

# Keeping Secrets in Integrated Avionics



Smiths Aerospace plans a MILS approach to security on its mission display processor for the C-130 Avionics Modernization Program.

By Charlotte Adams

Military aircraft will be operating in a networked environment, where data of the highest security levels will be readily available. How can avionics designers prevent classified data from leaking out through the aether and do it with today's integrated computers? Here's a snapshot of current research.

In the not-too-distant future, military aircraft may receive and exchange classified data with a variety of systems, as nodes in a global network. At the same time, military aircraft are equipping with civilian-compatible flight management and air traffic control (ATC) communications gear. As classified and unclassified data flows into and out of the aircraft, the task of protecting sensitive data and ensuring that it is sent only to the right places will become a major challenge. This challenge is magnified by the need to find an answer within the constraints of today's integrated avionics systems.

A military aircraft, for example, files a civilian flight plan, takes off on a routine flight into civil-controlled airspace, and contacts civil ATC. At some point on the route, in response to a new situation, the aircraft receives new commands and waypoints for a classified

mission. The pilot ceases to communicate with civil ATC and flies to the new coordinates. After completing the mission, the pilot recontacts ATC and lands. The right technology must be on board to keep data, such as special mission coordinates, separate from unclassified flight management information and to ensure that the classified data is not inadvertently transmitted to air traffic control.

## Rules Are Changing

This scenario is not new, but the rules of the game are changing. Military as well as civilian aircraft are expected to comply with evolving airspace rules, which entail more precise, civil-compatible navigation and communications equipment. Aircraft, for example, will be expected to maintain their position vis-à-vis other aircraft with less input from air traffic control. The civil flight management system (FMS) and military

FMS functions will need to share data, but must do it in a fashion that prevents the information relating to classified missions from leaking out.

It's possible to protect data by running it in separate hardware. But, with faster and faster processing chips, avionics is moving toward greater integration. If a design calls for hosting multiple applications—both unclassified and classified—on the same computer resources, then “you have to have a way to protect [the classified data] and convince the security people that you can run the classified applications safely,” explains Gerry Vossler, director of technology development with the Electronics Systems Division of Smiths Aerospace.

As Global Air Traffic Management (GATM) rules are applied and network-centric applications are developed, designers won't have the luxury of squeezing in more standalone computers.

The answer, security experts believe, is to separate different levels of security data through a software architecture leveraging hardware provisions. (The fundamental hardware is the processor's memory management unit [MMU], which controls access to memory.) The National Security Agency (NSA) and others have developed an approach

known as the Multiple Independent Levels of Security, or MILS. An important aspect of MILS is to distribute responsibility for security between different layers of software. If one layer, such as the operating system, were to take responsibility for all of the security functions, the thinking goes, it would become so large and unwieldy that it could not be certified.

Under the MILS concept, the core software of the operating system—known as the kernel, or microkernel—has overall responsibility for enforcing security policy. The kernel enforces the rules about which applications can communicate with each other, how much memory is allotted to each application, and how much time each application gets to run on the microprocessor. The kernel would be assisted by special-purpose security applications such as “guards,” security policy managers, and encryption algorithms.

Several real-time operating systems (RTOS) companies are working to certify their products to evaluation assurance level-7 (EAL-7), the highest security level defined in the international computer security guideline known as the “Common Criteria.” EAL-7-certified systems are expected to be able to separate three or more levels of data while

processing them on shared hardware resources.

### MILS Technology

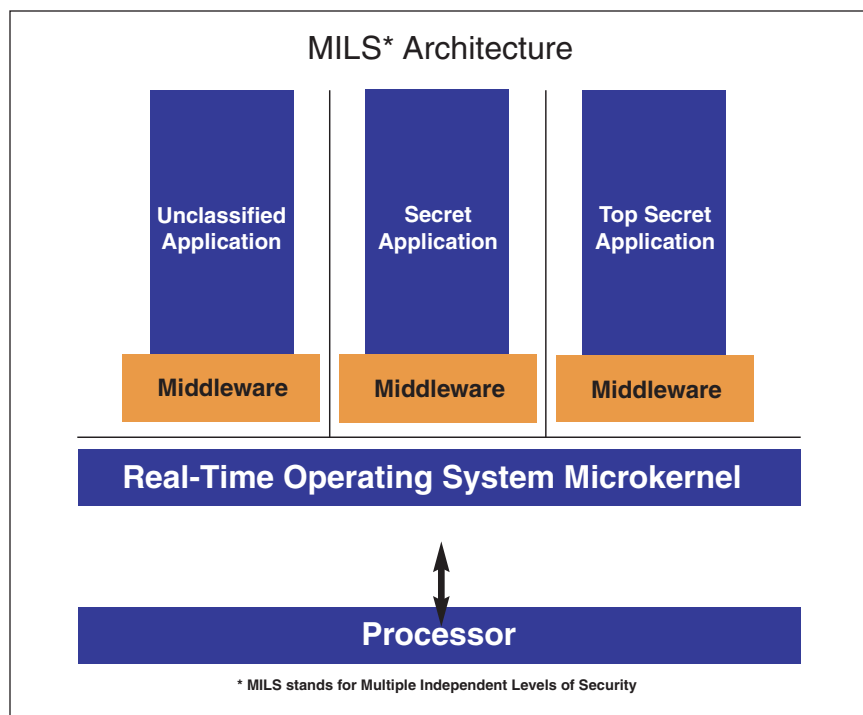
MILS-compliant technology already is planned for the C-130 Avionics Modernization Program (AMP). Wind River Systems is working with Smiths Aerospace to develop an NSA-certifiable implementation on the mission display processor for upgraded C-130 transports, gunships and special operations aircraft. Lockheed Martin, developer of the new F/A-22 and F-35 aircraft, is engaged in a security program funded by the Air Force Research Lab (AFRL). Both of these projects aim at EAL-7- certifiable software.

The AFRL program was first to determine the feasibility of using commercial RTOS and middleware to separate multiple levels of data. Green Hills Software, LynuxWorks and Object Interface Systems, a middleware company, were to provide plans on how much development work would be necessary and what the cost would be, say observers familiar with the program. A second phase was anticipated to evaluate the RTOS. Participants are understood to have provided information to Lockheed Martin, and AFRL is said to be seeking funding to accelerate the program. The effort also includes NSA, the Open Group, Rockwell Collins and the University of Idaho.

### Behind the Partition

Military aircraft manufacturers already are designing computers that host numerous aircraft functions on a single processor (see February 2004, page 16). A safety critical application, for example, may coexist with a non-safety critical application on the same avionics system. The operating system, however, protects the safety critical application by making sure that the various applications consume only their allotted time on the processing chip and only their allotted portion of memory—no more.

The RTOS guarantees that there is always processor time, memory space and memory access for the applications to run. This “time/space partitioning” concept—codified by the ARINC 653 standard—has been adopted by various real-time operating systems, both propri-



etary and off the shelf. Security researchers at NSA hope to use operating systems with partitioning as a baseline and push them one step further, so that the RTOS can separate security data, too.

Separation of multiple levels of security data through a MILS approach may eventually be required on numerous military programs. NSA PowerPoint presentations mention the F/A-22, F-35, C-130, Comanche, GPS, the Joint Tactical Radio System (JTRS) and the LandWarrior program as likely candidates.

The C-130 upgrade program already is developing a MILS implementation for the aircraft's mission display processor. Security certification is scheduled for 2006. This integrated computer will, among other things, run civil and military flight management, civil and military communications management, and weapons management applications. Smiths Aerospace is providing the computer hardware with the operating system and applications, such as flight management and communications management. Vossler indicates that each processing card will host multiple applications.

Wind River Systems, Smiths' RTOS partner, is developing a MILS-compliant operating system microkernel, the core software that would enforce separation between the levels of data. (The Smiths computer is currently running the ARINC 653 version of the RTOS, VxWorks AE653.)

### Great Leap?

The leap from safety partitioning to safety-and-security partitioning is not that great, RTOS developers say. ARINC 653-compliant operating systems already prevent any application from monopolizing processor time and memory space. The time-consuming and expensive part will be mathematically proving, to the satisfaction of NSA, that the RTOS microkernel enforces a system's security rules.

Another requirement is "covert channel analysis," which proves that there are no hidden pathways, or "holes," in the hardware or software to allow unauthorized communications between applications to take place. A secret application, for example, must not be permitted to access a top secret application's data by means of a hidden channel. And, if a top



**The Joint Strike Fighter, shown here, and the F/A-22 are key MILS candidates.**

secret application wants to say something to a secret application, it can do so only in the prescribed manner, typically, after the top secret data has been "scrubbed down" to the secret level by a "write-down guard" application.

In order to be mathematically analyzed and verified, security kernels need to be very small—from 4,000 to 10,000 lines of code. The operating system also must guarantee that when the processor switches from one application to another, there won't be any data "residue" for the next application to find—that all the temporary memory "registers" on the chip have been "sanitized." Security software also must meet more rigorous configuration management standards, delivery and documentation requirements, and not be developed and verified by foreign nationals, although the last requirement is open to some interpretation, depending upon the circumstances.

Layering security processing on top of avionics processing will cause a performance "penalty," but it is assumed that ever-increasing hardware speeds will offset the extra processing burden. Security guard applications, for example, will consume processor resources every time they have to "scrub" data down. The additional switching between additional applications also will consume time out of the system schedule. The size of the performance hit will depend on the system design—how many security tasks are added to the normal processing load. Two unclassified applications could communicate with each other more quickly than could a classified and an unclassified application, for example.

### Operating Systems

Three commercial operating systems companies are working on EAL-7 certification: Wind River Systems, Green Hills Software and LynuxWorks. Wind River is working with Smiths on the C-130 upgrade program; Green Hills is working with Lockheed Martin; and LynuxWorks is collaborating with an undisclosed military contractor.

Wind River is developing a MILS-compliant microkernel called VxWorks AESecure, a derivative of its current VxWorks AE653 operating system. The company is working with an accredited Common Criteria test lab, CygnaCom, to verify the security features. Introduced in October 2003, AE653 is in the pipeline for certification under DO-178B, Level A, the civil aviation safety standard, for Smiths equipment on the Boeing 767 tanker transport. AE653 also will be Level A-certified under the C-130 AMP program. Both AE653 and AESecure will be used in the C-130 upgrade. Wind River hopes to have DO-178B approval for AESecure in about 18 months. DO-178B approval is regarded as the "admission ticket," a starting point in undertaking a MILS development effort, according to one participant.

LynuxWorks is developing a MILS-compliant kernel, LynxSecure, which will contain fewer than 8,000 lines of code. EAL-7 certification for the new kernel is expected in a year and a half. The company also intends to get a less stringent, EAL-5 certification for its existing product, LynxOS-178, something it hopes to achieve in a year to 18 months, says Bob Morris, vice president

of sales and marketing.

LynxOS-178 is able to claim DO-178B, Level A, certification through Rockwell Collins, which uses the RTOS on the Challenger 300 adaptive display system. (Type certification from the Federal Aviation Administration [FAA] and Transport Canada was received in June 2003.) Collins earlier had developed an RTOS—supporting POSIX standards and partitioning—based on a prior version of LynxOS. This product, now called LynxOS-178, is maintained and enhanced by LinuxWorks.

DO-178B requires operating systems to support partitioning if more than one application is run on shared hardware resources. Collins' implementation on the Bombardier business jet involves the running of two Level A safety partitions on shared hardware, says Tony Johnson, chief architect with Collins' Integrated Applications business area. LynxOS-178 support for multiple partitions at different flight criticality levels—DO-178B, Levels A, B, C and D—also is used on military programs such as the KC-135, International C-130s, P-3, 767 tanker, UH-60 and the Army Common Avionics Architecture System, he adds.

Green Hills appears to be somewhat ahead of its competitors in the approval process. The company says it has completed covert channel analysis of its Integrity-178B operating system. The major remaining, and by far the most difficult task—the mathematical verification of the software's security functions—is expected to take another 18 months. Green Hills, LinuxWorks and Wind River are working closely with Objective Interface Systems, which provides a middleware product, ORBexpress. Integrity-178B achieved DO-178B, Level A, approval in 2002 as part of a display system on the Sikorsky S-92 (see story, page 18). Integrity-178B also has been selected for use in the F-35 mission computer and the F/A-22 integrated core processor.

Green Hills claims that Integrity-

178B's kernel, or core, is smaller than the kernels now offered by rival RTOS companies. The smaller the size, the easier it is to prove mathematically that the code does what it is supposed to do—and nothing else. The Integrity-178B kernel already is smaller than that of the version of the RTOS, known simply as Integrity. Services, such as the ability to create partitions dynamically, were removed from the core in order to make it easier to certify under the FAA standard, DO-178B. Dynamic partitioning probably would not be used in a MILS implementation, as the feature would make it more difficult to analyze the security policies being enforced and could serve as an entry point for an attack by malicious code.

### RTOS on an RTOS

LinuxWorks and Wind River, whose base operating systems are older than Integrity and have many legacy applications, say that their new kernels will fit the size constraints required for MILS evaluation. To do this, certain services must be removed from their kernels, a process known as "subsetting."

Both companies are trying to preserve customer investment by enabling full-featured, non-MILS versions of their operating systems to run in partitions—with legacy applications—over the secure kernel. An application using a full version of the RTOS in the partition could run at a single security level, making it easier to certify. Running operating systems in partitions, however, would require additional processing and communications.

Users of AESecure, for example, could run VxWorks/Cert—the DO-178B-approved version of the Wind River RTOS—in a partition. Likewise, LynxSecure could run an operating system like Linux in one partition and LynxOS-178 in another partition, Morris says.

An operating system running in a partition would function in "user mode," which means that it could not assign all

the processor's time and memory resources to itself. "You would not want any application you were trying to contain within a partition to be able to control the size and shape of its partition," explains Gordon Uchenick, a Wind River technical account manager. Only the low-level kernel can control time slots on the microprocessor and allocation of memory space to the applications.

Green Hills doesn't have to redesign Integrity-178B because the operating system's core software was developed to provide only the basic services—such as task and memory management and secure communications between partitions, says Patrick Huyck, Green Hills' systems certification manager. Using a non-MILS-protected operating system in a partition also raises security issues, he says. The operating system could be vulnerable to a rogue application, with effects on failure monitoring and failure reporting. But higher-level fault monitoring and reporting could address this issue.

While it's possible that the operating system running in a partition in application space could become corrupted by a rogue application, damage would be limited to the single partition, Morris says. The application could not communicate with any other application except through the security rules enforced by the MILS-certified kernel, thus protecting the integrity of the MILS structure.

By the same token, a very small kernel is limited to basic functions and calls, says Morris. LinuxWorks' approach will be well-suited for a complex application like command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR), he says. Green Hills' Integrity-178B, on the other hand, can support complex applications, too, Huyck contends, by tailoring services, such as file system and Ethernet data communication support, in partitions above the kernel.



[www.ghs.com](http://www.ghs.com)