensive development cycles when compared with ASICs. While an FPGA can be a design engineer's panacea for many systems issues, for the certification authorities, an FPGA can be a real challenge.

In the past, FPGAs tended to serve as interconnect logic, interfacing between various systems components. Today, the FPGA is more advanced and sophisticated allowing for ultra-high-speed signal interfaces and high-performance DSP capability. Many FPGA platforms now incorporate soft or hard IP, including soft or hard microprocessors. Gate counts have increased astronomically, and with this, the design teams have become larger. The use of COTS IP has become ubiquitous, and the overall complexity has skyrocketed. For these reasons, it is necessary to focus on the FPGA as a system within a system, hence the application of DO-254 to FPGAs. But it is still important to remember that an FPGA is part of a larger system where board or system-level mitigation can be used.

Figure 2 classifies hard and soft IP that can be employed within a custom FPGA design. The FPGA is shown with both hard IP and customizable/programmable FPGA logic. In addition, Figure 2 shows different types of soft IP that might be designed into the programmable FPGA logic as well as drawing boundaries to show where DO-254 and DO-178 apply. In Figure 2, rounded shapes represent areas of applicability with regard to DO-254 IP. Overlapping regions require application of DO-254 and DO-178, where gray shading represents DO-254 and white shading represents DO-178.

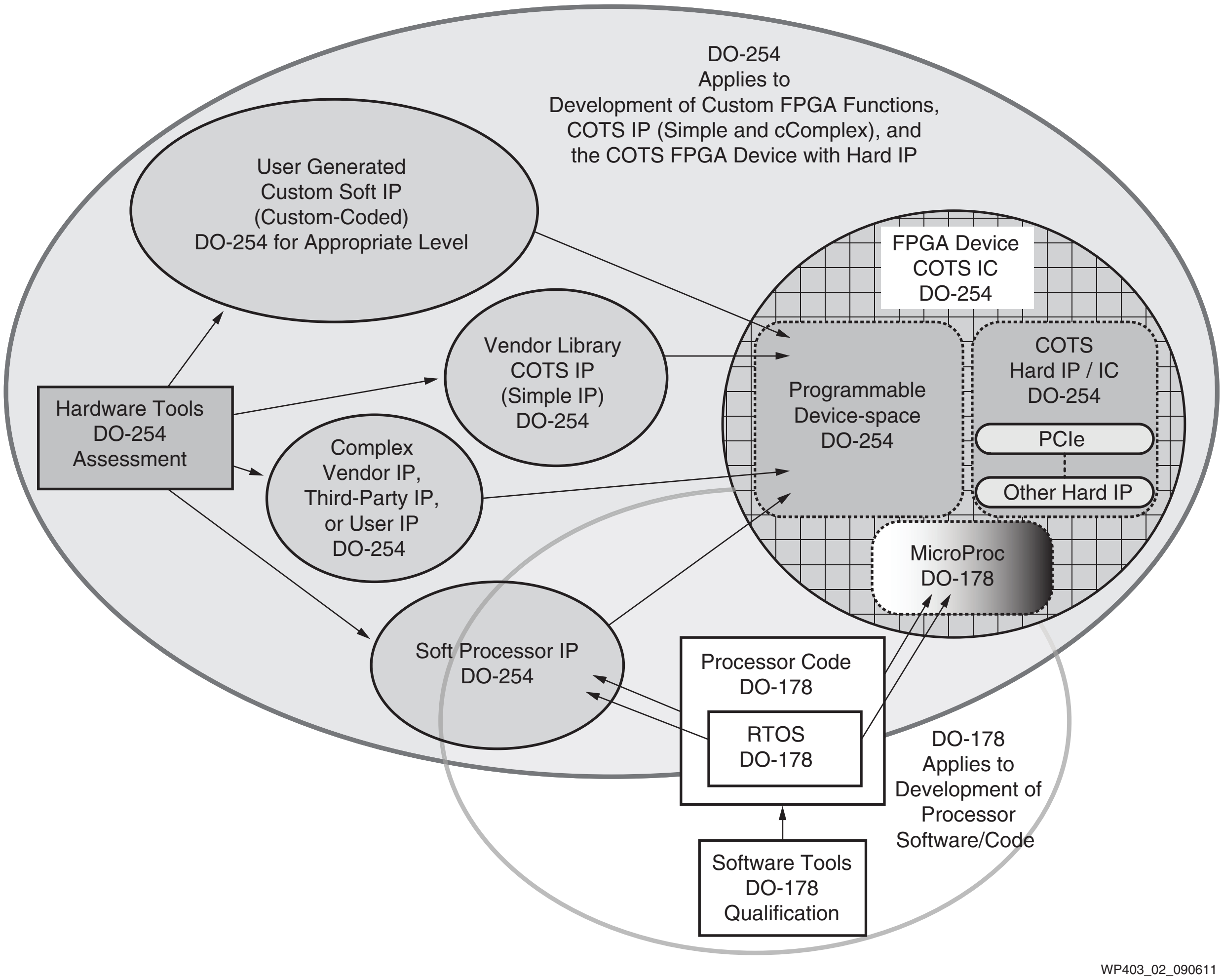

Figure 2: **Relevance of DO-254 and DO-178 to FPGAs and COTS IP**

FPGA Logic

The FPGA logic consists of hard IP elements and interconnects that are configured according to the user design. This device fabric is constructed of hard IP elements. A final customized FPGA design, including all custom and COTS soft and firm IP, is placed and routed then programmed into the FPGA logic. Current DO-254 guidance clearly applies to custom (user-generated) FPGA IP, which is finally implemented and verified in the device fabric. Custom generated IP must be fully compliant with DO-254. For more details on DO-254 design process, see *DO-254 for the FPGA Designer* [Ref 6].

What is less commonly addressed and understood is how COTS IP is integrated into a custom FPGA design alongside custom IP.

FPGA Hard IP

FPGA hard IP falls under DO-254 and should be considered and employed as a COTS device by the FPGA designer. COTS hard IP can be simulated as a black box at the design level, and then verified during hardware testing and qualification phases. See DO-254 Interpretations - The COTS Status of FPGAs.

Any ASIC, ASSP, or FPGA IP must be verified in the end-item avionic hardware, whether it is considered a COTS device or not, regardless of DAL. Architectural mitigations to cover broader failure modes of COTS IP can also be employed (and based on a safety assessment, it may be required). Fail-safe design architectures should be considered in all applications. COTS device quality and reliability should be broadly assessed under supporting hardware design processes, which include supplier qualification processes.

With broad COTS assessment in conjunction with system design assurance plans and requirements based verification, a program can justify the use of commercially available hard IP that is embedded in the COTS FPGA device. DO-254 development processes are not necessary for devices that have seen successful volume use across a broad range of markets or products. IP in this category includes DCMs, PLLs, PCIe endpoint blocks, high-speed transceivers, etc. A hard microprocessor is a special case: under DO-254 it can be considered a COTS device, but under DO-178, it requires additional qualification (these are two distinct and separate issues).

FPGA Vendor Library COTS IP

Vendor library COTS IP is similar to the hard IP. Its use is governed by DO-254, but exactly how the IP is approved under DO-254 is somewhat vague (see Vendor Library IP). Generally, a vendor library consists of relatively simple building-block IP—a DSP block implements a transfer function; a memory is easy to understand and it is simple in operation. This type of IP is certifiable based on service history in conjunction with requirements based black-box simulation as well as system-level verification and use within the vendor's guidance.

Complex and Specialized COTS IP

Current guidance draws a boundary between simple and complex IP, defining simple IP as having functionality where it is possible to comprehensively simulate all input and output scenarios. All other IP is then defined as complex. Under strict interpretations of DO-254, COTS IP deemed to be complex must be designed per DO-254 processes (i.e., access to the source code is required).

A more practical approach is to determine the dividing line based not on the ability to simulate all conditions, but rather on how understandable the function and structure of the IP is. A new classification based on the word obscure (relatively unknown or unclear, difficult to understand) can be used. For example, neither a DSP block, which has an associated transfer function, nor a multi-port memory which is easily comprehensible, is obscure. With this dividing line, non-obscure IP can be handled in the same manner as simple IP (simulated and verified as a black box in the user design, used in compliance with vendor guidelines, and its design assurance based on service experience, requirements based verification, and possibly architectural mitigation). More complex IP, such as a TEMAC or integrated Endpoint for PCIe, can be more debatable, but these vendor IP blocks have such wide use that they too should be considered to be COTS IP if sufficient volume use can be proven. On the other hand, avionics-specific IP such as avionics full-duplex Ethernet (AFDX) or ARINC 818

IP are not broadly used, and are thus obscure and require a full DO-254 certification package.

Custom IP

This case is relatively straight forward: Custom-generated IP that is targeted for a specific application must be fully compliant with DO-254 (also see FPGA Logic).

Processor IP

FPGA-based soft processors implemented in HDL as either soft or firm IP must be placed and routed for the FPGA. These soft processors should be developed or reassessed under a DO-254 compliant process because they are complex IPs. The processor implementation also requires DO-178 qualification. In contrast, hard processors embedded in device silicon do not require a fully compliant DO-254 process as they are standard COTS devices. These hard processors should be used on the basis of service history and qualification under DO-178.

Any object code written for soft or hard processors implemented in an FPGA or ASIC/ASSP require application of DO-178 compliant code development process. Likewise, the use of an RTOS is governed under DO-178.

Decision Flow for IP Used in DO-254 FPGA Designs

The diagram in Figure 3 allows a user to easily determine the best path for qualifying FPGA IP. When considering the flow diagram, use the following definitions.

IP can refer to soft, firm, or hard IP. Soft IP requires user synthesis as well as full place and route. Firm IP is pre-synthesized and requires only place and route in the user design. Hard IP is embedded in the device silicon and can require configuration but it does not require synthesis or place and route.

Service history threshold for COTS IP is 10 million hours of use across a broad industry and/or product base. This number is greater than or equal to that given in existing guidance but includes usage in markets beyond avionics that are also concerned with reliability. (Xilinx provides justification for its device IP upon request.)

Non-Obscure IP, whether simple or complex, is comprehensible or widely understood.

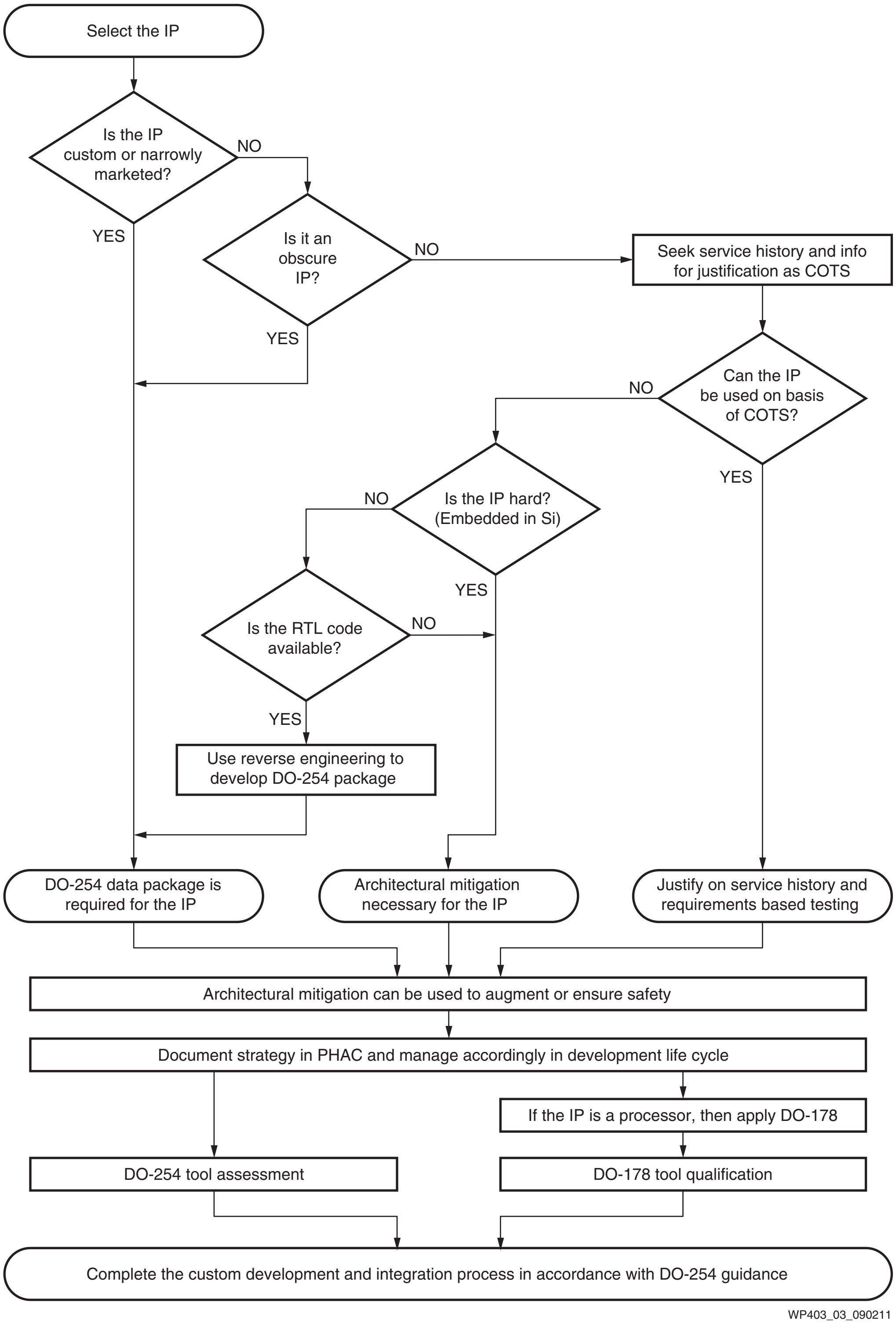
Select the IP
Is the IP custom or narrowly marketed?
NO
YES
Is it an obscure IP?
NO
YES
Seek service history and info for justification as COTS
Can the IP be used on basis of COTS?
NO
YES
Is the IP hard? (Embedded in Si)
NO
YES
Is the RTL code available?
NO
YES
Use reverse engineering to develop DO-254 package
DO-254 data package is required for the IP
Architectural mitigation necessary for the IP
Justify on service history and requirements based testing
Architectural mitigation can be used to augment or ensure safety
Document strategy in PHAC and manage accordingly in development life cycle
If the IP is a processor, then apply DO-178
DO-254 tool assessment
DO-178 tool qualification
Complete the custom development and integration process in accordance with DO-254 guidance
WP403_03_090211

Figure 3: **Decision Flow for IP Use in DO-254 FPGA Designs**

Development Process and Tool Assessment

For a description of standard DO-254 development process and FPGA tool assessment, see Xilinx WP401, *DO-254 for the FPGA Designer* [Ref 6].

Conclusion

There are significant variations in the current interpretation and application of DO-254 for FPGA developments targeting airborne applications. Acknowledging and accepting that some variation of interpretation will always exist is of benefit for the avionics community. The methods and definitions proposed in this white paper allow for greater consistency and efficiency in the way FPGAs are employed in DO-254 systems, ultimately leading to a more practical and effective application of DO-254. These proposals allow the industry to spend more time focused on areas of greater criticality, such as requirements validation and verification at the device and system level, with a higher degree of system-level focus.

There will always be the expectation that a fully compliant DO-254 process be used and that all of the objective evidence of compliance be made available. But the FAA acknowledges that it is necessary to rely on good judgment when it is impractical to cover all situations or conditions [Ref 3]. In cases where compliance data is not available, the integrator must provide an alternate means of compliance, such as service history, architectural mitigation, and reverse engineering. These alternative means of compliance should only be used to demonstrate an equivalent level of safety for specific DO-254 objectives (i.e., elemental analysis) that cannot be met by normal means. Nevertheless, a fully compliant DO-254 process should always be applied to the top-level custom FPGA design.

Xilinx works with customers and industry to solve DO-254 certification challenges. Compliance data artifacts for select IP can be obtained via license through some of our IP partners. CORE Generator™ interface IP service history requests can be made through your Xilinx sales representative. Visit the Xilinx Avionics website (http://www.xilinx.com/applications/aerospace-and-defense/avionics/index.htm) for more information.

References

1. FAA AC 20-152, Advisory Circular on RTCA/DO-254, Design Guidance for Airborne Electronic Hardware
2. FAA Order 8110.105 CHG 1, Simple And Complex Electronic Hardware Approval Guidance
3. EASA Proposed CM: SWCEH - 001 Issue No. 01, Development Assurance of Airborne Electronic Hardware
4. RTCA/DO-254, Design Assurance Guidance For Airborne Electronic Hardware
5. UG116, Xilinx Device Reliability Report
6. WP401, DO-254 for the FPGA Designer

Revision History

The following table shows the revision history for this document:

Date	Version	Description of Revisions
09/08/11	1.0	Initial Xilinx release.

Notice of Disclaimer

The information disclosed to you hereunder (the "Materials") is provided solely for the selection and use of Xilinx products. To the maximum extent permitted by applicable law: (1) Materials are made available "AS IS" and with all faults, Xilinx hereby DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, OR FITNESS FOR ANY PARTICULAR PURPOSE; and (2) Xilinx shall not be liable (whether in contract or tort, including negligence, or under any other theory of liability) for any loss or damage of any kind or nature related to, arising under, or in connection with, the Materials (including your use of the Materials), including for any direct, indirect, special, incidental, or consequential loss or damage (including loss of data, profits, goodwill, or any type of loss or damage suffered as a result of any action brought by a third party) even if such damage or loss was reasonably foreseeable or Xilinx had been advised of the possibility of the same. Xilinx assumes no obligation to correct any errors contained in the Materials or to notify you of updates to the Materials or to product specifications. You may not reproduce, modify, distribute, or publicly display the Materials without prior written consent. Certain products are subject to the terms and conditions of the Limited Warranties which can be viewed at http://www.xilinx.com/warranty.htm; IP cores may be subject to warranty and support terms contained in a license issued to you by Xilinx. Xilinx products are not designed or intended to be fail-safe or for use in any application requiring fail-safe performance; you assume sole risk and liability for use of Xilinx products in Critical Applications: http://www.xilinx.com/warranty.htm#critapps.