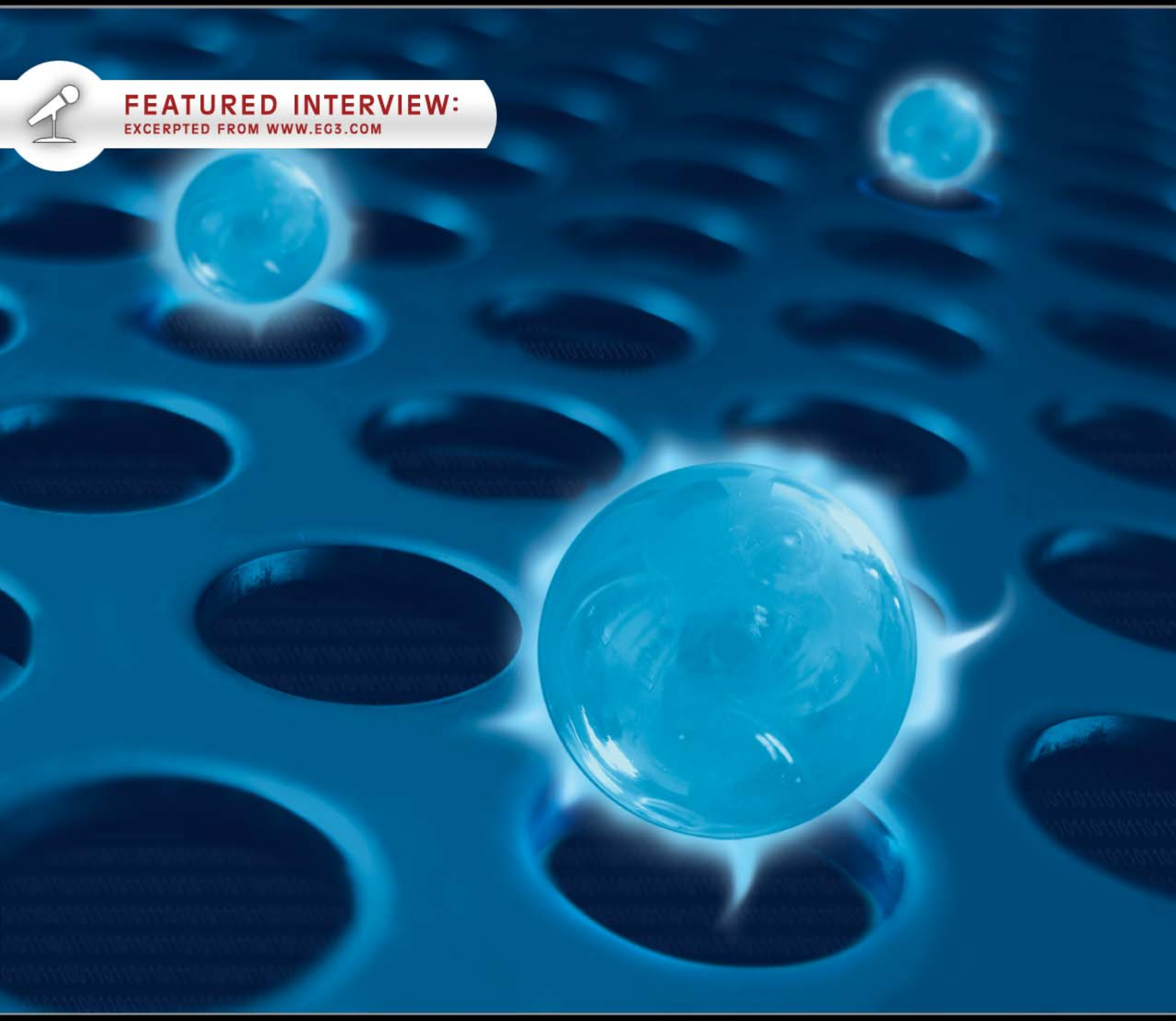
SELECTING AN EMBEDDED RTOS



FEATURED INTERVIEW:
EXCERPTED FROM WWW.EG3.COM

Prepared by:
eg3.com
Jason McDonald, Senior Editor

eg3.com
tel : 510.713.2150
email : info@eg3.com
web : http//www.eg3.com

GREEN HILLS SOFTWARE: EAL6+ SECURITY FOR MISSION CRITICAL APPLICATIONS

15 December 2008: EAL6+ Security for Mission Critical Applications

INTERVIEWEE. DAVID KLEIDERMACHER
CHIEF TECHNOLOGY OFFICER
TEL. 805.965.6044
EMAIL. bfrench@ghs.com
COMPANY. GREEN HILLS SOFTWARE
WEB. http://www.ghs.com/

Q. **First of all, tell us a little bit about yourself and your responsibilities at Green Hills Software.**

A. I have been at Green Hills Software for 17 years, currently as CTO. I am responsible for the company's technology direction. I interface with sales and customers to both communicate our technology vision as well as incorporate the proceeds from those interfaces into our technology strategy and solutions.

Q. **Elsewhere in the guide, we have a product Q&A interview on Green Hills, but would you just give us the briefest of overviews to Green Hills and your products or services?**

A. Green Hills is the foremost technology innovator in the areas of high reliability real-time operating systems (RTOS), software development tools, and related services and custom solutions. Our products and services enable our customers to achieve total reliability, absolute security, maximum performance, the lowest manufacturing and development costs, and the fastest time to market for their electronic products.

In addition, Green Hills has a subsidiary, INTEGRITY Global Security, LLC, (http://www.integrityglobalsecurity.com/) that provides security technology and services to the enterprise market.

Q. **In this keynote interview, we wanted to focus on "security" especially "security" as defined as security against malicious hacking or outside intrusion. Green Hills recently announced it reached EAL6+ Operating System Security Certification, but first would you please explain to us what the different levels of Common Criteria security levels (EAL) mean to different sorts of applications?**

A. Common Criteria security levels range from 1 to 7, in increasing assurance (or confidence that the product achieves its claimed security functions). EAL 6+ is roughly equivalent to EAL 7 and maps to what the U.S. Government deems to be "high robustness". High robustness systems are required for the protection of high value resources against determined and sophisticated attackers. There is no obvious mapping of applications to each common criteria security level, however. Developers need to assess the value of their resources against the probability of attack and the expected sophistication of the attackers. Sadly, much of the world's critical infrastructure is currently managed by IT products that are unable to meet high robustness requirements. Common general

purpose operating systems, firewalls, databases, and other IT products come in at EAL 4 or lower.

Q. **What are the different technical levels of security in EAL4+ vs. EAL 6+, the former being reached by Linux and Windows and the latter being reached by INTEGRITY?**

A. The EAL4+ specifications to which Windows and Linux have been certified state protection against "inadvertent or casual attempts to breach the system security." That is not even close to secure by anyone's definition.

EAL6+ is certified to protect classified information and other high value resources from hostile and well-funded attackers. This is secure by anyone's definition.

Technically, EAL4+ does not require that evaluators even examine the source code. EAL6+requires formal methods to mathematically prove the security policies, formal correspondence between design and implementation, complete test coverage of all functional requirements, and penetration testing by the NSA which has complete access to the source code.

Q. **Do you know what levels of security other common hard RTOSes have reached - for example, *LynxOS* from LynuxWorks or *Neutrino* from QNX? How is this new solution different from other RTOSes that have played in the DOD178b space?**

A. In December 2008, LynuxWorks announced that *LynxOS* was on a path towards achieving EAL 4+, which, if achieved, would put it in the same category as Windows and Linux with respect to security assurance level.

In April 2008, QNX announced that *Neutrino* has entered an EAL4+ evaluation with the Canadian government. Once complete, this too will put *Neutrino* in the same security assurance class as Windows and Linux.

The Common Criteria states that EAL4 is the highest level that can be feasibly retrofitted; thus it is unlikely for any legacy RTOS to reach EAL 5, and beyond hope to reach EAL6+/high robustness. INTEGRITY technology was able to reach EAL6+ because it was designed from the ground up to meet the highest levels of safety and security.

INTEGRITY is not only the first operating system technology certified to EAL6+, it is also the only one that has even begun the stringent, multi-year NIAP evaluation process that requires NSA involvement. This status can be easily verified because the NIAP keeps an online list of products that have either completed evaluation or are currently under evaluation.

Because of its advanced design, INTEGRITY is the only technology that has met both the highest aviation safety level (DO-178B Level A) and the highest security robustness level (EAL6+/high robustness). And INTEGRITY has more than 10 years of customer deployment. The only way for other vendors to accomplish this same three-peat is to start from scratch, throw away the legacy RTOS, and create a new product which will likely require at least a decade for development, deployment, and certification, assuming the product can meet other customer requirements for performance, cost and power efficiency, quality development tools integration, etc. With VxWorks AE, Wind River showed how easy it is for a new operating system design to fail to meet customer requirements: the product was introduced in 2001 and then discontinued from the general commercial market soon after, never making it past version 1.1.

Q. **Many embedded applications - especially in regulatory environments like military or medical - have lots of "legacy code." Are there ways to avoid re-writing this code, but getting some of the advantages of EAL6+ security?**

A. There are a number of ways, but the two most popular and promising methods are: 1. API portability, and 2. System virtualization. In the operating system world, API portability is achieved with conformance to POSIX, the only ubiquitous operating system API standard. INTEGRITY was the first operating system to be certified conformant to the modern POSIX.1 system interface specification (POSIX.1-2003). Other vendors, as well as Linux, have POSIX-like APIs. Thus, a lot of open source software can be easily ported to POSIX operating systems.

With system virtualization, the entire legacy operating system and its applications run under a virtual machine. This makes portability far easier, enabling binary reuse of applications, network protocols and other middleware, and other operating system components. Modern hardware is making it practical to run *full virtualization*, in which the operating systems are unmodified (as opposed to *paravirtualization* which requires operating system modifications, reducing portability and maintainability), and still execute with good performance. Green Hills first began providing system virtualization with Linux in 2003 and later added full virtualization of Intel Architecture platforms (and hence the ability to run unmodified versions of Windows, Solaris, Linux, etc.) in 2005.

While virtualization does not, in itself, enhance security, it can enable security-critical components to co-exist with legacy software on a single computer. It is this type of hybrid virtualization that enables many compelling architectures, including the ability to mix hard real-time and Linux/Windows in a secure manner; the ability to mix and match safety-critical functions with a Linux/Windows HMI, etc. We are seeing applications of this in automotive, military/aerospace, industrial control and critical infrastructure, gaming, and of course in various enterprise IT systems.

Q. **Apparently you use virtualization to achieve some of these characteristics, but other vendors ranging from Wind River to VirtualLogix to even VmWare offer virtualization - can't one use these solutions to achieve similar effects in terms of security?**

A. Actually, no. With the Green Hills approach, virtualization is performed within an application component and hence cannot impact the security boundary enforced by the certified INTEGRITY kernel. However, other approaches to use a hypervisor as the agent providing supervisor-mode resource management essentially end up creating just another operating system. Even so-called type-1 hypervisors, such as VMware ESX, designed for mission critical servers, are really very complicated pieces of software that are being entrusted with system security. On June 2, 2008, VMware announced its EAL4+ certification for ESX server, claiming it could now be used "for sensitive, government environments that demand the strictest security." Three days later, on June 5, several severe vulnerabilities in the certified hypervisor were published to U.S. CERT's National Vulnerability Database. Among other pitfalls, the vulnerabilities "allow guest operating system users to execute arbitrary code."

This should not come as a surprise given what I just explained EAL4+ means relative to EAL6+/high robustness.

VMware and VirtualLogix may have highly functional hypervisors, but they were not designed for high assurance and cannot be trusted to protect high value resources from sophisticated attackers (at least not until they can achieve a high robustness certification).

The other big difference between the INTEGRITY approach and other hypervisors is the ability to host native, security-critical applications. Because INTEGRITY is an operating system in its own right, other high assurance / high robustness applications can run on

top of it. In contrast, a traditional hypervisor only runs guest operating systems; it does not provide a platform for hosting trusted applications. A good example of this is a version of our INTEGRITY PC technology that has been deployed for government use. This product enables multiple disparate security levels to be managed on a single PC. Each security level can have its own dedicated Windows (or Linux) virtual environment. To do this on a laptop or desktop PC, we employ a multi-level secure window manager that can display the different environments with proper security labeling and provide a trusted path for shared keyboard and mouse devices. Because this software must be trusted, it must run natively on INTEGRITY. It cannot be trusted if controlled by an EAL4+ guest operating system.

Q. **How much does this cost? What are the business models of engagement? Traditionally, these sorts of high-level security solutions have been so expensive that only really high-end military, medical, and commercial applications have been able to deploy them. Are there any ways that Green Hills has brought the cost down so that a broader range of applications can be made secure?**

A. We have business models that bring the cost of a deployed secure virtualization solution to similar or even lower levels found in common commercial desktop virtualization products. We also have a number of customers who require custom solutions, and we have a services organization that has been developing and deploying such solutions for many years. The precise business model depends on how the technology will be deployed. As we have always been, we are committed to remaining very flexible with respect to business model.

Q. **Thank you for this interview.**