

TrueCore™

Software Safety Monitor for COTS Graphics Processors

FEATURES & BENEFITS

- Detects failures in the functionality of the GPU's graphics rendering pipeline (graphics command to framebuffer)
- Detects impact to graphics rendering resulting from a failure in any unused or undocumented functions
- Eliminates the need for expensive FPGA-based monitoring of a GPU output
 - Reduces development time
 - Reduces system complexity
 - Increases reliability
- Designed and developed from the ground up for safety-critical certification (including RTCA DO-178C/EUROCAE ED-12C level, and ISO 26262 ASIL D)
- Supports RTOS, including Wind River®, VxWorks®/VxWorks 653/VxWorks HPV, SYSGO PikeOS®, QNX OS, Green Hills Software® INTEGRITY®/INTEGRITY178 tuMP, DDC-I Deos™, Lynx Software Technologies LynxOS®/LynxOS178/LynxSecure, Linux, and is configurable for proprietary RTOS or 'bare metal' (no RTOS)
- Available with:
 - CertCore™ 178 avionics DO-178C/ED-12C software certification data package
 - CertCore™ 26262 automotive ISO 26262 Accredited Safety Assessment Certificate
- Option to enhance capabilities to detect an oversubscribed GPU when applications of different criticality levels are sharing a GPU

INTRODUCTION

TrueCore is a Safety Element out of Context (SEooC) GPU safety monitor library designed to interoperate with VkCore® SC Vulkan, ArgusCore™ SC1 OpenGL SC 1.0.1, and ArgusCore™ SC2 OpenGL SC 2.0 drivers.

TrueCore uses a patented approach to provide a suite of highly engineered Initiated Built-In-Tests (IBIT). These provide test coverage of the intended function of the GPU's graphics rendering pipeline (graphics command to framebuffer memory). Through the use of several tests, each with a unique test pattern that is verified independently by the CPU, applications are provided with flexibility in optimizing test execution and result filtering that may not be present with FPGA-based approaches. In testing the graphics rendering pipeline, TrueCore is testing one or more instances of each functional IP block, thereby providing test coverage for design errors, common-mode failures, and incorrect function caused by unused and undocumented functions.

While GPUs contain many instances of certain resources (like shader units), the control over the assignment of resources is shielded from software by the GPU's internal scheduler (job manager). Some GPU architectures provide mechanisms to slice the GPU resources into smaller segments or power gate resources that can be utilized with TrueCore to achieve Single Point Failure Metrics (SPFM) for all rendering hardware. For others, TrueCore can be

configured by CoreAVI to use larger data to force higher resource usage to achieve SPFM. Although achieving a higher SPFM may increase the Diagnostic Test Interval (DTI) and impact the application performance (this is true for FPGA approaches as well), some GPU implementations, when used with TrueCore, can achieve SPFM with minimal impact to DTI and application performance.

With the achievement of the SPFM for the graphics rendering, loss of information or incorrect information in the rendered image would be detected, thus enabling the application to take measures to preclude or mitigate the display of hazardously misleading information.

SPFM detection coverage is determined through a Failure Modes and Effects Analysis (FMEA) of the rendering path at a functional block level.

As TrueCore is a software-based safety net, the Latent Failure Metric (LFM) is high, specifically for the dual failure case of a hardware failure and a failure in the associated safety net.

TrueCore is available with an optional element to detect an oversubscribed GPU. For example, when running mixed-criticality applications on a single GPU where the GPU is non pre-emptive, this feature can detect if the GPU is not available to a high criticality application on time. The application can then make an appropriate mitigation response.

DEVELOPMENT INTERFACE AGREEMENT

The intent of a Development Interface Agreement (DIA) is to define the responsibilities of the customer and supplier in facilitating the development of a functional safety system. In custom developments, the DIA is a key document executed between customers and suppliers early in the process of developing both the system and the CoreAVI drivers and libraries. As the CoreAVI libraries are Commercial-Off-The-Shelf (COTS) SEooC products, an ISO 26262 DIA is not required. Please refer requests for custom DIAs to CoreAVI Sales. The following sections highlight key points of the standard DIA.

Requirements Transfer

TrueCore is developed as a Safety Element out of Context (SEooC). Detailed safety requirements were not available from lead customers during development; therefore, the safety requirements used were based on CoreAVI's analysis of target safety applications. CoreAVI is willing to discuss acceptance of new customer safety requirements for future designs. Please contact CoreAVI Sales for further information.

Availability of Safety Documentation

The following table lists the safety documentation for the library.

DELIVERABLE	CONTENTS	AVAILABILITY	DELIVERY
Safety Manual	Documents usage, assumptions, issues, etc. of SEooC to put the SEooC into a safety context (application)	NDA Material	TBD

Table 1: Available Safety Documentation

External Product Audits

CoreAVI works with TUV Rheinland® for an external audit of TrueCore to ISO 26262 standards.

Contact CoreAVI for more information: sales@coreavi.com