



The Journal of
Military Electronics & Computing

High Barrier of Entry

By: Jeff Child, Editor-in-Chief

June 2009

It's nice to see signs now that our economic troubles may not be as catastrophic as once feared. And, for its part, the defense electronics business—especially compared to the rest of the economy—has been humming along nicely. Of course, as a reader of COTS Journal, you already work in the defense industry—or a technology area that does business in the defense market—so you already know that. Likewise, our magazine (knock on wood) seems to have fared much, much better on average than the rest of the trade publishing industry.

I recall during the last recession (2001/2002) how many technology suppliers looked to the military market as a possible “safe haven”—a place to shift into in order to compensate for the drying up of the non-military business they'd focused on before. During that era, I remember that trend most vividly amongst embedded computer vendors and power suppliers that had been focused on the telecom market. Many such suppliers made an attempt to shift into the defense market, but very few were able to mount the high barrier of entry into this market. Beyond any particular expertise in developing products appropriate for military systems, there's just a simple matter of establishing trust and relationships with military customers. That trust is much more hard won than outsiders understand. As a result, many have failed to make the transition.

Fast forward to the current recession and I'm seeing that same trend again of non-military-focused suppliers hungry to enter into the lucrative, stable defense arena. This time around the barriers are even higher thanks to the increased concerns about security, tighter enforcement of International Traffic in Arms Regulations (ITAR), anti-tamper regulations, the complications of RoHS and so on.

In some ways, there's a benefit to entering the defense market now. I recently spoke to the folks at Columbia Tech, a small U.S.-based turnkey contract manufacturer, about their recent efforts to achieve ITAR registration with the goal of growing its presence in the military market.

According to Richard Schulman, VP of Quality and ITAR Technology Control Officer for Columbia Tech, it took the company several months to get themselves educated and prepared for ITAR approval. But once achieved, their military customers told them that Columbia Tech exhibited a greater level of awareness of ITAR than many other long-time established military electronics suppliers. The chance to "come at the issue fresh" is not such a bad thing these days.

Meanwhile, companies with a long history of playing in the defense market appear to be enhancing their focus on security. It seems like this past month in particular, has seen a flurry of security-related initiatives and product offerings from the military embedded market. For example, Curtiss-Wright Controls Embedded Computing launched a new initiative dubbed "Trusted COTS," an effort aimed at responding to the DoD's mandate that all critical military technologies and data be protected. The specific mandate in question is the DoD's directive DoDD 5200.39, Research and Technology Protection Procedures. Re-issued last summer, the directive declares that all military systems must provide protection of Critical Program Information (CPI). Under its Trusted COTS initiative, Curtiss-Wright Controls is developing standards, methodologies, tools and knowledge that will define improved engineering product design and development processes. This will involve seeking out partners with whom the company can work with to customize and integrate security-focused solutions into deployable products.

In response to that same directive, DoDD 5200.39, processor and tool vendor CPU Tech earlier this year rolled out its Acalis CPU872 secure processor. The CPU872 is, according to CPU Tech, the first processor with anti-tamper capability in accordance with 5200.39, which defines anti-tamper as "Systems engineering activities intended to deter and/or delay exploitation of critical technologies in a U.S. defense system in order to impede countermeasure development, unintended technology transfer, or alteration of a system."

Advanced security features—such as anti-tamper capability and design separation—have been available before on large FPGAs, like the Xilinx Virtex. Xilinx, for its part, recently announced a defense grade version of the Virtex FPGA family that marries ruggedized packaging and advanced cryptographic capabilities. Meanwhile, Altera has instead chosen its lower power Cyclone line of FPGAs for its first offering of sophisticated anti-tamper and security features. The security features of this new family of Cyclone FPGAs enable it to serve as a single-chip solution for next-generation military applications such as software defined radio, crypto-subsystems and crypto modernization equipment.

As I talk to various board, IC and software vendors about their latest security-targeted offerings, I get a clear message that the whole area of security is, in some ways, in its infancy. In other

words, even the most knowledgeable of today's developers of military, embedded computer-based systems are not, on average, experts on all the nuances, methods and regulations having to do with anti-tamper capabilities, security and trusted component sources. That's why it's imperative that the education process along those lines gets kicked into higher gear. Security may on one hand be all about restricting information, but now more than ever, the development of secure, trusted systems and tools available to make them should be moved into the foreground of today's military electronics engineering knowledge. The barriers of entry may be high, but the defense industry needs all the expertise and experts it can get its hands on.