Green Hills Software

Safety-Critical Products

INTEGRITY-178B
Real-Time Operating System

Green Hills®
• SOFTWARE, INC. •

A complete safety critical line

Green Hills Software offers a complete safety critical product line that includes:

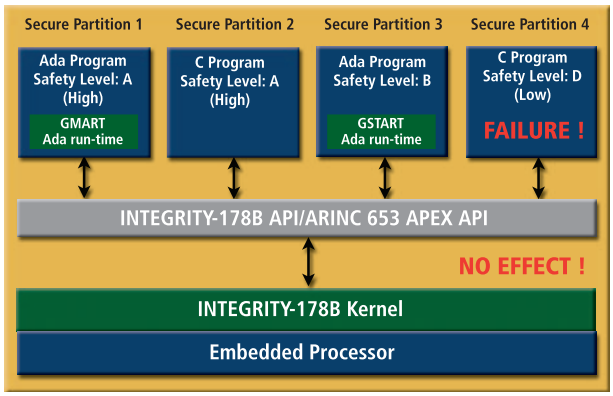
- **INTEGRITY-178B**—a full time and memory-partitioned ARINC-653-1 real-time operating system (RTOS)
- **GMART**—a safety critical minimal Ada run-time kernel
- **GSTART**—a safety critical small-tasking Ada run-time
- language support for C, C++ and Ada
- a full set of safety critical testing tools

GMART, GSTART, and INTEGRITY-178B are available with full off-the-shelf DO-178B Level A certification material. All have formally passed DO-178B Level A multiple times and thus are certified and not just certifiable.

Multiple safety levels executing on a single processor

In the past, safety critical software systems with multiple levels of safety criticality have been deployed on federated systems, with each function executing on a dedicated processor. The advent of modern processor technology as well as the need to reduce maintenance costs and the size/weight/power of older systems led to a demand for a commercial run-time system that supports multiple programs at different safety levels executing on a single processor. The run-time system must also be certifiable to a level of criticality as high or higher than any program running on the processor.

The cost to test and certify safety critical software is directly proportional to the level of safety criticality: the higher the safety level, the more complex and expensive the certification process. The most cost-effective certification solution then would be to reserve the highest levels of certification to only those programs operating at highest safety-criticality. Programs or functions operating at lower levels of criticality could be certified at the lower-cost low levels.



As a result of secure partitioning, INTEGRITY-178B can guarantee that any failure in a lower safety level program will not disrupt the operation of high safety level functions.

The Rockwell-Collins Avionics Management and Display System aboard the S-92 Sikorsky helicopter is one of the INTEGRITY-178B applications that have been certified to DO-178B Level A, the most stringent safety level for avionics software.

This solution is valid only if the run-time system can guarantee that any failure resulting from a defect in a program operating at a lower safety level CAN NOT—under any circumstances—disrupt the operation of the higher safety level functions. The run-time system must also guarantee protection in both the space and time domains. For a commercial RTOS to achieve this, it must be securely partitioned so to provide both memory protection and real-time scheduling protection.

INTEGRITY-178B RTOS Features

- Securely partitioned
- Protection in both the time and space domains
- Resource/IO protection
- ARINC-653-1 compliant APEX interface
- Support for multiple levels of safety criticality
- Support for Ada95, C, and Embedded C++
- Support for Rate Monotonic Analysis (RMA)
- DO-178B Level A certification package

Protection in time & space domains

INTEGRITY-178B is an ARINC-653-1 compliant, securely partitioned Real-Time Operating System (RTOS) that targets demanding safety critical applications containing multiple programs with different levels of safety criticality, all executing on a single processor. INTEGRITY-178B has been engineered from the ground up to provide safety, security and determinism. As a result it guarantees protection across both the time and space domains.

The design of INTEGRITY-178B kernel guarantees bounded computation times by only using fully deterministic features. All memory allocation happens only once at system start-up time so memory fragmentation is never an issue. All kernel data structures are then static after creation. Underlying hardware mechanisms provide full system memory protection for all components, including user applications, device drivers, and inter-partition communications. Clocks and timers are protected with access permissions and implemented entirely in software. The kernel's memory-protection and error-handling features provide a secure system with built-in fault isolation and tolerance. At the lowest level, the kernel is protected from malicious access through its object-oriented design and access verification. Traditional kernel access problems such as invalid kernel addresses and invalid system call parameters are eliminated by the kernel's secure design.

As a result of its unique approach to resource management —which includes processor utilization and memory management—the INTEGRITY-178B RTOS can provide guaranteed resource availability for multiple safety-critical programs on a single processor operating at different safety levels.

With its securely partitioned design, deterministic behavior, real-time responsiveness and small footprint, INTEGRITY-178B offers a universal run-time environment that is capable of executing a variety of avionics and flight control functionality operating at different safety and security levels.

Protection in the Time Domain

- **Deterministic**—given state, input -> same state transition
- **Schedulability Analysis**
  - RMA support within a partition or across the entire processor
  - Task utilization statistics
  - Execution overrun detection
  - No heuristics in scheduler
- **No Priority Inversion**
  - No semaphores in kernel implementation
  - Highest Locker Semaphores, no unbounded blocking times
- **ARINC-653-1 Partition Scheduler**
  - Optimized two-level scheduler
  - Guaranteed time window to run with intra- and inter-partition allocation of idle time
- **Bounded Computation Time For All System Calls**
  - No dynamic memory allocation in kernel space
- **No hidden execution time/latency**
  - Message transfers use task's execution time
  - Never disable interrupts to update kernel structures
- **Pure Software Timers With Access Permissions**

Protection in the Space Domain

- **Guaranteed Resource Availability**—Partition's memory is protected from access by another partition
- **Memory Protection**—Utilizes underlying HW MMU, applies execute-read-write permissions
- **"Hard Currency" OS**—Programs in Secure Partitions donate own memory to satisfy system call
- **Statically verifiable MMU settings**—No dynamic manipulation of MMU to support message passing
- **No Recursion in Kernel**—Static call graph guarantees max kernel stack size
- **Static Verification of System Resources (kernel objects)**
- **Connections**—Secure interpartition communications
- **Secure Device Drivers**—User Mode tasks which use connections as interface to the ISR/Synchronous Call

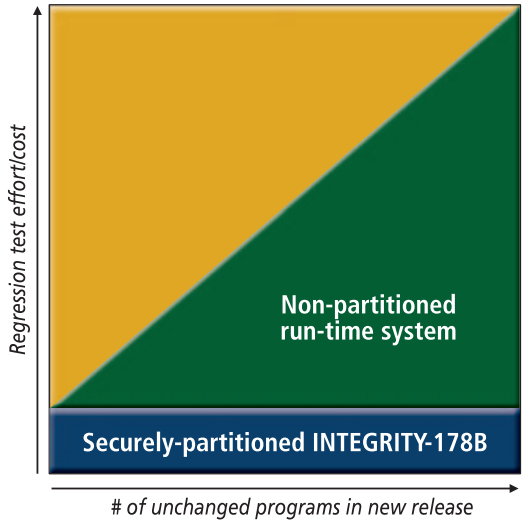
Safety-Critical Products: INTEGRITY-178B RTOS

Minimized regression testing lowers certification costs

INTEGRITY-178B's ARINC-653-1-Application/EXecutive (APEX) interface provides a recognized standard interface between the operating system of an avionics computer resource (ACR) and the application software. Its ability to fully support ARINC-653-1 while complying with DO-178B Level A provides a COTS baseline avionics operating environment that meets standards already adopted and accepted by the commercial avionics industry for Integrated Modular Avionics.

INTEGRITY-178B reduces the time to introduce new functionality into existing systems. Through secure partitioning in both time and space, minimal regression testing is required for a system's preexisting components. Testing is often the most expensive activity of any certification effort.

This reduction of effort translates into large cost savings and decreased time to market. For systems without secure partitioning, regression tests/analysis must be performed to guarantee schedulability, as well as ensuring no data access violations, by the new functionality. As a result, both performance and functional tests are required, for operating systems not supporting full partitioning.



As a result of its secure partitioning, INTEGRITY-178B RTOS can lower certification costs because only minimal regression testing is required for a system's preexisting components.

INTEGRITY-178B - DO-178B Certification Package

Green Hills Software in-house safety and security experts; develops, verifies, supports and maintains the DO-178B Level A compliant Software Life-Cycle Data Package for the INTEGRITY-178B product line. Green Hills does not use external subcontractors for this work, as is common with other RTOS providers. Thus Green Hills is able to support their customers throughout their safety critical certification efforts. Below is the list of DO-178B Level A software life-cycle artifacts delivered with the INTEGRITY-178B DO-178B Level A certification package:

- Customer specific Plan for Software Aspects of Certification (PSAC)
- Software Development Plan
- Software Verification Plan
- Software Configuration Management Plan
- Software Quality Assurance Plan
- Software Requirements Standards
- Software Design Standards
- Software Code Standards
- Source Code to applicable tested software
- Executable Code to applicable tested software
- Software Design Document
- Software Requirements Specification
- Software Verification Test Cases and Procedures
- Software Verification Results
- Software Life Cycle Environment Configuration Index
- Software Configuration Index
- Problem Reports
- Software Configuration Management Records
- Software Quality Assurance Records
- Traceability Matrices
- Tool Accomplishment Summary
- Software Accomplishment Summary (SAS)

The above certification package includes Green Hills Software services for all DO-178B Level A compliant verification activities for the INTEGRITY-178B operating on the processor architecture specified by a customer's requirements. All audits, reviews, analysis and testing of the INTEGRITY-178B real-time operating system is performed by Green Hills Software using the customer's target processor system.

Green Hills® SOFTWARE, INC.

30 West Sola Street ▲ Santa Barbara, CA 93101 ▲ ph. 805.965.6044 ▲ fax 805.965.6343 ▲ www.ghs.com ▲ sales@ghs.com