Extended-life COTS hardware ushers in the *Secure, Reliable and Scalable* era for cross-domain network communications

By Jim Renehan

Jim updates us on the diverse range of COTS hardware platforms using multicore processors that come with built-in security features. Merging PICMG platforms with advanced software security tools is one way developers are addressing the challenge of cross-domain communications.

Post 9/11 crisis prevention and response have made improving communications, information sharing, and collaboration critical Department of Defense (DoD) and Department of Homeland Security (DHS) goals. A number of other federal and state organizations share these goals. Binding all of these organizations together is the critical need to share information seamlessly and on a secure basis. The National Security Intelligence Reform Act of 2004 recognized the need to improve cross-domain communications. This act established the Director of National Intelligence (DNI) and specifically required the DNI to "ensure development of information technology systems that include multi-level security and intelligence integration capabilities[1]."

Cross-domain communications and Multiple Independent Levels of Security (MILS)

The DoD and DHS have a multitude of computer networks or domains with differing security classifications. These domains are made up of end-points or clients such as workstations, vehicles, PDAs, and individuals. Host servers managing the domains have differing requirements for separation, information flow control, and end-point integrity based on the security level of the domain. One secure network communication solution called Multilevel Security (MLS) enables the processing of information with varying security levels and permits access to users with different security clearances while denying access to unauthorized users[2].

A more recent development is the concept of Multiple Independent Levels of Security or MILS. In MILS architecture, the secured networks' computer hardware and software components work together to automatically satisfy the security needs of domain separation and information flow. This enables communications between users with different security clearances. The MILS approach is a modular one that utilizes strict component isolation intended to increase security while at the same time cutting both development time and costs and those for platform certification and accreditation.

In addition to accessing information from multiple domains, many users also need to transfer information between domains. The controlled interfaces that make this happen go by the name "cross-domain solutions[3]." Cross-domain solutions must maintain separation, flow control, network security, and end-point integrity requirements when enabling communications across networks with different security levels. New cross-domain hardware options include multicore processors with advanced virtualization technology. Multicore processors on COTS hardware platforms like PICMG 1.3 single board computers (SBCs) and MicroTCA Processor AMCs (PrAMCs) provide new capabilities critical in cross-domain platforms. COTS hardware advancements make it possible to answer the secure network communication challenges in a variety of cost-effective cross-domain platforms.

Until recently implementing a MILS architecture required too many hardware boxes with excessive power demands and offered limited system flexibility and scalability. This situation has changed for the better with the introduction of advanced multicore Intel® processors with improved power efficiencies. Processor capabilities such as those found with Intel® Trusted Execution Technology (Intel® TXT) and Intel® Virtualization Technology (Intel® VT) are key elements in some cross-domain solutions.

The PICMG 1.3 System Host Boards (SHBs) and MicroTCA PrAMC illustrated in Figure 1 utilize today's multicore processor technology to solve cross-domain application challenges. These COTS hardware platforms reduce the number of boxes needed, saving power and space while increasing system scalability.

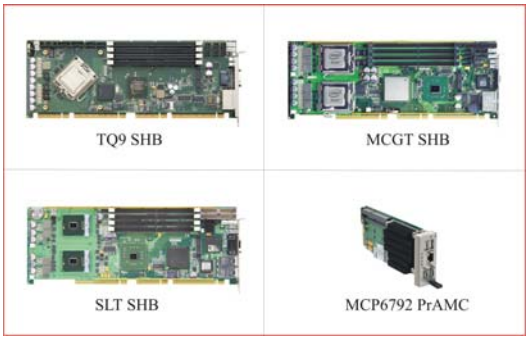

Figure 1 - PICMG 1.3 SHBs and PrAMC Examples

Some cross-domain implementations do not need processor features such as Intel® TXT. These platform options satisfy the cross-domain requirements using a guard-board hardware architecture and/or employ specific application software and operating system components. These multi-domain implementations use dual-processor PICMG 1.3 SHBs with multicore Intel® Xeon® processors. Examples of these SHBs are the Trenton MCXT or MCGT as well as a new product called the JXT6966. PICMG 1.3 SHBs with low-voltage Intel® Xeon® processors like those used on the Trenton SLT are common in secure cross-domain platforms with a guard-board implementation where power savings is a prime system consideration.

A standard PICMG 1.3 multi-segment backplane enables a cross-domain platform design that supports multiple SHBs in one 19-inch rackmount server enclosure. This hardware design approach helps meet network separation requirements. SHB multicore processors, along with virtualization, a hypervisor, and secure embedded operating system software, allow software running on a High Assurance Platform (HAP) client to function in a cross-domain communications network. This rackmount server design approach with Intel® Virtualization Technology as a key processor feature, paired with the HAP client, meets the MILS requirements for a cross-domain

solution. The following is a brief summary of how virtualization is utilized in these applications.

Virtualization in cross-domain applications

Today's dual and quad-core processors with core-level virtualization technology allow multiple operating systems and/or applications to run independently of each other on an SBC or PrAMC. This eliminates the need for a one-to-one correlation of operating system and application software with the computer hardware. As a result one single board computer or processor AMC can use its separate processor cores to run multiple applications within the same rackmount server. This capability saves precious rack space (S) thereby requiring less floor space, which cuts down on overall system weight (W) and needs less power (P). A PICMG 1.3 multisegment backplane with multiple single board computers or a MicroTCA chassis with several processor AdvancedMCs enhances this concentration of secure applications. It's a solution that maximizes SWaP savings for a secure cross-domain implementation. Reducing the number of individual computer chassis needed and deploying secure cross-domain solutions using today's power-efficient processors maximizes the installation's total power savings. What follows is a summary of four cross-domain implementations, each using a different COTS hardware platform.

PICMG 1.3 cross-domain platform – SHBs using single, quad-core processors

Figure 2 shows a four-segment PICMG 1.3 backplane called the Trenton BP4FS6890 to support up to four PICMG 1.3 system host boards. In this system, the Trenton TQ9 SHB with a single Intel® Core™ 2 Quad Processor Q9400 is being used because the processor is a long-life embedded CPU. The scalability, upgradability, and long-life features of the hardware enable a stable cross-domain hardware platform that supports the extended deployment cycles common in DoD applications. The processor used on the SHBs support four execution cores, Intel® VT, Intel® TXT, and (with Trenton's IOB32 optional module) provides TPM 1.2 support for trusted computing platform security. This cross-domain platform using four TQ9 boards makes multiple applications virtualized at different security levels on each system host board possible, and multiple HAP clients can access each SHB simultaneously.

Figure 2 - Four SHB Platforms Using Single CPUs

PICMG 1.3 Multi-domain platform – SHBs using two quad-core processors

This system variation uses the same four-segment backplane described previously, but with dual-processor SHBs such as the MCGT. As with the previous implementation, the backplane shown in Figure 3 enables each single board computer to operate independently of each other to manage its particular security domain.

Figure 3 - PICMG 1.3 Multi-segment Backplane

Each SHB in this system uses two, long-life, quad-core Intel® Xeon® processors featuring Intel® VT. This solution offers more processing horsepower at the expense of on-board system security. The security needed to support the MILS requirement that was provided on the SBCs with Intel® TXT support in the previous platform example needs to come from other elements within the system such as the application software. Like the previous platform option, the IOB32 module can provide TPM 1.2 capability. Figure 4 illustrates four PICMG 1.3 system host boards inside a 19-inch rackmount multi-domain server chassis with a 5U rack height.

Figure 4 - Four SHB Platforms Using Dual CPUs

Each dual-processor SHB shown in Figure 4 supports eight unique processing cores running discrete applications, so a two-board system supports 16 cores, while a four-board system doubles this capability to 32 cores. Multiple processing cores and virtualization technology deliver SWaP savings by reducing the number of unique hardware boxes required to achieve Multiple Levels of Independent Security.

PICMG 1.3 cross domain approach – SHBs using two dual-core LV processors in a guard-board configuration

The DoD has used the guard-board approach to a secure cross-domain solution extensively. The latest incarnation of this design approach (Figure 5) uses a six-segment PICMG 1.3 backplane (Trenton BP6FS6605) and the low-power SLT system host boards.

Figure 5 - Three/Five SHB Platform with LV CPUs

This system is available in a two-network/three-SHB configuration or the five-network/six-SHB system implementation shown in Figure 5. The dual-core processors used in this system are low-voltage CPUs that support various "Green IT" initiatives while enabling high-performance message transfer capacities. Like the system in Figure 4, the long-life, dual-core Intel® Xeon® LV processors used in the Figure 5 system feature Intel® VT, but do not offer Intel® TXT or support a built-in TPM 1.2 capability. However, this guard-board platform approach eliminates the need for these processor features.

This guard-board platform is a completely secure cross-domain solution that meets DCID 6/3 PL4 requirements by virtue of the security components of the application software, flexible mandatory access control capability, and the Security Enhanced Linux (SELinux) operating system. The system delivers high-performance message transfer capacity rates of up to 10,000 messages per second between domains. The current implementation focuses on data transfers between Java Message Service (JMS) servers, but it also offers quick deployment and certification in other secure cross-domain network environments.

Stretching SWaP savings with a MicroTCA approach

The newest approach to implementing a secure cross-domain solution is very similar to the PICMG 1.3 option using the TQ9 SHBs discussed earlier. Figure 6 shows a typical MicroTCA chassis with two MCP6792 Processor AMCs (PrAMCs). Of course, a wide variety of MicroTCA chassis configurations are possible; Figure 6 shows just one example.

Figure 6 - MicroTCA Option with Dual PrAMCs

The PICMG MTCA.0 and PICMG AMC.0 specifications enable a wide degree of backplane, MicroTCA chassis, and AdvancedMC configuration latitude to address unique application requirements with standard products. The MCP6792 PrAMC with a single Intel® Core™ 2 Duo Processor SP9300 is a long-life embedded CPU that supports two execution cores, Intel® VT, and Intel® TXT, and has an onboard TPM 1.2. Multiple PrAMC front panel form factors are available that maximize the MicroTCA secure cross-domain system scalability. The MicroTCA approach offers an expanded level of SWaP savings due to the smaller hardware form factors supported and the lower power consumption of the PrAMCs. A MicroTCA cross-domain solution is still in the conceptualization and prototyping stages. The various software products used in this system implementation are similar to those used in the PICMG 1.3 hardware platform using SHBs with one quad-core processor.

Cross-domain platform scalability and longevity

Scalability is a key element in supporting any COTS hardware solution, so too is the ability of the cross-domain hardware platform to remain viable and available for the maximum length of time possible. Trenton designs in extended-life components on all SBC/SHBs, backplanes, and PrAMCs with availability timelines frequently extending beyond seven years. This design approach extends to processors and chipsets and shields the end-users from the constant technology churn common in the COTS component market. Avoiding frequent hardware platform re-certifications caused by product obsolescence issues result in favorable ROIs and cost savings over the life of the secured network.

Sample demonstration systems of multi-domain platforms using PICMG hardware with various virtualization software and RTOS software components running on HAP client platforms have been developed by Cornerstone Integration, Inc. of Marshall, Virginia. These sample systems are available for viewing at the Intel® Solutions Center in Chantilly, Virginia. Demonstrations of the secure cross-domain solution using the guard-board approach shown in Figure 5 require special arrangements. Contact Trenton for details on arranging demonstrations of any of these systems.

Conclusion

SWaP savings with hardware platform flexibility and scalability are all made possible by today's PICMG 1.3 system host boards using multi-segment backplanes or PrAMCs in a MicroTCA chassis. Combining COTS hardware with the appropriate application and O/S software enables a secured virtualized server environment necessary for an effective cross-domain platform. Virtualization technology is a key element in making a COTS cross-domain platform feasible. COTS hardware platforms using PICMG 1.3 or MicroTCA components deliver secure, cost-effective communications across multiple security domains while ensuring the end-point integrity advanced computer networks require.

Jim Renehan *is Director of Marketing and Business Development for Trenton Technology. Jim has held various marketing and application engineering positions in the embedded computing, industrial automation, and automatic identification industries. Jim holds a BS in Industrial Technology from Iowa State University of Science and Technology in Ames, Iowa.*

TRENTON
2350 Centennial Drive
Gainesville, GA 30504
Tel: 770-287-3100
Fax: 770-287-3150
jrenehan@trentontechnology.com
www.trentontechnology.com

References

[1] Security Intelligence Reform Act of 2004, Sec. 102A(g)(1)(C).
[2,3] National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, Revised June 2006.