New safety critical radio altimeter for Airbus and related design flow

HAIRION D., EMERIAU S., COMBOT E., SARLOTTE M.
THALES Communications,
160 bd de Valmy, 92704 Colombes, France
david.hairion@fr.thalesgroup.com
simon.emeriau@fr.thalesgroup.com

Abstract

The latest generation of the ERT560 Digital Radio Altimeter (DRA) developed for the Airbus A380 is the result of Thales' 40 years experience. Over 40,000 radio-altimeters have been produced over that period based on dual technology, meeting the stringent requirements of the civil aircraft. This new version takes advantages of the FPGA technology to implement the main treatment of the equipment.

The present article introduces the main capabilities of the ERT560 product and focus on the FPGA which is the key element of the safety critical analysis of the radio-altimeter. Then the paper presents the application of the new "design Assurance guidance for Airborne Electronic Hardware (DO254) which has been raised in 2000 (this guide is the equivalent for the HW of the DO178B for the SW). DO254 related activities are mainly developed such as a dedicated workflow, validation (give evidence of the completeness and correctness of all design life cycle outputs) and verification (evaluation of an implementation of requirements to determine that they have been met) and also verification tool qualification.

1. Introduction

The unique Thales approach - FM/CW modulation with a slope controlled by height (altitude) featuring superior Spectrum Leading Edge Detection (SLED) and tracking of the nearest point on the ground and with exceptional ECCM/Stealth performance. These advanced digital signal processing (terrain following, optimized spectrum analysis algorithms) require some customization and tuning to cope with the aircraft characteristics (antenna installation for instance). These flexibility required during the engineering phase is one of the main reason of the FPGA implementation.

The purpose of this paper is to highlight additional activities required to develop this safety critical FPGA to fulfill the certification requirement. The main role of the radio altimeter is to provide the height of the aircraft and is mainly used during the landing phase. A defect or a failure of this equipment could lead to the aircraft loss and classify therefore this equipment as critical and impose the highest design assurance level of the DO254 (DAL A).

After a quick overview of the ERT560 DRA product, the used workflow is detailed including development milestones, certification liaison, FPGA design flow, quality assurance process, configuration management process, tool qualification process.

2. Product overview

2.1. Product capabilities

Thales radio-altimeters use up to date digital technologies in signal generation and signal processing, providing a wide range of operational benefits, which are resulting in an important improvement in the safety and reliability.

First of all, digital signal processing nearly eliminates bright spot phenomenon and antenna coupling effects. It also reduces detection of over-flown aircraft, and rain echoes effects.

In addition, the ERT560 DRA design enables, among others benefits an efficient BITE performing installation status check of the unit. The ERT560 DRA has a dual dissymmetrical architecture to support CATIIIB landing. The figure below explain briefly the role of the DRA and its usage.

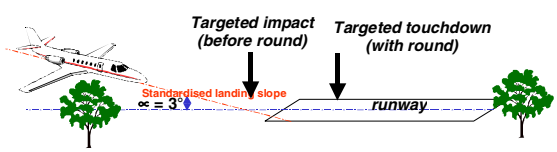

Figure 1: landing phase

2.2. Safety consideration

As a classical approach in safety critical system, an aircraft integrates two or three DRA in order to be able to cope with a failure of one the equipment. Furthermore, each DRA includes locally a redundancy and some mechanism to filter any "non

978-3-9810801-2-4/DATE07 © 2007 EDAA

consolidated height" in order to be sure that all the information provided to the global system (and finally to the pilot) is correct. The solution adopted within the DRA is the integration of two dissymetric channels with different technology implementation: a FPGA on main channel (CMD) and a DSP on second channel (MON). The two processor channels are based on different language and conception to perform redundant radar altimeter functions : the CMD channel is made out of a FPGA coded in VHDL and microcode, and the MON channel is made out of a DSP coded mainly in C and some part in Assembly language (mainly the drivers and the signal processing).
The two CMD and MON sections are developed by two different teams and the independence of the development team are reached.

Design Assurance Guidance For Airborne Electronic Hardware (DO254) for CoMmanD section and Software Considerations in Airborne Systems and Equipment Certification (DO178B) for MONitor section are applicable.

In addition, specific CRIs (Certification Review Item) regarding Complex component, Embedded software configuration files, Management of software open problem reports are applied during all the development process.

The workflow detailed below is related to the FPGA development.

3. FPGA Workflow

3.1. Design Assurance Level

There are five system development assurance levels defined in DO254, Level A through Level E, corresponding to the five classes of failure conditions: catastrophic, hazardous/severe major, major, minor and no effect.

As previously explained and according to the critical functionalities of this FPGA, it is classified as a DO254 DAL A component.

3.2. Development milestones

Hereafter the main development milestones and the beginning of phase criterions.

- Plan : FPGA planning process is established,
- Requirements capture : FPGA Requirement Specification (FRS) is written according to the above "functional base line" (FBL),
- Preliminary Design : FPGA Design document (FDD) are written declined from the FRS, the FPGA Test Document (FTD-HL) is established to verify the FRS level,
- Detailed Design & Low level verification : Implementation into VHDL and microcode languages, the FPGA Test Document (FTD-LL) is established to verify the FDD level, the FPGA Test Report (FTR-LL) is available,
- Implementation & High level verification : Bitstream is produced, the FPGA Test Report (FTR-HL) is available,
- Delivery, support and certification : The FPGA Version Description Document (VDD) and the FPGA Accomplishment Summary (FAS) established.

3.3. Certification liaison

The certification liaison activities are handled by the certification and system expert of the ERT-560 DRA transceiver.

The purpose of the certification liaison process is to :

- establish communication and understanding between THALES Communication and the certification authorities throughout the different phases of the FPGA life cycle to assist in the certification process.
- demonstrate that the FPGA complies with the DO254 recommendations.

Associated activities include:

- elaborate the FPGA Test Plan (FTP), Plan for FPGA Aspects of Certification (PFAC) and FPGA Configuration Management Plan (FCMP),
- submit the documents to the certification authorities with the interface of the aircraft manufacturer,
- participate to the Certification Authorities reviews,
- elaborate new versions of the documents taking into account the certification authorities remarks provided with the interface of the aircraft manufacturer,
- obtain approval of these documents with the interface of the aircraft manufacturer.

At the completion of the FPGA development, a summary of the design processes followed, outputs produced and status of the FPGA is described in the FPGA Accomplishment Summary (FAS).

The FAS is submitted to the certification authorities (DGAC) for approval with the interface of the aircraft manufacturer and other readable data or evidence of compliance requested by the

certification authority are provided or made available to the certification authority with the interface of the aircraft manufacturer.
The primary objective of the FAS is to show the certification authority compliance to the PFAC and justify the possible shift.

The FAS document is updated in case of major modifications. The new document version is edited and transmitted to the customer and/or certification authority for next end of phase review.

3.4. FPGA Design Flow

The FPGA Development Environment (FDE) is a set of scripts that manage both FPGA Design flow (synthesis and place-and-route) and associated Configuration Management for the FPGA.
This design environment has been especially developed by THALES to ensure DO254 requirements and has been adapted from the standard internal workbench..

The global design flow uses a routing strategy that consists in synthesizing the 5 partitions and the top level and then routing the FPGA, as depicted on the following scheme:

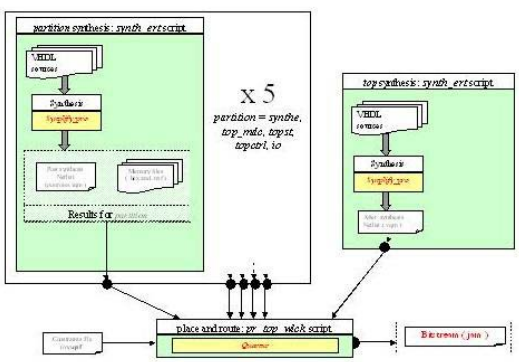

Figure 2: FPGA Design Flow

For this flow, the FDE provides 2 main scripts to perform synthesis and top level place and route with associated configuration management:
· performs the synthesis of a partition (coherent group of function) or of the top
· performs the place and route

Synplify_Pro tool is used for synthesis. Place and route is performed using Quartus-II tool.

3.5. Implementation

The aim of the VHDL implementation is to translate the FPGA design description (FDD) into the VHDL format.

The FPGA shall be coded in VHDL following the FPGA Requirements and design rules document. Each function shall be associated with the traceability to the FDD numbered requirement for which it has been coded.

3.6. Validation activities

The aim of the validation activities, is to give evidence of the completeness and correctness of all design life cycle outputs. The validation activities consists to check a subset of defined criteria by a peer. Those peer reviews are consigned into a "Inspection report" (IR). Common and specific criteria are defined inside IR document.

Completeness means:
- the item will satisfy the rules (coding & writing),
- all related requirements are fully considered.

Correctness means:
- the item is coherent,
- the item is unambiguous, realizable and in accordance with the addressed requirement.

Validation can identify subtle errors or omissions early in the development cycle and reduce exposure to subsequent redesign or inadequate FPGA performance.

Hereafter all the validation performed during the FPGA life cycle.

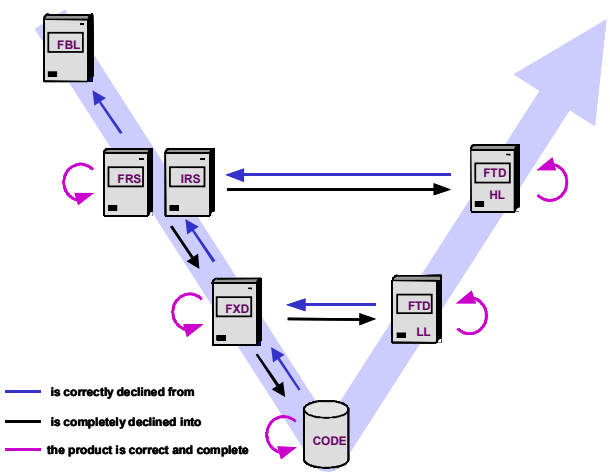

Figure 3: Validation activities

About FTD-HL, in many cases each requirement is verified by a unique verification procedure. In that case the proof that verification procedure is

complete is integrated inside that procedure using color association. The Verification Completeness Report document (VCR) contain the completeness justification when a requirement is verified by several verification procedures.

Concerning FTD-LL the case of a requirement which is verified by several procedures do not exists. However, the proof that verification is complete is integrated inside that procedure using comments.

This activity is performed by the FPGA Development Team who is assisted by an independent Quality Manager for quality assurance aspect of DO254. Validation activities are performed with independence.
This activity is performed before any delivery.

3.7. Verification activities

The aim of the Verification is the evaluation of an implementation of requirements (act of creating a physical reality from a specification) to determine that they have been met.
By the use of verification tools, these activities guarantee:

- a fully functional coverage of requirements,
- a fully structural coverage of code products (branch, condition, statement, Expression)

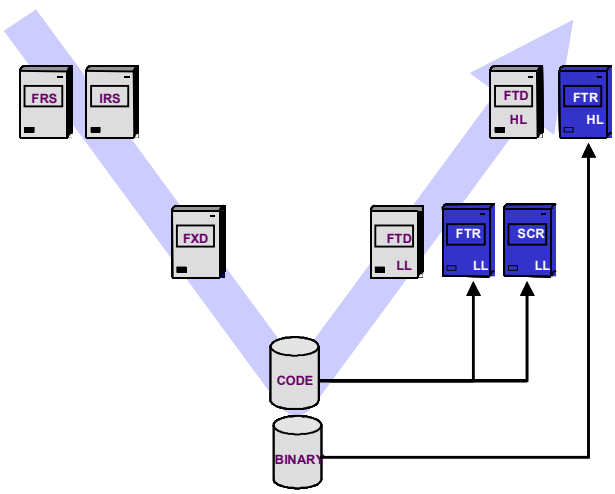

Figure 4: Verification activities

During the last phase and before any delivery to our customer, all verification procedures will be performed again.

It must be noted that as required by DO254 recommendations, some verification activities shall be performed with independence.

3.8. Functional coverage

As required in the DO254, each requirement level have to be fully covered by one or more verification method. The FPGA has two verification levels: FPGA Test Document High Level (FTD-HL) and FPGA Test Document Low Level (FTD-LL) associated to FPGA Requirement Specifications (FRS) and FPGA Design Document (FDD).
The two verification methods used are test and analysis.

3.9. Structural coverage

For both VHDL code and micro code, a structural dedicated tool generates a report on each category. If necessary an analysis is performed to justify uncovered branch, condition, statement or expression. Structural Coverage Report documents (SCR) contain all reports and justifications.

3.10. Quality assurance process

Objectives of Quality Assurance is to ensure life cycle processes comply with the approved plans, produced FPGA life cycle design data are compliant with approved plans.
The quality activities are performed by the FPGA Development Team who is assisted by an independent Quality Manager for quality assurance aspect of DO254.

The certification and system expert of the ERT560 DRA Transceiver takes part in reviews and audits based on the program activity. Audits have been scheduled to be done during the course of the development between two FPGA transitional reviews by the certification and system expert, when judged necessary. Their objective is to check the development baseline of the FPGA.

The certification and system expert is responsible of each main review closure. The compliance to the defined processes is a key item to close each main review. The description of each review or audit and of the assigned responsibilities shall be given.

3.11. Configuration management process

The FPGA development environment have been updated to include configuration management inside development tool to ensure that every generated version is identified with a unique tag. The FPGA Design Environment Tool (FDE) is a set

of scripts that manage both FPGA Design flow (synthesis and place-and-route) and associated Configuration Management for the ERT560 FPGA.

This activity is performed by the FPGA Development Team who is assisted by an independent Quality Manager for quality assurance aspect of DO254.

3.12. Tool qualification process

When design tools are used to generate the hardware item or the hardware design, an error in the tool could introduce an error in the hardware item.
When verification tools are used to verify the hardware item, an error in the tool may cause the tool to fail to detect an error in the hardware item or hardware design. Prior to the use of a tool, a tool qualification should be performed.

The purpose of tool qualification is to ensure that the tool is capable of performing the verification activity to an acceptable level of confidence for which the tool will be used.

The same methodology has been used for all the tools which are qualified for the FPGA:

- A specification calls TRS (Tools Requirements Specification) has been written in a requirements manner.
- A test description calls TTD (Tools Tests Description) which describes all the tests performed on the tool. A traceability is established with the TRS.
- A Test report calls TTR (Tools Tests Report) which gathers all the results of all the verification performed. A traceability is established with the TTD.

All the documents have been validated through peer review by using check lists included in the inspection reports.

4. Conclusions

As a conclusion, a safety critical FPGA implies a consequent methodology to be compliant with the certification requirement and the DO254 recommendation. The in-place process is generally at the C level (or close to) and should be extended with additional activities or practices to reach the A level of such critical development. The key element to succeed is the stability of the requirements before starting the other development phase in order to avoid costly iterations. The second point is the necessity to train people to complete their standard process knowledge with the complementary actions to be performed and also the safety consideration of such design.