Green Hills Software

INTEGRITY®

The most advanced RTOS technology

Green Hills®
• SOFTWARE, INC. •

The most secure & reliable RTOS

The flagship of our family of operating systems, the INTEGRITY® RTOS, is built around a microkernel architecture that provides embedded systems with total reliability, absolute security, and maximum real-time response. With its leadership pedigree underscored by certifications from a range of industries, INTEGRITY sets the standard for real-time operating systems.

Maximum performance, security, reliability

From inception, the INTEGRITY RTOS was designed so that embedded developers could ensure their applications met the highest possible requirements for security, reliability, and performance.

To achieve this, INTEGRITY uses hardware memory protection to create secure partitions that isolate and protect embedded applications. Secure partitions guarantee each task the resources it needs to run correctly and fully protect the operating system and user tasks from errant and malicious code—including denial-of-service attacks, worms, and Trojan horses.

Unlike other memory-protected operating systems, INTEGRITY never sacrifices real-time performance for security and protection.

Integrated middleware and platforms

To help developers jump-start product development, Green Hills Software offers an extensive array of middleware integrated and validated for INTEGRITY, including:

- FFS, FAT, NFS and journaling file systems
- IPv4/IPv6 host and routing networking stacks
- Network security protocols
- Advanced layer 3 routing and layer 2 switching protocols
- Complete Wi-Fi support
- USB host stack, device stack and class drivers
- 2D, 3D and OpenGL graphics

Each of these middleware packages has been pre-integrated and tested to run seamlessly with and take full advantage of INTEGRITY's advanced RTOS capabilities.

For selected industries, Green Hills Software offers platforms that provide a completely integrated ecosystem. Each platform includes the INTEGRITY RTOS as well as development tools, industry-specific middleware, reference hardware, and documentation. Platforms are available for:

- automotive
- avionics
- industrial safety
- medical devices
- secure mobile devices
- secure networking
- software defined radio
- wireless devices

By combining all the core software and documentation into a highly-integrated platform developers can:

- more readily develop and deploy a targeted device
- accelerate time-to-market
- reduce development risk
- focus more on quality and innovation

Safety and security certifications

Since its release over 13 years ago, the INTEGRITY RTOS has received the following certifications and accreditations that testify to its robustness, enabling developers to achieve the highest levels of safety, security, and reliability in their designs.

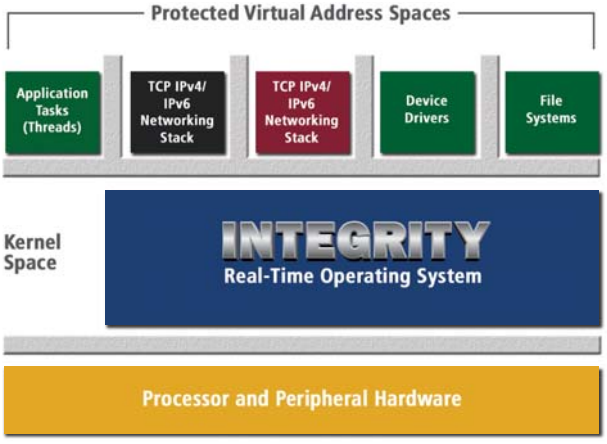
- FAA: DO-178B, Level A
- Common Criteria: EAL 6+ High Robustness, the highest security level ever achieved for an operating system
- FDA: Class II and Class III medical devices
- IEC: Industrial safety 61508 SIL 3
- CENELEC: Railway EN 50128 SWSIL 4

Guaranteed security

INTEGRITY provides all the capabilities embedded designers need to enforce the policies of separation, damage limitation, and information flow control as well as provide secure networking for today's more complex and connected applications.

INTEGRITY's Multiple Independent Levels of Security (MILS) *separation kernel architecture* provides a highly robust mechanism to separate security functions. A true MILS kernel, INTEGRITY has been certified to EAL 6+ High Robustness, the most rigorous Common Criteria security evaluation ever achieved for a commercial operating system.

INTEGRITY's separation kernel protects against damage from errant or malicious code by preventing processes from writing beyond assigned memory regions. In addition, INTEGRITY's partitions prevent unintended access to data from outside the partition where the data resides.



The INTEGRITY architecture supports multiple protected virtual address spaces, each of which can contain multiple application tasks. The INTEGRITY kernel is itself protected in its own address space, along with kernel-mode tasks.

Architected for reliability

Traditional operating systems can crash, lock up, or execute uncontrollably, resulting in costly consequences—a lost satellite, a stalled car, a failing medical monitor. But the INTEGRITY RTOS protects both critical applications and itself from the malfunctions that can lead to these failures.

To do this, INTEGRITY provides *guaranteed system resources* that ensure that CPU time and memory resources will always be available to individual processes, no matter what any other process attempts to do.

Malicious or unintended events can deny access to system resources and keep system processes from running as intended. To prevent these denial-of-service attacks, INTEGRITY can assign fixed budgets of CPU time and memory to each process. By guaranteeing a time window for a particular process, these fixed budgets also preserve the integrity of other processes by preventing running tasks from executing beyond their window.

True, hard real-time performance

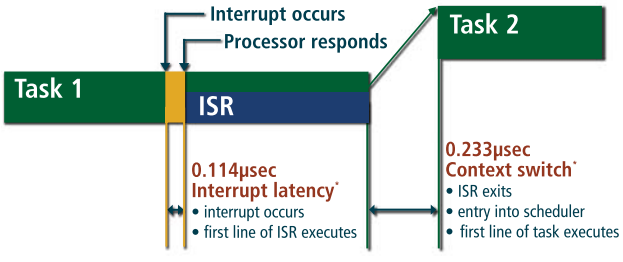
As one of the first RTOSes to leverage hardware memory-management units (MMUs), INTEGRITY is a true, hard real-time operating system that never sacrifices real-time performance for security and protection. INTEGRITY can respond to events in nanoseconds, guaranteed.

All INTEGRITY kernel services have been carefully optimized to minimize the overhead of system calls. Complex system calls can be suspended to allow others to execute. INTEGRITY uses a true *real-time scheduler* that supports multiple priority levels and enables complete control over CPU percentage allocation.

The INTEGRITY RTOS always services the highest priority interrupt with absolute minimum latency. To guarantee this, the kernel never masks or blocks interrupts. The kernel also avoids instructions with long latencies that could temporarily block interrupts on some systems.

Meeting critical deadlines

With the INTEGRITY RTOS, the kernel only uses the CPU time resources the requesting process supplies to perform the requested services. Hidden execution time is further avoided because kernel service times are bounded by a measurable maximum kernel service time regardless of any process actions.



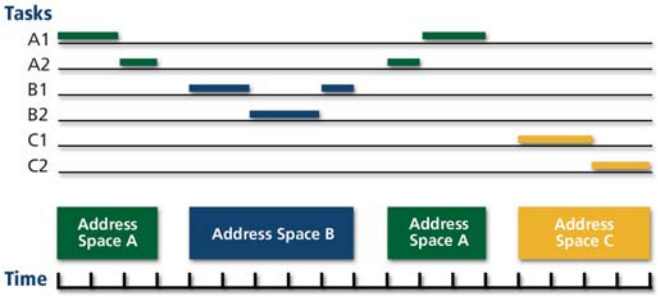
*Based on the Freescale QorIQ P2020 at 1200MHz

To guarantee minimum interrupt latency, the INTEGRITY kernel never blocks masks or interrupts even while manipulating critical data structures.

INTEGRITY also uses its unique *highest locker semaphore* capabilities to prevent priority inversion. Priority inversion can cause missed deadlines and execution failure when a lower-priority task denies a higher priority task for an indeterminate amount of time.

Scheduling by partitions

The INTEGRITY RTOS incorporates a multi-level optimized *enhanced partition scheduler* (EPS)—with optional ARINC 653-1—that can guarantee a specific percentage of CPU time support to a given address space regardless of other system or process events. For each partition, the EPS designates a CPU time window to always be available for tasks within that address space. The EPS also enforces the CPU time window boundaries to prevent bugs, malicious code, viruses, and hacker intrusion from adversely affecting tasks in other partitions.



INTEGRITY incorporates an optional ARINC-653 two-level partition scheduler.

Guaranteed memory resources

The INTEGRITY RTOS protects memory many ways:

- from exhaustion
- from damage
- from unauthorized access

INTEGRITY's unique *memory quota system* keeps one address space from exhausting the memory of any other.

To ensure adequate kernel memory, INTEGRITY requires that kernel memory not be used for messages, semaphores, or other kernel objects created in response to process requests. Instead, the kernel performs all services requested by a process using the memory resources that the requesting process supplies.

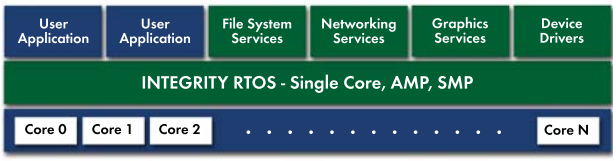
To prevent the risk of user stack overflow, INTEGRITY's kernel has its own memory stack. Without this, the kernel would need to access the user process' stack. But this can lead to problems because it is impossible for the user process to anticipate the maximum stack size if it is subject to use by unknown code (i.e., the kernel).

Multicore and embedded virtualization support

Embedded microprocessor trends, including hypervisor modes and multicore, are paving the way for a new breed of system software architectures in embedded systems. INTEGRITY's flexible deployment models, including AMP, true SMP, and integrated Multivisor virtualization technology, enable compelling new applications and capabilities.

Advanced multicore support

The modern architecture of INTEGRITY is well suited for multicore processors targeting embedded systems. INTEGRITY provides complete Asymmetrical Multiprocessing (AMP) and Symmetrical Multiprocessing (SMP) support that is optimized for embedded and real-time use. Embedded system designers can select the multiprocessing architecture that is right for the task. When coupled with the advanced multicore debugging features found in the Green Hills MULTI® tool suite, developers will reduce their time-to-market while increasing system performance and reliability.



INTEGRITY's flexible multicore processor support provides users with a wide range of system architecture possibilities while delivering real-time deterministic performance with secure, reliable separation policies

INTEGRITY AMP support

With AMP, one instance of the INTEGRITY kernel runs on each processor core. User applications are separated and stationary on a given core and each core owns its own area of memory. AMP is well suited for heterogeneous CPUs and offers a potential for higher performance and efficiency than other multicore architectures. It also provides deterministic behavior while providing the designer control over the choice of core where the process will execute.

INTEGRITY SMP support

SMP was a natural extension for the existing INTEGRITY architecture due to its simple microkernel design, fast and deterministic interrupt response time, and policy of not disabling interrupts in the kernel. INTEGRITY's SMP support does not disturb its real-time guarantees. In addition, INTEGRITY middleware is implemented as processes in user space and is easily distributed to cores.

INTEGRITY SMP Features:

- Advanced separation kernel architecture with security and safety certified pedigree
- Automatically runs *n* highest priority tasks on *n* cores … for better determinism
- Optional mode to require all running tasks have same priority … aids in porting from single-core
- Support for both natural and user-defined core affinity
- "Smart SMP locks" for far fewer kernel locks than other SMP OSes

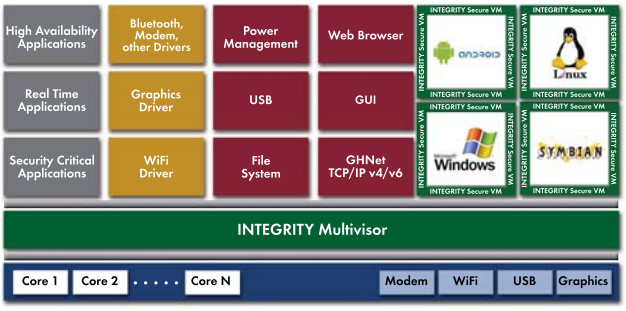
INTEGRITY secure virtualization

INTEGRITY Secure Virtualization™ (ISV) is a robust and portable virtualization infrastructure with an architecture flexible enough to handle the wide variety of hardware capabilities available across today's microprocessors. ISV maximizes the use of available hardware virtualization facilities while minimizing or eliminating modifications to guest operating systems.

On hypervisor acceleration-enabled processors such as Intel VT, Freescale QorIQ, and ARM TrustZone, ISV supports high performance "full virtualization" where no changes to the guest operating system are needed.

On processors lacking hypervisor mode assistance, ISV applies carefully crafted, minimally intrusive modifications to the guest operating system to maximize performance without sacrificing ease of migration and portability.

INTEGRITY® Multivisor™—Green Hills Software's ISV implementation for multicore processors—provides flexible and powerful mechanisms for managing cores. The Multivisor can statically bind guest operating systems to cores, in an AMP model, or dynamically schedule workloads in a SMP model, depending on system requirements.



INTEGRITY Multivisor: combining general purpose guest operating systems with a comprehensive ecosystem of real-time applications, middleware, and drivers.

Integrated platforms and middleware

Built on the INTEGRITY separation kernel, Green Hills Platforms provide complete, pre-integrated solutions customized to application-specific requirements for a range of applications. By bringing together all the tools and middleware required, Green Hills Platforms enable manufacturers to reduce both development cost and time-to-market.

Automotive platform

Green Hills offers development solutions for all automotive electronic subsystems—powertrain, body, chassis and infotainment. For chassis and powertrain software development, the MULTI IDE provides state-of-the-art compilers (with built-in MISRA C checker), debuggers, simulators, and profiling tools and is optionally available with tightly integrated Mathworks™ and UML® 2.0 solutions.

For infotainment, INTEGRITY Secure Virtualization (ISV) can securely host any legacy or future infotainment operating systems like Windows® or Linux® and simultaneously execute hard real-time control modules on the same processor.

Avionics platform

INTEGRITY has a long-running history of successful deployment in numerous commercial and military aircraft. The Platform for Avionics combines the INTEGRITY (or INTEGRITY®-178B) RTOSes, support for the aviation industry standard ARINC 653-1 application software interface, and the documentation required for FAA safety certification. INTEGRITY-178B has been certified to the FAA's most stringent standard for flight-critical avionics systems, RTCA/DO-178B Level A.

Industrial safety platform

With its focus on safety and reliability, INTEGRITY is ideal for systems in the industrial, rail, automotive, and nuclear industries that require safety certifications. The INTEGRITY and *velOSity*™ RTOSes have been certified by TÜV and exida for EN 61508 functional product safety at Safety Integrity Level 3 (SIL3), and CENELEC EN 50128 SWSIL4. This platform includes the pre-certified INTEGRITY RTOS, integrated middleware, as well as the SIL3 / SWSIL4 certification report and safety manual.

Medical devices platform

The Platform for Medical devices was designed to meet FDA requirements for up to Class III medical devices, the most stringent type of FDA certification. Along with INTEGRITY, this platform includes integrated middleware for networking, file systems, USB, embedded databases, graphics, and video as well as an integrated design, development, and verification toolset for the entire software life cycle.

Secure mobile devices platform

The Platform for Secure Mobile Devices couples a high security microkernel with virtualization features. INTEGRITY controls the mobile device's applications microprocessor, memory, and I/O devices, and ISV hosts one or more instances of "guest" mobile operating systems, such as Linux or Windows Mobile®. The platform also provides a software development kit device manufacturers and service providers can use to incorporate secure applications and manage critical data that cannot be compromised.

Secure networking platform

INTEGRITY, with its EAL6+ pedigree, provides the features and policies that can thwart even the most well thought-out or funded hacker attacks. This platform secures the network device at its core—the operating system level—and also delivers a complete suite of integrated RFC-compliant networking middleware, including a mature IPv4/v6 TCP/IP stack, IP networking applications, security protocols, layer 2 switching, layer 3 routing, H.323, wireless LAN, NDDS, CORBA, and more.

Software defined radio platform

The Platform for Software Defined Radio (SDR) provides standards-based RTOS, tools, and middleware for developing SDR systems that range from the armed forces' Joint Tactical Radio Systems (JTRS) to public safety radios to commercial small form-factor reconfigurable radios. This platform complies with Software Communications Architecture (SCA) Operating Environment and includes the POSIX-conformant INTEGRITY RTOS, a TCP/IP stack, CORBA, SCA core framework, and waveform development solutions and reference platforms.

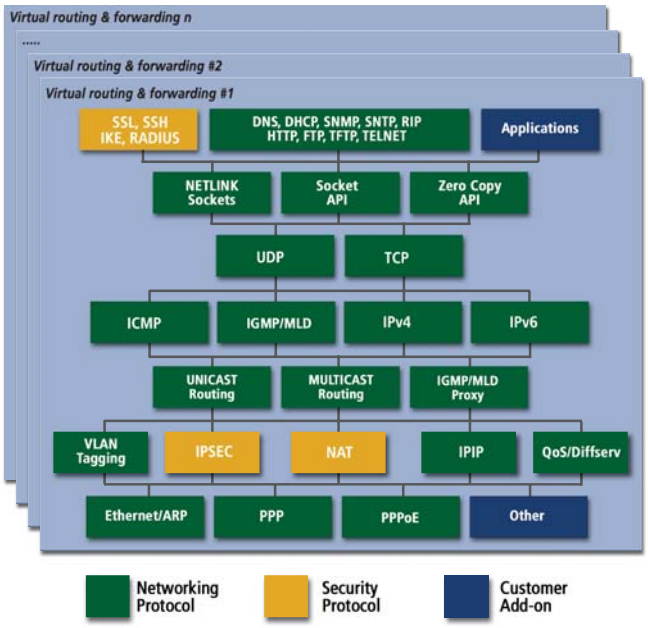
Wireless devices platform

For developers building electronic devices that require secure wireless connectivity, this platform integrates INTEGRITY with mainstream wireless chipset drivers and a complete, mature supplicant agent. These software technologies are validated together on a commercial hardware reference platform. For devices that require compatibility with Cisco® enterprise deployments, a CCX Client is available to provide Cisco compatibility where required.

IPv4/IPv6 networking

INTEGRITY supports comprehensive IPv4/IPv6 networking capabilities that offer a choice of advanced solutions tailored to meet the demands of your end product. Built specifically for embedded applications, the stack applies advanced algorithms for optimized performance and scalability and goes through extensive protocol conformance and interoperability testing.

The networking suite was developed from the ground up to address the specific needs of embedded systems and span a range of applications: wireless, automotive, consumer, residential, gateways, enterprise routers, cellular infrastructure and cellular handsets.



INTEGRITY's TCP/IP stack provides a comprehensive set of industry standard protocols in a high-performance, scalable stack.

File systems

INTEGRITY supports a wide variety of file systems, including UNIX-like file systems, DOS/FAT 12/16/32, ISO9660, Wear Leveling NOR/NAND Flash File Systems, Network File Systems, and others. INTEGRITY's file system framework model, commonly referred to as a virtual file system (VFS), makes it easy to add and remove support for these various file systems or add your own. INTEGRITY provides additional advanced file system functionality:

- **Partitioning Journaling File System (PJFS) Library** The PJFS Library is a high reliability file server for safe recovery from power failure and quick boot. It preserves data integrity through transactional journaling and client partitioning.

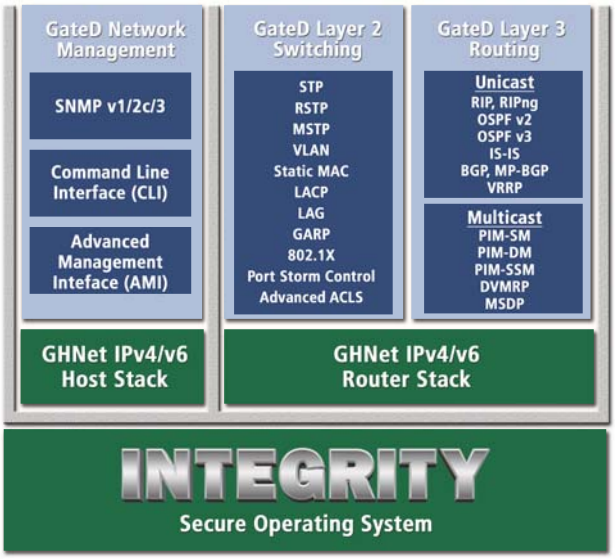
Advanced routing and switching

Green Hills Software's GateD® family of routing and switching software is a processor-neutral, comprehensive control and data plane solution that provides complete source code for layer 2 switching and layer 3 routing protocols.

For next-generation carrier devices, GateD products support all requisite Layer 2 and Layer 3 protocols—including OSPF, BGP, MP-BGP, OSPFv3, RIP, ISIS, VRRP, PIM, DVMRP, MSDP, STP, RSTP, GVRP, VLAN, IGMP, GARP, and more—and have been integrated, validated and tested with INTEGRITY and the IPv4/v6 router stack, GHNet™. Because this complete stack (OS+TCP/IP+L2+L3) has been pre-integrated and validated, customers can significantly reduce time-to-deployment, increase device reliability and security, and lower development costs for their products.

All the GateD protocols have been integrated with a robust, configurable and extensible Command Line Interface (CLI) for device management. The GateD CLI module provides complete configuration and management functionality for both the control and data-plane software, covering everything from static routing to routing with BGP, OSPF, and more.

The scalability of the code, complete RFC-compliant functionality, and extent of product integration and validation make these commercial-grade protocols ideal for inclusion in any carrier-grade core, edge, or aggregation device being developed today.



The GateD family of routing and switching software supports all requisite Layer 2 and Layer 3 protocols and provides a processor-neutral, comprehensive control plane and data plane solution for next-generation carrier devices.

Complete wireless support

For devices that need wireless LAN (WLAN) interfaces, INTEGRITY couples its own robust security capabilities with support for the latest IEEE 802.11 and Wi-Fi Alliance standards, including:

- static and dynamic WEP
- WPA and WPA2 in both personal and enterprise mode
- the full range of 802.1X Extensible Authentication Protocol (EAP) types
- Wi-Fi Protected Setup (WPS) for easy network setup

For devices that require compatibility with Cisco enterprise deployments, a CCX Client is available to provide a certification-ready device stack.

To jump-start development of devices that need wireless connections, INTEGRITY has been pre-integrated with a full package of industry-standard security protocols and reference hardware.

USB solutions

In addition to complete USB 1.1 and high-speed USB 2.0 host and device stacks, numerous class drivers and example applications for using both types of stacks are available for INTEGRITY. These products enable you to quickly and easily add USB connectivity to your applications.

USB Host and Device Controller Libraries

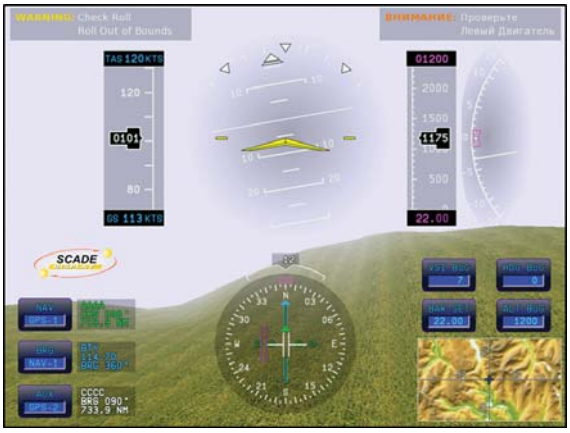
A USB device controller library simplifies the task of writing USB device driver code. It handles most of the generic USB and IODevice details, allowing the user to concentrate on product-specific requirements. A USB 2.0 host stack uses standard UHCI, OHCI, and EHCI controllers.

Supported Class Drivers:

- Mouse, keyboard and hub
- Audio class for output devices
- Mass storage class
- Communications class

Media solutions

The Portable Embedded GUI (PEG) provides a comprehensive library for creating 2D graphical user interfaces for touch screens and LCD displays while requiring a minimal memory footprint. 3D graphics—including OpenGL—and highly tuned graphics accelerator drivers for next generation displays, are also integrated with INTEGRITY.



INTEGRITY supports 3D graphics—including OpenGL—via leading-edge embedded products from ALT Software.

Available board support packages

The INTEGRITY RTOS comes with a variety of board support packages (BSPs) that help jump-start development. INTEGRITY BSPs provide board memory initialization and support for many peripherals including serial and Ethernet devices. INTEGRITY can be stored in ROM or flash memory, and most BSPs include support for easy flash programming. INTEGRITY provides a simple API for easy access to flash memory.

Reference BSPs and associated hardware support are available for boards from these vendors:

- Advanced Micro Devices (AMD)
- Analog Devices
- Avnet
- Cirrus Logic
- Digi
- Freescale Semiconductor
- Goodrich
- Kontron
- MAI Logic Teron
- NEC
- Rockwell-Collins
- Texas Instruments
- Xilinx
- Advantech
- ARM, Ltd.
- Axiom
- Cogent
- Embedded Planet
- Fujitsu
- IBM
- Lockheed Martin
- Marvell
- North Atlantic
- SHARP Microelectronic
- Thales Computers
- Aitech Defense Systems
- Atlas
- BAE
- Curtiss-Wright Corporation
- Emerson
- GE Intelligent Systems
- IDT
- LogicPD
- MEN Mikroelektronik
- Phytec
- ST Microelectronics
- Toshiba
- AMCC/AMP
- Atmel
- Creative Electronic Systems (CES)
- Data Devices
- Eurotech
- General Dynamics
- Intel
- Lucent
- MIPS Technologies
- Pico Computing
- Tews Technology
- X-ES

Create, debug, and optimize with ease

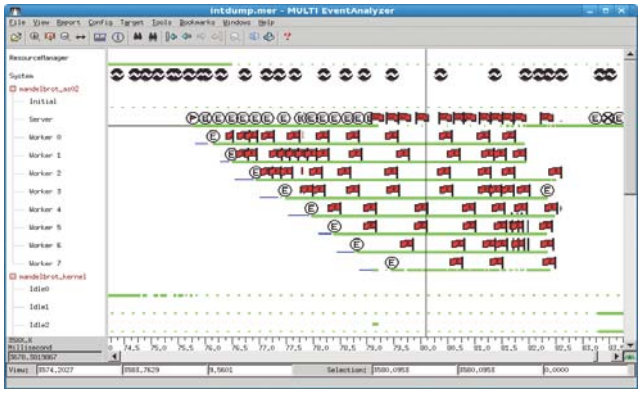
A powerful suite of multicore-enabled, OS-aware graphical development and analysis tools enables you to easily configure, debug, and optimize your INTEGRITY applications. These tools can guide you through creating complex INTEGRITY applications, graphically configuring resources for an entire system, and visualizing a myriad of system events.

INTEGRITY Project Wizard

With the Project Wizard, you can easily create INTEGRITY applications or projects with just a few clicks. Working through a graphical interface, you can select from various project attributes, such as the desired BSP, the number of address spaces desired, and whether the image will be loaded dynamically or statically defined. The Project Wizard also provides a selection of shared libraries, file systems, TCP/IP stacks, resource analysis, and debug agents.

Event logging with the EventAnalyzer

With the powerful EventAnalyzer™ you can readily understand the complex real-time interactions of your system. Important OS events such as semaphore calls, task context-switches, and interrupts are logged on the target in real-time. Event information is then transferred to the host where it is displayed graphically in the EventAnalyzer GUI. You can fully control and configure event logging and even create your own user-defined events.



Any event displayed in the EventAnalyzer view window can be selected for debugging with a single click, opening a debug window showing that event's source code, ready to debug.

INTEGRITY can log system events in postmortem or live modes. In postmortem mode, data is gathered on the target with minimal overhead. You can upload the event log upon request—such as after a failure—and analyze the information to determine the root cause of the failure. In live mode, data is continually sent to the host via TCP/IP or serial, allowing a virtually unlimited history of data to be collected and analyzed as the system runs.

The EventAnalyzer GUI provides convenient navigation features such as zooming and searching and also lets you selectively hide various events. In addition, the EventAnalyzer's one-click source code correlation makes low-level analysis easy and convenient.

INTEGRITY simulators

With the INTEGRITY simulator (ISIM), you can develop and test your embedded INTEGRITY-based applications without the need for target hardware. ISIM simulates the same binary code that runs on the target processor for more realistic results than conventional native simulators. Users can simulate the complete INTEGRITY API, including virtual memory, peripherals, and TCP/IP.

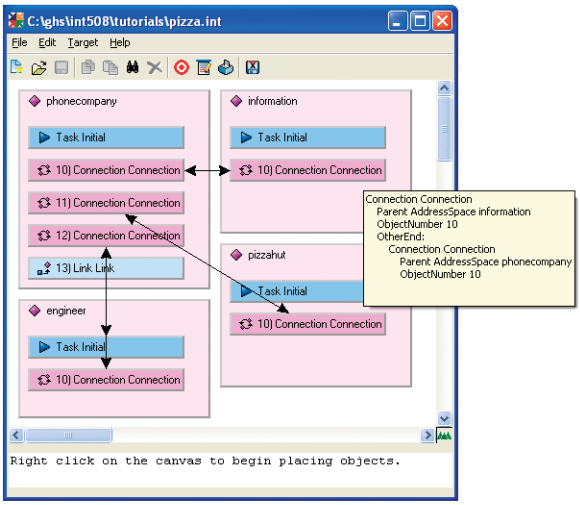
System viewing with ResourceAnalyzer

Customized for the INTEGRITY RTOS, the ResourceAnalyzer is an advanced run-time analysis tool that helps you track and visualize CPU and memory usage statistics for the entire system. With this information, you can maximize the efficiency of tasks and address spaces and improve overall system performance.

The Integrate utility

The Integrate™ utility is a unique industry-leading innovation that enables you to establish an initial state of tasks, connections, and other kernel objects across multiple address spaces to verify system security and guarantee resource availability. Through Integrate's easy-to-use yet powerful interface, you can configure all resources in the entire INTEGRITY system, including address spaces, clocks, tasks, semaphores, connections, etc.

Integrate generates a formatted printable configuration file that is used in building the INTEGRITY application. Integrate reads the configuration file and displays the contents graphically, so that address spaces and operating system objects can be easily viewed.



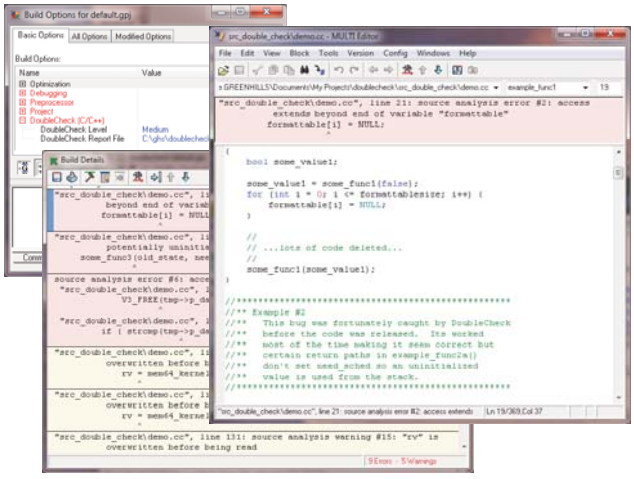
Integrate provides a powerful, easy-to-use interface for graphically visualizing the initial system state.

MULTI integrated development environment

The Green Hills MULTI IDE includes the industry's most powerful and proven tools for developing, debugging, and optimizing embedded software in C, C++, EC++, and MISRA C. MULTI runs on Windows, Unix®, Linux, and HP-UX® hosts and provides a direct graphical interface for all Green Hills compilers, supporting remote debugging to INTEGRITY targets. With its wide array of sophisticated tools, MULTI can help reduce development and manufacturing costs and improve device performance and reliability.

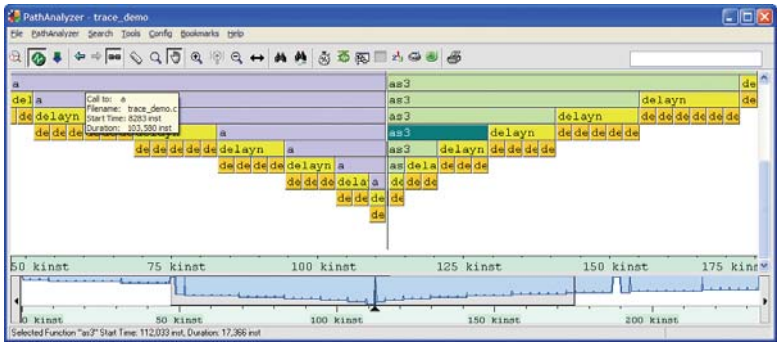
DoubleCheck™

DoubleCheck™ is a powerful static analysis tool used to find bugs early in development, when they can be fixed more easily. It can quickly analyze large pieces of code spanning many source files and identify bugs caused by complex interactions. Built in to the compiler, DoubleCheck makes it easy to automate debugging with project building, avoiding the need for external tools or complicated scheduling.



TimeMachine™ debugging suite

Green Hills Software's TimeMachine™ suite offers a wide variety of trace analysis tools that enable embedded software developers to find and fix bugs faster, optimize with ease, and test with confidence. The TimeMachine debugger combines a familiar debugger interface with innovative functionality that enables developers to step and run forward and backward through their code.



The TimeMachine debugger interface is integrated with advanced analysis tools such as the PathAnalyzer, which shows your call stack over time.

MULTI Profiler

The MULTI Profiler offers code coverage reports that make it easy to determine what blocks and source lines have not been executed. You can use this information to better understand program execution, complete your test suite, or quickly identify performance bottlenecks.

PathAnalyzer

By providing a graphical view of an application's call stack over time, the TimeMachine Suite's PathAnalyzer helps identify incorrect execution paths, inefficiencies in code, and anomalous bugs caused by events such as unexpected interrupts or random glitches.

Optimizing compilers

Green Hills Software's world class C, C++, Embedded C++, MISRA C, and Ada Compilers support the INTEGRITY RTOS. These optimizing compilers consist of a *language-specific front-end,* a *global optimizer*, and a *target-specific optimizer* and *code generator*.

Conformance to key industry standards provides increased compatibility across different projects and source code files. The Green Hills C compilers fully conform to ANSI X3.159-1989 Standard C (ISO/IEC 9899 and FIPS PUB 160) and support multiple programming language dialects including Strict ANSI, Permissive ANSI, Transition Mode, MISRA C, K+R, and GNU C. The Green Hills C++ libraries are scalable and tuned for the specific level of C++ support requested. Green Hills Optimizing C++ Compilers support multiple dialects including Standard (ANSI/ISO) C++, C++ as defined by The Annotated C++ Reference Manual (ARM, by Ellis & Stroustrop), Embedded C++ (EC++), and Embedded C++ with Templates. Extensive C++ dialect support includes conformance for namespaces and templates, and GNU C/C++ extension compatibility used to build the entire Linux kernel.

Simplified migration

To support legacy and third-party code reuse and integration, the INTEGRITY RTOS can host applications written for a different environment. Developers can integrate legacy applications, such as those that use Linux, VxWorks® or other operating systems with very limited recoding. API support for other operating systems can also be provided.

With the INTEGRITY RTOS' conformant POSIX API calls and/or ISV technology, Linux applications can run on INTEGRITY with minimal to no effort or change. A basic VxWorks API layer supports core VxWorks service calls for Message Queue and Semaphore, Task, Watchdog, and kernel space interrupt services.

Extensive kernel visibility

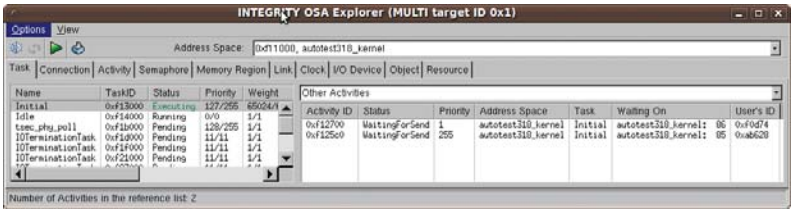
The tight integration between the MULTI IDE and INTEGRITY RTOS provides extensive visibility into kernel events. With unprecedented views into kernel data structures, task roster, and resources, system developers can more easily track down bugs and finely tune systems performance to meet applications requirements.

Multiple-task debugging

The MULTI IDE provides multiple-task debugging for a variety of configurations running INTEGRITY. Each task can be running on a different processor, the same processor, the ISIM simulator, or any combination of these environments for true heterogeneous multiprocessor debugging.

Advanced multiple-task debugging features include:

- The ability to debug multiple tasks across multiple address spaces across multiple processors simultaneously, each task has it own color-coded debugger window.
- A task roster window for tracking the tasks in the system and choosing which tasks to debug. The task window shows useful per-task information such as name, execution status, priority, stack size, and stack use (high watermark).
- The ability to automatically bring up a new debugger window upon task creation.
- The ability to set task-specific as well as address space-wide (also called "AnyTask") breakpoints.
- Simultaneous multiple-task debugging support over both serial and Ethernet for most boards.
- Host emulation of file and terminal I/O.
- The ability to display the relative execution time of all tasks (including the "idle" task).



The INTEGRITY object browser gives the developer a detailed yet simple to navigate snapshot of the entire kernel state, including threads, semaphores, memory regions, and I/O devices.

Supported processors

The INTEGRITY Architecture Support Package (ASP) provides CPU initialization, exception handling, and fast context-switching for the following processor families:

- AppliedMicro Power Architecture
- Analog Devices Blackfin
- ARM Ltd. ARM
- Cavium Networks OCTEON
- Freescale ColdFire
- Freescale Power Architecture
- IBM Power Architecture
- Intel x86/IA/Atom
- Marvell XScale
- MIPS Technologies MIPS
- Texas Instruments DaVinci
- Texas Instruments OMAP

Kernel awareness

MULTI provides a comprehensive picture of INTEGRITY kernel objects, tasks and resources, and their statuses. Even without source, developers can view a complete snapshot of INTEGRITY's state, and can debug and view virtual address spaces.

INTEGRITY debug agent

INTEGRITY includes a powerful debug agent that enables remote debugging of multi-processor systems—including boards and chassis—from a single hardware network connection (TCP/IP Ethernet or serial) to the host and a single instance of the MULTI IDE.

INTEGRITY shell

INTEGRITY provides a target shell, network accessible via telnet or rlogin, that enables you to communicate directly with the target, even before any application code is running. The shell enables loading and unloading of modules independent of MULTI, FTP, listing of tasks and modules, setting network configuration, reading/writing target memory, and performing file system services.

Training and consulting services

Expert training from Green Hills Software consultants allows developers using INTEGRITY to become productive faster and to learn how to take full advantage of the power of INTEGRITY and integrated products.

Training sessions

Green Hills Software holds scheduled training sessions throughout the year in a variety of international locations. Through both lectures and hands-on exercises, attendees are taught how to:

- apply RTOS concepts to their designs
- leverage key INTEGRITY features in their applications
- determine the best mechanism to accomplish a specific objective using the INTEGRITY RTOS
- and much more

Express and *Intensive* training sessions are offered to accommodate a range of familiarity with the INTEGRITY RTOS as well as developers' busy schedules. The Express training includes a quick overview of the INTEGRITY RTOS, while the Intensive training exposes attendees to advanced concepts and techniques used to get the most of Green Hills Software's products. The Intensive training also allows for the flexibility to focus on those concepts of particular interest to attendees.

Quick Start program

Getting started with a new RTOS can take time. Green Hills Software developed the *Quick Start* program to ensure that you will be up to speed developing software as quickly as possible.

After studying how new customers get familiar with our software, we developed the components of the Quick Start program to address every stage of a new project ramp up. This can include on-site installation and configuration of the INTEGRITY RTOS, custom board support package development, application porting, product customization, tool interface development, and general training.

On-site support and consulting

We understand that some challenges are sooner overcome through on-site contact. We also recognize live coaching as a valuable tool to gain better understanding and receive the full benefit of INTEGRITY and related products. To this end, Green Hills Software offers on-site support and consulting with expert engineers.

Custom engineering services

Green Hills Software is world-renowned as the leader in embedded software technology. But some applications have very particular requirements that are difficult to anticipate. For these situations, Green Hills Software created our Custom Engineering Services Division, a group that specializes in custom software development. These engineers can add special features, customize existing products, and invent new technologies. You tell us what you need, and we deliver it exactly how and when you need it.

Partner ecosystem

INTEGRITY is integrated with a variety of popular third party embedded products, including:

- SNMP Research—SNMP
- Visuality Systems—CIFS
- Data Connection—ATM
- iAnyWhere—Bluetooth
- Stollmann—Bluetooth
- DeviceScape—Wi-Fi
- ACE/TAO Open Source ORB
- aicas—Java
- Averna—IEEE 1394
- Raima—RDBM
- RTI—NDDS
- Aonix—Java
- Presagis—OpenGL/X11
- KW Software—SoftPLC
- McObject—in memory database
- M-System—solid state memory
- Swell Software—Portable Embedded GUI (PEG)
- Vector Software—Unit Level Testing
- Objective Interface—CORBA
- Allegro Software—internet applications
- ALT Software—OpenGL/X11
- Embedded Planet—hardware platforms
- IBM Rational Rhapsody—UML 2.0 application modeling
- RadVision—VOIP, SIP, RTP/RTCP
- Esterel—SCADE software modeling
- Altia—Graphics building tools
- TeamF1—Kerberos, K509, TACACS+
- Virtutech—system virtualization
- 3S Smart Software Solutions—CoDeSys IEC 61131-3 development system
- CriticalBlue—multicore analysis tools
- Ixxat—industrial data communications protocols
- HCC Embedded—file system solutions
- TTTech Computertechnik—time-triggered protocols
- Nokia Qt—application and UI framework

Corporate Headquarters

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

European Headquarters

Fleming Business Centre ▲ Leigh Road ▲ Eastleigh ▲ Hampshire SO50 9PD ▲ United Kingdom
ph: +44 (0)2380.649660 ▲ fax: +44 (0)2380.649661 ▲ email: info-emea@ghs.com

Embedded Safety & Security Critical Products

34125 US Hwy 19 North ▲ Suite 100 ▲ Palm Harbor, FL 34684 ▲ ph: 727.781.4909
fax: 727.781.3915 ▲ email: info-sscp@ghs.com

Network Design Center

825 Victors Way ▲ Suite 100 ▲ Ann Arbor, MI 48108 ▲ ph: 734.222.1610
fax: 734.222.1602 ▲ email: GateD-info@ghs.com