Is your RTOS safe and secure?

Defense primes and system integrators are demanding that software for their programs meet safety-critical requirements and have built-in security. Meanwhile POSIX certification and Linux continue to influence product development and in the case of Linux — heated discussions.

Vendors of real-time operating systems (RTOS) find themselves being pulled in two directions at once. Their customers demand lower costs while at the same time want more security and safety certification than ever before.

Click here to enlarge image

Developers at Boeing Integrated Defense Systems chose an RTOS from Green Hills for their X-45 Joint-Unmanned Combat Air System (J-UCAS). The unmanned craft is a DARPA project for use by the Air Force and Navy.

Military designers want commercial off-the-shelf (COTS) hardware and software to build less expensive, more easily updated computers. Yet at the same time, rising concerns about safety are forcing regulators to enforce ever-stricter standards for software security, determinism, partitioning, and immunity from hacking attacks.

As the opening years of this century are teaching the world, security always comes first.

Safe and secure

Defense contractors are requiring software vendors to certify their RTOSs to one or all of three safety and security standards: ARINC 653, DO-178B, and EAL-7.

ARINC 653 requires that each operating system must have dedicated time, space, and resources on its computer. Those partitions mean that software applications of various levels can run on the same processor.

Regulators at the U.S. Federal Aviation Administration (FAA) require DO-178B as the software-security standard for all commercial planes. Pentagon planners have also adopted the standard, which ranges from Level A — where a software crash would have fatal results — to Level E — a software crash would have no impact.

The U.S. National Security Agency (NSA) enforces the third standard: Common Criteria Evaluation Assurance Level (EAL). EAL measures an operating system's security strength and its ability to handle classified and open data on the same machine, ranging from the weakest at Level 1 to the ultimate security, Level 7.

No RTOS has yet reached that mark. "Some people are not sure if this can even be reached, but we believe it can," says Marc Serughetti, director of product management at Wind River Systems, Alameda, Calif.

However, defense contractors have recently been extending ARINC 653-certified platforms to support higher levels of security, Serughetti says. On platforms such as the C-130M cargo plane, customers require an RTOS that meets ARINC 653 as well as DO-178B requirements.

Software engineers at Wind River meet the challenge by extending their VxWorks AE653 product to be certifiable to DO-178B. The result is called Platform for Safety Critical ARINC 653, a device that enables applications of different security levels to share the same computing resources.

As part of this effort, officials at Wind River and Smiths Aerospace, in Grand Rapids, Mich., announced earlier this year they would extend Platform for Safety Critical ARINC 653 to meet the National Security Agency's highest security level, EAL-7. The software will be used in Boeing's C-130 Avionics Modernization Program (AMP), in the avionics system aboard 500 Air Force transport aircraft.

To reach that level, the platform will use a Multiple Independent Level Security (MILS) architecture, to store and transfer data at varying security levels, from secret to classified to unclassified. Its secure partitioning will let users add applications at a later date without recertifying the system.

Designers at EADS subsidiary Eurocopter, in Marignane, France, also chose Platform for Safety Critical ARINC 653 for two new helicopters, the civilian Super Puma EC 225 and military Cougar EC 725. On both aircraft, it will act as the software foundation for flight display systems. Likewise, Eurocopter designers expect DO-178B certification later this summer.

Click here to enlarge image

Army leaders chose a LynuxWorks RTOS for the Common Avionics Architecture System (CAAS) on special operations helicopters like the MH-60.

SmartKernel, a new product from Aonix in San Diego, is a safety-critical kernel that uses ARINC 653 partitioning between multiple components that are individually certified to DO-178B.

"The SmartKernel technology is important for next-generation safety- or mission-critical systems that require the protection of one application from the potential failure of another application on the same board," says Greg Gicca, the company's director of product marketing, Ada Products. "SmartKernel provides time and memory partitioning to support multiple safety levels on a single embedded processor board. By using multiple safety levels on a single board, developers are able to reduce the hardware cost of embedded systems since fewer physical processors are needed to implement an embedded system."

Developers using SmartKernel will be able to create single-board systems that run multiple applications in multiple languages — including C/C++, Ada83, Ada95, and embedded Java, Aonix officials say.

Engineers at LynuxWorks in San Jose, Calif., are currently developing a Common Criteria level EAL-7 secure separation kernel. Such a kernel would eliminate the government's OS-evaluation process by ensuring that any OS, including Linux and other open standards–based systems (like Solaris, HP-RT, HPUX, and UNIX), could run in a secure partition in an EAL-7 environment.

"The old paradigm of 'security through obscurity' is out the window," says LynuxWorks chairman and chief executive officer Inder Singh. "Perception is that you cannot trust software that you did not create yourself. Reality is that with the advent of an EAL-7 separation kernel, you can. We're on the cusp of reaching a monumental milestone never before achieved in the embedded software industry."

LynuxWorks planners cite a significant overlap between the DO-178B and Common Criteria (EAL) standards, and predict their LynxOS-178 product will soon be certified to EAL level 4 or 5.

"In the next 12 months, we'll see Linux reach EAL level 4-plus," says Bob Morris, president of LynuxWorks. "They'll start with SE Linux (safety enhanced) and go through the long process of code analysis. And in Linux there are lots of lines of code. A year from now, you'll see prototypes of EAL level 7 microkernels."

The strength of small-sized microkernels is that several can run on a single device. "That's for systems that require multiple levels of security, so you could have unclassified, classified, and top secret on the same OS and hardware," Morris says. "You can't do that today; you must use several pieces of hardware. So microkernels will save cost and weight."

RTOS vendors are racing to develop separation kernels with time and space partitioning, so each partition can run its own OS.

Safety-certified firmware

The increasing demand for safety-certified embedded software is a challenge not only for operating-system vendors, but also hardware manufacturers.

Until recently, contractors like Rockwell Collins and Honeywell would build their own hardware, then load an RTOS from Green Hills Software in Santa Barbara or Wind River on it, says Grant Courville, product marketing manager for safety-certifiable software, graphics, and Compact PCI at Curtiss-Wright Controls Embedded Computing in Kanata, Ontario — his division was formerly called Dy 4 Systems.

When COTS procurement took off, contractors began loading those RTOS brands onto commercial hardware. This works, but it ignores the software that runs underneath the operating system — the embedded system called firmware, Courville says.

Therefore, Curtiss-Wright engineers created a product called Certifiable Foundation Firmware (CFFW), designed to simplify the process of winning DO-178B safety certification.

CFFW is an RTOS-independent process that boots as soon as the power comes on. It acts as the layer of glue between the hardware and the RTOS, board support package, and application software. It has been certified to DO-178B Level B, while running on Curtiss-Wright's S/DMV-181 6U VME single-board computer. The company is working on Level A certification. It has customer projects underway with all the major certifiable COTS RTOS products: CsLEOS from BAE Systems in Johnson, N.Y., Green Hills' Integrity-178B, LynuxWorks' LynxOS 178, and Wind River's VxWorks AE-653.

"We've traditionally been more of a hardware vendor, but in the last five years, and particularly in the last two years, our customers have had much more interest in software," Courville says, noting that attaining DO-178B Levels C to A is now an absolute requirement in the latest request for proposals.

POSIX

Many players in the embedded RTOS community are talking about the importance of POSIX compliance.

The loudest voice in that crowd belongs to experts in the U.S. Navy, who have demanded that all future software agrees with their Open Architecture Computing Environment (OACE). In practice, that means every RTOS must agree with POSIX, the Portable Operating System Interface.

Navy Open Architecture mandates all future software development be open standards–based, to ensure easy future upgrades on ships, aircraft, submarines, and other platforms. That covers the future platforms DD(X) and the Littoral Combat Ship, as well as 75 surface-ship programs today like Lockheed Martin's Aegis COTS refresh and Raytheon's shipboard self-defense system (SSDS).

The only exception Navy leaders allow is for very small devices, such as a simple sensor that carries just enough memory to support a microkernel.

A POSIX-certified RTOS can run software from any other system, as long as it uses the same API (application programming interface). The Integrity 5.0 RTOS from Green Hills has been certified to that standard, while most others are compliant (the lowest standard) or conformant, Green Hills officials say.

There are even different levels of conformance, reaching from the lowest — profile 51 — to the highest, profile 54, as certified by the Institute of Electrical and Electronics Engineers (IEEE).

"Last year, POSIX and Linux were just being heralded for military applications; now they're reality," LynuxWorks' Morris says. Open standards gain momentum fast in military applications because they ease application portability, software reuse, and system interoperability.

"Also, military spending can't continue at this rate, so an open operating system is the best way to keep adding technology inserts through development spirals," Morris continues. "The bottom line for an RTOS company is if they're not POSIX-conformant, they'll be left out."

LynuxWorks' entire product line is POSIX conformant, including LynxOS RTOS, LynxOS-178, and Blue Cat Linux 5.0 — the company's enhancement of Linux 2.6.

LynxOS itself is used on the Integrated Data modem that supplies combat situational awareness for pilots of BlackHawk helicopters, Raytheon's Patriot missile trainer, and the British Navy's Thomson Marconi Sonar. Army systems include the Future Combat System's fire-control network and non-line-of-sight cannon, and the Common Avionics Architecture System for special operations helicopters like the MH-60, MH-47, and A/MH-6.

Planners at Wind River say they pledged in July to expand their support for POSIX. Their VxWorks General Purpose Platform is currently POSIX compliant. And VxWorks 6.0 — due out later this year — will reach full conformance with profile 54. The profile enables an RTOS to have a standard POSIX interface without running a full UNIX kernel.

Green Hills Software offers the Integrity operating system, available in flavors such as Integrity 5.0 POSIX, the Velosity microkernel 5.0, and Integrity-178B.

"The Integrity RTOS provides everything that developers are looking for from embedded Linux — POSIX interfaces, roust networking support, no royalties, and source-code availability — but the Integrity RTOS is orders of magnitude smaller, faster, more reliable, and more secure," says Dan O'Dowd, founder and chief executive officer of Green Hills Software in Santa Barbara, Calif.

Developers at Boeing Integrated Defense Systems chose Integrity for their X-45 Joint-Unmanned Combat Air System (J-UCAS). The unmanned craft is a DARPA project for use by the Air Force and Navy.

Integrity 5.0 features POSIX certification, simplified application development, support for shared-memory multiprocessor systems, and a platform for resource-constrained systems, Green Hills officials say.

POSIX certification provides faster time to market and enables the sharing of software from various operating systems and between product versions and generations. It also gives developers vendor independence, so they can procure systems from multiple suppliers, Green Hills officials say.

The U.S. Army's Joint Tactical Radio System (JTRS) is an example of a new defense program requiring POSIX, Green Hills officials say. In November, Boeing chose Integrity for two Software-Defined Radio (SDR) programs; JTRS Cluster 1 and the U.S. Air Force's satellite-based Family of Advanced Beyond-Line-of-Sight Terminals (FAB-T).

JTRS radios are based on the Software Communications Architecture (SCA), which requires POSIX programming interfaces for software portability, and an efficient, low-overhead operating system for maximum system throughput and low power consumption. It also demands a partitioned memory design to isolate classified data and processes.

"The SDR concept is such a fundamental change that all communications vendors are going to have to change, not just military but also commercial," O'Dowd says. "Within the next five years, there will be no reason to build custom hardware to do communication protocols."

Users will not need individual devices for different wireless standards like FM, AM, TDMA, CDMA, GPS, UHF, VHF, Bluetooth, and WiFi, because software will evaluate all those waveforms in a single device, O'Dowd adds.

Company information

Aonix	San Diego, Calif.	800-972-6649	www.aonix.com.
Curtiss-Wright Controls Embedded Computing	Kanata, Ontario	613-599-9191	www.dy4.com.
Enea Embedded Technology	San Jose, Calif.	866-844-7867	www.enea.com.
Express Logic	San Diego, Calif.	858-613-6640	www.expresslogic.com.
Green Hills Software	Santa Barbara, Calif.	805-965-6044	www.ghs.com.
LynuxWorks	San Jose, Calif.	408-979-3900	www.lynuxworks.com.
Wind River Systems	Alameda, Calif.	510-748-4100	www.windriver.com.

Linux makes strides in real-time world, yet RTOS vendors are still skeptical

The Linux open-source operating system is already strong in the commercial networking and telecommunications markets, often running as embedded software. In recent years it has crossed over to the military and aerospace markets, where designers use it for non-real- time networking servers.

Leaders at Wind River Systems in Alameda, Calif., see VxWorks and Linux as complementary systems, one good for hard-real-time jobs, one good for general embedded jobs, says Marc Serughetti, director of product management at Wind River.

"Linux can do real time, but the question is how much? What is hard real time and what is soft real time?" he says. There is no specific, since an operating system's speed depends on its platform, Serughetti says. A network-centric operation would optimize protocol performance to pass data quickly, whereas a flight control system would demand fast response times.

No matter how it is used, Linux development tools still need to improve, Serughetti says. With that in mind, planners at Wind River announced early this year a plan to develop Red Hat Embedded Linux for the device software-optimization market. That product will be targeted at the commercial-off-the-shelf (COTS) segment of the device software market for carrier-grade network equipment like high-end routers and switches.

Earlier this summer they announced Workbench 2.0, an integrated development environment (IDE) that supports multiple operating systems, processors, languages, and target environments. The software enables developers to create applications in VxWorks, Linux, or proprietary operating systems.

"There are some good places for Linux and some not," says Adrian Leufven, vice president of marketing at Enea Embedded Technology, in San Jose, Calif. "The drawbacks of Linux include its large size and lack of real time. The benefits of OSE include its small footprint, real time performance, and support for DSPs."

Enea's latest product — Enea Orchestra includes the hard-real-time OSE system and an embedded Linux operating system, intended to run on different processors. Developers use MetroWerks' Code Warrior to build platforms with both operating systems.

The best application for Orchestra would not be mobile telephones, but rather big, central communications nodes running multi-CPU systems, Leufven says. In that application, Linux would run on the management plane, while OSE ran on the PowerPC or ARM, and OSEck (a scaled down version) would run on the DSP.

"High availability communications applications frequently combine a server-based IT component with a time-critical embedded component. The best solution for these applications is often a hybrid solution utilizing two operating systems: Linux for the IT component and a hard-real-time OS for the time-critical embedded component."

However, "don't run out and buy a Linux RTOS yet," warns Dan O'Dowd, founder and chief executive officer of Green Hills Software in Santa Barbara, Calif. "Everyone but us is going open-source. It represents a short-cut to catch up to Green Hills."

Linux may be royalty-free in terms of money, but it costs more in computing, since it demands extra memory to process all the code, he says. Furthermore, Linux is not high-security memory protected, and does not comply with POSIX, O'Dowd says.

"Whether you want to use DO-178B, EAL-7, or resource-constrained systems, you'll never get there with Linux," he says. "That's because they're trying to adapt a desktop environment to be embedded, while we built it from scratch."

Linux is less popular, because it is not up to standards for real-time speed or security partitioning, says Bob Morris of LynuxWorks in San Jose, Calif. "Linux is satisfactory for 80 percent of all non-secure, non-safety applications. But you'll never see Linux for flight control applications because there'd be too much work to do. And then it wouldn't really be Linux anymore, anyway."

Designers who need a real-time operating system would probably choose another system if they are concerned with priority interrupt times, he says.

"Real time has different meanings to different people," Morris says. "If you're running the 2.6 kernel of Linux, loaded with features, maxing out its processor, you could get a 2-millisecond interrupt response time. That could be microseconds for a hard-real-time OS."

"We say hard real time is in the sub-10 number of microseconds in response time, not in milliseconds, which is detectable by people," O'Dowd says. In contrast, soft real time means a system will usually — not always — respond in time.

When designers are shopping for an RTOS, they care primarily about issues like royalty cost, security certification, development tools, and code portability. When it comes to speed, they simply ask whether it's real-time or not.

"I'm more worried about people who buy Linux and think they're getting real time, because it's nowhere near," O'Dowd says. "You can get real time in Integrity, VxWorks, LynxOS, or CUNIX, but Linux is 10 or 100 times slower. That's because it's designed for the desktop, where the performance standard was that it's OK for the computer to hang up for a tenth of a second or two.

"It's like entering a Mack truck in Le Mans," O'Dowd says. "Both a racecar and a truck have a steering wheel, both have an engine, and both have a suspension, but it's all the wrong magnitude. If you want to build a racecar, start from scratch or from a similar kind of car. But don't start with a truck and try to change it, because you'll fail. And that's embedded Linux."

Still, its wide use and open standards have won it a place on several platforms, including Force XXI Battle Command, Brigade-and-Below (FBCB2) and many submarine fire-control and command-and-control systems.

"Submarines use it because they need speed, power, and size while getting the latest technology, and proprietary operating systems couldn't do it," LynuxWorks' Morris says.

The number of Linux adoptions in military platforms could accelerate soon. "In the next 12 months, we will see some Linux types develop to be 100 percent POSIX conformant," Morris says. They do not have far to go; Linux is 94 percent compliant already, he adds.

Small computer, small RTOS

Engineers at Express Logic in San Diego have designed a real-time operating system (RTOS) to work with small computers.

Defense contractors usually design computers with a control processor like a PowerPC running on top of a digital signal processor (DSP) to crunch the numbers. Now recent designs are shrinking that platform down to a single processor, to save cost, weight, and battery life.

However, when they try to load an RTOS onto that system, they face a problem, says Bill Lamie, chief executive officer of Express Logic in San Diego. Mainstream operating systems like VxWorks and Linux do not run well on DSPs because they use so much code, and that overhead can slow them down on a single chip.

Lamie and his team claim they solve this problem with Express Logic's ThreadX, a royalty-free RTOS that is designed to run on devices with restrictions in memory, cost, or processor speed. Until now, that has meant digital cameras, wireless networking, and printers, with companies like Hewlett-Packard or Panasonic.

ThreadX is currently running on an infrared camera from Xybion Electronic Systems Corp. in San Diego, used by surveillance planes for counter-terrorism.

"The advantage of ThreadX is its small size, so it requires very few files to have an operating system on your embedded gadget," Lambie says.

That is also good news for power efficiency because a smaller RTOS runs fewer cycles so it needs less power and less memory, says John Carbone, vice president of marketing at Express Logic. "VxWorks has tremendous awareness in military and aerospace. It's smaller than Linux but is still much larger than ThreadX. It offers hundreds of services, and it has every feature you could ever want; that's its strength. But if you want something that's compact and efficient, look to ThreadX."

In March, the company announced embedded memory protection (EMP) for embedded applications using the ThreadX operating system. EMP enables developers to set up watertight compartments around threads, preventing possible bugs from damaging other threads or the kernel. The compartment would contain any damage, using a fail-safe mode to keep the computer running at reduced speed until being repaired.

The networked RTOS

Vendors of real-time operating systems (RTOS) view the latest Internet Protocol version 6 (IPv6) as more important than POSIX, because the initiative covers the entire Department of Defense, as opposed to one branch of the Navy, says Marc Serughetti, director of product management at Wind River Systems in Alameda, Calif.

It will replace IPv4, the 30-year-old standard that has governed traffic on the Internet since its inception. With a 32-bit address space, IPv4 cannot handle growing demands for address space, mobility, or security for peer-to-peer networking.

In contrast, IPv6 supports a 128-bit address space. In the short term, that change will solve the shortage of IP addresses, and in long term it will allow tightened security, better connections for mobile devices, and improvements for routing and networking autoconfiguration.

Leaders at the U.S. Department of Defense are so excited about the promise of IPv6 that they have mandated full network compliance by 2008. Already, all department acquisitions taking place after October 2003 must be IPv6-compatible.

The standard is already spreading through the commercial world. On July 22, ICANN (the Internet Corp. for Assigned Names and Numbers) added the IPv6 nameserver address to the Internet's root server system. The standard will be implemented at first in Japan (.JP) and Korea (.KR), then France (.FR), before spreading worldwide.

At the network level, IPv6 builds better security through authentication, making sure a data-sender is who he claims to be. At the operating system level, it helps ensure secure and non-secure data are not mixed.

IPv6 does not directly affect an OS, but does impact its network stack, Serughetti says. No one builds isolated devices any more; they network everything from automotive to industrial applications, therefore vendors package the network stack along with the OS.

During the transition, Wind River will build dual stacks to cover IPv4 and IPv6. "We have a small number of customers using IPv6 now, but you will see it explode in the next couple of years," Serughetti says.

That networking trend is also driven by the Future Combat System, since Army planners are calling for auto-reconfigure backup systems, to enable seamless recovery if the primary system goes down, says Grant Courville, product marketing manager for safety certifiable software, graphics, and Compact PCI at Curtiss-Wright Controls Embedded Computing in Kanata, Ontario. It is supposed to be the ultimate in distributed processing, and enable more fault-tolerance than ever before.

That can be a challenge for RTOS provides because to maintain safety certification, they must functionally partition across processors, slots, and chasses. That means they now need a communication link above the TCPIP/IPv6 to reach between those nodes, without worrying about where each system is, Courville says.

Military & Aerospace Electronics September, 2004
Author(s) : Ben Ames