

Green Hills Software



INTEGRITY

Secure Virtualization

Confronting the new challenges of embedded devices

Engineers creating the next generation of embedded devices are faced with the challenge of controlling power, footprint, and bill of materials while meeting demand for more capabilities, delivered faster and with higher reliability. Any organization that can achieve these goals while reducing risks will gain significant advantages over the competition.

Virtualization revolutionizes product development

In response to these growing challenges, designers are increasingly turning to system virtualization—a technology that revolutionizes product development. Virtualization consolidates disparate systems onto dedicated virtual machines, running on a single hardware platform. In addition, the hardware abstraction afforded by virtualization enables rapid migration to new hardware, freeing developers to focus on differentiating features and functionality.

Based on the market leading high reliability operating system, INTEGRITY® Secure Virtualization™ delivers on this promise.

Introducing INTEGRITY Secure Virtualization

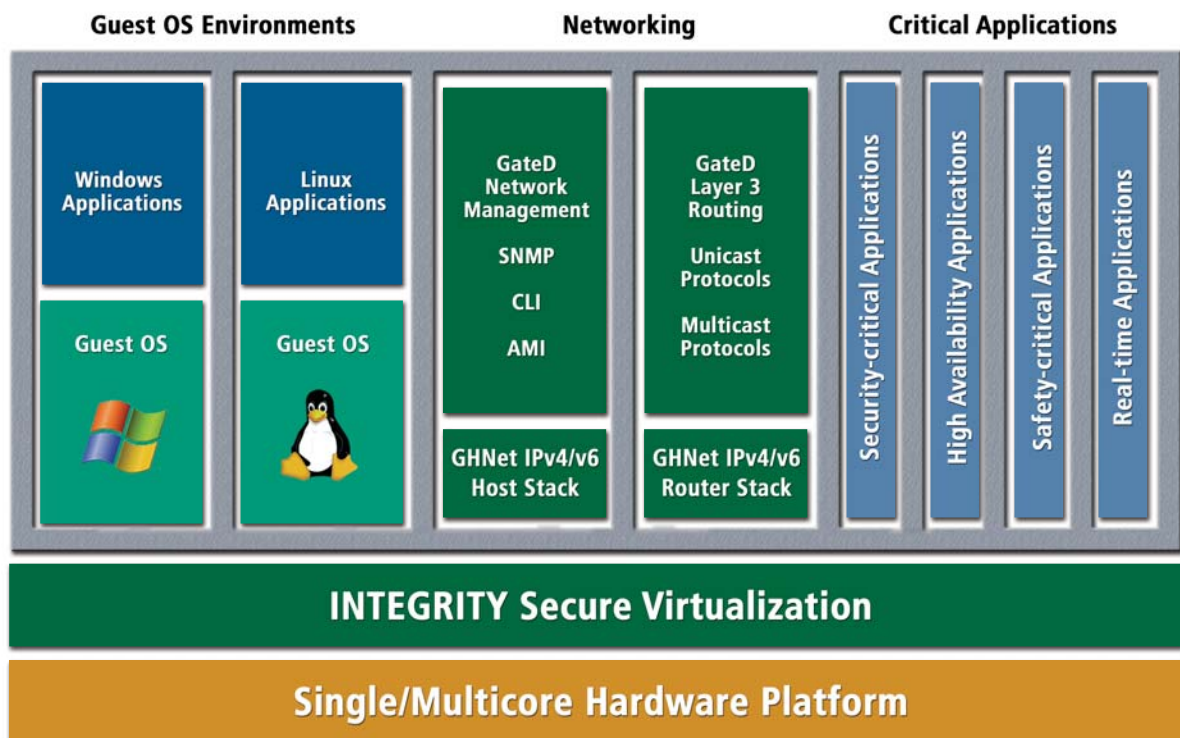
Deployed since 2003, INTEGRITY Secure Virtualization is the industry's most powerful, reliable, and flexible embedded virtualization solution. As shown in the figure below, the platform can host arbitrary guest operating systems alongside a comprehensive suite of real-time applications and middleware. Applications and guest operating systems

are flexibly scheduled across one or multiple cores, can communicate efficiently with each other, and utilize system peripherals according to a strict access control model.

A range of benefits

INTEGRITY Secure Virtualization offers a number of compelling benefits:

- ▲ Lowering production costs through hardware consolidation
- ▲ Faster time-to-market by removing the pain of porting operating systems to new hardware
- ▲ Eliminating the need to port existing applications to new operating systems
- ▲ Longer time-in-market by reusing legacy operating systems and software
- ▲ Higher product pricing power due to increased features in smaller form factors
- ▲ Flexibility to run arbitrary, unmodified guest operating systems, including Windows, Linux, VxWorks, and Android
- ▲ Ability to combine hard real-time and/or reliability-critical processing with guest operating system functionality



INTEGRITY Secure Virtualization delivers a unique hybrid architecture that extends the safety- and security-certified INTEGRITY real-time operating system technology to enable safe execution of trusted real-time critical software side-by-side with untrusted applications running on general purpose operating systems.

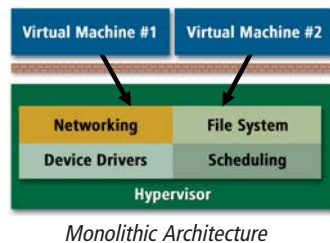
- ▲ A greener product, enabled by hardware consolidation and hypervisor power management
- ▲ Built on the world's only Common Criteria EAL6+ High Robustness-certified operating system technology—for absolute security, total reliability, and maximum availability
- ▲ Products and expert engineering support from a trusted, independent virtualization supplier that you can partner with for the long term

Consolidation requires trust

Organizations trust INTEGRITY technology in systems with the most demanding reliability requirements:

- ▲ NSA-certified secure mobile phones and PDAs
- ▲ FAA DO-178B Level A-certified avionics controlling passenger and military jets
- ▲ FDA Class III life-critical medical devices
- ▲ IEC-61508 SIL3-certified industrial control systems
- ▲ Automotive, consumer, networking, and many other reliability-critical systems

Many hypervisors bundle the software required to support guest environments, such as device drivers and middleware, in a monolithic architecture. The results look much like a general purpose operating system, with unknown exposure and many vulnerabilities. Numerous guest operating systems "escapes" and other subversions have been discovered in other hypervisors, such as Xen and VMware. The INTEGRITY Secure Virtualization architecture relies on a trustworthy security kernel to provide domain isolation, certified to protect against even the most sophisticated attacks.



Features

- ▲ **Architecture families:** supports single and multicore processors across ARM, Power, and Intel architectures and leverages the latest virtualization hardware assist technology, including Intel VT, ARM TrustZone, and Freescale P4080 hardware hypervisor mode. Additional processor support is also available.
- ▲ **Guest operating systems:** supports running multiple instances of Linux, Windows, Solaris, VxWorks and other operating systems
- ▲ **Devices and peripherals:** allows devices and peripherals to be exclusively assigned or shared between virtual environments and applications
- ▲ **Managed communications:** provides for managed inter-process communications (IPC) between virtual environments and applications

- ▲ **Configurability:** provisioning of system resources, including memory and devices, can be fixed at build-time or dynamically adjusted at run-time
- ▲ **Health Monitoring:** provides features for performance monitoring, fault detection, and guest operating system and application restart
- ▲ **Software Development Kit (SDK):** award-winning, MULTI® integrated development environment, addressing the needs of sophisticated software developers for more than 15 years

Market examples

INTEGRITY Secure Virtualization enables engineers to innovate in ways not otherwise possible. The following market examples come directly from Green Hills Software's customer base:

Telecom blade consolidation

- ▲ Execute control plane operating systems (e.g. Linux) alongside real-time data plane processing on a single SoC
- ▲ Take maximum advantage of next-generation multicore network processors from ARM, Freescale, and Intel

In-vehicle infotainment

- ▲ Host audio and video as real-time applications to ensure instant-on, continually reliable performance
- ▲ Consolidate head unit and rear-seat entertainment (Windows) systems to reduce automotive cost and footprint
- ▲ Allow Internet connection without risk of corruption to critical applications

Next-generation mobile devices

- ▲ Run multiple instances of Mobile OS (e.g. Linux) to separate corporate and personal environments
- ▲ Reduce time-to-market by enabling multiple OS flavors to run without porting drivers to each OS
- ▲ Provide common smart phone functions while enabling next-generation security applications such as virtual credit card, virtual ticketing (e.g. public transportation), virtual keys and identification

Electronic flight bag

- ▲ Replaces pilot's pen and paper with PC functionality for calculating take-off parameters and validating navigational charts
- ▲ Enable virtualized Windows Office applications while guaranteeing validation and programming of cockpit avionics using safety-critical native applications on the same portable PC

Intelligent weapons systems

- ▲ Netbook form factor with sophisticated Linux graphical interface
- ▲ Real-time applications provide trusted display of weapons state (securely multiplexed with Linux GUI) as well as safety-critical munitions programming



Corporate Headquarters

30 West Sola Street ▲ Santa Barbara, CA 93101 ▲ ph: 805.965.6044 ▲ fax: 805.965.6343
email: virtual-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