

COTS steps up to embedded computing security



By John Wemekamp



Armed forces worldwide continue to be concerned for their security as they become increasingly dependent on the use of high technology in critical war-fighting arenas. The network-enabled battlefield and Global Information Grid (GIG) have introduced the need for more vigilant network security. This, in turn, has motivated the move to IPv6, with all implementations required to support Authentication Headers (AHs) and Encapsulating Security Payloads (ESPs). However, this is only one piece of the puzzle. Any situation where high-technology equipment, from manpack radios to armored vehicles or combat aircraft, is deployed on the front line poses a risk if the technology unintentionally falls into the wrong hands. Technology can be reverse engineered to discover its operation or to replicate it. In addition, unraveling its firmware and software code to reveal its algorithmic and performance data might also expose potentially compromising information such as orders, codes, and keys of much wider significance.

Protection of critical technology is now considered to be an essential element in the overall system design and procurement processes of new equipment. Identification of Critical Program Information (CPI), whether it is data or technology based, starts at the system level. It is then decomposed to application software, operating system, firmware, communications, subsystems, chassis, modules, deployment, operation, and maintenance down to the lowest level. New programs must identify CPI and develop a comprehensive protection plan to mitigate every aspect that could compromise its technical superiority if it were to be reverse engineered – or if details of its performance or operation were to be revealed.

Layered approach is best

Typical good practice means taking a layered approach to providing protection. In the context of an embedded system, this would start at the chassis or enclosure level with volume protection. Volume protection is designed to prevent physical intrusion, or if prevention is not possible, then detection of intrusion must trigger irreversible indications. Equipment is often recovered or returned at a later date, so understanding the depth of intrusion is of vital interest. The simplest example of this form of detection is a *warranty seal* to indicate that the enclosure has been opened. However, this is obviously not enough, and further active and passive measures must be taken for greater assurance. External I/O connections must also be considered, for example, debug ports, network connections, or special-to-type I/O. These could reveal critical performance parameters or provide access via potentially vulnerable information.

Additional stages of hardware protection might be necessary to protect FPGA or nonvolatile memory contents. Often electronic assemblies in transit for maintenance or repair, or in an emergency, will have had their nonvolatile memory erased. This basic feature has been incorporated by many COTS vendors into their products offered for military applications. However, erasure is not always practical for FPGAs or other types of programmable

devices. Thus, other techniques might warrant consideration, such as encrypting or obfuscating the contents. Similarly, software and firmware require protection from the lowest levels of code storage, retrieval, and execution through I/O, communications, and the application layers.

Custom versus COTS in the military

The traditional method for the military to protect their critical technology leadership has been to employ custom hardware and software design. Each project has its own specific security requirements; therefore, off-the-shelf embedded computing equipment is perceived as unlikely to incorporate entirely. But as technology becomes more widely diffused across the battlefield, even as far as fleets of trucks or handheld devices for individual soldiers, the cost of this purely custom approach is escalating. Through much greater understanding of the issues, plus dialog with end users and integrators, COTS vendors are able to bridge the cost/capability gap between fully custom and off-the-shelf products. This gap is narrowed when COTS vendors introduce key protection capabilities into their products that meet many critical program requirements. Features such as active perimeter defense, a secure computing environment, and standards-based, NIST-approved cryptographic engines are examples of how COTS vendors like Curtiss-Wright Controls Embedded Computing (CWCEC) are addressing these security needs (Figure 1).



FIGURE 1: Curtiss-Wright Controls Embedded Computing's VPX3-1100 Atomic SBC is designed to address today's security needs via its active perimeter defense, secure computing environment, and standards-based, NIST-approved cryptographic engines.

Including security features early in systems engineering and development will reduce overall costs of implementation and eventual retrofit following deployment. At the higher layers, requirements and solutions to those requirements will vary significantly from project to project. However, for embedded computing hardware, it is possible to take a more generic approach, one that provides a comprehensive set of secure enabling technologies that can be used intelligently to create a safer environment to support those very specific outer layers.

To learn more, e-mail John at john.wemekamp@curtiswright.com.