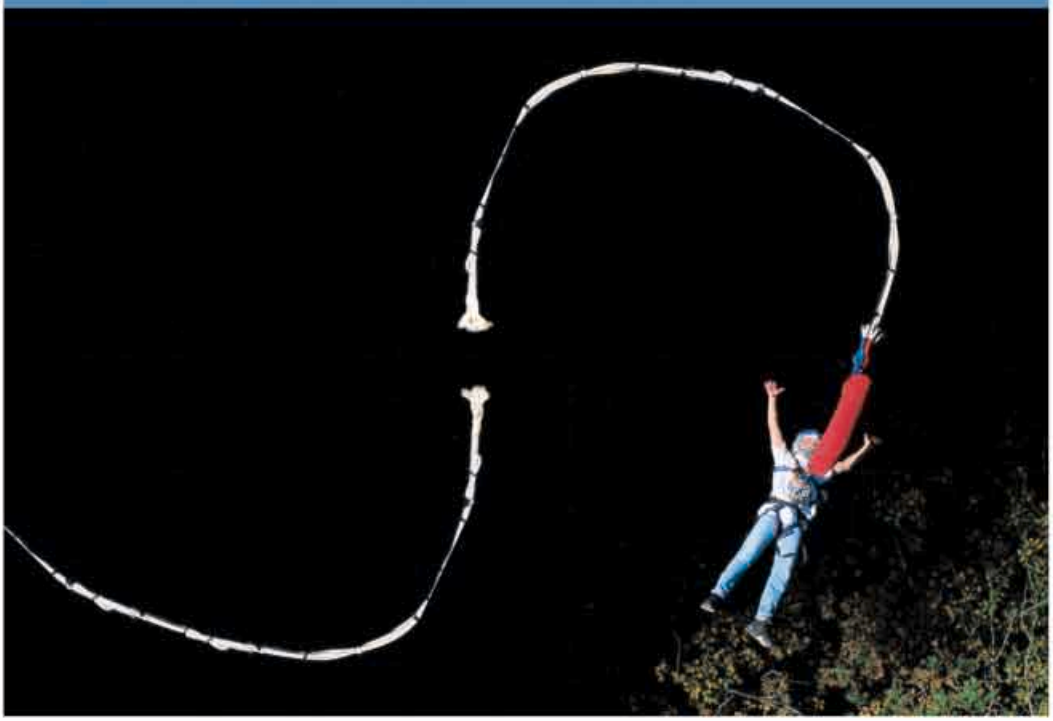
AVIONICS®
magazine

Real-Time Operating Systems

Versatility Plus Security

If only bungees had RTOS.



SBS knows RTOS.
Trust us for your mission and safety critical applications.

When you choose to work with SBS, you're also choosing to work with our partners, the leading Real Time Operating Systems software makers. We have long-term relationships with Green Hills®, Wind River®, LynuxWorks™ and BAE Systems, and we work closely together to help you implement a better RTOS system.

No matter what your platform, SBS has you covered. We offer Intel and PowerPC CPU's, graphics, MIL-STD-1553, IEEE 1394, ARINC 429, serial, fibre channel, Gigabit Ethernet, discrete & analog I/O, and integrated systems. When you need Board Support Packages, Drivers, DO-178B Certification, User Libraries, OpenGL and API's, we'll be there. Because when it comes to RTOS, there's no such thing as "too safe."

www.sbs.com

SBS Technologies.

SBS knows. To find out more, visit us at **www.sbs.com** or call us at **800.SBS.1553**

Real-Time Operating Systems

For long-term success in the government market, real-time operating systems need to be versatile, safe, secure and supportable.

The operating system is a computer's core software. It manages all of the computer's other software programs. Everyone is familiar with PC operating systems. They are large, feature-rich and prone to crash when overstressed. But a PC typically works in a home or office environment. If the system slows to a crawl or occasionally crashes and must be rebooted, it is irritating but no catastrophe.

> *"Hard freezes are not acceptable in embedded operating systems."*

But computers flying airplanes or releasing weapons have to be extremely reliable. At the software level, this calls for government-approved and standards-based real-time operating systems (RTOSes). RTOSes are employed widely, not just in the military/aerospace sector, but across the board in must-not-fail telecom, medical and automotive equipment.

For many years individual companies developed their own operating systems, which were used in their own products. "Proprietary" operating systems, optimized for particular applications, are still being developed and used today. But increasingly, systems developers are looking for commercial solutions that are created, maintained and supported by information technology specialists, freeing higher-level designers to focus on the applications instead.

The demand for commercially supported software RTOSes and tools is substantial and growing. In 2002, the worldwide market for commercial RTOSes and associated software tools, exclusive of maintenance and consulting work, was $675 million. The market is expected to grow to $914 million in 2007, according to the analyst group Gartner Dataquest.

Unlike a desktop operating system, an RTOS is far smaller in size, more modular in structure and focused on the most essential functions, explains Daya Nadamuni, principal analyst with Gartner Dataquest. There is no need for an RTOS to include programming interfaces to the hundreds of popular software packages that desktop operating systems must provide.

Key COTS RTOS Attributes:

- Versatility—applicable to multiple systems;
- Safety—compliant to the DO-178B standard;
- Security—able to separate multiple levels of data; and
- Supportability—maintained and enhanced by specialist companies.

In "hard" real-time applications, such as aerospace, the RTOS must be particularly compact. The core, or kernel, may feature only essential functions such as memory management and time scheduler support. It must respond to requests for service within guaranteed time windows, often measured in millionths of a second. "Hard freezes are not acceptable in embedded operating systems," Nadamuni says.

Inside:

RTOSes' Multiple Applications 4
Certification: Gold Standard 8
New Approach to Security 12
From Proprietary to COTS 14

Commercial RTOSes' Broad Appeal

A crucial role across the aviation spectrum

Commercial real-time operating systems are proving their value across a wide range of aircraft types and avionics systems.

Real-time operating systems (RTOSes) play a crucial role in avionics computers across the spectrum of aviation—from small, private aircraft to the most advanced airliners and military jets. This complex software controls the running of safety-critical functions that keep airplanes aloft, guide them along their intended flight paths and "paint" the cockpit displays. For military aircraft, the software also manages mission-critical functions like evading attack and releasing weapons.

Speed and Predictability

A key feature of an RTOS is its ability to meet tight processing deadlines. An application program controlling the release of a weapon may require an action from the operating system in less than one-thousandth of a second. The deadlines for servicing flight control functions are measured in millionths of a second. The operating system must perform predictably, with guaranteed response times, in this "hard" real-time environment, despite the frequent occurrence of unscheduled demands for services.

Notwithstanding the trend toward greater integration of avionics functions, most aircraft still contain many different computers, provided with different operating systems. The next-generation Airbus 380 super jumbo airliner, for example, will use at least four companies' RTOS products, and probably more. Even a single computer—such as the mission computer planned for the U.S.

military's new Joint Strike Fighter—can host more than one "embedded" RTOS.

RTOS Examples

Over the past decade the U.S. government has stressed the use of commercial off-the-shelf (COTS) technologies in order to control costs and simplify logistics. Commercial technologies, the thinking goes, have been employed and tested by more users across a wider range of industries than have their "proprietary" counterparts. Commercial real-time operating systems have proved themselves in various industries and are being adopted by avionics manufacturers as well. Among the key suppliers of COTS RTOSes are Green Hills Software, LynuxWorks and Wind River Systems. Green Hills Software's INTEGRITY-178B and INTEGRITY RTOSes are being used or designed into military bombers, fighters and unmanned air vehicles, as well as civilian helicopters and airliners.

INTEGRITY-178B is a fairly new commercial RTOS, an evolution of the original INTEGRITY product released in 1997. Introduced in 2000, INTEGRITY-178B is one of the first commercial products to comply with a standardized approach to partitioning. This key feature enables the RTOS to safely orchestrate the demands of multiple application programs sharing a single set of hardware resources. Partitioning involves dividing processing tasks in time and in space so that the programs can coexist safely on a single computer. ARINC 653 is the specification that standardizes partitioning for aerospace RTOSes.

The U.S. Air Force's B-1B program adopted the original INTEGRITY RTOS in 1997 as part of a project to convert the bomber from a nuclear to a conventional warfighting role. The B-1B prime contractor, Boeing, may move to newer versions of the Green Hills operating system in a further avionics upgrade. Lockheed Martin's new F-16E/F, Block 60, fighter aircraft uses INTEGRITY to power its mission and display computers as part of a move towards commonality of software tools and resources within the company. And Sikorsky's new medium-lift helicopter, the S-92, uses INTEGRITY-178B as part of its Avionics Management System (AMS).

Green Hills RTOS Design-Ins

Airbus 380
B-1B
B-52
F-16E/F, Block 60
F/A-22
F-35 Joint Strike Fighter
S-92

B-1B Lancer

As part of the B-1B's conversion to a conventional role, Boeing replaced the six Avionics Flight Software (AFS) computers responsible for flight control, cockpit displays, terrain following, radar control, navigation, self-defense management and weapons delivery. Faster hardware and more sophisticated software allowed all of the applications programs to be run in a smaller "footprint" on the aircraft. At this time Boeing also adopted the INTEGRITY RTOS as part of a move to commercial technology.

The software applications described above reside in two active computers. Two additional computers serve as backup. The first computer hosts the flight-critical, terrain-following applications code. The remaining applications reside in one card in the second computer. Both computers and their backups include a second processor card to allow for future enhancements.

Because of key, real-time interaction between the B-1B software applications—required to ensure precision weapon delivery and critical flight controls—as well as current applications structuring, engineers now must retest existing code when new software is added. This is to assure that existing functions have not been changed, explains Nancy Anderson, Boeing's B-1/B-2 senior site engineering manager.

Green Hills RTOSes support processing for the panel displays and head-up display of the F-16E/F, Block 60.

AFS Partitioning Prototype

The government has funded Boeing to develop a proof-of-concept software partitioning architecture prototype that provides greater protection against the effects of changes. One aim of the project is to show that when changes are made the amount of retesting can be reduced to support quick-reaction turnarounds.

Changes are anticipated for the B-1B, as it adapts to priorities, such as "network-centric warfare" and new rules for flying in civil-controlled airspace. "But the immediate need is to be an important and integral part of the global warfighting network," Anderson says.

The Global Air Traffic Management (GATM) program—for making military aircraft compliant with civil ATM rules—"requires navigation software to be DO-178B-certified," Anderson notes. (DO-178B is the primary safety-software development standard used in both commercial and military aviation.) "Dividing the applications and upgrading to INTEGRITY-178B will be one step along the way to ensuring the B-1B meets GATM requirements," Anderson says.

The prototype effort involves some restructuring of existing applications programs to distribute and execute applications on both cards in the computer. The restructuring also will position future applications to take advantage of operating system features, such as partitioning. In the prototype architecture the memory partitioning and memory access control provided by the memory management unit (MMU) would be enforced by the commercial RTOS. "The beauty of partitioning is that we can make modifications in one partition and not have to 'regression-test' the others because partition protection is in place," explains Devron Hanks, Boeing's B-1B AFS system architect.

In the prototype project, Boeing software engineers will "split up" the applications software, Hanks says. Programmers,

for example, will enforce strict and consistent interfaces between the applications. Modules need to be clearly separated and identified so that the RTOS can enforce the rules for their access to the microprocessor, memory, data buses and other hardware resources.

The prototyping effort includes:

- Verifying the time and space partitioning concepts and the available communications protocols,
- Restructuring the applications software to execute on distributed cards and take advantage of partitioning,
- Defining which partitions need to talk to each other and how they talk to each other, and
- Verifying the communications medium between the applications—a VME backplane—and INTEGRITY-178B partition communication protocols.

Safety-critical software—such as navigation and terrain following code—and selected pieces of the weapons code would remain on the second computer's active card. This code is the most expensive to retest in the event of change. It is closest to the hardware and has the tightest deadlines.

Although final software allocation between the cards remains to be determined, Boeing plans to host display, self-defense management systems, mission planning and some weapons functions on the second card of the second computer. That still will leave about 60 percent of the card's resources available for new applications. Full time and space partitioning will be done on the second card, Hanks says.

F-16E/F, Block 60

The newest version of the F-16 Fighting Falcon, which Lockheed Martin developed for the United Arab Emirates, incorporates a new radar, integrated forward-looking infrared (FLIR) targeting system, electronic warfare suite, digital flight control system and high-speed, fiber optic data communications links. At the heart of these systems is the advanced mission computer (AMC), which hosts multiple applications, or domains. Among them are weapons and fuel management, data formatting for the data buses and fiber optic links, navigation and the head-up display (HUD).

The F-16E/F, Block 60, will feature new sensors, displays and high-speed fiber optic links.

Within the AMC, the INTEGRITY RTOS executes on multiple Motorola PowerPC processors. Each processor hosts more than one software domain. The RTOS helps to protect the applications from each other, allowing them to share the same hardware resources.

Lockheed also has developed Joint Software Execution Platform (JSEP) software which runs on top of the RTOS, insulating the applications programs from the hardware. Along with JSEP, the RTOS enforces priorities for the execution of functions on the microprocessor.

Application programs for the mission computer that have been carried over to the new aircraft from the current, Block 50 version of the F-16 were basically unchanged in the F-16E/F. These programs already had been structured to take advantage of partitioning. They required only to be converted from Ada to the C++ programming language.

A second key computer, the color display suite (CDS), processes data for the F-16E/F's three, 5-by-7-inch color cockpit displays. The CDS also uses multiple Motorola PowerPC processors, running an OpenGL server on top of the INTEGRITY RTOS, for display processing and display generation. One type of processor card, known as the general-purpose processor, or GPP, hosts multiple software domains. The GPP, for example, controls the tactical display, the "upfront controls" for pilot interaction with radios and other avionics systems, and the weapons displays. It uses INTEGRITY to enable multiple applications to run safely on the same hardware resources.

Rockwell Collins' AMS for the Sikorsky S-92 uses the INTEGRITY-178B RTOS.

S-92 Helicopter

INTEGRITY-178B also is used in the Avionics Management System developed by Rockwell Collins for Sikorsky's new S-92 medium-lift helicopter. AMS not only manages and displays primary flight data and navigation information, but also processes and displays flight management, digital map, weather radar, terrain warning, and engine indication and crew alert system (EICAS) information.

The S-92 cockpit features four Collins 6-by-8-inch, liquid crystal, multifunctional flight displays. These include a primary flight display and an EICAS/navigation display for each pilot. A fifth display is optional.

The Collins display system, using the INTEGRITY RTOS, was approved to Level A of the civil aviation safety standard, DO-178B, in 2002. Level A certification was required for the Collins display system because it manages and displays primary flight data, explains Tony Johnson, chief architect for Collins' Integrated Applications business area. The aircraft received Federal Aviation Administration (FAA) type certification in December of 2002.

A version of the Collins avionics system will use the partitioning feature of the Green Hills Software operating system to create three software partitions of varying criticality levels, says Johnson: Level A for flight display functions; Level C for surveillance functions, such as terrain awareness warning system (TAWS) and weather radar; and Level D for maintenance and status functions. ■

Are your avionics ready for the Global Information Grid?

Completely interconnected airspace
Software-defined radios
Real-time targeting information

Today's advanced avionics are interconnecting air, space, and ground-based systems. This is enabling a new generation of avionics capabilities. It also introduces new threats to security and safety.

So how do you connect your avionics without compromising safety and exposing the design to new security vulnerabilities?

Compromise of sensitive information
Software and data tampering
Cascading system failures
Computer viruses
Bypass of critical software

MILS is a foundational security architecture based on mathematical verification that draws from ARINC-653 and supports strong level separation. MILS is about TRUSTED foundations. MILS middleware enables smart push/pull of multi-level information to protect, separate, and control end-to-end national information flow and data separation security policies.

Security by design...

Objective Interface is leading the MILS middleware initiative to secure the communications between safety-critical and security-critical systems with EAL-7 COTS software. The MILS middleware team includes Objective Interface, National Security Agency, U.S. Air Force Research Laboratory, Lockheed Martin, and the University of Idaho.

OBJECTIVE INTERFACE™

For more information on this architecture for high-assurance communications security, visit **http://mils.ois.com**, email **info@mils.ois.com**, or call us at 800-800-OIS7 or +1-703-295-6500.

Smart communications for secure, real-time systems.

Avio
Cert
DO-178B,

The commercial standard dominates in operating system approvals, even in military avionics. But there's more to DO-178B compliance than one would guess.

Software developed for safety-critical systems on passenger jets must pass a high level of scrutiny in order to ensure that it is safe to use for public transport. More than the final lines of software code must be carefully reviewed and certified. So, too, must the processes involved in planning, developing and testing the software. Companies developing such software must show that they have met the requirements of the commercial aviation standard, DO-178B, at all stages of development—from planning through documentation and testing. This standard is so well-accepted that government avionics projects increasingly require it as well.

Origins of DO-178B

DO-178B was developed to address the certification needs of emerging digital avionics systems. Certification agencies recognized that they needed a standard to define software development processes that assure aircraft safety. These processes are designed to supersede the procedures used in previous decades for analog equipment.

Most software installed in commercial aircraft—including commercial off-the-shelf (COTS) software—has been developed using processes that comply with DO-178B. RTCA Inc.

nics ification

the Gold Standard

produced the standard, which is called "Software Considerations in Airborne Systems and Equipment Certification." First published as DO-178 in 1982, it was established to "develop and document software practices that would support the development of software-based airborne systems and equipment."

The standard has been revised twice—DO-178A, approved in 1985, and DO-178B, approved in 1992—to reflect advances in software technology and lessons learned from earlier certifications. As directed by the Federal Aviation Administration (FAA), Advisory Circular 20-115B, DO-178B is an acceptable means to "secure FAA approval of digital computer software." Information to purchase the standard is available at www.rtca.org. In Europe the equivalent document is EUROCAE ED-12B which is available at www.eurocae.org. A joint RTCA/EUROCAE committee is expected to commence work on a third revision to the standard, DO-178C, in September 2005.

Recognizing that not all equipment installed on an aircraft affects safety to the same degree, RTCA incorporated multiple assurance levels in DO-178B. The non-profit industry organization understood that failures in, say, the flight control system have much greater consequence than a failed seat-back passenger entertainment display. It took into account the equipment certification process which recognizes five failure condition categories: catastrophic, hazardous/ severe-major, major, minor and no-effect. These categories are applied as part of the system-level safety assessment for the systems and equipment installed on aircraft.

Levels A Through E

In tandem with these failure conditions, DO-178B describes five software assurance levels—Level A through Level E—for aviation systems containing software. Level A of DO-178B, for example, applies to equipment whose failure would be deemed catastrophic. If an avionics system is classified in the highest failure condition category, its software programs must meet the highest assurance level. Exceptions can only be made when there is a means for "partitioning" in which the operation of one software program does not affect the operation of another software program executing on the same hardware.

The number of DO-178B objectives that must be satisfied rises from Level D to Level A—with corresponding increases in the certification effort required. (For Level E, the lowest level of DO-178B, no objectives apply.) Level A requires compliance to all 66 DO-178B objectives which include such disciplines as planning, development, verification, configuration management, quality assurance, tool qualification and liaison with certification authorities.

Unlike some other standards, DO-178B is not proscriptive. It doesn't dictate what should be done or what precise data format should be used. Instead, DO-178B is objective-based. It states the "objectives for software life-cycle processes" but allows individual developers to comply with the objectives. Software developers therefore can employ whatever means are appropriate for their projects and company practices. However, while degrees of compliance to other standards may be negotiable, compliance to the DO-178B objectives for a particular software level are mandatory.

> *"Unless an acceptable alternative is proposed, compliance to DO-178B is mandatory before FAA places its stamp of approval on a product containing software."*

Software Approval Process

FAA won't evaluate COTS software unless the software has been designed into an avionics system. The agency's involvement with a COTS supplier usually consists of audits of compliance to DO-178B objectives but may also include examination of novel product features such as partitioning or use of object-oriented constructs. Keys to achieving successful audits include first-hand knowledge of DO-178B, well-defined development processes, and a highly disci-

DO-178B Software Certification Levels

Level A

Software that could cause or contribute to the failure of the system, resulting in a catastrophic condition.

Level B

Software that could cause or contribute to the failure of the system, resulting in a hazardous or severe failure condition.

Level C

Software that could cause or contribute to the failure of the system, resulting in a major failure condition.

Level D

Software that could cause or contribute to the failure of the system, resulting in a minor failure condition.

Level E

Software that could cause or contribute to the failure of the system, resulting in no effect on the system.

plined effort to follow the processes.

The first step for any project involves defining the fundamental processes for the product's software development, verification, quality assurance and configuration management. A document, called the "Plan for Software Aspects of Certification," then is created. This plan and the supporting plans and standards constitute the initial building blocks for an audit.

Planning is followed by product development and verification. Development includes the production of high-level requirements, low-level requirements, source code (the code in which a program is written), and corresponding traceability between these elements and the requirements for the system as a whole. These verification activities are significant, going beyond traditional code reviews and testing. All development data, from planning to testing, is reviewed and analyzed. In addition, all requirements, high- and low-level, are rigorously tested in both normal and robust test scenarios. FAA also examines the source code structure, and additional changes and tests are made, until 100 percent of the source code structure is verified.

The development data and verification results are then summarized in a "Software Accomplishment Summary." With this document, along with the supporting certification evidence, the FAA enters the picture, auditing for compliance to DO-178B. Overall, thousands of pages of development and verification certification evidence are produced and archived for each product. Unless an acceptable alternative is proposed, compliance to DO-178B is mandatory before FAA places its stamp of approval on a product containing software.

Risk Reduction

The rigor of the DO-178B process is important when one considers the use of the term, "certified," in regard to evidence. "Certified" should only be used for software already flying in certified systems. The use of COTS products already embedded in FAA- or military-approved aircraft systems reduces the risk to a program's development schedule.

Avionics developers can gain a leg up, as well, when integrating COTS software developed for another industry or to another industry's standard interface, such as the popular Internet standard, TCP/IP. This allows the developer to focus on core competencies. Better yet, if the COTS software supplier can provide reusable certification evidence for a product, the costs of the approval process will decrease. COTS products that can be considered for integration into avionics include runtime libraries, real-time operating systems (both partitioned and shared-address space), device drivers (such as Mil-Std-1553, Ethernet and Firewire), communications stacks, file systems and object resource brokers (ORBs). Manuals and brochures for these products probably will indicate they have been certified or are certifiable.

Developers may initially set the goal of compliance to a lower level of DO-178B to reduce development costs. However, such an approach may lead to excessive rework later on. The number of DO-178B objectives requiring independent activities—activities that can not be performed by the same software engineer—increases with each ascending software level. For a project that does not initially apply such independence, some activities may have to be redeveloped to raise the product to the next software level. A well-developed plan should include considerations for potential future software levels in order to avoid redundant efforts.

Cost-Saving Partitioning

Another means to potentially reduce system development costs and schedules is to separate the software into partitions, or vir-

Green Hills Products at Work

Green Hills Software completed DO-178B, Level A, life-cycle data for INTEGRITY-178B in November 2002. This life-cycle data was used by Rockwell Collins as part of the technical data submitted for the technical standard order (TSO) of the Avionics Management System (AMS), which is used on Sikorsky's new S-92 helicopter. The Federal Aviation Administration (FAA) certified the S-92 helicopter in December 2002.

ACSS, jointly owned by L-3 Communications and Thales, completed a TSO for its Terrain and Traffic Collision Avoidance System (T^2CAS) in February 2003, using INTEGRITY-178B and Green Hills DO-178B life-cycle data.

Green Hills Software's INTEGRITY-178B is the first commercial RTOS with full time and space partitioning to be used in products certified to Level A of DO-178B for commercial aircraft.

Following these initial certifications, Green Hills Software has delivered INTEGRITY-178B to other customers who have used the product in computing platforms for engine controllers, collision avoidance systems, data concentration units, displays, inertial reference units and radio equipment.

To complement INTEGRITY-178B, Green Hills provides language support libraries with DO-178B, Level A, certification evidence for safe subsets of C, C++, and Ada95.

tual applications. When applications are partitioned, the faults occurring in one partition are prevented from:

- Propagating into, and causing the failure of other partitions; and
- Causing the partitioning mechanism to fail.

Processor designs have included virtual applications support (e.g., memory management units) for over 20 years. But the early processors lacked sufficient throughput to support real-time operation for multiple applications simultaneously. Over the years processor throughput has increased and so, too, has the potential for real-time multiprocessing. The basis for partitioning on a single processor was achieved by coupling today's fast processors, memory management units, and a supporting real-time operating system.

Historically, avionics functions have been separated from each other by hardware, in a federated architecture. The individual computers may even have included operating systems that provided no protection between the applications. In other words, all applications shared the same address space. In a federated system the software level applied to each computing platform and all the software running on it adheres to the highest level assigned from the safety assessment. This is true even if the high failure condition category represents only a minor portion of the software.

Now that avionics manufacturers can include partitioning operating systems in their equipment, they can:

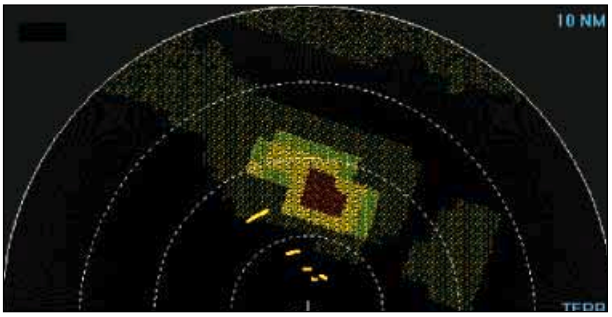
- Use less hardware to provide the same functions. System costs may be reduced while retaining, and potentially improving, reliability.
- Isolate higher-criticality software from lower-criticality software. Since lower "criticalities" require fewer DO-178B objectives, compliance for these applications will require less effort.
- Isolate functions that change from project to project from functions that remain stable. Since partitioning implies that the functions are isolated from each other, retest efforts for the stable functions may be reduced.
- Isolate functions originating from different suppliers, partners or development teams and maintain them as separate partitions during the integration process. Thus, less rework may be required to resolve integration issues.

Military aircraft programs are not required to comply with DO-178B, as are commercial aircraft programs.

Yet a contract or manufacturer may require DO-178B compliance. Reasons include:

- The increasing substitution of "commercial best practices" for military standards, a trend that has gathered momentum since the early 1990s. DO-178B is considered to be the current best practice for commercial aircraft software certification.
- Military service requirements. Military communication, navigation, surveillance/air traffic management (CNS/ATM) equipment covered by the Global Air Traffic Management (GATM) program must comply with civil airworthiness standards in order to be used in civilian-controlled airspace.
- Dual-use (commercial/military) equipment requirement to comply with DO-178B for commercial applications.
- Wide technical support base for DO-178B, a published standard, with readily available industry experts, consultants and trained staff.
- And reusability of developed life-cycle data for other purposes (e.g., security assurance standards).

As more and more COTS products with DO-178B compliance become available, one can expect their increased use in military aircraft. ■



ACSS's Terrain and Traffic Collision Avoidance System was approved in 2003, using the INTEGRITY-178B RTOS.

> *"Equipment covered by the Global Air Traffic Management (GATM) program must comply with civil airworthiness standards."*

"Certifiable" Partitioned RTOSes

Four commercial vendors of real-time operating systems (RTOSes) have generated or are in the process of generating certification evidence for their partitioned operating systems:

1. Green Hills Software, whose Level A, INTEGRITY-178B RTOS was accepted for approval in the Avionics Management System (AMS) of the Sikorsky S-92 helicopter in November 2002.

2. LynuxWorks, which distributes, enhances and maintains a Level A operating system originally developed by Rockwell Collins (from a prior version of LynxOS), as LynxOS-178. Collins achieved Level A approval in June 2003, using the RTOS as part of the adaptive flight display system on the Bombardier Challenger 300 business jet.

3. Wind River Systems, which introduced its AE653 product in October 2003. AE653 is planned to be Level A-approved for Smiths Aerospace equipment on the Boeing 767 Tanker Transport and the C-130 Avionics Modernization Program (AMP).

4. BAE Systems, which is providing its CsLEOS RTOS for a planned, fly-by-wire flight control system upgrade to the Sikorsky S-92. While all programs using CsLEOS have DO-178B, Level A, requirements, the S-92 system will be the RTOS's first commercial aircraft, Level A approval.

Guarding Secrets

Commercial RTOSes Offering Safety and Security

Government users are demanding not only reliability, but also bulletproof protection for sensitive data.

Real-time operating systems (RTOSes) are designed to perform reliably and predictably in demanding, safety-critical environments. But U.S. government security experts now want these operating systems—with the aid of hardware and software provisions—to enforce security "rules," as well. At the highest level of capability, the RTOS would securely separate the multiple levels of data that will be present in integrated avionics processors.

This "assurance" feature is important, as the military adapts to emerging priorities such as network-centric warfare, which envisions the transmission of highly classified data between network nodes. The requirement to equip military airplanes with civil-compatible flight management and communications gear, in order to continue flying in civil-controlled airspace, makes the need to separate classified and unclassified data more urgent.

Over the last three decades, security experts have developed concepts to allow the implementation of computing systems that can protect sensitive data. The U.S. computer

security guideline, known as the "Orange Book," was first published in 1983. Orange Book concepts, such as "security domains," "trusted path" and "mandatory access control," continue to be applied in the *Common Criteria*, the international security handbook that replaced the U.S. document in the late 1990s. The *Common Criteria* defines seven evaluation assurance levels, or EALs, corresponding to earlier Orange Book categories. Systems that are approved to the highest level, EAL-7, are expected to be "multilevel-secure"—able to separate three or more levels of data while processing them on shared hardware resources.

Early attempts to develop operating systems providing the highest level of assurance floundered because the operating systems were expected to do everything. In the process the software programs became too large and unwieldy to evaluate. These failures sparked work on a new way to implement long-held security concepts.

Called MILS, for Multiple Independent Levels of Security, this new approach relies on a multilayered software architecture, backed by hardware devices such as the microprocessor's memory management unit (MMU). The core software of the RTOS, known as the microkernel, is responsible for enforcing a system's security rules, or security policy. MILS also envisions single-purpose security applications, such as "guards," security policy managers and encryption algorithms.

Several programs, such as the C-130 avionics upgrade, the F/A-22 and the Joint Unmanned Combat Air System, are considering MILS. A program managed by Lockheed Martin, with funding from the Air Force Research Lab (AFRL), has studied the feasibility and cost of using commercial RTOSes and middleware to separate multiple levels of data. Green Hills Software, with its INTEGRITY-178B RTOS, and LynuxWorks, with a planned LynxSecure microkernel, are participating in this program, along with Objective Interface Systems (a middleware company), the National Security Agency (NSA), the Open Group (a standards body), Rockwell Collins and the University of Idaho.

A second phase of the AFRL program is anticipated, which would test the two operating systems to EAL-7. EAL-7-certified systems are expected to be able to simultaneously separate multiple levels of data—from top secret to unclassified—while processing the data on shared hardware resources. Green Hills plans to achieve EAL-7 approval in 2005.

C-130 to GPS to JTRS

MILS-compliant technology also is planned for the U.S. Air Force's C-130 Avionics Modernization Program (AMP). RTOS supplier, Wind River Systems, is working with Smiths Aerospace to provide a MILS-compliant microkernel for Smiths' mission display processor on upgraded C-130 aircraft. The target assurance level for the new Wind River microkernel, AESecure, is also EAL-7, and the planned security certification date is in 2006.

NSA is briefing the MILS concept to military officials. Agency presentations mention not only the F/A-22, F-35 and C-130, but also the Global Positioning System (GPS) satellite navigation system and the Joint Tactical Radio System (JTRS), a foundation stone for network-centric warfare.

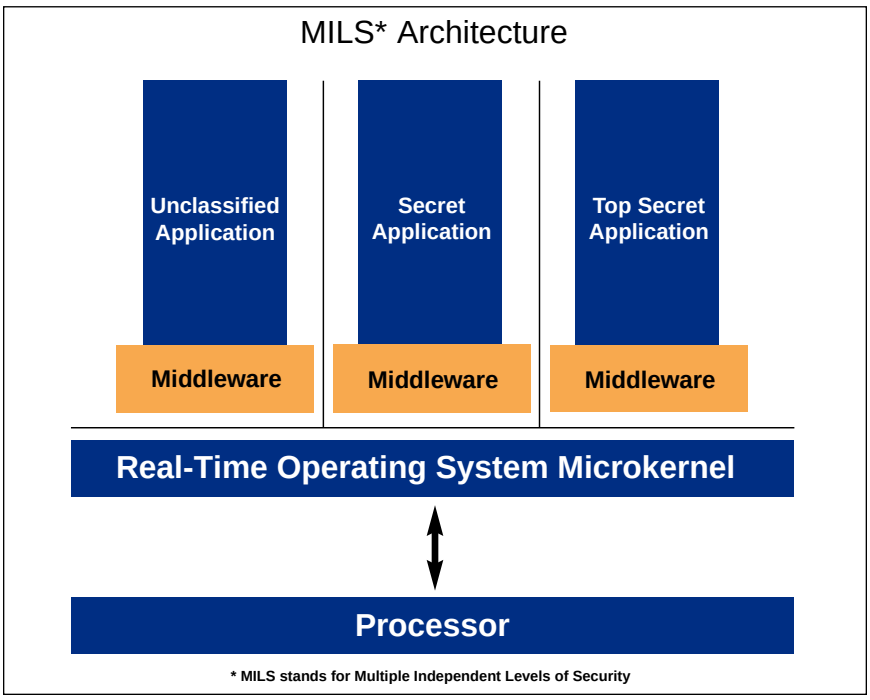
But a MILS development effort is far from simple. For starters, the microkernel must be very small—from 4,000 to 10,000 lines of code. The RTOS company writes a document, explaining how its product complies with security requirements outlined in a "protection profile." The RTOS protection profile describes threats and vulnerabilities that are to be guarded against, and assurances that are to be provided to achieve an appropriate security objective, such as EAL-7.

Another requirement for an EAL-7-approved RTOS is "covert channel" analysis, in order to prove that there are no hidden pathways in hardware or software to allow unauthorized communications—and data sharing—between applications. Applications programs also must leave no data "residue" behind when the microprocessor switches from one task to another. "Trusted" software also has stricter requirements than "non-secure" software for documentation of life-cycle data, configuration management and delivery.

Most important, an EAL-7 RTOS must undergo an evaluation process known as "formal methods," which involves proving mathematically that the kernel code performs its required security functions.

MILS can be built on top of the partitioning concepts defined in ARINC 653, a commercial aviation specification developed by avionics industry experts. ARINC 653 provides a standardized approach to partitioning so that applications with different levels of safety criticality can run at different times on the same microprocessor, coexist safely in memory, and share other hardware resources. The MILS concept extends the idea of partitioning into the security domain so that the microkernel assures the confidentiality, as well as the integrity, of the data.

"Fifteen years ago, we could not have done the MILS architecture," says a government security expert. But now the cost of security is only one-half of 1 percent of a modern microprocessor's capacity. ■



From Proprietary to COTS

Manufacturers are turning to commercial real-time operating systems. The reason: cost and efficiency.

Over the past decade, the U.S. government has encouraged the move from military-specific, or "proprietary," technology to commercial off-the-shelf (COTS) products in order to reduce development and maintenance costs. Many aviation programs have chosen COTS over traditional "roll-your-own" real-time operating systems (RTOSes).

A proprietary RTOS is built by a single manufacturer and is used only in that company's products. Commercial RTOSes, on the other hand, are available to other hardware manufacturers and have been tested by a wider range of users.

> *"Commercial RTOSes are more easily enhanced without changing their basic purpose."*

COTS products are available from multiple suppliers, which compete with each other to provide the most effective, reliable, supportable, yet flexible and adaptable systems. In the aviation industry the major suppliers are Green Hills Software, Wind River Systems, BAE Systems and LynuxWorks.

"Roll-your-own made sense a long time ago," says Jerry Krasner, founder of Embedded Market Forecasters. "But 32-bit [commercial technology] is cheaper, easier to use and better supported." Use of proprietary systems has decreased from 30 percent a few years ago to 20 percent today, Krasner says.

The commercial world has moved from proprietary to COTS RTOSes in many applications. But the more conservative avionics world has been slower to change. If a proprietary RTOS has been perfected for a particular system, there may be no reason to change it. But where there are evolving requirements, a COTS RTOS may be the answer. Commercial RTOSes are more easily enhanced without changing their basic purpose, says Paul Zorfass, a senior analyst with IDC/FTI. Interfaces to extend an RTOS's networking capability—through protocols such as TCP/IP—are more easily added to commercial software.

Another driver for COTS RTOSes is long-term cost-effectiveness. Using this technology shifts the burden of developing and supporting the key software from platform and application designers to the RTOS companies, which are dedicated to supporting, testing and enhancing the products.

Standards-Based

The COTS RTOS market also is standards-driven, in order to satisfy demands for flexibility in porting applications and even substituting other RTOSes. The software is expected to conform rapidly to the latest versions of global standards, such as the Portable Operating System Interface for UNIX (POSIX), and to industry standards such as commercial aviation's DO-178B software development spec and ARINC 653 partitioning guidelines. Staff members at RTOS companies must be familiar with research at universities, agencies and industry organizations in order to keep their products viable in the market.

Key Standards and Architectures:

- POSIX application programming interfaces,
- DO-178B—commercial aviation software spec,
- ARINC 653—commercial aviation partitioning guideline,
- SCA 2.2 (software communications architecture), for software-defined radios, and
- Multiple Independent Levels of Security (MILS), an architecture for multilevel-secure systems.

Green Hills Software's INTEGRITY RTOS conforms to the latest POSIX standard, 2003 POSIX.1. INTEGRITY-178B, a more compact version of the RTOS, also has been approved to Level A of DO-178B. It is in the process of approval to evaluation assurance level-7 (EAL-7), the highest level of assurance for an operating system.

INTEGRITY is being designed into aircraft mission computers, display systems and traffic/terrain warning systems, as well as software-defined radios, a Space Station pad abort demonstrator, telecom equipment, process and industrial controllers, printers and even an Internet-connected oven. INTEGRITY supports most common microprocessor families. ■

Certifiable COTS

Demanding avionics applications require high-integrity processing hardware combined with certifiable software. Dy 4 is the only rugged COTS vendor offering both.

If your application demands a certifiable solution, speak to Dy 4. Dy 4 has developed DO-178B certifiable firmware that is compatible with leading real-time operating systems including Green Hills INTEGRITY-178B. Dy 4 has established the infrastructure to support DO-178B projects on any of our hardware products.

Contact Dy 4 to learn how we can deliver a total hardware and software solution for your safety certifiable needs.

SAFETY CERTIFIABLE software.

Contact: +1 613 599 9191 | Visit: *www.dy4.com*

Dy 4 Systems

A Curtiss-Wright Company

GREEN HILLS SOFTWARE DOMINATES THE AIR

Boeing C-17

Boeing B-1B

Airbus A380

Lockheed Martin F-16

Sikorsky S-92 (2002 Collier Trophy winner)

Lockheed Martin Joint Strike Fighter

Our INTEGRITY® operating system has been selected for more than 100 flight-critical systems

The INTEGRITY real-time operating system (RTOS) has been selected for more safety-critical applications than all other COTS partitioned RTOSes combined. Here's why:

- The INTEGRITY RTOS is proven in applications certified to DO-178B Level A, the most stringent safety standard for avionics software
- Green Hills Software has experienced on-staff experts to help you achieve certification
- The INTEGRITY RTOS is true COTS; the same technology is deployed in commercial communications applications

With Green Hills Software, your avionics systems get to market faster, with less risk, and far lower costs.

To learn more about flight-proven, true COTS solutions and certification expertise from Green Hills Software, call us at 805-965-6044 extension 201 or visit www.ghs.com/flight.

Green Hills®
• SOFTWARE, INC. •