

AVIATION WEEK

& SPACE TECHNOLOGY

INFORMATION TECHNOLOGY

Isolating Safety

Operating system picked for 787 controls finds applications in secure communications

MICHAEL A. DORNHEIM/LOS ANGELES

The Boeing 787 will trust its fly-by-wire control system to a commercially available real-time operating system from an outside vendor, instead of the proprietary or simpler systems that are being used on existing fly-by-wire airliners.

This type of operating system is also making inroads into the secure communications world, where the strict isolation of different functions necessary for aircraft safety translates into maintaining separation and protocol between several tasks operating at different security levels. It may be adopted by several U.S. Air Force programs.

Honeywell has picked the Integrity-178B real-time operating system by Green Hills Software for the 787 fly-by-wire system it is building for Boeing. Honeywell has used its own operating systems for prior flight control projects, but chose Integrity-178B from an outside vendor because it was written around more-up-to-date industry standards and the latest processors.

Integrity-178B is also being used by Honeywell for the 787 navigation system; by Rockwell Collins for the 787

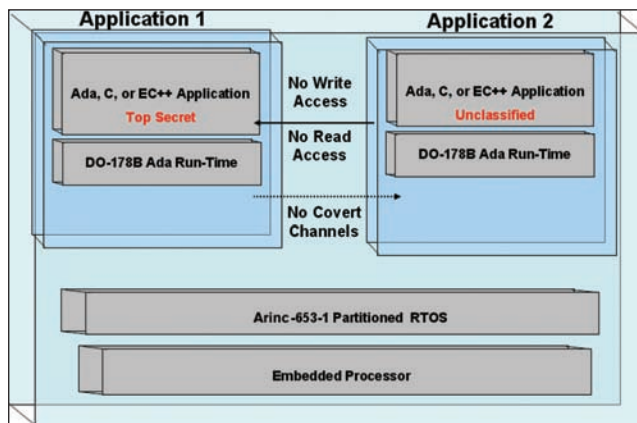
surveillance system comprising weather depiction and traffic and terrain avoidance; and by Vibro-Meter for the 787 engine vibration and health systems.

The more recent standards make it easier to certify and update flight-critical software, as well as run several different programs on the same computer without risk that the crash of one could take out the others, says David S. Bar-

nett, Green Hills director of product marketing. The main standard is Arinc-653, which defines strong partitions between multiple programs running on a single processor. And Integrity-178B works with modern PowerPC and MIPS processors, whereas most proprietary operating

systems are for the prior-generation Motorola 68000-series chips. Arinc-653 allows programs to be broken into smaller pieces that are easier to certify and that can be updated without having to retest everything else.

The FAA requires that flight software be developed and proven with a methodology developed by the RTCA called DO-178B. This has several levels, with Level A being the most difficult and intended for critical functions like flight control systems and primary flight displays. Green Hills has designed its operating system around the DO-178B standard and it adheres to the Arinc-653-1 specification for independent partitions. The company has certified several systems to Level A and says this has eased subsequent FAA certifications where much of the documentation is carried over. The cost for FAA certification is roughly \$100 per line of code for Level A, but only about \$10 per line for Level C, Barnett says.



To run programs at different levels of security, the Real-Time Operating System must go beyond commercial Arinc-653 requirements and prevent covert communications.

nett, Green Hills director of product marketing. The main standard is Arinc-653, which defines strong partitions between multiple programs running on a single processor. And Integrity-178B works with modern PowerPC and MIPS processors, whereas most proprietary operating

The best-defined safety standards for software have come from avionics, so it is not surprising that they overlap with secure systems, Barnett says. The main standard for certifying secure software is the Common Criteria used by the U.S. and 20 other countries. A study by the

University of Idaho said that Common Criteria and DO-178B are almost alike.

Secure software is measured by two dimensions—the level of security it is designed to achieve, and how certain it is to meet that goal. A standard of security similar to the Arinc-653 fire-walling of separate programs is the National Security Agency's Separation Kernel Protection Profile (SKPP), which is the most demanding profile for multiple independent levels of security. To rank the latter dimension, the Common Criteria have seven Evaluation Assurance Levels (EALs), of which EAL7 is most assured.

The Idaho study concluded that DO-178B Level A was about the same as EAL5, while the NSA separately concluded it was equivalent to EAL4+ or 5. Barnett says the fact that different groups are drawing equivalences

between avionics and security systems indicates a distinct but convergent evolution in their design.

Most commercial operating systems, such as Unix and Windows, have only been certified to EAL4. "No commercial operating system has succeeded in being certified to beyond EAL5, and that's been to a lax protection profile," Barnett says.

The Air Force F/A-22, F-35 and Joint Unmanned Combat Air System (J-UCAS) program offices may want to use Integrity-178B for secure tasks on their aircraft. With Air Force Research Laboratory and Lockheed Martin coordination, they are partly funding Green Hills' effort to certify the operating system to EAL6+ while implementing the SKPP architecture, a complex task. To that end, Rockwell Collins is creating a formal description of Integrity-178B

and SAIC is conducting an independent security evaluation.

These aircraft will have battlefield data flowing through them at different levels of security and SKPP is to help keep it sorted out. One area where the military goes beyond DO-178B Level A is checking for covert paths between supposedly independent programs. For example, one program might give clues to what it is doing by leaving a disk head at a certain position that can be deduced by another program sharing the drive.

Experts say it is in practice impossible to certify to EAL6 a program with more than 5,000 lines of source code because the evaluation grows exponentially. But by breaking a program into smaller chunks that each run in their own secure partition made available by Integrity-178B, each can be individually assessed, simplifying certification. ❏

