

Reconfiguring the Battlespace

You can develop aerospace and defense applications with Xilinx and Wind River technologies.

by Paul Parkinson
Senior Systems Architect
Wind River
paul.parkinson@windriver.com

The development of modern defense systems presents a familiar technological challenge in that the requirements for increased application functionality conflict with the requirements for minimal footprint in terms of space, weight, and power (often referred to as “SWaP”). This is a particular concern for airborne platforms, especially unmanned air vehicles (UAVs) that have physical constraints.

Some defense systems are physically vulnerable to interception by hostile forces because of their operational role, including intelligence, surveillance, and reconnaissance (ISTAR) assets such as reconnaissance aircraft, UAVs, and land-based sensor systems. If these platforms are to use leading-edge technology, it must be technology that cannot be compromised or reverse-engineered.

In addition, field-based configuration and upgradability are essential to achieve interoperability between new and rapidly deployed coalition forces.

In this article, I’ll explain how Xilinx® Virtex™-II Pro and Virtex-4 platform FPGAs, along with Wind River software platforms, are ideal for the development of ISTAR systems, and present design techniques that will enable secure deployment, with the use of partial reconfiguration in the field to help enable interoperability between coalition forces.

Technology Challenges

In previous decades, defense systems used military-grade components from semiconductor manufacturers. These components had long life cycles, which were essential to support the in-service use of deployed hardware for 20, 30, or even 40 years.

In 1994, when U.S. Secretary of Defense William Perry first advocated the use of commercial off-the-shelf (COTS) components on U.S. military programs where appropriate, other governments around the world subsequently adopted this philosophy (to varying degrees). The migration to

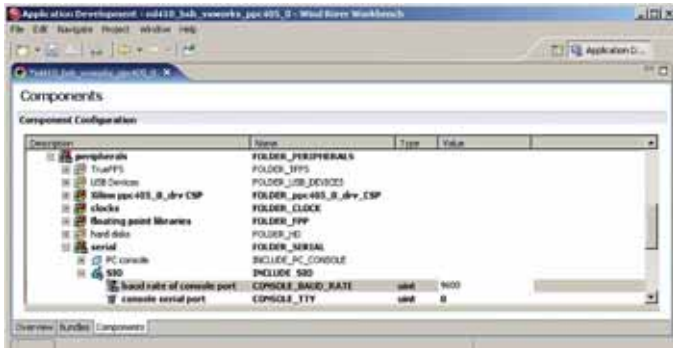


Figure 1 – Workbench kernel configuration for Xilinx ML410 VxWorks 6 BSP

COTS has led to a move away from specific military-grade components and toward a greater reliance on industrial-grade components. The latter’s shorter supported life cycles could impact in-service lifetimes.

In addition, defense companies have developed custom ASICs at great expense for specialized functions in defense systems, particularly ISTAR systems. Replacing these devices in deployed systems can be prohibitively expensive. There is also an ever-growing requirement to extend the in-service life of ASICs as the operational lifetimes of front-line defense systems are extended.

These challenges can now be addressed through the use of Virtex-II Pro and Virtex-4 FX FPGAs, given their increased gate counts and incorporation of CPU and DSP functionality.

The platform FPGA also has the potential to be used for algorithmic operations, but until recent years this has not been exploited because it is difficult to express software algorithmic operations in million-gate applications in VHDL. However, the ability to program reconfigurable logic from high-level software languages such as C as well as VHDL opens up the potential of these devices to further exploitation.

Platform Development

You can readily exploit the potential of the platform FPGA through the Xilinx Platform Studio (XPS), which generates hardware peripheral and IP definitions in VHDL, closely coupled with the automatic generation of a VxWorks board support package (BSP) in C source code for the PowerPC 405 processor core(s) contained within the Virtex-II Pro and Virtex-4 FX device fabric.

(The details of this approach were previously discussed by Rick Moleres and Milan Saini in their article, “Generating Efficient Board Support Packages” [Xilinx *Embedded* magazine, March 2006] and included integration with Wind River’s Tornado 2.2 IDE and VxWorks 5.5 RTOS.)

Since the publication of that article, it has become possible to undertake similar developments using the state-of-the-art Wind River Workbench development suite and VxWorks 6 RTOS. VxWorks 6 provides a

number of enhanced capabilities when compared to VxWorks 5.5, including technologies that are critical in defense applications; advanced memory protection for application isolation using real-time processes; and a dual-mode IPv4 and IPv6 network stack, which the U.S. Department of Defense mandated for new programs in 2003.

After XPS generates the VxWorks 6 BSP, it can be configured in the Workbench project configurator (Figure 1). The configurator enables components to be configured in a hierarchical manner and parameter values to be specified. When this has been completed, you can build the VxWorks 6 kernel for your target device from Workbench through automated processes (Figure 2). Once VxWorks is running on the PowerPC 405 core(s), you can use Workbench for source-level application development (Figure 3).

The integration between XPS and Workbench allows you to use a VxWorks 6-based common software platform on Virtex FPGAs for application or algorithm control or gateway network interfaces. This provides a very flexible approach that you can exploit for functions such as image compression and data link encryption to relevant NATO standardization agreements.

System and application software in these devices (known as device software) are often implemented in an architecture-specific manner, using low-level programming languages such as assembly language and custom software schedulers. Although this has enabled exploitation of the hardware’s performance potential, it has also made the task of technology insertion and program upgrades more difficult.

You can overcome this problem by using software platforms based on open standards. For example, the Wind River General Purpose Platform – VxWorks Edition incorporates the Wind River Workbench development suite, which uses the Eclipse open-source framework to provide seamless integration between tools for different parts of the device software development life cycle, as well as a consistent GUI for developers. This approach has tangible benefits in terms of developer efficiency, transferable skills, and knowledge retention.



Figure 2 – Workbench build of Xilinx board VxWorks 6 kernel image



Figure 3 – Workbench target connection to PowerPC 405 core in Virtex FPGA

On the runtime side, VxWorks 6.4 introduced 100% conformance to the POSIX PSE52 real-time controller profile, enabling software reuse from legacy systems and the development of new portable applications.

Communications Security in Defense Systems Design

Communications security (ComSec) is an important requirement in many defense systems, especially in UAVs, which often need to maintain continuous communications links for remote piloting and real-time image streaming. These communication links must be secure from eavesdropping and interference by hostile forces, so encryption is required for flight control and sensor data transmissions. You could implement this encryption in software (which places an additional load on the processor) or in dedicated hardware logic. You could also use reconfigurable technology, which provides benefits in terms of performance and secure design (which I'll soon discuss).

Let's consider a hypothetical scenario involving the use of Triple DES-encryption on a communications link. Triple DES encryption provides a relatively high level of security by encrypting data three times using three 64-bit private encryption keys. This is inherently more secure than single DES encryption but will take a processor three times longer to compute, because the processor performs the encryption as three sequential steps.

Given the parallelism inherent in a Xilinx platform FPGA, you can implement three encryption stages operating in parallel, with the output of one stage pipelined into the next stage in 64-bit words. This acceleration enables the passing of data at higher rates over secure downlinks.

For example, a 350-MHz PowerPC can Triple DES-encrypt a data stream at the rate of 1.2 Mbps, whereas a lower power 20-MHz Xilinx Virtex-II Pro FPGA can Triple DES-encrypt a data stream at the rate of 22 Mbps, with each 64-bit word processed in 57 clock cycles.

You could apply this encryption accel-

eration technique to provide a secure TCP/IP-based communications framework (using IPSec in conjunction with Triple DES or potentially 256-bit AES encryption) and data link protocols. This would involve performing the network packet processing on the PowerPC processor, with computationally intensive encryption offloaded to the FPGA, acting as a coprocessor.

Information Security in Defense Systems Design

Defense systems now contain an increasing number of subsystems. In an airborne platform, for example, there are avionic systems (for flight control), mission systems, and sensor systems for payloads such as electro-optic/infrared sensors (EO/IR) and synthetic aperture radar (SAR) (Figure 3). ComSec in this case refers to the use of firewalls and encryp-

not provide a rapid, complete, and irreversible destruction of subsystems; although they may achieve software destruction, they may not sufficiently destroy all of the hardware architecture, especially fixed hardware components such as ASICs.

Thus, it could still be possible to perform reverse engineering on some aspects of the hardware design. To prevent this, reconfigurable technology offers the ability to achieve rapid and complete destruct sequences and prevent reverse engineering.

FPGA devices can be erased completely, leaving no trace of their original application. By asserting a specific signal, the device could be cleared in hardware in a few hundred microseconds. You could also perform the software destruct sequence through programmatic software control issued from a remote system, a sensible scenario in the case of a UAV capture.

You can implement the sequence from a



Figure 3 – Military airborne data networks

tion for the transmission and reception of information securely between networks without transforming the information during transport.

Data communication between the avionics systems and mission systems will include the passing of global positioning information, bearing, and altitude. However, information with differing security classifications may also need to be transformed securely between applications, subsystems, or networks – this is known as InfoSec.

Preventing Reverse Engineering by Secure Design

The implementation of a system destruct sequence capability is possible for systems that are vulnerable to compromise or capture by foreign forces. However, previous implementations of destruct sequences may

VxWorks-based common software platform connected to the command and control center through a secure IP-based network, permanently and irreversibly erasing the content of a Xilinx FPGA using the PLD API for VxWorks Embedded Systems (PAVE), as shown in Figure 4.

I referred to Triple DES encryption in the context of secure communication links earlier, but you can also employ this method within the content of the Xilinx FPGA (also known as the payload, not to be confused with a UAV payload). When the bitstream is read out from the FPGA, the Triple DES encryption must be decrypted before the bitstream can be decoded. This not only protects the FPGA content from being copied blindly and reused; it also prevents it from being reverse-engineered should the UAV be intercepted.

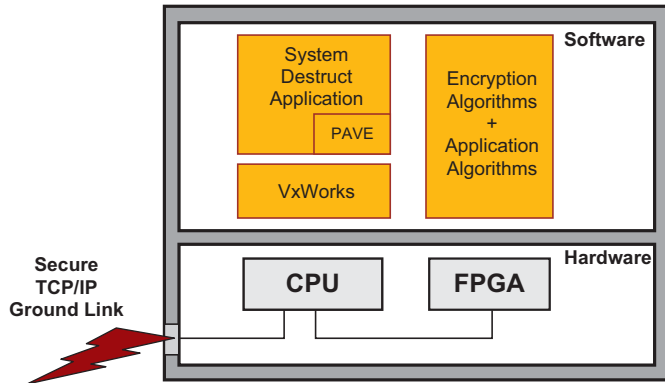
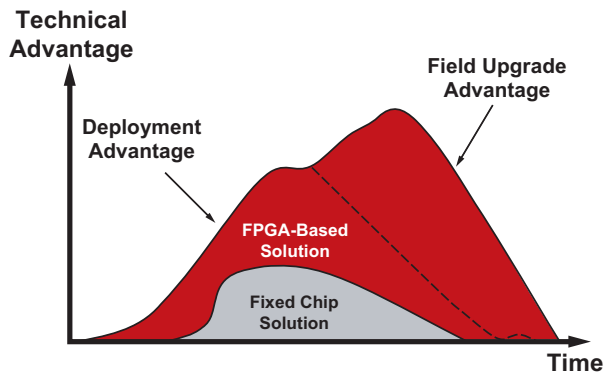


Figure 4 – CPU-controlled reconfiguration of a Xilinx FPGA



Time to Deployment - First to deploy increases technical advantage
Time in Field - Increases the in-life support yield while in field

Figure 5 – Reconfigurable technology life cycle

Conclusion

ISTAR systems will spearhead the deployment of new coalitions in response to potential or emerging conflicts, providing vital imagery intelligence and situational awareness from reconnaissance missions. A common software platform and reconfigurable technology could be used to implement codecs that support reconfiguration in the field, assisting in the rapid deployment and interoperability with NATO and/or other coalition forces by sharing encryption keys. Platforms can also be reconfigured on the fly to communicate with legacy or incompatible systems belonging to other coalition members (if a suitable codec exists).

Reconfigurable technology not only provides the ability to rapidly deploy new technology, but also the means to extend the in-service lifetimes of deployed systems. A network-enabled software plat-

form acts as a secure gateway to deliver new content and perform partial or full reconfiguration of FPGAs while deployed in the field. This approach would harvest the architecture shown in Figure 4, but employ an upgrade application instead of a system destruct application.

When considered together, these capabilities provide a technical advantage over traditional fixed-chip solutions (Figure 5) and present a powerful argument for their adoption on defense programs.

For more information, I recommend a paper by Saar Drimer of the University of Cambridge on the use of FPGAs in the design of secure defense systems. To read "Volatile FPGA Design Security – A Survey," visit www.cl.cam.ac.uk/~sd410/papers/fpga_security.pdf.

For more information about the Wind River General Purpose Platform – VxWorks Edition, visit www.windriver.com.

Supporting Your Future
HUNT ENGINEERING
 USB connected Programmable FPGA systems

V-II Pro PowerPC

- Virtex-II Pro XC2VP7
- 256 Mbytes DDR Memory
- Configurable digital I/Os
- PowerPC boot FLASH
- USB 2 or Standalone

Software Defined Radio

- Virtex-II FPGA 1M gates
- 2 ch 125Msps A/D and D/A
- TI C6203 DSP
- 32Mbytes SDRAM
- Configurable Digital I/O
- USB 2 or Standalone

Imaging with Virtex-4FX

- Virtex-4 FPGA FX12
- 128Mbytes DDR Memory
- CameraLink connection
- VHDL and PowerPC Imaging Libs
- USB 2 or Standalone

Programmable hardware with cables, device drivers, loading tools, examples and Power Supply. Systems can be used connected to a PC using USB, or can function standalone (without USB) using the initialisation PROMs.

sales@hunteng.co.uk
 +44 (0)1278 760188
www.hunt-rtg.com