DO254 User group, an industry initiative

Anne Sénéchal[1], Françoise Crestey[2]

1: Barco, President Kennedy Park - 8500 Kortrijk, Belgium
2: Rockwell-Collins France, 6 avenue Didier Daurat, 31700 Blagnac, France

Abstract: Facing the increasing use of complex electronic hardware for most of the safety critical aircraft functions, a joint RTCA/EUROCAE committee elaborated and released, in 2000, the first standard applicable to hardware development : DO-254/ED-80 « Design assurance guidance for airborne electronic hardware » standard. This document, providing guidance on design assurance activities, became the standard to design hardware components like FPGAs, ASICs and other PLD components, mandatory for certification of civil aircraft programs.

In 2004, several European avionic companies decided to collaborate on application of DO-254/ED-80, and created DO-254/ED-80 User Group. Objectives shared by members were to clarify DO-254/ED-80 recommendations, define "industry" practices compliant with certification objectives, share good or bad experiences and practices, and also propose industrial feedback to certification authorities.

This paper presents the DO254 User Group. Two members companies Barco and Rockwell Collins are sharing their experiences with DO254 and the User group, and develop their interest through such an initiative.

Keywords: certification, safety, DO-254/ED-80, Hardware Design and Verification

1. Introduction

The use of increasingly complex electronic hardware for most of the safety critical aircraft functions generates new safety and certification challenges. These challenges arise from a concern that aircraft functions may be more and more vulnerable to the adverse effects of hardware design errors which become difficult to manage due to the increasing complexity of the hardware. To counteract this perceived increased risk it has become necessary to ensure that the potential for hardware design errors is addressed in a more consistent and verifiable manner during both the design and certification processes.
In April 2000, a joint RTCA/EUROCAE committee released the DO-254/ED-80 "Design assurance guidance for airborne electronic hardware" document, in which guidance resides on conducting design assurance activities along hardware development process.
Today, the DO-254/ED-80 compliance is mandatory for aircraft programs, DO-254/ED-80 application being required by Airworthiness Authorities (for example by FAA AC 20-152) and customer directives.
This document is now the standard for the design of hardware components like FPGAs, ASICs and other PLD components.
European aircraft manufacturers have been applying DO-254/ED-80 during their development activities on most of the recent programs.
As mentioned before, the standard, released in 2000, was the first standard applicable to hardware.

2. DO-254 and User Group origins

Although giving recommendations for hardware design process, the DO-254 standard created quite a number of clarification needs, which were emphasized by the fact that misinterpretations could finally result in safety issues, and in unacceptable extra costs.

Founding of DO254 User Group

In 2004 a number of companies decided to collaborate and join efforts to climb the learning curve. The initiative started with 13 companies around a common objective "Have a clear and common understanding of the DO-254/ED-80 objectives and processes".

For avionic industrials it is indeed essential to be capable of converting standards into industrial processes compliant for certification activities. Actually the DO254 User Group created the opportunity to exchange good and "less good" experiences, challenge own practices and techniques, while respecting each other's technology discretion.
After few meetings to "get in touch", the companies involved quickly understood the benefits of such initiative. Sharing is consequently giving an opportunity to learn from others' experience, but also procuring a chance to provide feedback.

From time to time, members have shared feedback from audits with customers and Airworthiness

Authorities, thus having access to the kind of request or concerns that they would have to be prepared for.

Barco sharing experience and interest for DO254 User Group

Barco joined DO254 User Group since its creation in 2004 and is as such a founding member.

At start, for Barco, Avionics Display specialist, the main objective when new standard got released was to fully understand the new requirements, avoiding misinterpretation of terminology in order to obtain full compliance of its development process to the new standard. It is indeed essential on aircraft programs as also in other domains like automotive, to be first time right when designing the hardware as well as on certification aspects. Sharing feedbacks and clarification from authorities between User group members helped and accelerated each other's in getting knowledge and awareness.

The challenging part when having new standards for Barco as for other companies is to translate standards into concrete steps in the design and verification flow. Starting from plans elaboration, requirement capture & validation up to the details of formulating dedicated questions in checklists, all of these activities need to address the core essence or spirit of DO-254 standard.

For Barco, it was a crucial target at the time of User group's creation as its first DO-254 project was a level A Primary Flight Display for Honeywell. Flying today on Pilatus Aircraft PC12, this primary Flight Display has been successfully developed and certified with highest Design Assurance Level (DAL A)[1].

Understanding and anticipating the evolution of certification requests are key assets for Barco to prepare its future, upgrade its hardware development process, train its personnel.

Over the past few years, Barco has collected a successful DO-254 experience on various avionics programs like for instance on its multi-purpose display development in DO-254 DAL B, selected by Thales for ATR 600, Sikorsky S76D, Lockheed C130 and Dassault ATL2. Moreover with its Primary Flight Displays DAL A on Falcon900 and some coming platforms ongoing in certification process, Barco has consolidated its hardware "DO-254 compliant" process.

DO254 User group is also offering the possibility for experienced industrial companies to provide some feedbacks on DO-254 implementation, which (when converging) can result in proposal of new practices.

Distinction between Simple and Complex electronic Hardware is an example of topic on which User Group members expressed feedbacks, challenged their opinions and finally proposed some methodology by defining specific criteria for Simple/Complex electronic Hardware classification, used in the certification process.

Establishing a process and having it performed efficiently needs efforts for development teams, which have to adapt and constantly align their processes with technology evolution and also certification concerns.

DO-254 objectives and what is beyond the DO-254 document itself (Certification Review Items, Issue Papers, CAST guidance...) can represent important challenges for equipment suppliers and their subcontractors.

Exchanging feedback between industrial companies on audits with customers and Airworthiness Authorities eases independent Avionic display provider Barco, to speed up its process evolution towards the requests of aircraft manufacturers and certification authorities.

In addition to the civil aviation requests development process compliant to DO-254 has become attractive for military programs for safety aspects as well as for reliability objective. Barco is currently providing DO-254 compliant equipments on various military programs, such as the multifunctional display "Touch-screen Unit" developed for Agusta Westland selected by UK Royal Navy for its helicopter Merlin fleet..

3- DO254 User Group Evolution

User Group organization

DO254 User Group is currently composed of 35 members from aerospace companies, certification experts, components manufacturers. An exhaustive list of participants can be found on DO254 User Group Website (www.do254.com).

User Group meetings take place about four times a year, and are hosted by one company member. It is the occasion to share the progress per topic in plenary sessions.

[1] Note: Highest Design Assurance Level DAL A is requested to equipments or subsystems whose failure or anomalous behavior would result in a catastrophic failure condition for the aircraft. There are five system development assurance levels, A through E, corresponding to the five classes of failure conditions: catastrophic, hazardous/severe-major, major, minor and no effect.

Sub-groups have been constituted to particularly address specific hardware topics, being currently:

- Verification coverage in FPGA/ASICs development - What are the current verification practices and various combinations to fulfil 100% of functional coverage?
- IP/SOC – How to include them in a DO-254 project, what is needed from IP provider?
- Simple/Complex devices - What are the criteria for classifying a component as simple? What is the "minimum" verification flow associated for simple devices?
- COTS - How to get design assurance on these components?
- Reliability - How to know if components are produced in a reliable way? What are the inevitable key features to survey?
- Alternative methods - What are other current methods used for development and verification in a certification context?
- HDL design rules - Collecting careful practices to achieve safe design and avoid synthesis errors

Besides plenary meetings, each sub-group leader organizes necessary conference calls to work on specific guidance / lessons learnt papers. These working sessions, with additional e-mail exchanges among members, allow elaborating these papers, which are then submitted to the whole User Group during plenary meeting.

The Group is exclusively open to industrial companies (equipment suppliers or aircraft manufacturers). Other contributors like tool vendors, IP providers… can be concerned but usually it is more effective to invite them for specific topics, after preliminary discussion with them about their objectives.

The Group has reached a high level of maturity in the discussions. Newcomers are welcome when they can contribute and present:

- Experience on several DO-254 DAL A projects
- Experience of certification audits, and of several certification contexts like EASA/FAA,
- Technical capabilities for the topics and contexts discussed

In addition the company is supposed to allocate time for 3-4 meetings per year, in Europe, and to actively participate to subgroup discussions, through meetings and phone calls. The company member is also requested to write or review the different papers, presentations… for the User Group.

In 2009, Rockwell Collins joined the DO254 User Group and is sharing its interest and motivation to contribute to this organization.

Rockwell Collins sharing experience and interest for DO254 User Group

One of the first experiences of Rockwell Collins in term of DO254 hardware design is the development of first DAL A Ethernet Switch unit (AFDX) for Airbus A380. This development has been submitted to several audits conducted on hardware by European authorities JAA/CEAT. Afterwards, final approval was given at end of 2003, with a good appraisal from Airbus and CEAT.

In mid-2005, the FAA recognized the use of DO-254 via AC 20-152. Since this time, DO-254 findings of compliance have been generated for approximately 40 different equipment types including Air Data Computers, Displays, Radios and Navigation equipments. Among these, we can mention different versions of display for Eurocopter and Agusta Westland helicopters (equipments DAL A and C). These products, initially designed in years 1996-1997, were later modified under DO-254 application.

The hardware design process, which was already in place, has been evolving from that time, to reach DO-254 objectives, especially in term of process formalization and documentation production. For these equipments, demonstration for certification used product service experience and TSO authorization, and moreover, DO-254 process was applied on FPGA modification. Certification approvals were obtained for them in 2006-2007, from DGAC for Eurocopter Dauphin, and from ENAC for Agusta A109.

While not currently a requirement for all TSO equipments, since the 2005 time frame, Rockwell Collins has been proactively anticipating the introduction of DO-254 requirement in development of TSO equipments by including DO-254 compliance artifacts with the TSO applications.

Today, various hardware developments (around display, radar, navigation, communication systems) are in progress at RCF and/or RCI premises, applying DO-254 guidance. These projects concern DAL A, B, C equipments, with use of COTSs, and development or reuse of ASICs and HPLDs.

Over the past ten years, these various projects involving hardware development have contributed to give to Rockwell Collins a solid experience in term of DO-254 hardware development.

One big interest for a company like Rockwell Collins to participate to DO-254 user group is obviously the possibility to share experience with other avionic suppliers. It allows highlighting good practices (in term of both efficiency and compliance with DO-254), and defining some generic acceptable means to apply DO-254 on hardware development.

Discussing with hardware components/tools vendors is also profitable. On our side, we have the opportunity to present them our needs with regard to technical performance and application of DO-254. This can be then collated with their own requirements and constraints.

Linked to our own experiences (use of new technology, application of new regulation …), we can propose new hardware design topics. Working together with sharing of experiences and opinions on the introduction of these new topics in our hardware design can help us defining appropriate practices.
This can result in production of technical/process notes which will be then introduced into methodologies put in place by companies.

Finally, establishment of a liaison between DO-254 users Group and Airworthiness Authorities is very important. Giving them our problematic and our proposals in term of hardware development, and collecting their feedback with regard to the certification requirements and their potential evolution, will allow industries to move forward in an acceptable and efficient way in their conduction of hardware development processes compliant with DO-254.

New phase & activities for DO254 User Group

The DO254 User Group, having acquired a certain maturity in hardware certification process, is now entering a new phase. From fruitful discussions and work collaboration, industrial companies are elaborating some proposals on various technical subjects.

These proposals can be either oriented towards industry or more intended to certification organizations (CAST, certification authorities…) depending on the subject they address.

One pending proposal relates to the IP/SoC paper, intended for IP/SoC providers. Target of the paper is to ease their use in DO-254 projects by promoting somehow IP/SoC design practices. This paper will help to perform a gap analysis, promote design and verification activities and encourage the production of some necessary output data. Indeed, to use IPs in a DO-254 context, IP providers could contribute by giving access to IP-related data and/or by preparing DO254-oriented packages.

Thus the IP/SoC paper will also help IP providers to better understand what their avionic customer's challenges are.

Some other subjects are on the roadmap such as

- How to address robustness in design and test?
- Discuss what is not written in the document, underlying processes & key practices in HDL design & verification flows
- How to address or even integrate emerging technologies and techniques in a DO-254 context? …

DO254 User Group is swarming…in US

In 2007, the European DO254 User Group initiative was presented at the FAA Conference in New Orleans. It was well received and created some interests from FAA as well as from the US avionic industry. The year after, some European members (including Barco) were attending the first meeting launching the US DO254 User Group. Key US avionic companies with knowledgeable participants were already present, ready to contribute.

Since the challenges in the US and FAA context may differ from challenges in the European and EASA context, roadmaps are shared and activities are synchronized when necessary between EU and US groups.

The prepared proposals can be "challenged" when relevant by US industry, giving a wider impact and collection of feedbacks through European and US DO254 User Groups.

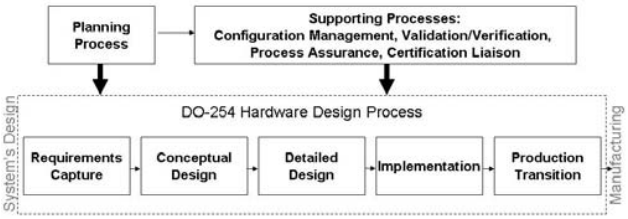
The work performed on HDL design rules, collecting practices and formulating a proposal of design rules set illustrates the cross-collaboration between the US and European User Groups. This package has already been implemented by some tools, what helps to perform effective verification of these rules. These coding guidelines have also been recently submitted to the CAST.

4- DO254 Standard in few words

The main concern which is at the origin of certification principle is Safety. The question is: how to ensure that avionics systems have been safely designed and manufactured? I.e. how to avoid design and manufacturing errors that could lead to occurrence of hazardous events? To cover problematic of design errors, different standards were jointly issued by US RTCA and European EUROCAE committees: ARP4754 at system level,

DO-178B at software level and DO-254 at hardware level. These guidance documents propose structured development processes allowing meeting the safety requirements emitted by Airworthiness Authorities.

The DO-254 document describes the hardware design life cycle processes, detailing objectives and activities associated to each phase of the life cycle (see Figure below).



One could say that among DO-254 processes, requirement is the kernel. Then each process is defined to "serve requirement".

Announcing upfront how product will be developed

Starting with planning process, DO-254 requests to define the methodology and the means to produce hardware items, which ones will have to satisfy System and Certification requirements. All development plans are the foundations of development and certification, and need to be released at start of product development cycle.

Defining "WHAT" has to be developed

Once having collected the system requirements, how will these requirements be flowed down to hardware level? The work consists in identifying and documenting the hardware requirements in accordance with the system requirements. The resulting hardware specification contains requirements inferred from system requirements, and derived requirements which are resulting from design decisions.

Requirements need to be carefully reviewed and validated to guarantee from start that they are adequate with the system safety and well responding to the target application of the product.

This validation allows identifying errors or omissions early in the development cycle, and thus reducing exposure to subsequent redesign or inadequate system performance.

During requirements validation, traceability is established between hardware requirements and system requirements, providing trace of how system requirements are covered at hardware level.

Describing Product architecture at Concept level

It is essential prior to rush upon HDL coding or board design that HW architecture is defined early in development phase. This concept phase obviously focuses on defining an architecture that allows to fulfil simultaneously all hardware requirements, while identifying reliability, maintenance and test features.

Designing and implementing Hardware in order to fulfil requirements

One can say that detailed design and Implementation processes are very close to most of HDL design house standard hardware development flows.

Indeed writing HDL code, synthesis and place & route steps are the heart of HDL design activity. Nevertheless, what guarantees that requirements have been completely and correctly implemented? Are the constraints files completely in line with requirements? Do they contain all conditions?

A way to get this confidence is to review HDL design with regard to hardware requirements, and to establish the traceability between these two steps.

Unused functions are also to be considered according to DO-254. It is mandatory to identify the potential effects on safety of the unused functions implemented in the product.

The next step called "implementation process" builds the physical hardware item according to its associated design data.

At the end of the hardware life cycle, the production transition phase establishes the baseline that includes all design and manufacturing data needed to support the consistent replication of the hardware item, in line with the key attributes of the unit on which the certification is based.

DO-254 also identifies several supporting processes, which are of a matter of importance to establish design assurance of the final hardware product.

Does the designed hardware meet its requirements?

The supporting process to answer this question is obviously called the verification process, whose objective is getting assurance that each level of the hardware design life cycle meets its specified requirements. It provides confirmation that the intended functions have been correctly implemented.

Verification is one of the key areas of concern within any project. As design grows, becoming more and more complex, verification is responsible for an increasing proportion of the design cycle. Moreover an ineffective verification methodology can result in

months or even years of debugging work in laboratory. Thus, establishing a verification methodology that catches more bugs, earlier in the design process, and reduces debugging time in the lab, should be the goal for any project.

Today, elsewhere in industry, electronics companies are adopting a whole breed of verification technologies to ensure a high quality of results as well as more productive and efficient verification process.

Avionic domain with DO-254 adds a strong but powerful request: the independence of verification. Despite sometimes the effort it demands, getting "new eyes" in a review, using an independent verification or analysis tool in a flow, can procure a considerable added value. For DAL A&B Hardware development, independence is mandatory in verification activities.

To get insurance that performed verification correctly and completely covers the hardware requirements, reviews should be organized, and traceability should be established between hardware requirements and the verification procedures and results.

Are the development tools bug-free? Are the tools telling the truth?

Tool assessment is another challenging area of DO-254 that occurs alongside each step in the development methodology. Any time a life cycle task is automated, reduced or eliminated, the tool that takes over this work must go through a process called "tool assessment and qualification". The purpose of this assessment is to ensure that the tools used to design, generate or verify the hardware don't introduce any error in the hardware or don't corrupt verification results.

What is released? Which release is applicable? What are the changes since previous release?

Configuration management process provides a technical and an administrative control of the configuration. It allows controlling the changes of the equipment/component and associated relevant documentation, and gives assurance that physical archiving, recovery, and control are maintained for documentation. Especially, version management is used for hardware design files. Typically, tools used for configuration management run the entire project, including the hardware, software, and parts systems.

Who guarantee that the development has been done according to the plans?

Avionic company who pretends to certify products shall perform process assurance activities, which consists on verifying that each process has been performed according to the plan. Organization of audits, identification of non-compliances and/or inadequacies and follow up of actions contribute to this process.

Get the Hardware certified!

Certification liaison consists in establishing communication and understanding between the company (air framer or equipment supplier) and the certification authority. This includes approval by certification authority of certification data (like hardware certification plan).

The certification is the legal recognition by the certification authority that a product, service, organization or person complies with the requirements. For avionic certification, to reach this recognition, airworthiness authorities conduct audits at various steps of the development process. In this frame, specific audits are conducted on hardware processes to assess their compliance with DO-254 and associated regulations.

For a company manufacturing hardware equipments and components, compliance with DO-254 standard implies finding acceptable ways of meeting the objectives of each phase of the DO-254 life cycle. Indeed, the challenge for companies is to manage maintaining profitability, while setting up and applying a methodology compliant with DO-254 recommendations. One interest of DO254 User Group is precisely to help companies defining appropriate methodologies.

5. Conclusion

This DO254 User Group is a great success, and has been recognized internationally as a model to use when new standards are released. There is no fee to join, and each member contributes and benefits from the quality of the exchanges among a large number of stakeholders.

Work performed by the DO-254/ED-80 Users Group over the years has provided real interest for industrial companies (avionics suppliers, components manufacturers …).

Based on the success of the DO254 User Group, similar initiatives for the DO178C and ARP4754A are currently being prepared[2] as these updates will be released soon.

[2] For more information, refer to Certification Together website (www.certification-together.com)

6. Acknowledgement

The authors acknowledge the contribution of Lionel Burgaud, chairman of DO254 User Group, who provided some input data for this paper.

7. References

[1] DO254/ED-80 Authors: RTCA/EUROCAE, "*Design Assurance Guidance for Airborne Electronic Hardware*", April 19, 2000.

[2] DO254 User Group website: www.do254.com

[3] Certification Together website: www.certification-together.com

8. Glossary

AC : Advisory Circular
AFDX : Avionics Full DupleX
COTS : Component Off The Shelf
DAL : Design Assurance Level
EASA : European Aviation Safety Agency
FAA : Federal Aviation Administration
IP : Intellectual Property
HDL : Hardware Description Language
HW : Hardware
PDF : Portable Document Format
PLD : Programmable Logic Device
RC : Rockwell Collins
RCF : Rockwell Collins France
RCI : Rockwell Collins Inc.
SOC : System On Chip
TSO : Technical Standard Order