Certification Authorities Software Team (CAST)

Position Paper CAST-29

Use of COTS Graphical Processors (CGP) in Airborne Display Systems

COMPLETED February 2007

(Rev 0)

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

Use of COTS Graphical Processors (CGP) in Airborne Display Systems

1. Introduction

Commercial-Off-The-Shelf (COTS) Graphical Processors (CGP) are currently being used in airborne display systems. These devices represent a different class of devices than the COTS microprocessors being used in critical airborne applications. CGPs were designed for non-aerospace, graphics intensive applications, such as video games and computer graphics. Although hardware graphical processors have been available on the commercial market for many years, the latest generation of CGPs represent a substantial increase in the complexity of the device and the functionality the device is able to provide. As a result, more and more of the functionality of airborne display systems that was previously implemented in software running on the main system processor is now being implemented in these high speed hardware devices. These devices are now able to fulfill the needs of graphics intensive systems, such as Primary Flight Displays, contoured terrain displays, and enhanced or synthetic vision display systems.

These components have typically not been developed to the guidance of RTCA DO-254/EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware" or other design assurance standards recognized by international certification authorities. The typical CGP uses multiple embedded microprocessors that are running asynchronously and may contain 30 to 100 million transistors. A CGP cannot therefore be considered a simple device. Verification activities or use of reverse engineering techniques to make these devices DO-254/ED-80 compliant is highly problematic and, most likely, impractical. Due to the very rapid life cycle of these components, it is also very difficult to provide confidence that the device does not contain any design errors using service experience.

2.0 Certification Concerns and Issues with the use of CGPs

This following is a list of concerns and issues that *may* arise when CGPs are used in safety critical airborne display systems. The concerns and issues include, but may not be limited to, the items contained in the following paragraphs.

2.1 Use of DO-254/ED-80

DO-254/ED-80, paragraph 11.2 (Commercial-Off-The-Shelf Components Usage), states, "the use of COTS components will be verified through the overall design

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

process, including the supporting processes, as defined in this document." Although DO-254/ED-80 section 11.2 provides valuable information that could be used in assisting the applicant/system developer or avionics supplier in how to approach using a CGP in an airborne display application, the certification authority involved in the project may not currently recognize DO-254/ED-80 as an acceptable means of compliance when it is applied at the system level. Also, the applicant/system developer may not adequately address the design assurance of the complex COTS device if DO-254/ED-80 is applied at the system level only.

> **Note**: Please see CAST-27, "Clarifications on the Use of RTCA Document DO-254 and EUROCAE Document ED-80, *Design Assurance Guidance for Airborne Electronic Hardware*" for further information.

2.2 Possible CGP contribution to Hazardously Misleading Information (HMI) on Airborne Display Systems

One of the primary concerns involved in the development of an airborne display system is the potential for displaying Hazardously Misleading Information (HMI) to the flight crew. HMI could come in the form of incorrect or missing flight deck alerts, incorrect navigation or system status information, or "frozen data". If this erroneous information is not flagged as Invalid Data, it could induce the flight crew to make inappropriate and potentially hazardous actions based on that erroneous data, or not take appropriate actions when action is required.

CGPs could potentially contribute to HMI due to:

a. Hardware failures within the CGP.
b. Design errors within the CGP.
c. Failures or inappropriate responses to external events, such as EMI, lightning, high operating temperature, or "out of nominal" input power specifications.

> **Note**: The last two items in the list above include the potential for inducing HMI in multiple redundant displays simultaneously due to a common cause.

2.3 Display System Availability

The use of identical CGPs in multiple, redundant displays within an airborne display system could negatively impact the required availability of the display system, due to the possibility of generic design errors in the CGP or failures of multiple CGPs due to common causes. Additionally, architectural mitigations included in the design of the display system intending to prevent HMI can possibly reduce the availability of the display system if that architectural

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

mitigation is improperly designed and suffers from nuisance monitor trips (i.e., a monitor that is designed to detect a certain failure condition trips when no fault is actually present).

2.4 CGP Device Variations during Production Life

CGPs, depending on the type, complexity, and supplier, may exhibit performance variations across the production lifetime of the device. These variations may manifest themselves at temperature extremes, overvoltage conditions, or other abusive operating environmental conditions. Alternatively, these variations may not require any extreme operating condition to be revealed. These variations could have unexpected, adverse affects on the display system.

2.5 CGP Configurable Elements

Many CGPs contain configurable elements. Some of these may be selectable by loading specific microcode instructions into the device. This capability leads to concerns regarding the configuration control of the CGP installed in the display system.

2.6 CGP Device Changes after Initial Certification

The CGP part numbering, change control process, and revision identification scheme used by the individual CGP suppliers may not be understood by the system developer or applicant. In other words, each change of the CGP device that is significant to the system in which it is installed may not be reflected in the CGP part number.

2.7 Unused CGP Functionality

The CGP design may include functionality that will not be used in the specific design of the airborne display system that could result in unintended operation of the device if that function were to be activated under unusual operating conditions or failures.

2.8 Open GL Software Drivers Compliance to DO-178B/ED-12B

CGPs may require graphics software that allows functional applications to draw visual components on the display, e.g., a software package that implements the OpenGL (Graphics Library) graphics drivers and applications. The developer of the display system may not be the same company that develops the graphics software. In addition, the software graphics packages for the CGPs may not have

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

been developed to the guidance of DO-178B/ED-12B (or other acceptable means of compliance for software).

3.0 Certification Authorities' Position on use of CGPs

This section elaborates on issues and concerns identified in section 2 and provides a certification authorities' position on each.

3.1 Use of DO-254/ED-80

COTS Graphical Processors have been developed primarily for a non-aerospace, non-safety critical market. As such, it may be problematic, if not impossible, for an applicant or display system developer to obtain the requisite documentation necessary to show compliance to a design assurance process, such as the one contained in DO-254/ED-80. Therefore, reliance on a design assurance process for a CGP as an acceptable means of compliance will likely be very difficult to substantiate.

DO-254/ED-80 paragraphs 11.2 and 11.3 contain information regarding how a specific CGP device should be chosen for use in an airborne system, and how possible certification credit can be obtained by using the documented service experience of the device. Several of the main points made in those sections are summarized below:

1. Electronic component management principles apply to COTS devices. That is, concepts such as the supplier track record, quality control, establishment of device reliability, and the device suitability for intended use should all be taken into account when choosing a CGP.
2. The applicant/system developer should have plans to address probable issues such as lack of CGP device design assurance data, possible variations in device parameters from one production batch to the next, and eventual redesign or complete phase-out of that device by the CGP supplier.
3. Product service experience may be used to substantiate partial design assurance of a COTS device. Non-airborne systems experience of the device may be used if gathered in a similar usage domain and/or critical operating environment. However, data of this nature carries some expectations. Formal documentation (such as specifications, data sheets, application notes, errata sheets, etc.), a formal problem reporting and resolution scheme, a method of determining actual failure rates of the device experienced in the field, etc., should be a requirement for obtaining certification credit. If an applicant/system developer intends to develop a service experience case to obtain certification credit, they should be aware that this certification credit requires substantiation.

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

An applicant/system developer that intends to utilize any of the information contained in either Section 11.2 or 11.3 of DO-254/ED-80 should coordinate their primary certification authority early in the display system development to reduce program risk.

3.2 Possible CGP contribution to Hazardously Misleading Information on Airborne Display Systems

The applicant/system developer should show that the CGP used in the display system cannot display HMI to the level of assurance commensurate with the hazard classification (e.g., Catastrophic, Hazardous, Major) of the HMI in question.

As discussed in the previous section, reliance upon a design assurance process, such as the one described in DO-254/ED-80, Sections 2 through 9, as an acceptable means of compliance may not be practical. Additionally, even if an applicant/system developer is able to show compliance to DO-254/ED-80 for a CGP, reliance on design assurance *alone* may not be adequate to protect against undetected HMI that the System safety assessment has identified as Catastrophic or Hazardous.

> **Note**: Please see CAST-24, "Reliance on Development Assurance Alone when Performing a Complex and Full-Time Critical Function" for further information.

Given the points made in the preceding paragraph, the most likely and obvious means to ensure protection against display of HMI is for the display system incorporating the CGP to include architectural mitigation(s), such that the mitigation is adequate and commensurate for the hazard classification of that event. Architectural mitigation for erroneous operation of CGPs in the display system may take many different forms. Examples include a CRC signature pattern monitor for a portion of the displayed information or comparisons of selected displayed pixels to commanded pixels for specific data fields such as a numeric display or a needle on a static dial display.

The most desirable response of any mitigation should be that HMI output by the CGP should be detected and not allowed to be displayed on the displays. Alternatively, the displayed HMI data could be displayed but flagged as invalid. The mitigation(s) should also be independent of the mechanisms that are causing the anomalous behavior.

Appendix B of DO-254/ED-80, although not written specifically with COTS devices in mind, provides descriptions of the Functional Failure Path Analysis

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

method, architectural mitigation methods and advanced verification methods that can be used when designing a display system that utilizes a CGP as one of the main components.

> **Note:** Most display systems make use of multiple redundant displays. Redundant displays ensure that at least one usable display in the flight deck remains operable after system, input power, or input data failures. Redundant displays also provide a means for the flight crew to crosscheck the pilot's and first officer's displays (i.e., compare the data on the two displays) to ensure that the displayed data provided by redundant systems agree with each other. However, if the HMI on a single display is not flagged as invalid and is compelling enough by itself, the flight crewmember whose display is affected may have no reason to crosscheck his/her display with a redundant display. Due to these reasons, an applicant/system developer should not claim that HMI that is displayed on a single display of a multiple, redundant display system is automatically mitigated by a redundant display that shows the correct information unless that claim is substantiated by the piloting community. For any proposed mitigation scheme that depends upon pilot recognition of the anomalous behavior by crosschecking the data on a redundant display or by some other method, the applicant/system developer should describe the cues (e.g., visual, aural, tactile) on which the pilot recognition of the erroneous data depends. The applicant/system developer should also describe the testing, such as flight test or flight simulator, which will be used to evaluate recognition by the pilot of possible failure conditions which are not reliably detectable by the display system health monitoring.

3.3 Display System Availability

Possible causes for simultaneous loss of redundant displays are similar to the possible causes for HMI listed in paragraph 2.2, with the exception of item a. A hardware failure of a single CGP within a single display is not expected to cause more than the loss of that one display.

The display system architecture should be such that the availability of the displayed critical data meets the probability numbers required by the system safety assessment. The applicant/system developer should demonstrate that a flight deck display system utilizing CGPs provides the required flight deck display functions to a level of assurance commensurate with the hazard classification (e.g., Catastrophic, Hazardous, Major).

If the display system fault trees use specific failure rates for CGPs, the applicant/system developer should include substantiating data or other appropriate justification for these failure rates. The applicant/system developer should work with the appropriate certification authority to determine an acceptable method of calculating an estimated failure rate or determining an appropriate empirical one.

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

Any architectural mitigations used to address the concerns of contained in Section 3.2 should not adversely impact the overall display system availability, such that the availability requirements of the display system are not met due to a single common cause or cascading failure. This includes not only faults and design errors within the CGP, but also the hardware supporting the operation of the CGP. Events such as loss of cooling air, extreme vibration or mechanical "shock", etc., should not cause the loss of multiple displays, unless the probability of that event is commensurate with the hazard of loss of multiple displays.

The Standby (Backup) flight instrument installed on an aircraft should not be designed using the same CGP that is used in the primary displays, such that a CGP common failure mode could possibly affect both the primary and secondary flight instruments simultaneously due to a common cause or stimulus.

> **Note**: Refer to Aerospace Recommended Practice (ARP) 4754, "Certification Considerations for Highly Integrated or Complex Aircraft Systems", Section 6.4 and ARP 4761, "Guidelines and Methods for Conducting the Safety Assessment process on Civil Airborne Systems and Equipment", Sections 4.4 and 4.4.3 for more information on Common Cause Analysis and common cause fault sources.

3.4 CGP Device Variations during Production Life

There is a possibility that during the production lifetime of the device, the CGP may exhibit variations or degradations of the device performance or operating characteristics. These changes in the device operating performance and characteristics could manifest themselves in various ways, including but not limited to, the following:

- Changes in the operational environment range (e.g. variation in performance over the expected thermal operation range, or a cascading failure initiated by over-voltage).
- The introduction of a failure mechanism that was not present in the original design of the device.

The applicant/system developer must have a manufacturing quality system in place that will address the concerns listed in this section. Possible methods to address these concerns may include:

- Environmental screening of the specific components (e.g. verify that a statistically significant sample of a production run does not contain manufacturing errors).
- Acceptance testing of different productions runs of the same device to determine if the critical performance aspects of the device have changed.

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

- An in-service program to analyze actual single-display failure events. This may include design features to support root cause investigation, such as a fault code logging memory feature.

The applicant, system developer and authorized manufacturing or assembly facility should identify CGP component variations which could have an adverse impact on the display system, identify appropriate tolerances, and implement display system mitigation to address these variations or component screening to detect out of tolerance components.

3.5 CGP Configurable Items

Many CGPs contain configurable items, such as separately loadable microcode or hardware "straps". The applicant/system developer should show that the configurable items of the CGP, such as the loadable microcode, are controlled and that any production/manufacturing errors involving the display system configurable items, such as selectable options by hardware strapping, will be detectable by the proposed system operation and monitoring, end item acceptance test, or other applicable check. The applicant and display system developer are responsible for ensuring the configuration control of the display system and its components.

3.6 CGP Device Changes after Initial Certification

The applicant/system developer should ensure awareness of any changes that may be made to the CGP by the manufacturer of the device that may affect the display system certification. These include, but are not limited to:

- Changes in fit, form, size or manufacturing techniques that may affect the CGP physical layout, timing, mechanical, electrical or thermal characteristics.
- Changes or additions in functionality, including ones that are not used in the display system application, including firmware, device drivers and libraries.
- Performance enhancements, such as increased speed of operation.

The applicant/system developer should have a process in place that ensures CGP supplier data (such as device specification sheets and errata sheets) is continually monitored, such that newly discovered problems with the device or instructions for future usage are known to the software and/or hardware design teams and to determine if any action is required to be taken.

3.7 Unused CGP Functionality

The latest generation of CGPs will, most likely, contain functionality that will not be used in the airborne display system being designed. System or component

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

certification plans should provide clear information on which functions provided by the CGP are used in the system design and on those that are not used by the design. The applicant/system developer should provide assurance (e.g., robustness testing, analysis) that the CGP unused functionality will not adversely affect the integrity and availability of the displayed data, commensurate with the hazard classification of that failure, if that unused functionality is inadvertently used or activated.

3.8 Open GL Software Drivers

CGPs require many complex software drivers that execute in the main system processor. Some software packages may be obtained from third party suppliers which implement the OpenGL graphics application. Irrespective of source (co-supplier or third party), the applicant/system developer should demonstrate compliance to the guidance of RTCA DO-178B/ EUROCAE ED-12B (or some other acceptable means of compliance) for this software to the appropriate software level as determined by the system safety assessment. The applicant/system developer should address software design assurance when evaluating their choice of graphics generators and drivers, and developing the design.

4.0 Conclusions

Many of the issues discussed in this paper may also be applicable to the larger subject of COTS devices in general. However, it is not the intent of this paper to address the general issue of COTS devices in airborne display systems. This paper is limited to the subject of COTS Graphical Processors only. The latest generation of CGP devices are highly complex and present several issues regarding certification of a flight deck display system that the more traditional COTS devices may not. Therefore, special attention needs to be given to the use of these devices in flight deck display systems.

The issues presented in Section 2 of this paper should be addressed by applicants using CGPs as well as any other project specific issues that may arise when using these devices. Section 3 represents the certification authorities' position on these issues. Applicants should address use of CGPs and the approach to address these issues in an appropriate hardware certification plan. In some cases, a project-specific issue paper or certification review item may be needed to obtain agreement between the certification authority and applicant.

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

5.0 References

a. RTCA/DO-254 (EUROCAE ED-80), *Design Assurance Guidance For Airborne Electronic Hardware*;
b. RTCA/DO-178B (EUROCAE ED-12B), *Software Considerations in Airborne Systems and Equipment Certification*;
c. FAA AC 20-152, RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance For Airborne Electronic Hardware;
d. FAA Order 8110.49, Software Approval Guidelines;
e. FAA Order 8110.4, Type Certification;
f. SAE ARP 4754/EUROCAE ED-79, Certification Considerations for Highly-Integrated or Complex Aircraft Systems.
g. SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems;
h. FAA Advisory Circular 23.1309-1, Equipment, Systems, and Installations in Part 23 Airplanes;
i. FAA Advisory Circular 25.1309-1, System Design and Analysis;
j. FAA Advisory Circular 27-1, Certification of Normal Category Rotorcraft;
k. FAA Advisory Circular 29-2, Certification of Transport Category Rotorcraft.

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