Building Trusted Embedded Systems

Intel® vPro™ capable solutions from Kontron provide OEMs with cost-effective solutions for enhanced security, reliability and remote management.
Building Trusted Embedded Systems
Intel® vPro™ capable solutions from Kontron provide OEMs with cost-effective solutions for enhanced security, reliability and remote management

Multiple sectors and industries are motivated to deliver secure embedded solutions. Yet, historically, embedded system security has been the focus of a limited set of embedded solutions. Today, embedded system designers are facing pressure to increase the level of security and privacy protection in the system while simultaneously driving down cost and reducing time to market. These embedded security solutions must also be flexible enough to adapt to the unique implementation of each embedded system. By building trust, as well as manageability, into these embedded systems, we can provide security enhancements that will help ensure the system will behave as intended even while it is unmanned or remote. Kontron, a leader in embedded computing solutions, is leveraging Intel® vPro™ technology to provide commercial off the shelf (COTS) trusted systems products for embedded computing applications.

CONTENTS
Building Trusted Embedded Systems. .............................. 1
Summary ......................................................... 2
Contents .......................................................... 2
Background of Embedded Computing and Security Standards .......... 3
Intel® vPro™ Technologies: Benefits at a Glance ....................... 4
Secure Isolation with Intel® VT .................................. 4
System Integrity with Intel® TXT .................................. 5
Remote Management of Embedded Systems with Intel® AMT .......... 6
Harnessing Intel® vPro™ Benefits with Kontron’s ETXexpress®-AI .... 6
Kontron Embedded Motherboards and Slot Computer boards also support Intel® vPro™ ........................................ 7
Taking Trusted Platforms to the Next Level .......................... 7
Conclusion ......................................................... 8
About Kontron ...................................................... 9

www.kontron.com
To further improve system security and remote manageability, Intel has created advanced processors that benefit from the hardware-assisted capabilities of Intel® vPro™ technology. The benefits of Intel® vPro™ technology include: enhanced security, increased system uptime and reliability, lower total cost of ownership, and size, weight and power (SWaP) reduction. Kontron provides an Intel® vPro™ compliant platform on its new ETXexpress®-AI computer-on-module, as well as on several other board and system products. Kontron and Intel are using Intel® vPro™ technology to address three key security and reliability challenges facing embedded systems today, namely system integrity, secure isolation and remote systems management. Various technologies employed by the Intel® vPro™ platform and the contribution of each are introduced. The base design and options in the ETXexpress®-AI architecture are then shown to provide a robust, flexible, and scalable COTS product that is designed to harness the advantages of Intel® vPro™ technology.

Background of Embedded Computing and Security Standards

Threats against embedded systems are on the rise. Even systems of no monetary or political significance have been the victim of attacks. Physical isolation can no longer provide reliable system security, which was the case where the Stuxnet worm infected the isolated supervisory control and data acquisition (SCADA) system. Information or capabilities intended to be protected on the system have proven to be accessible, a result of the increasing vectors of malicious attacks. Methods such as “jailbreaking” give the malicious user root access to the device, bypassing restrictions and allowing unintended configurations to be created. With other methods, such as persistent cross-site scripting (XSS), scanning for connections on the default port 80 or other device ports, and a growing suite of hacking tricks, old assumptions for the security of an embedded system no longer hold true.

Driving forces for security standards in the embedded space historically originated from military and aerospace. However, today, we see almost every segment in embedded systems with standards and regulations related to system security, safety and data privacy. Standards for a variety of embedded system applications, and a listing of driving standards by industry, are given in Table 1. These standards begin to provide a framework for security, safety and data privacy for the respective segment and use case. Even so, embedded systems no longer can be assumed intrinsically secure simply because there is minimal to no Internet connectivity, or because there has been no perceived motivation to target these devices for malicious activities.

<table>
<thead>
<tr>
<th>Standards Drivers by Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry</td>
</tr>
<tr>
<td>Medical</td>
</tr>
<tr>
<td>Gaming</td>
</tr>
<tr>
<td>Industrial</td>
</tr>
<tr>
<td>Military, Aerospace, Government</td>
</tr>
<tr>
<td>Retail</td>
</tr>
</tbody>
</table>

The motivations and definitions for security, safety and data privacy vary across market segments. For instance, the International Electrotechnical Commission (IEC) is responsible for creating standards and specifications concerned with safety, technical requirements, and competencies. By defining regulations around these areas, the IEC seeks to deliver safety and supply chain efficiency in the industries it serves, such as machinery, medical, nuclear, process, and others with IEC 61508. The government and military sectors are more interested
in protecting sensitive information at all stages, where we see standards from the National Security Association (NSA). Among the many standards the NSA has published is the definition of a High Assurance Platform (HAP), which defines a framework for the development of secure computing platforms, focusing on commercial off-the-shelf (COTS) components. Retail segments use Payment Card Industry Data Security Standard (PCI-DSS), a set of comprehensive requirements for enhancing payment account data security. The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around payment data and its exposure to compromise.

Security in trusted systems is necessary for tasks including credentialing, system setup and configuration, and accessing critical system data, BIOS settings, access management features, and other data. These protections are implemented on various layers platform. Intel® vPro™ technology provides hardware assisted capabilities to software in order to provide secure network communications, including out-of-band (OOB) communications. Intel® vPro™ technology works within numerous industry-standard security standards and methodologies. With such a broad spectrum of security requirements, it is even more important today to be able to leverage existing, proven platform features to deliver time to market solutions quickly while also capitalizing on the supply chain efficiencies of high volume manufacturing. By leveraging Intel® vPro™ capabilities, Kontron is able to deliver enhanced security and manageability capabilities while leveraging industry-accepted technology.

**Intel® vPro™ Technology: Benefits at a Glance**

Kontron and Intel are addressing the security and manageability challenges facing embedded systems today with the implementation of Intel® vPro™ technology to enable:

» System integrity
» Secure isolation
» Remote systems management

First, system integrity is the ability to identify whether the system hardware or system software has been modified without authorization. When a system’s integrity is known, the system can be thought of as a trusted system. Second, secure isolation is the ability to use platform hardware to separate processes, resources, and data on the system such that they cannot interact with each other in unintended ways. By providing hardware-assisted isolation, there are limitless security, privacy, and cost savings that can be realized through consolidation and workload isolation. Finally, remote systems management is the ability to troubleshoot, perform power management or system verification through secure channels. Significant cost savings and efficiencies can be realized through remote management allowing for increased system up time and the ability to manage or diagnose a system, even when powered down.

Intel® vPro™ technology itself is special functionality designed into both the processor and the chipset. The three technologies that comprise Intel® vPro™ technology are: Intel Virtualization Technology (Intel® VT), Intel Trusted Execution Technology (Intel® TXT) and Intel Active Management Technology (Intel® AMT). The following paragraphs provide a brief introduction to each technology; a more detailed discussion is provided for each technology in the three following sections.

Intel® VT provides hardware-based assists making secure isolation more efficient and decreases the virtualization footprint, lowering the effective attack surface of a solution. This hardware-based technology can help to protect applications and information by running multiple operating systems (OSs) in isolation on the same physical system. A virtual guest OS can be created in an entirely separate space on the physical system to run specialized or critical applications. Virtual environments leverage Intel® VT for memory, CPU, and Direct I/O virtualization.

Intel® TXT provides the ability to use hardware-based mechanisms to verify system integrity during the boot process. It also provides system memory scrubbing that protects against soft reset attacks. Virtualized environments take advantage of Intel® TXT launch environment verification to establish a dynamic root of trust providing added security to hypervisor or virtual machine monitor (VMM).

Mechanisms employed by Intel® AMT include domain authentication, session keys, persistent data storage in the Intel® AMT hardware, and access control lists. Only firmware images that are digitally signed by Intel are permitted to load and execute. This set of hardware-based features is targeted for businesses and allows remote access to the system, whether wired or wireless, for management and security tasks. Because of the special hardware capabilities provided by Intel® AMT, out of band access is available even when the OS is not functional or system power is off.

**Secure Isolation with Intel® VT**

Secure isolation is the ability to use platform hardware to separate processes, resources and data on the system such that they cannot interact with each other in unintended ways. Intel® VT is the component of Intel® vPro™ that focuses on secure isolation. For example, data privacy is achieved by isolating system resources using Intel® VT, such as in isolating credit card data on one virtual guest on the system while providing another lower security guest on the system for user interactions. Isolation between the two guests is provided through Intel® VT’s interrupt remapping, direct memory access (DMA) mapping, and input/output (I/O) device assignment.
As virtualization security matures, the growing synergy between hardware and software virtualization components is becoming extensive. Intel® VT hardware-based extensions are expanding to offer enhanced protection capabilities to virtualization software, particularly by reducing the virtual machine managers (VMM) size and complexity while increasing functionality and improving performance. Offloading tasks from the VMM and instead handling them in hardware can enhance security since Intel® VT reduces the potential attack surface associated with the software platform and increases tamper resistance.

Functional consolidation provides additional isolation for security and simplifies the physical infrastructure by reducing the number of physical assets to be managed. By running on a bare-metal virtual space, a trusted isolated environment is created in which tasks are discretely quarantined. With VMMs running outside the operating system, browsing an infected website or opening a compromised spreadsheet located on the virtual machine will not impact the physical machine’s operation or integrity. If malware is discovered, only the affected virtual machine needs to be fixed while the rest of the system continues operating normally. Secure virtualization isolates vulnerabilities for specific tasks such as remote access and web browsing, and ultimately protects the underlying physical machine and its OS from various threats.

This software partitioning and hypervisor virtualization helps in the consolidation of hardware and the reduction of SWaP, which is of particular interest in many military applications. By running separate systems in their own partitions, and allowing for different OSs and applications to be run in those partitions, there can be a true consolidation of physically separate systems on a single physical piece of hardware. Applying this approach to virtual networking is an additional compelling feature of Intel® VT. Here, the guest OSs and applications can communicate virtually with other guest OSs and applications, even though they reside in separate partitions of the same physical hardware. Applications perceive the virtual network as a collection of actual network ports. Internal communication occurs as if among physically separate networked devices. A secure separation kernel can enforce security policies and dictate the permissions and direction of communication among partitions.

Successive generations of Intel hardware platforms offer new virtualization and security features, and collaboration between Intel and the major providers of VMMs from a very early point in the development of those hardware features, ensures their rapid support by the virtualization software ecosystem. As with many other computing technologies, security challenges will remain part of the virtualization landscape. Since deployment of virtual machines (VMs) is much easier than physical servers, controlling the growth of VMs should be considered a part of the security model under consolidation and can be addressed by a combination of process and technology. Early and ongoing collaboration and testing will result in a higher quality, increasingly robust set of solutions.

**System Integrity with Intel® TXT**

The ability to determine a system’s integrity is becoming an increasingly important platform function. System integrity is the ability to identify whether the system hardware or system software has been modified without authorization. A system with established hardware and software integrity can be thought of as a trusted system. Intel® TXT is part of the Intel® vPro™ technology, providing hardware based mechanisms to assist in verifying system integrity.

Integrity measurements are generally stored in a set of 24 unique platform configuration registers (PCRs). These PCRs are protected by locality. Intel® TXT defines Launch Control Policies (LCPs) that are used by the Intel® TXT policy engine to control system launch by verifying the LCP against the PCRs. The composition of the LCP allows for flexibility in defining the allowed system configuration. The system will only boot if an exact policy match is found. By enforcing LCP during system boot, Intel® TXT controls system launch and prevents unauthorized system configuration from launching. The ability of a system to verify its integrity upon boot has been one of the primary motivating factors in the inclusion of Intel® TXT in the definitions set by the NSA for HAP.

Other segments are beginning to explore Intel® TXT including research projects focused on casino gaming as well as industrial applications. Intel® TXT adds functionality to an already well-established definition of a trusted platform, as described by the Trusted Computing Group (TCG). The TCG is responsible for several design documents pertaining to the key functionality and behavior of a trusted platform. One of the central hardware components to the TCG’s trusted platform is the Trusted Platform Module (TPM).

On the Intel-based platform, the TPM is a discrete coprocessor that provides protected capabilities and key cryptographic functions. The TPM’s functionality is the backbone for many security solutions, from Intel® TXT to hardware and software-based data encryption solutions. Since it is a cryptographic coprocessor, certain import and export conditions may exist depending on the application and in which country it is deployed. Some TPMs have reached Common Criteria EAL 4 certification, while some sub components of the TPM have achieved higher Common Criteria certification. Leveraging the TPM, Intel® TXT is able to establish a robust set of LCPs for the system that are referenced during system boot when verifying the system configuration. System software, using Intel® TXT using Safer Mode Extensions (SMX), is what is responsible for invoking policy enforcement. The LCPs and SMX architecture within the system can be defined in numerous ways to allow for flexible policy enforcement for various degrees of system security.
Remote Management of Embedded Systems with Intel® AMT

The last of the three key security areas is the ability to manage embedded systems remotely through secure channels. Common tasks like troubleshooting, power management, and system verification are included in such activities. Applications may be attended or unattended, and the latter introduces unique challenges when managing system farms in embedded networks or fleets. Unattended, remote or harsh environments require security and reliability without the luxury of manned access on demand, such as in obscure installations like wind farm turbines. Intel® AMT is the technology component of Intel® vPro™ that handles remote management. Intel® AMT allows keyboard, video, and mouse (KVM) remote control and IDE redirect enabling remote diagnostic and repair for unattended machines. Mission critical systems or systems that can be powered down also stand to take advantage of secure remote management capabilities.

Intel® AMT provides essential power management for embedded systems. Intel® AMT permits OOB manageability, allowing for the system to be managed even when the power is off or the OS is broken, functionality made possible by the capabilities of the Intel® Management Engine (Intel® ME). The Intel® ME to provides diagnosis and repair independent of major systems components. With built-in manageability, Intel® AMT allows assets to be discovered even while systems are powered down. The management server can issue a power-on command for patch and reboot deployment as needed to a system that had been powered down, leading to energy savings. Once the process is complete the management server can issue the power-off command to return the computer to its previous powered down state. A benefit of this technology is that system remediation and content updates can be handled remotely for systems that are not always running and proves especially useful in unmanned applications. Remote troubleshooting allows for diagnosing system problems regardless of the system’s power state or if a failure of the hardware or OS has occurred.

Additional hardware-based mechanisms such as agent presence checking are employed by Intel® AMT to verify system functionality. Agent presence detection proactively detects the running software agents and sends alerts to the management console automatically when missing agents are detected. Intel® AMT System Defense is another proactive element that blocks incoming threats, contains infected clients before they impact the network, and alerts IT when critical software agents are removed.

Harnessing Intel® vPro™ Benefits with Kontron’s ETXexpress®-AI

Each of the three elements of Intel® vPro™ technology discussed offers a tremendous advantage to a trusted system, and Kontron envelops these technologies in its ETXexpress®-AI computer-on-module (COM). The architecture of Kontron ETXexpress®-AI harnesses Intel® vPro™ technology’s benefits in a cost effective solution that provides superior security while maintaining flexible hardware options. The ETXexpress®-AI module has gone through Intel® vPro™ Use Case Validation at Intel’s hardware enabling lab. Although Intel® TP, Intel® AMT, and Intel® TXT are disabled by default, since validation has been done already, each technology can be turned on easily in the BIOS with confidence of performance. Instructions for turning each technology on in the BIOS are detailed in the module’s user manual.

Intel® TXT is of the component of Intel® vPro™ technology responsible for verifying system integrity during launch, working to ensure only authorized software runs on an allowed hardware configuration. Embedded designers can take advantage of the base hardware, chipset, Ethernet controllers, and BIOS already provided in the Kontron ETXexpress®-AI and expand based on specific system or application requirements. The TPM, a mandatory discrete component in an Intel® vPro™ platform, is available to provide several other key cryptographic functions essential to a trusted platform. One example of Intel® TXT is the use of ETXexpress®-AI in digital out of home (DOOH) applications, where Intel® TXT technology allows hardware-based integrity verification of the system during launch; LCPs are used to represent two authorized system configurations, which represent the allowed display and analytics application configuration firmware. When the system boots, measurements are stored in the PCRs and the Intel® TXT hardware-based policy engine is evoked. If there is a match between an LPC and PCR, then the boot will continue, but a TXT.ERRORCODE is set and the system reboots for remediation otherwise.

Intel® VT provides the COM with secure isolation, consolidating resources and providing hardware-assisted isolation to realize security, privacy and cost savings. To use our DOOH example, two operating systems may be in use to support the graphic/video display versus the analytics engine. With up to 8 GB of secure ECC DDR3 system memory available, there is ample space for numerous virtual machines to be deployed, each taking advantage of the error correction capabilities of the deployed memory.

Options built into the new Kontron ETXexpress®-AI benefit designers creating graphics-intensive applications such as those in medical, military, gaming, digital signage and automation. Three additional digital display interfaces (DDIs) are available on Kontron ETXexpress®-AI, which provides more display options and simplifies the design of carrier boards. The DDIs and PCI Express Graphics port are separate, so integrated Intel HD graphics and an additional PCI graphics card can be used in parallel. The graphics card can be used for connecting additional displays or for high-performance data processing as a general-purpose computation on graphics processing unit (GPGPU) in image processing or data encoding applications.
Significant cost savings and efficiencies can be realized with Intel® AMT provided on Kontron ETXexpress®-AI. Remote management allows for increased system uptime and the ability to manage or diagnose a system even when it is powered down. New avenues to manage remote systems are available with this technology, including power management. Providing OOB management capabilities allows IT to isolate and recover systems remotely while alerting and event logging help prevent and reduce downtime. For example, a remote patch can be downloaded securely after a system reboot fails and enable the system to come back online. To keep software and virus protection up-to-date across the enterprise, third-party software can store version numbers or policy data in non-volatile memory for unmanned or off-hours retrieval or updates. Shorter time to market is achieved and maintained between generations when the module is paired with the application-specific carrier board that now can be simplified because of the features built in to the new Kontron ETXexpress®-AI.

Kontron Embedded Motherboards and Slot Computer boards also support Intel® vPro™

The KTGM45 and the KTQ45 families of motherboards also support the full suite of Intel® vPro™ technology. Each motherboard in the family is flexible and the Intel® vPro™ features can be turned off using easy to use tools provided by Kontron if not required for the OEM’s application. Kontron design teams made sure to include the necessary hardware, such as a TPM v1.2, which is mandatory for Intel® vPro® to be enabled. The motherboards are now shipping in volume production. The slot computer board, the PCI-761, which complies with the PIGMG 1.3 standard, is also fully Intel® vPro compliant. These Kontron boards are used in Kontron Industrial Silent Servers (KISS) for configurations from 1U short to 4U. KISS industrial PCs are often a good starting point for OEMs that want a semi-custom, configurable and cost effective platform that is Intel® vPro® capable.

Taking Trusted Platforms to the Next Level

Intel® vPro™ technology is a forward-looking suite of platform features that have proven invaluable for the trusted platforms of today. Going forward, Intel® vPro™ technology is set to provide the solutions for tomorrow’s demanding security solutions, allowing for OEMs to provide additional options and enhancements for both existing and future Intel® vPro™ products.

Some industries need other non-vPro technologies as part of their trusted platform. For example, some OEMs serving the military market need to provide rapid shutdown mechanisms for their defense customers. Sometimes this capability is referred to nuclear event detection (NED) or Rapid Shutdown. These capabilities can be added to custom platform solutions, although they are not widely required by most OEMs.

Secure socket layer (SSL) technology is already widely used by financially-oriented applications, and Advanced Encryption Standard (AES) cryptography is used for military and other applications requiring high levels of security. Over time, these and other technologies will become part of many embedded trusted systems platforms, taking advantage of existing platform features such as the hardware accelerated AES instructions in the Intel processor.
Conclusion

Connected embedded devices already outnumber PCs by at least five to one, and their numbers are growing. Security for these embedded devices is often poorly defined, yet these systems often handle crucial information. The proliferation of remote access, compliance requirements, increasing threats and an expanding network perimeter is making system security and data privacy difficult to characterize and control; and the deployment of these systems on a global scale further exasperates these realities. These factors are mandating that security, privacy and reliability become an inherent quality in embedded system design. Kontron and Intel are leading the way in delivering features that can be used to begin to provide a wide array of security and privacy solutions to address these new paradigms, as described in this paper. Kontron has enabled Intel® vPro™ technology on the ETXexpress®-AI module and other boards by adding TPM v1.2, Intel LAN capabilities, and incorporating an Intel® vPro™ compliant BIOS support into the Intel® vPro™ compliant Kontron products. By enabling and verifying Intel® vPro™ technology in these Kontron products, Kontron is providing an excellent opportunity for OEMs to deliver COTS based system solutions in the areas of system integrity, secure isolation and remote systems management: trusted systems.

Embedded system designers now can focus on unique details of the military vehicle, robotic network, or computing application while harnessing the security, flexibility, and scalability of Intel® vPro™ running on a Kontron solution. Kontron based COTS products provide a hardware verification model to accelerate development and reduce the time to market. Over the life of the product, these enhancements deliver a lower total cost of ownership, greater return on investment and the opportunity to more easily integrate security and privacy features to address the evolving security and privacy concerns facing embedded systems today.
About Kontron

Kontron is a global leader in embedded computing technology. With more than 30% of its employees in Research and Development, Kontron creates many of the standards that drive the world’s embedded computing platforms. Kontron’s product longevity, local engineering and support, and value-added services, help create a sustainable and viable embedded solution for OEMs and system integrators. Kontron works closely with its customers on their embedded application-ready platforms and custom solutions, enabling them to focus on their core competencies. The result is an accelerated time-to-market, reduced total-cost-of-ownership and an improved overall application with leading-edge, highly-reliable embedded technology.

Kontron is listed on the German TecDAX stock exchange under the symbol "KBC".

For more information, please visit: www.kontron.com