RTCA/DO-254 COMMERCIAL-OFF-THE-SHELF GRAPHICAL PROCESSORS USAGE IN AIRBORNE DISPLAY SYSTEMS

Randall Fulton,
SoftwAir Assurance Inc.

Abstract

RTCA/DO-254 *Design Assurance Guidance for Airborne Electronic Hardware* [1] is a set of considerations or guidelines for the assurance of electronic hardware in the certification of a specific aircraft system. Additionally, the Federal Aviation Administration (FAA) Advisory Circular (AC) 20-152 [2] describes how applicants creating complex custom coded components programmable logic devices such as Field Programmable Gate Arrays (FPGA) and Application Specific Integrated Circuits (ASIC) can use DO-254 to comply with airworthiness regulations.

Section 11.2 of RTCA/DO-254 addresses the use of commercial off the shelf (COTS) components in safety critical aircraft systems. COTS components are commercially available devices such as a graphics processor, a microprocessor, a power supply assembly or a ruggedized processor board. Section 11.2 of RTCA/DO-254 outlines considerations for gaining certification credit for the use of COTS devices or subassemblies that were not designed exclusively for use in avionics systems.

The Certification Authorities Software Team has produced a position paper CAST-29 [3] regarding the use of COTS Graphical Processors (CGP) in Airborne Display Systems.

This paper discusses the use of CGP components in avionics systems and addresses DO-254 and CAST-29 related issues with particular emphasis on the data available from the CGP manufacturing process.

This paper does not cover the system safety aspects of using a CGP in an aircraft display system. The failure modes, hazards, and their mitigation in a display design need to be considered regardless of the technology selected. A display system design should thoroughly evaluate the impact of any selected technology and any functionality included in a CGP. The data from a CGP supplier, as described in this document, will support the safety and reliability analysis and demonstrate whether the device, when appropriately designed into the system, will operate correctly in the aircraft environment.

Introduction

Displays used in aircraft systems contain COTS parts. These parts are used to shorten the design time and reduce costs associated with custom hardware design and verification. Some examples include:

- graphics processor
- microprocessor
- processor board for integrated modular avionics

In real time embedded safety critical systems, consideration needs to be given to the contribution of a part or a system to functional hazards. These hazards are assessed at the aircraft level for their respective impact. For display systems, the most common hazards are hazardously misleading information (HMI) and loss of function. HMI is incorrect information on a display; loss of function is the result of loss of some or all of the display data (i.e. a blank display).

In order to more fully assess the use of COTS components, it is typically necessary to get data from the device manufacturer that demonstrates that the device is suitable for the avionics environment and meets the reliability and availability requirements. A CGP vendor is often the gateway to accessing the device manufacturer's foundry engineers and quality personnel who have access to the CGP qualification and manufacturing test data.

Certification Authority Position on the use of Graphics Processors in Airborne Displays

COTS graphics processors can be used for non safety related systems such as in flight entertainment and also in safety critical systems such as primary and secondary flight displays. Use of CGP in safety critical systems became an industry concern in the 2006 time frame.

The FAA and the international certification authorities have expressed their concerns regarding the use of COTS graphical processors in airborne display systems. The concerns and issues are described in Certification Authorities Software Team (CAST) Position Paper CAST-29, *Use of COTS Graphical Processors (CGP) in Airborne Display Systems*. CAST-29 specifics are discussed in a later Section in this paper.

RTCA/DO-254 COTS Considerations

Section 11.2 of RTCA/DO-254 addresses issues for COTS components usage. DO-254 acknowledges the extensive use of COTS components in electronic systems and discusses the basis for usage of these components. COTS components need to be verified through the overall system design process. This verification should include test coverage of the display and graphics functions during the requirements based testing.

An electronics component management process is also discussed as an extremely important supporting process under DO-254. Section 11.2.1 discusses certification credit that can be obtained from an electronics component management process. The four aspects of electronics component management process as applied to a CGP include:

- CGP manufacturer consistently demonstrates production of high quality components
- CGP manufacturer follows established quality control procedures
- Service experience demonstrates successful operation of the CGP
- The GCP component reliability is established by device qualification tests or other additional testing

An Electronics Component Management Plan (ECMP) implements the electronics component management process. An excellent resource for creating an ECMP is the International Electrotechnical Commission (IES) Technical Specification (TS) IEC TS 62239 - *Process management for avionics – Preparation of an electronic components management plan*. [4] Technical Specification 62239 outlines the technical requirements for electronic components and the administration requirements for the plan. The intended audience is avionics equipment manufacturers.

Acquisition of ECMP data for component qualification testing will require access to the CGP

designer, foundry and packaging house. The foundry and packaging is often performed off-shore and access to data and personnel is limited due to business concerns. A competent and knowledgeable CGP vendor will facilitate access to the data for a DO-254 COTS data package. In many cases, CGPs are designed by one company while manufacturing, packaging, and testing is outsourced to key companies in the semiconductor industry. Some of the data for the COTS data package would need to come from the graphics processor designer and the rest comes from their manufacturing fabrication and packaging resources. It is evident that it is the CGP vendor who is best suited to collecting this dispersed, but necessary data.

Evidence for the production of high quality components can be demonstrated in part by wafer fabrication qualification. Device qualification testing is performed on the packaged CGP and includes temperature cycling, moisture and life tests. These tests ensure suitable quality and reliability of CGP components. In particular, tests described in JEDEC Standard JESD22-A108-B, Temperature, Bias and Operating Life [5] are used in device failure rate and reliability prediction.

Foundry and packaging facilities often publish their quality and standards credentials on their website. Companies that fabricate and package CGP components should comply with International Standards Organization (ISO) specifications for manufacturing quality management systems.

Semiconductor Device Qualification

New device qualification consists of a series of tests that ensure that a device is capable of performing reliably under normal operating conditions over their expected operating lives. Device qualification includes failure rate requirements and conformance to visual, mechanical, and material requirements. The qualification tests also expose the packaged device to accelerated stress tests which evaluate design and fabrication process integrity. These tests subject the device to the mechanical stresses typically encountered during incoming inspection and manufacturing assembly. The manufacturability tests include lead straightening and automatic insertion operation tests. The device qualification typically follows one of several industry standard suites of tests:

- EIA/JESD47 - Stress-Test-Driven Qualification of Integrated Circuits [6]
- STACK 0001 - General Requirements for Integrated Circuits and Discrete Semiconductors [7]
- GEIA-STD-0002-1 Aerospace Qualified Electronic Component (AQEC) Requirements, Volume 1 – Integrated Circuits and Semiconductors [8]
- AEC-Q100 Stress Test Qualification for Integrated Circuits [9]

Quality or reliability monitor tests can be set up on periodic cycles to ensure the quality of the production of the die.

CAST-29 Considerations

The certification authorities team that produced CAST-29 listed the issues that may arise from the use of CGPs in airborne display systems. The issues include:

- Use of DO-254/ED-80
- Possible CGP contribution to Hazardously Misleading Information (HMI) on Airborne Display Systems
- Display System Availability
- CGP Device Variations during Production Life
- CGP Configurable Elements
- CGP Device Changes after Initial Certification
- Unused CGP Functionality
- Open GL Software Drivers Compliance to DO-178B/ED-12B

For the first bullet, it is always recommended that any certification approach be coordinated with the certification authority early in the lifecycle of the program. A meeting should be set up to discuss the use and applicability of DO-254/ED-80 and the approach for demonstrating that the CGP is suitable

for the environment and intended function. This meeting should be conducted before the design phase starts to ensure that all concerns and issues are addressed and to also ensure that the certification plan will be acceptable to all parties.

For the second bullet, the system will need architectural mitigation to protect against undetected Hazardously Misleading Information. The mitigation could include dissimilarity, such as different CGP devices, or monitors that can detect errors in the output display data.

The third bullet will depend on using CGPs that will operate correctly in the airborne environment. Devices need to be selected that are suitable for the intended operating temperature range and that will survive the system environmental qualification testing regime. Failure in time (FIT) and CGP reliability data should be derived from industry standard device qualification testing as discussed in previous sections. This data can also potentially be directly supplied by the CGP vendor.

The fourth bullet can be easily addressed by procuring the devices from a single fabrication run. Most fabrication runs take several weeks and produce 100,000 devices. The devices can be selected, packaged and stored, or the wafers can be nitrogen banked for subsequent packaging and testing. The device marking should show the fabrication date and die version. Any variation needs to be explained and justified by test. Hence, it is best to use devices from the same fabrication lot. When devices come from different fabrication runs, the die version should be checked to ensure that changes were not introduced in the device. The display manufacturer should deploy and enforce an Electronic Component Management Plan compliant with IEC TS 62239 as previously described. The ECMP should include change notification for any fabrication or packaging changes. Ongoing reliability testing can also be utilized to monitor device performance and behavior.The easiest approach to the fifth bullet is to eliminate the use of CGP microcode for shaders or other features. If microcode is used, the code must be compliant to RTCA/DO-178B [10] and mechanisms should be employed to ensure the version of the microcode is correct. System manufacturing and acceptance tests should verify the correct configuration and operation of any CGP microcode.

The sixth bullet can be addressed by procuring the devices from a single fabrication run as described in the commentary regarding the fourth bullet. When devices from different fabrication runs are used, care should be taken to ensure the photolithography masks were not changed. The display manufacturer should deploy and enforce an Electronic Component Management Plan compliant with IEC TS 62239 as previously described.

The seventh bullet can be addressed with several techniques including circuit design, proper termination of unused device pins, monitors to check or update critical CGP control registers, excluding access to CGP functions in the software driver, system test, software test, hardware test and robustness tests that demonstrate that the CGP performs its intended function of correctly displaying information under all foreseeable operating conditions.

The last bullet will require either writing a CGP driver compliant to RTCA/DO-178B or procuring a COTS OpenGL driver that is RTCA/DO-178B compliant.

Recommendations

The following questions should be asked of the CGP vendor before part selection is finalized:

- Is a Users Manuals available to graphics library or driver software developers?
    - Does the manual include a definition and description for all control registers? (In this context, “all” includes all relevant 2D and 3D rendering-related registers.)
    - Does the manual include a definition and description for all data registers? (In this context, “all” includes all relevant 2D and 3D rendering-related registers.)
    - Does the manual include a complete definition of microcode instructions and the relevant Instruction Set Architecture(s)?
- Is the device pin out and mechanical drawing, including dimensions, available?

- Are device functional and performance descriptions available?
- Does the vendor have the manufacturer's device qualification test results available?
- Is the device failure in time (FIT) rate specified?
- Is the device power consumption and dissipation and factors that influence it specified?
- Are the devices all from the same fabrication run?
    - Are all devices fabricated from the same photomask set?
    - Are all devices from the fabrication run packaged?
    - Are unpackaged devices stored in nitrogen bank or equivalent?
- Is a reference software driver available?
    - Is it OpenGL compatible?
    - Are requirements and design documents available for the driver?
- Is the errata sheet available?

Starting with the answers to these questions will go a long way towards ensuring that certification authorities' concerns can be addressed.

Summary

Choose a device from a manufacturer or distribution channel that makes the device qualification test results readily available. Ask for a summary report.

Coordinate with the system safety and reliability analysts to ensure that the data they need for the safety analysis is available.

Compliance with RTCA/DO-254 and the issues discussed in CAST-29 are achievable. There is a lot of work and planning necessary to ensure success. Early coordination in a certification program with the certification authority is recommended to ensure that all certification authority issues are addressed.

An Electronic Component Management Plan should be used for the selection, procurement and qualification of a CGP. The device qualification data will require behind the scenes access to CGP designer, foundry and packaging. This can be facilitated by the CGP vendor.

Start by asking the questions listed above and evaluate the data provided in response.

References

[1] RTCA/DO-254 Design Assurance Guidance for Airborne Electronic Hardware, 2000, RTCA, Inc.

[2] AC 20-152 RTCA, Inc. Document RTCA/DO-254 Design Assurance Guidance for Airborne Electronic Hardware, 2005, Federal Aviation Administration

[3] Certification Authorities Software Team (CAST) Position Paper CAST-29, Use of COTS Graphical Processors (CGP) in Airborne Display Systems, February 2007, Rev. 0

[4] IEC TS 62239 - Process management for avionics – Preparation of an electronic components management plan, International Electrotechnical Commission, First Edition 2003-05

[5] JEDEC Standard JESD22-A108-B, Temperature, Bias and Operating Life, JEDEC Solid State Technology Association 2000, December 2000

[6] JESD47D Stress-Test-Driven Qualification of Integrated Circuits, 2004, JEDEC Solid State Technology Association

[7] Stack 001 General Requirements for Integrated Circuits and Discrete Semiconductors, 2004, STACK International

[8] GEIA-STD-0002-1 Aerospace Qualified Electronic Component (AQEC) Requirements, Volume 1 – Integrated Circuits and Semiconductors, 2005, Government Electronics and Information Technology Association

[9] AEC-Q100 Stress Test Qualification for Integrated Circuits, 2003, Automotive Electronics Council

[10] RTCA/DO-178B Software Considerations in Airborne Systems and Equipment Certification, 1992, RTCA, Inc.