

Real-time software **goes modular**

Reliability and security are crucial for embedded real-time operating systems in mission- and life-critical military and aerospace applications, so RTOS designers seek to improve their offerings by isolating and fine-tuning the most important parts of their operating systems.

As they try to sell embedded real-time operating systems (RTOSs) to defense contractors, software vendors have a lot of demands to meet.

Planes, trucks, and ships increasingly rely on automated controls using commercial off-the-shelf (COTS) components and a standardized Windows-style interface. So defense prime contractors are demanding an RTOS that is secure from hackers and viruses, uses very little memory, responds quickly to priority interrupts, and works well with COTS components and relatively old versions of Windows.

Those are a lot of demands, but a lot is at stake. When sending signals to a nuclear-armed bomber or to an unmanned aerial vehicle (UAV) operating autonomously, there is no room for a system crash.

Traditionally, the prime directive for an embedded RTOS has been to make it reliable enough to prevent the operating system from crashing in the middle of a mission. But to build a truly safe system, developers must place security first.

"Basically all new infrastructure is being miniaturized, controlled by embedded systems, and then put on the Internet," says Dan O'Dowd, president and chief executive officer of Green Hills Software in Santa Barbara, Calif.

"Security is tougher than reliability; because unreliable security isn't secure," he



Above: This STOVL (short takeoff and vertical landing) version of the J-35 Joint Strike Fighter uses a Green Hills RTOS.

says. "If the system fails, then you can get around it."

DO-178B

Green Hills's answer to this challenge is Integrity, a DO-178B-certified RTOS. Auditors from the U.S. Federal Aviation Administration (FAA) certify software security for all commercial planes according to the DO-178B standard, created by the Radio Technical Commission for Aeronautics — better known as the RTCA — in Washington.

Leaders of the U.S. Department of Defense (DOD) now require DO-178B for military aircraft, too. Five grades of certification rank the effect of a software crash, from catastrophic (A) to none (E). In a nutshell, the certification means that an error in any software application will not stop another application from running.

Effectively this system of classification helps software developers put a security priority on the most mission- and life-critical software routines. For more information on the DO-178-B approach, contact the RTCA on the World Wide Web at <http://www.rtca.org>.

For instance, engineers from Rockwell Collins in Cedar Rapids, Iowa, were designing avionics for the Sikorsky S-92, a 20-passenger commercial helicopter, they needed an operating system to run the Multi-Function Display application, which displays and manages primary flight data and navigation data.

For the Motorola PowerPC-based system they chose the Green Hills Integrity-178B RTOS since it was certified to Level A of the DO-178B standard.

To achieve DO-178B requirements, the RTOS provides time, space, and resource partitioning between all applications running on the same hardware. It also achieves high security by protecting memory and real-time scheduling.

ARINC-653

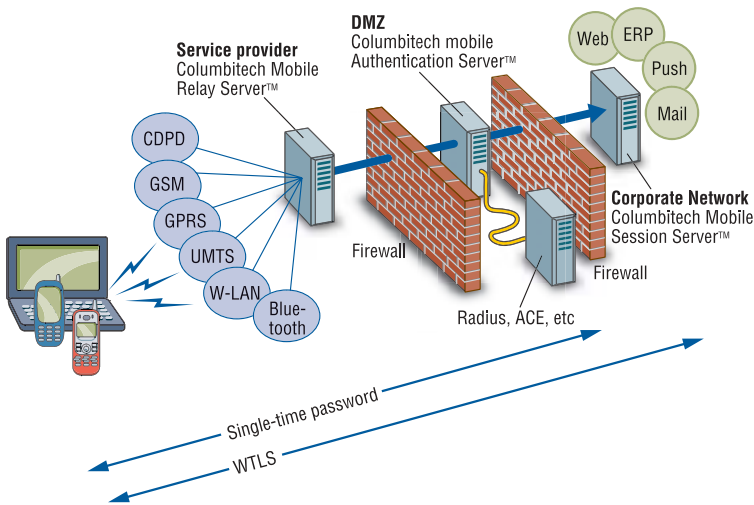
Another standard certifies those software partitions; ARINC-653 is an APEX (application/executive) interface for avionics operating systems and software applications. Its partition requirement means that software with various levels of criticality can run on the same processor. See <http://www.arinc.com> for more information.

An RTOS that meets those two standards could also see applications in homeland security, such as protecting vehicular traffic-control networks. A hacker could cause massive damage if he took over the country's traffic lights and turned them all green at once, O'Dowd says.

In fact, a character in the recent Charlize Theron/ Mark Wahlberg movie "The Italian Job" did exactly that, and wrecked dozens of cars as the actors staged a bank robbery.

Much change is on the horizon, agrees Steve Blackman, director of market development

Columbitech wireless VPN™



Security is crucial for wireless networks like Columbitech's VPN.

for aerospace and defense at Wind River Systems in Canton, Mass.

FAA regulators have tested safety in commercial aviation for years through their DO-178B requirement. Today, military designers are quickly adopting the standard, driven by Global Air Traffic Management (GATM), the civilian and military effort to handle burgeoning air traffic. In fact, the European Union has already mandated that any planes in EU airspace must meet commercial standards such as DO-178B.

So Wind River has offered a DO-178B-certified, COTS solution for two years, now part of projects such as the Lockheed Martin C-130 utility turboprop and the Boeing KC-767 jet tanker, Blackman said.

More recently, many aviation electronics applications have moved to the modular partitions of ARINC 653 so they can run a wide range of programs on the same hardware, from luggage tag databases to engine controls. Motivating that trend, in part, is the drive to reduce operating costs; engineers can now modify systems without expensive recertification. So Wind River plans an October release for a platform safety critical-ARINC 653 RTOS called VXWorks-AE653.

Company engineers are also working with the U.S. National Security Agency (NSA) to apply ARINC partitions to data security. That type of application could save time and money by allowing users to store classified and open data on the same machine — even up to evaluation assurance level seven (EAL7), Blackman says.

NSTISSP 11

Another pending change is NSTISSP 11, the

<http://niap.nist.gov/cc-scheme/> for more information.

All DOD computer acquisitions will soon require this feature, he predicts, though most application will merely have to meet EAL3 or 4, not full 7.

Yet another pending change is the adoption of IPv6, the expanded TCIP Internet standard. DOD planners have mandated that all computer purchases after October must feature IPv6, and all DOD networks must be able to run the new standard by 2005.

The upgrade will leapfrog IPv4, the current standard that falls short in security, mobility, and number of available IP addresses. Facing a huge cost to build new networks, commercial designers have not yet adopted the new standard, but military planners want to ensure their networks can handle the Land Warrior and Objective Force Warrior models that will make every soldier a node in a battlefield network.

That is a lot of change, so in November, Wind River officials began selling platforms — or bundles of software tools — as well as components. A customer who buys an operating system can now get the appropriate integrated development environment (IDE), tools, and

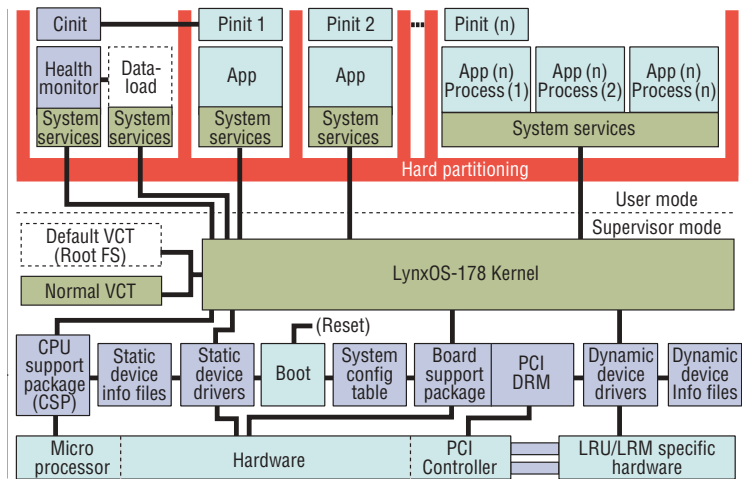
National Security Telecommunications and Information Systems Security Policy #11. The regulation requires engineers to evaluate any computer system that touches secure information. The rule has been on the books since 1990, but only now is being enforced. See

middleware alongside it. Customers are now applying platforms to projects such as the joint tactical radio system (JTRS), future combat system (FCS), and common ground system.

Demanding security and reliability from the same operating system is a tall order, says Green Hills's O'Dowd. The busier a system is, the more chance it has for problems.

But not everyone can agree on a standard for reliability. One of the highest standards is "five nines" reliability, which mandates a system operate 99.999 percent of the time. But that is not good enough for all military applications.

"Microsoft says five nines reliability is their goal, which calculates out to five minutes of downtime per year. Five minutes sounds really good until you start talking about airplanes," O'Dowd says. "That's because one in 100,000 times you need it, it won't be there. Airplanes have hardly any mechanical linkages left between the pilot and the plane; there is essentially nothing that doesn't go through the plane's RTOS. So five nines is totally unacceptable in cars, airplanes, and medical systems. Our customers don't like to hear about nines."



Partitioned operating systems like LynxOS must conform to the DO-178B standard to handle classified data in military applications.

Simplifying the operating system

Pushing reliability beyond five nines is a matter of balancing priorities, O'Dowd explains.

Avionics reliability is a combination of good software and a good operating system. But Green Hills engineers say they believe the typical operating system tries to do too much. So they made Integrity-178B a more secure system by forgoing most of the features that desktop users are accustomed to.

"Integrity is a microkernel, while UNIX, Linux, and VX Works use monolithic kernels,

with everything thrown in," he says. "We've stripped out everything but the security, reliability, and resource allocations. Everything else is added on; any bells and whistles would be built on top of it, including all the software that you'd think of as an operating system in Windows or Linux."

That makes Integrity tiny compared to most other operating systems — a tenth the size of Linux, and a quarter the size of VX Works. An Integrity system needs just 70 kilobytes on a PowerPC or 40 kilobytes on an ARM processor.

"The way you build something secure is to make it small and simple," he says. "We avoid heuristics; we avoid anything that smacks of cleverness or intelligence."

That simplicity means the system does not offer many features, but it offers a tight focus on each task. In fact, it guarantees memory and CPU cycles for any given job, company officials say. The ARINC-653 standard certifies this type of memory partition, ensuring that an overloaded computer can never starve an application to death.

Avionics systems typically have three sectors that demand such a secure and reliable RTOS — past, present, and future.

In upgrades, technicians sometimes rip all the electronics out of an old plane, such as the B-1 or B-52 bomber, and retrofit it with brand new wiring. In new airplanes, such as the Airbus 380 or Lockheed Martin F-35 joint strike fighter, engineers specify the latest wiring from the beginning. And in unmanned aerial vehicles (UAVs), engineers rely on cutting-edge computing to drive aircraft like the Global Hawk or Predator.

Green Hills officials are also looking outside the military sector for new Integrity applications. The RTOS could soon be running drive-by-wire controls in passenger cars and partitioned memory in office desktop computers.

Guaranteed memory

Until now, engineers who had to guarantee enough memory for every application had a simple solution — they ran each program on its own computer.

But today Pentagon planners are trying to reduce size, cost, and power demands. The fastest way to achieve those goals is to start loading several applications on each machine.

"It used to be that cost and size were no object in the military, but now that's not true. The Land Warrior next-generation soldier will have a whole computer running on his body," says Robert N. Morris, vice president of sales and

marketing at LynuxWorks of San Jose, Calif.

But there is a catch; intelligence agencies demand that classified and unclassified data cannot be stored on the same disk. Yet airplanes routinely juggle simultaneous data from radar, navigation, targeting, defensive maneuvers, and communications with air traffic control.

One solution to the dilemma is LynuxSoft 178, a secure RTOS that enforces a time/space partition to run several different virtual machines on the same hardware, he says. The company also makes LynxOS, a real-time operating system certified by IEEE as POSIX conformant so it can run many government applications.

Engineers at Innovative Concepts of McLean, Va. needed a strong operating system to support their Improved Data Modem, called IDM Technology. It had to be a rock-steady platform since U.S. forces in the Iraq War used the modem to share real-time digital battlefield data between positions on land, air, and sea. Loaded on the Army's AH-64 Apache Longbow, CH-47 Chinook, OH-58D Kiowa Warrior, and UH-60 Black Hawk helicopters, the modem supported digital maps with target icons, controlled weapons, coordinated attack strategies, and avoided friendly fire. So, the engineers chose LynxOS as their platform.

Another trend in operating systems is the Pentagon's push for open standards, to maintain the value of their relatively old applications. A highly specialized, proprietary RTOS can make hundreds of existing applications useless, so military IT planners demand open architecture. Accordingly, IDM can handle UNIX, Linux, or any other Posix-based application, he said.

Future applications of IDM could include a small manpack version. Soldiers increasingly act as nodes in a battlefield network, but their power has always been restricted by the challenge of carrying heavy computer memory and batteries. LynuxWorks could solve that problem since the company's stripped-down RTOS can run on just 500 kilobytes of memory, compared to 10 or 20 megabytes for a typical UNIX system, company officials claim.

Other LynuxSoft adoptions include the U.S. Navy's open architecture VDX system for shipboard communications, the U.S. Army's future combat system for autonomous fighting vehicles, the Army's non-line-of-sight cannon (formerly called Crusader), an unmanned

combat air vehicle (UCAV), and the pending RAH-66 Comanche helicopter from Boeing and Sikorsky.

Such applications all demand high security, so an enemy force cannot hack in and take control. They require quick priority interrupt times, not only to react fast to incoming missiles, but also to maintain data links as fast as a 1,000 GHz bitstream. And they need high reliability, since they are running crucial applications like IFF (identify friend or foe).

Another challenge is segregating classified and open information, he says. For example, ground control must often upload secret targeting data to fighter jets, but those jets also have constant communication links to air traffic control. To avoid the danger of mixing data streams, the LynuxSoft system can virtually partition its memory, dedicating certain parts to classified messages.

Make networking easier

Open architecture and DO-178B certification are basic requirements for any military RTOS, but all operating systems leverage great computing power from their connections to a network.

That is why Nucleus Plus is up for three big changes, says Kyle Craig, product marketing manager at Accelerated Technology (ATI), a division of Mentor Graphics in Mobile, Ala.

For 10 years now, the kernel has offered engineers open-source code and royalty-free billing for applications such as ground proximity warning, ground proximity avoidance, global positioning satellite (GPS) navigation, personal digital assistants (PDAs) in avionics, communications management, radar, electronic flight instrumentation, and satellite grid arrays.

Now ATI engineers are working on three projects for the next version of Nucleus: D)-178B certification, the new web standard IPv6, and the wireless LAN standard 802.11.



AH-64 Apache Longbow helicopters in Iraq used LynxOS to drive their data modems for crucial communications.

The engineers are busy stripping out redundant code, and partnering with certification companies like Cascade Engineering. But of course, no OS earns 178B certification on its own — just as part of a complete system.

“The operating system and middleware are essentially lumber,” Craig says. “You can test it all you want, but it doesn’t really mean anything until after you’ve built the Taj Mahal. Then you want to know if it’s structurally solid, if the foundation is strong, or if it will fall down in a hard rain storm or in a hurricane.”

ATI engineers are also configuring Nucleus to accept the 802.11 wireless LAN standard because they expect that will be another crucial part of the “netted battlefield” vision. In contrast to IPv6, the 802.11 technology is fairly commercial today, although ATI will be using the high security version (802.11x) instead of the office version (802.11b).

Military customers are specifying more wireless local area networks (LANs) for real time applications, agrees Pontus Bergdahl, chief executive officer of Columbitech, in Stockholm, Sweden.

But adoptions are slowed by security concerns, he said from the company’s New York offices.

That was a major concern for designers of the U.S. Department of Defense’s Common Access Card system as they drafted specifications for card readers. Columbitech’s secure wireless VPN (virtual private network) now supports CAC smart card authentication, so it can process data from this standard identification card, and allow its four million users to access data securely from any location.

Windows works, too

An embedded RTOS is supposed to be small and sturdy, but Microsoft Windows — known for being big and buggy — can work,

too. Venturcom, of Waltham, Mass., makes embedded Windows operating systems used in military and aerospace applications.

The system works because Venturcom uses Windows just to load its own kernel. After it boots, the system will keep running even if Windows crashes.

The three main options include RTX (real time extensions), which offers real-time control, determinism, scheduling, and blue-screen survivability for nearly any Windows flavor. ETS (embedded tool suite) is a small-footprint RTOS based on the Win32 API, originally developed by a company called Phar Lap and used for applications in industrial automation, medical, and transportation. And BXP balances local processing with diskless computing for jobs in homeland security, simulation, industrial automation, education, and government.

The federal departments of energy and defense use BXP to better enforce security. In the past, they traced data by requiring users to check in and check out hard drives. But BXP enables diskless desktops, so now users have no chance to copy classified data, says Dennis Gullotti, director of strategic and product marketing for Venturcom.

For even tighter security, users can chose BXP secure. That variety expands the diskless model with secure disk on media (SDOM) and 128-bit encryption, as used in DOE facilities at Oakridge, Tenn.

Another benefit of using Windows is its support for the Pentagon’s move to use off-the-shelf platforms, as opposed to proprietary, in-house code, says Larry Allen, a Venturcom senior field applications engineer.

The Venturcom kernel is a greatly simplified version of the Windows on the typical office desktop PC, but developers can still program it through the familiar Win32 API using com-


mercial tools like Visual Studio, he says. That is crucial because systems get more powerful as they are connected to larger networks.

“The embedded system is no longer a stand-alone box,” Allen says. “It’s integrated and connected to other embedded systems.” That is particularly important in applications like training simulators, where the system must handle strong graphics content and control the operation, speed, and determinism of the virtual craft.

“The basic rule is, you can’t train someone wrong, whether you’re turning the steering wheel on a HMMWV, moving a tank turret, or putting the landing gear down,” he says. “When you play a car racing game in an arcade, you often turn the wheel and wait a second until the car turns. That’s not good enough for training. It’s like they say; train as you fight, fight as you train.”

Quick reaction time was crucial for a tank simulator that designers at Cubic Defense Applications in San Diego were building for the Spanish army. The Spaniards complained that their existing simulator required troops to keep their guns aimed at each target until the shell hit — an unrealistic demand that could waste as much as five seconds of crucial battlefield maneuvering time. So the Cubic designers chose Venturcom’s ETS to run a real-time simulator.

In other applications, Venturcom’s RTX package drives the Lockheed Martin rudder control system for U.S. Navy Ticonderoga-class guided missile cruisers, and helps launch fighter jets off carrier decks by timing the window of opportunity between pitch and yaw to catapult a plane into the air at the perfect time.

“We use windows for the famous things that windows is good at, and we use RTX for the real time computing,” he says. 



www.ghs.com • ph: 805.965.6044