Solution Brief

Intel® Product Technologies

Medical Equipment

Computing Technologies for Medical Equipment

Advanced Intel® Product Technologies Boost Reliability, Manageability and Security

The healthcare industry, continually striving to improve patient care, benefits from advanced computing technology used in a range of equipment such as intelligent, networked patient monitors, handheld diagnostic devices and CT scanners. And just as doctors seek out the latest treatment methods for their patients, health-care IT professionals look for technology breakthroughs that enable a more reliable and secure computing infrastructure. For that reason, Intel® product technologies with proven capabilities to increase reliability, manageability and security in PCs and servers are being adopted by medical equipment manufacturers.

Healthcare providers require highly available equipment to maintain peak patient throughput levels and minimize maintenance costs. This starts with ensuring software runs in a stable and reliable environment that prevents unwanted software interactions from bringing down a system. These software conflicts can be curtailed by using virtualization, which executes software in secure partitions. Addressing costly repairs, Intel® Active Management Technology (Intel® AMT)[1] improves the remote management of equipment and helps fix a large number of problems over the network, as opposed to sending a technician on-site.

Equipment manufacturers must also provide cost-effective solutions to address world-wide government regulations such as the Health Insurance Portability and Accountability Act (HIPAA), enacted to improve the effectiveness and efficiency of the U.S. health care system. Providing a more secure, trusted environment, Intel® Trusted Execution Technology (Intel® TXT)[2] has special hardware-based functions that can stop malicious software and hackers from accessing confidential patient records. All of these Intel® technologies are supported by many Intel® processors and chipsets, thus providing the computing platforms for various types of medical equipment and delivering enhanced capabilities, including:

- **Increasing software reliability** by isolating application code and preventing dangerous interactions
- **Increasing equipment manageability** by improving remote diagnostic and repair capabilities
- **Enhancing data security** by stopping any device from executing malicious software

This solution brief discusses how technologies built into Intel® silicon components can improve the virtualization, remote management and security of medical devices.

Improving Software Reliability with Virtualization

Many medical devices perform safety-critical functions such as controlling infusion pumps or monitoring a patient's vitals during surgery. They run software for controlling the actuators and sensors used to help administer and monitor patient treatment. At the same time, these medical products may run non-safety-critical applications like graphical user interfaces (GUIs), image and data processing and database engines. To improve system reliability, developers can run safety-critical code in safe, virtualized execution environments that isolate different workloads and prevent them from interfering with one another.

Addressing Software Challenges

Today, most medical systems run a single OS, typically either real-time, general-purpose or homegrown. If developers or system integrators want to add an application that runs on a different OS, they probably have to rewrite the software, which can be time-consuming and risky. It's particularly challenging to port time-critical software, like X-Ray or an ultrasound running on a real-time OS, to a general-purpose OS while maintaining a comparable level of determinism.

Alternatively, developers can choose to run multiple OSs and their associated applications in secure partitions using virtualization. Virtualization has been around for many years, most notably used in data centers where many applications are consolidated onto a single server. Complementing software-based virtualization solutions, Intel® Virtualization Technology (Intel® VT)[3] improves their fundamental flexibility and robustness and gives software developers greater control over operating systems and applications. This capability can simplify the migration of legacy applications onto new platforms, improve the determinism of time-critical functions and avoid hardware rebooting delays, as shown in Table 1 and described in the next three sections.

Simplify Software Migration

As medical systems consolidate more applications and networking software, it's essential that latent defects, like software conflicts or bugs, don't crash the system. For example, a safety-critical application can run in its own partition, protected from unintended interactions with other applications, as shown in Figure 1. In addition, applications can run on their native OS, with little or no modification, which eases software migration and shortens development time.

Increase Real-Time Determinism

The determinism of real-time functions, like processing diagnostic system input/output (I/O), can be negatively impacted when they must compete for CPU resources with non-real-time applications such as a full-featured user interface. It's possible to eliminate this contention with virtualization and multi-core processors, a combination that enables systems to run time-critical functions on a real-time OS and on a dedicated processor core. As a result, real-time functions don't have to share interrupts or CPU resources, which can increase their determinism and performance.

Capabilities	Benefits
Isolates applications in secure partitions	Eases software migration and consolidation
Runs RTOS on a dedicated processor core	Improves real-time determinism
Restarts applications without booting the hardware	Gets the system working faster

Table 1. Intel® Virtualization Technology Capabilities and Benefits

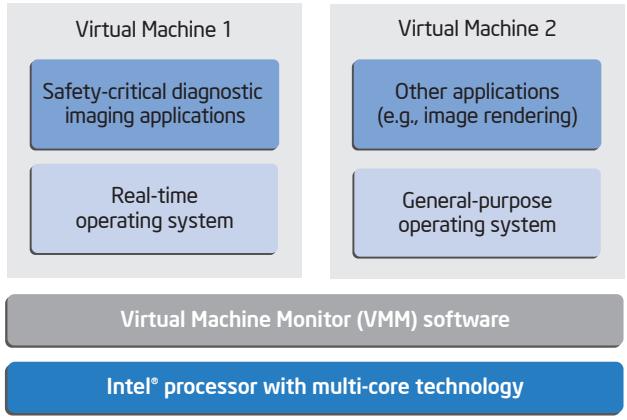

Figure 1. Virtualization Isolates Real-Time Code

Avoid Rebooting the System

When an application running on a medical system fails, the only solution may be a hardware reboot, which takes the system offline for a period of time. Using virtualization, developers can implement a software failover mechanism that restarts the software running in one partition without impacting the other partitions. For example, if an image rendering application running in a partition fails, it can be reloaded and restarted without interrupting applications running in other partitions. It's also possible to deploy an automatic failover mechanism, where the system maintains duplicate copies of an application in two virtual machines and quickly transfers processing to the backup in the event of an application failure.

Lowering Service Costs with Remote Management

With an escalation in the number of devices, Medical IT professionals need to find more efficient ways to provide support, such as configuring systems, updating security signatures and repairing systems when they break. Since on-site service calls are expensive, IT departments are turning to remote management, which can often get systems online faster and at lower cost.

Providing a significant remote management breakthrough, Intel AMT implements a special circuit in the Intel® chipset that can access and control the system, even when the system is powered off or the software is corrupted. This circuit establishes an "out-of-band" link that allows the system to communicate with a management console without relying on the system's standard networking functionality. By employing Intel AMT-based management solutions, healthcare IT

departments can fix a wide assortment of system defects over the network or use remote diagnostics to determine which system part may require replacement, as described in Table 2. This capability reduces costs and saves time by supporting devices without requiring hands on intervention. Intel® Core™2 Duo processors combined with Intel AMT can support a wide variety of devices, including diagnostic equipment, infusion pumps and bedside terminals, as shown in Figure 2.

Reduce Costly Repairs

When a medical system won't boot due to corrupted software (e.g., OS, driver or critical application), the usual remedy is to send a technician on-site to reload the software image. Using Intel AMT, it's possible to remotely boot a device from a networked drive (golden disk in Figure 2) with known good software, which greatly aids troubleshooting. IT can also remotely change BIOS configuration settings, load new drivers or load a new operating system, whether or not the system is running.

Track Intermittent Failure Modes

When logging events and errors, medical devices can leave valuable clues about their health, including intermittent fail conditions that could eventually turn into a hard failure. With Intel AMT, systems continually store this information in non-volatile memory, accessible at all times to the remote management system, regardless of the system state. If the unit needs to be sent to a repair center, this capability can help identify failed components quickly and speed up repairs. Status information may also be stored in non-volatile memory, which enables equipment manufacturers to more easily assess a device's health at the end-of-life.

Track Inventory without Physical Interaction

Many hospital IT departments resort to physical methods to perform a fixed asset inventory, especially to track equipment that's turned off, non-functioning or dispersed across multiple clinical sites. Eliminating human intervention, Intel AMT enables management systems to generate a comprehensive list of hardware and software components for any device that's plugged into the network and an electric socket. This capability also enables IT departments to monitor the software, by version, warranty and license, of every device on the network.

Keep System Virus Signatures Up-to-Date

Medical equipment connected to a network should be protected by the most up-to-date security software. With Intel AMT, IT departments can ensure each device has the latest virus signatures, without user assistance or the device powered-on. If a third-party contractor using an Intel AMT-enabled system connects to the network, but has out-of-date security profiles, the remote management system can quarantine the device and keep it from possibly spreading any viruses. Once the system is updated with the latest virus definitions, it is allowed to reconnect to the network.

Capabilities	Results
Fix hung systems	Restore systems by reloading software or booting from a "gold" hard drive at the management console.
Track intermittent failure modes	Access error log and event records from FLASH, accessible at all times to the remote console.
Run inventory reports	Remotely read system configuration data from non-volatile memory, even if the system is switched off.
Detect system tampering	Use "alert" functionality to send a message to the remote console if anybody opens up the device.

Table 2. Intel® Active Management Technology (Intel® AMT) Capabilities and Results

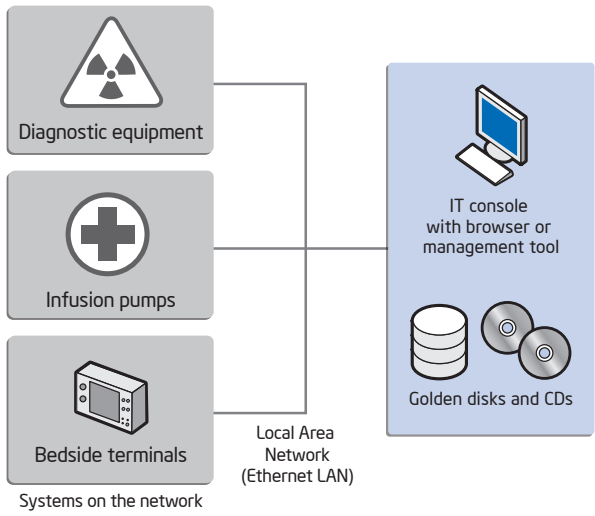

Figure 2. Remote Management Solution for Healthcare Facilities

Increasing Security with Hardware-Assist

When securing medical equipment, one of the biggest challenges is preventing hackers from wreaking havoc, like accessing confidential patient records. It's possible to stop such malicious software from even executing by using hardware-based security features that are built into many of today's computing systems. This technology creates a trusted execution environment, whereby equipment manufacturers and system administrators can define a list of trusted, validated software, and only applications or device drivers on this list can be loaded.

Designed to help protect against software-based attacks, Intel TXT integrates new security capabilities into the processor, chipset and other platform components. These hardware-based security features, unalterable by rogue software, run mission-critical applications in a safe partition, protect crucial platform data and keep malware from launching in the first place, as described in Table 3, on the next page.

Protect Critical Software from Malware

"Health insurance identification and other medical records are stolen about 250,000 times a year nationwide (U.S.) in an offense believed to be rising,"[4] reports Tom Kisken of the Ventura County Star. Cybercriminals, looking to profit from infiltrating medical systems, are attacking application software and databases to access confidential data. Using Intel TXT, OEMs can put software and data out of reach of hackers by running applications, operating systems and virtual machine monitors (VMMs) in the highest privilege level, permission granted only by system developers. As a result, application code and data are stored in hardware-secured memory regions, inaccessible to malware. OEMs and system administrators can define a list of trusted, validated software, and only applications or device drivers on this list can be loaded.

Stop Unauthorized Access of Data

Spoofing and phishing – when a system or program masquerades as another – are fraudulent activities used to gain access to confidential information. Helping to prevent these attacks, Intel TXT provides sealed storage in the trusted platform module (TPM) for security codes, like VPN encryption keys, which keeps perpetrators from intercepting secured communications links between medical systems. Intel TXT encrypts and stores critical security codes and ensures they are only released (decrypted) to the executing environment that originally encrypted them.

Prevent Booting a Compromised System

Compromised medical devices, possibly infected with a virus or breached by malicious software, need to be deactivated before they can cause harm. One solution is to stop these systems from booting whenever the software or hardware configuration differs from the trusted state. This is achievable with Intel TXT, which compares the hash (a number generated by a formula of all system software of the trusted state) with the current state and blocks system startup when differences are detected. The hashing function will detect single bit changes, as shown in Figure 3, and prevent the system from booting.

Features	Benefits
Protected execution environment	Safeguards critical applications and data
Encrypted keys and secrets (e.g., platform configuration registers)	Eliminates potential security holes
Launch control policies	Stops compromised systems from booting
Measured launch environment	Prevents execution of untrusted software

Table 3. Features and Benefits of Intel® Trusted Execution Technology (Intel® TXT)

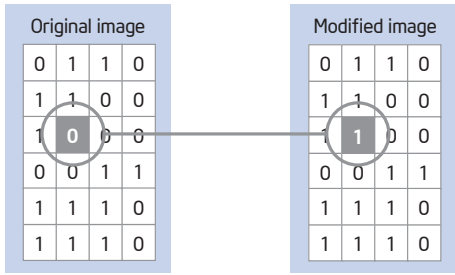

Figure 3. Hashing Detects Single-Bit Discrepancies

Improving the Patient Care

The healthcare profession is known for applying the latest medical research to better treat patients. Likewise, healthcare IT professionals ensure their computing systems and medical equipment are benefiting from the latest advances in computing technology. As a result, medical equipment manufacturers are employing Intel product technologies that offer developers new capabilities to increase software reliability, improve device manageability and enhance security. These solutions can be applied across the healthcare network, from end-to-end in the healthcare network.

For More Information

For more information on Intel® medical embedded computing solutions, visit www.intel.com/go/medical.

For more information on Intel® product technologies, visit www.intel.com/technology/advanced_comm.

Additional information about Intel® embedded products can be found at www.intel.com/products/embedded/index.htm.

[1] Intel® Active Management Technology (Intel® AMT) requires the computer system to have an Intel AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/technology/platform-technology/intel-amt/.

[2] No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group and specific software for some uses. For more information, see http://www.intel.com/technology/security.

[3] Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain platform software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

[4] Source: http://www.venturacountystar.com/news/2008/mar/06/stolen-medical-records-can-be-costly-deadly/, March 6, 2008.

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit Intel Performance Benchmark Limitations.

Printed in USA 0909/LK/OCG/XX/PDF Please Recycle 322560-001US