VIRTUALIZATION TECHNOLOGY FROM GREEN HILLS SOFTWARE® AND INTEL HELPS AUTOMAKERS AND SUPPLIERS COMPLY WITH SAFETY STANDARDS.

The Car’s Many Computers

Ever since the introduction of electronic engine control (EEC) in the early 80’s, automakers have been putting more and more CPUs into vehicles, sometimes as many as one hundred. The amount of compute performance required is expected to balloon further when advanced driver assistance systems (ADAS) and more connected-car features come to market. The vehicle cockpit has become a hub for all sorts of electronics for infotainment, digital instrument clusters, driver assistance, secure communications, and safety.

Each time a new computer system is added to a vehicle platform, there is a cost associated with the bill of materials (BOM), weight, cabling, energy consumption, spares, device lifetime management, etc. With the increased availability of multicore CPUs, an increasingly attractive approach is to consolidate multiple electronic control units onto a single automotive computing platform through virtualization. This requires a platform that is safe and secure, and delivers high performance, which is exactly what Green Hills Software® and Intel are making available to automotive developers. Now it is possible to run safety-critical and infotainment applications on the same System-on-Chip (SoC) while satisfying stringent “freedom-from-interference” requirements, like those outlined the ISO 26262 functional safety standard.
Cockpit Challenges

For many drivers, being connected and enjoying a rich infotainment experience is at the top of their list, so apps and services are an important way for automakers to differentiate themselves. But as more third-party software gets downloaded to vehicles, it becomes increasingly difficult to protect against errant or malicious code that could cause disruption to vehicle electronics. Even common operating systems (OSes) like Linux* are known to require regular software updates to plug security holes. Moreover, cars face increasing vulnerabilities when connected to the Internet and mobile networks, which are potential gateways for malware.

One method used to avoid unauthorized or unexpected software behavior is to implement virtualization technology to securely partition the various automotive applications running on a platform. Virtualization introduces a software separation layer via a hypervisor that allows applications to run in dedicated, isolated silos, called virtual machines (VMs). Although every hypervisor is intended to prevent applications from breaching or intruding on each other, they are not all equal in this regard. In other words, hypervisors on the market today provide different levels of safety and security, requiring automotive designers to take a close look under the hood before making a final decision.

Solution Overview

Providing very high levels of safety and security through multiple layers of application protection, Green Hills Software and Intel developed a powerful in-vehicle solution based on a tight interworking between hardware and software. The solution combines the INTEGRITY* real-time operating system (RTOS) and INTEGRITY Multivisor* secure virtualization from Green Hills Software, an Affiliate member of the Intel® Internet of Things Solutions Alliance. The INTEGRITY RTOS provides the capabilities automotive designers need to enforce the policies of separation, damage limitation, and information flow control, as well as to ensure secure networking for today’s more complex and connected applications.

Automotive Application Consolidation

Green Hills Software's safety-certified INTEGRITY RTOS running on the scalable Intel® Atom™ processor E3800 product family, which provides the performance headroom to simultaneously support infotainment, graphics, and safety applications, as shown in Figure 1. This includes reconfigurable digital instrument clusters, backup camera, heads-up displays (HUD), and applications with real-time requirements, such as ADAS and vehicle bus. Applications can run either in a virtual machine or on their native INTEGRITY RTOS. The INTEGRITY Multivisor can combine various general-purpose guest OSes with a comprehensive ecosystem of real-time applications, middleware, and drivers. By consolidating the automotive functions on one SoC, automakers can reduce system cost, complexity, footprint, energy consumption, and associated integration and support efforts.

Application Isolation

Today's operating systems (e.g., Linux* or Android*) and automotive applications can have millions of lines of code, making it challenging for an automaker to ensure the software is safe all the time. But with virtualization, software can be compartmentalized and put into partitions that prevent it from doing harm to safety-critical applications running on the same system, or elsewhere in the car. This capability is particularly useful when a new application is introduced since it can be safely isolated, eliminating the need to examine every instruction and inter-process interaction.

Delivering a high level of application isolation, the INTEGRITY RTOS was designed from inception to allow developers to meet the highest possible requirements for security, safety, and performance. This is achieved by using the proven separation architecture and policies of INTEGRITY with the hardware memory protection in Intel® Virtualization Technology (Intel® VT)2 to isolate and protect embedded applications. INTEGRITY RTOS’ secure partitions guarantee every task has the resources it needs to run correctly, and they protect the operating system and user tasks from errant and malicious code – including denial-of-service attacks, worms, and Trojan horses.
Intel VT has been available on Intel® processors for over 10 years, and over this period, Intel has continued to improve the technology and minimize performance overhead of virtualization. It provides hardware-assist to virtualization software, thereby reducing its size, cost, and complexity. Performance is also improved by reducing virtualization overhead related to cache, I/O, and memory.

Unlike other memory-protected operating systems, the INTEGRITY RTOS never sacrifices real-time performance for security and safety. Traditional operating systems can crash, lock up, or execute uncontrollably, resulting in costly consequences, like a stalled car. This can be avoided with the INTEGRITY RTOS, which protects both critical applications and itself from the malfunctions that can lead to these failures. This is accomplished by providing guaranteed system resources that ensure CPU time and memory resources are always available to individual processes, no matter what any other process attempts to do.

To prevent denial-of-service attacks, the INTEGRITY RTOS 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 windows. Moreover, malicious or unintended events are denied access to system resources, thus keeping system processes running as intended.

**Safety and Security**

Application isolation is fundamental to ensuring safety and security, which is why Green Hills Software's INTEGRITY Multivisor takes advantage of Intel VT capabilities to enable an industry-leading, multi-domain, execution environment. Shipping since 2003, INTEGRITY Multivisor is built on a safety-certified, separation kernel technology that provides highly-assured isolation between safety-critical automotive subsystems and popular infotainment operating systems such as Linux and Android. The INTEGRITY Multivisor is unique compared to other hypervisors, as detailed in the following:

**Hypervisor Overview**

Virtualization technology allows a computing platform to share its resources across multiple software applications, which all run as if they had their own dedicated system. This is done by inserting a software hypervisor (or a virtual machine manager) between the hardware and operating system layer, consisting of two or more guest OSes, as shown in Figure 2. Each guest OS and its associated applications run in a virtual machine (VM) that functions as if it were a dedicated hardware platform. VMs allow the hypervisor to monitor and manage the execution of guest OSes, such as their access to I/O devices, memory, and storage.

**Three Types of Hypervisors**

Hypervisors typically employ one of three architectures: Type-1, Type-2, and microkernel-based.

**Type-1 hypervisors** replace the OS as the software layer controlling the hardware platform (Figure 2), requiring them to replicate OS functionality, including memory allocation and partitioning, CPU time scheduling, and I/O device management. Sometimes referred to as bare-metal hypervisors, Type-1 hypervisors typically have a lean software footprint and provide a fairly secure virtualization mechanism to host dissimilar application environments, but they are not ideal for hard, real-time, deterministic use due to the multiple layers of scheduling of the guest OS's.

**Type-2 hypervisors** operate as an application on top of an existing host OS, such as Microsoft® Windows® or Linux, and take advantage of the OS’s resource management services instead of duplicating them. This type of virtualization solution, shown in Figure 3, is essentially an OS modified to host not just applications but also complete guest OSes. Due to the requirement for this heavyweight layer, Type-2 hypervisors are largely nonexistent in embedded systems.
Microkernel-based hypervisors can be thought of as a hybrid between Type-1 and Type-2, providing the best characteristics of both approaches. They bring virtualization features to a proven, lightweight RTOS and can run native applications directly on the microkernel, which is a key benefit over Type-1 hypervisors. This capability is particularly useful when a guest OS may be unsuitable for critical automotive applications, such as real-time device drivers, network security protocols, fast boot requirements, and high-performance graphics packages.

Figure 4 illustrates an example of a microkernel-based hypervisor, the INTEGRITY Multivisor from Green Hills Software. This hypervisor is particularly well suited for embedded applications because it is built on a Common Criteria EAL6+ High Robustness-certified operating system technology. This foundation ensures the highest levels of security, reliability, and availability.

**Deterministic Performance**

Due to the overhead typically associated with virtualization processes and interrupted latency, there is a valid concern that virtualized platforms will be unable to deliver the real-time and deterministic response required by some automotive functions. As experts in this area, Green Hills Software built a lightweight hypervisor into its RTOS - INTEGRITY Multivisor – and integrated Intel VT to significantly boost the responsiveness of virtualized systems.

As one of the first RTOSes to employ hardware memory-management units (MMUs), INTEGRITY is a true, hard real-time RTOS that never sacrifices real-time, deterministic performance for security and protection, and is capable of responding to events in nanoseconds, guaranteed.

All INTEGRITY kernel services have been carefully optimized to minimize the overhead of system calls (e.g., access hard drive), suspending them, if necessary, to allow time-critical processes to execute. INTEGRITY uses a true real-time scheduler that supports multiple priority levels and enables complete control over the allocation of CPU cycles.

The INTEGRITY RTOS always services the highest priority interrupt with absolute minimum latency. When deterministic performance is of the utmost importance, a critical process can be assigned to a dedicated core on the Intel® Atom™ processor so it runs unencumbered by other processes running on the system.

Application Consolidation, Safety, Security, and Performance

The vehicle cockpit presents challenges and opportunities that demand powerful, flexible, scalable, cost-effective computing platforms. Green Hills Software’s INTEGRITY Multivisor combined with Intel VT create a safe, secure, and high-performance environment for consolidating safety-critical and infotainment applications onto a single Intel SoC. Intel In-Vehicle Solutions based on the Intel Atom processor E3800 product family provide the compelling compute platform automotive designers require for the next-generation designs that must deliver a transformative consumer experience.


---

2. Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, and virtual machine monitor (VMM). Functionality, performance or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit [www.intel.com/go/virtualization](http://www.intel.com/go/virtualization).