



Igniting New Industrial Opportunities

Enabling a new era of industrial automation solutions with the 4th generation Intel® Core™ processor family



Faster time to market is critical for industrial manufacturers, and that's why access to the world's largest base of mature development tools—Intel tools—is critical to success.

CHALLENGES

- **Manufacturing is rapidly evolving**, stretching industrial organizations to address growing operational complexity and aging infrastructure, while striving for faster time to market to meet emerging opportunities.
- **Customers require systems that future-proof big investments**, allowing for gains in performance, efficiency, performance per watt, and other benefits over time.
- **Cyberattacks and other security concerns are an increasingly critical** consideration in the rapidly developing Internet of Things in which automated industrial systems are growing ever more connected.

SOLUTIONS

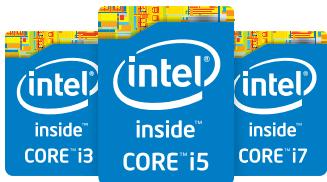
- Consolidating multiple automation workloads (such as control and human machine interfaces (HMIs)) on a single computing device requires superior performance. **The 4th generation Intel® Core™ processor family delivers incredible CPU processing performance** and outstanding graphics performance.
- The single-chip footprint of the U-processor platform of **the 4th generation Intel Core processor family offers the same high performance** of 3rd generation Intel® Core™ processors at significantly less power! This enables support for smaller form factors, while helping industrial managers save factory floor space and address new environments and approach 1:1 HMI per worker.
- **The 4th generation Intel Core processor family offers security enhancements** not available in 3rd generation Intel® Core™ processors, providing faster data encryption with Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) and greater "below the OS" malware protection on industrial devices, such as controllers and human machine interfaces (HMIs) with enhanced malware protection, which increases the performance of virtualization-based security solutions, such as McAfee Deep Defender*.

Trusted ecosystem, robust and reliable solutions

Intel's scalable architecture, extensive development tools, and leading-edge silicon—with built-in remote management and virtualization—enable faster time to market, lower total cost of ownership, and enhanced security and efficiency. At the same time, Intel's decades of experience deliver deep ecosystem relationships, holistic security expertise, and a broad

portfolio of solutions spanning hardware, software, and other critical components to help you differentiate your business.

Faster time to market is critical for industrial manufacturers, and that's why access to the world's largest base of mature development tools—Intel® tools—is critical to success. Off-the-



The 4th generation Intel® Core™ processor family enables a new era in automation

shelf hardware options like controllers, sensors, HMI displays, and more speed the development process. Multicore designs deliver outstanding energy efficiency and support real-time deterministic control, virtualization capabilities, and real-time I/O (including PCI Express* and fast, real-time Ethernet).

Enjoy the benefits of Intel's extensive ecosystem of products. Wide support from popular operating systems—both general purpose and real-time—allows developers to manage code across multiple operating systems. Multiple lines of processors from low power to ultra-high performance share a common microarchitecture that makes it easy to migrate code and scale your solution based on need.

Feel the security of knowing you can focus your development efforts on creating code that makes systems unique, rather than on drivers and other lower level issues that worked previously on other Intel® processors. And look forward to future developments knowing Intel is committed to providing an extended roadmap so that every generation of Intel® Core™ processor supports your projects with gains in performance, efficiency, performance per watt, and other benefits over time.

Intel® Active Management Technology

Using integrated platform capabilities and popular third-party management and security applications, Intel® Active Management Technology (Intel® AMT) allows IT or managed service providers to better discover, repair, and protect their networked computing assets.

Intel AMT also enables you to manage and repair not only your PC assets, but also workstations, entry servers, HMIs, and other industrial devices as well, utilizing the same infrastructure and tools across platforms for management consistency. For embedded developers, this means that devices can be diagnosed and repaired remotely, ultimately lowering IT support costs.

Intel AMT is a feature of 4th generation Intel Core processors with Intel® vPro™ technology^{1,2} and workstation platforms based on select Intel® Xeon® processors. Benefits include:

- **Out-of-band system access.** With built-in manageability, Intel AMT allows IT and operations technology (OT) to discover assets even while platforms are powered off.^{1,2}
- **Remote troubleshooting and recovery.** With out-of-band management capabilities, including Keyboard-Video-Mouse (KVM) Remote Control,³ Intel AMT allows IT to remotely remediate and recover systems after OS failures. Out-of-band alerting and event logging also help to reduce downtime.
- **Hardware-based agent presence checking.** Ensuring better protection for your enterprise, hardware-based agent presence checking proactively detects when software agents are running. When missing agents are detected, alerts are sent to the management console.
- **Proactive alerting.** Intel® AMT System Defense Manager proactively blocks incoming threats, containing infected clients before they impact the network, and alerting IT when critical software agents are removed.
- **Remote hardware and software asset tracking.** Intel AMT helps keep software and virus protection up-to-date across the enterprise, enabling third-party software to store version numbers or policy data in nonvolatile memory for off-hours retrieval or updates.
- **Expanded capabilities.** With the Intel® vPro™ Technology Module for Microsoft Windows PowerShell*, IT has direct access to the powerful 4th generation management available with Intel AMT, enabling use of Windows PowerShell scripts to access features not available in their existing management console—such as remotely configuring alarm clock settings.

Intel developed a complete set of hardware-based virtualization features

designed to improve performance and security for virtualized applications for 4th generation Intel Core processors with vPro technology.

- **Increased efficiency and effectiveness.** Windows PowerShell scripts integrate seamlessly into existing tools, enabling IT to quickly and easily execute Intel AMT commands on Intel vPro-based managed clients and workstations and Intel AMT-capable entry servers.

All this means better management capabilities on the factory floor by eliminating the difficult and time-consuming need to manually track assets and keep them up-to-date with the latest software, policies, and licenses. IT professionals can remotely query, update, and inventory factory floor systems from a single management console, regardless of the operating system or platform configuration. Asset information resides in the system's nonvolatile memory, and it can be accessed by the console no matter the state of the machine.

Accelerating Key Functions of the Virtualized Platform

Hardware-based Intel® Virtualization Technology⁴ (Intel® VT) is used in a wide variety of embedded applications to improve trust and protect critical applications. An important benefit is its support of industrial system consolidation, which can help reduce bill of materials (BOM) costs and design complexity, while accelerating time to market. Intel VT also helps improve the fundamental flexibility and robustness of traditional software-based virtualization solutions by accelerating key functions

of the virtualized platform. In fact, Intel developed a complete set of hardware-based virtualization features designed to improve performance and security for virtualized applications for 4th generation Intel Core processors with vPro technology, including:

- Intel® Trusted Execution Technology⁵ (Intel® TXT) provides a hardware-based root-of-trust.
- Intel Virtualization Technology⁴ (Intel VT) hardware assists and improves application performance.
- Intel® Virtualization Technology for Directed I/O (Intel® VT-d) improves I/O efficiency.
- Intel® Virtual Machine Control Structure Shadowing (Intel® VMCS Shadowing) improves performance for multi-VMM usage models.

Many embedded developers are using virtualization to run multiple operating systems on their devices, enabling them to:

- Simplify the porting of legacy applications onto new platforms
- Increase the determination of time-critical functions

SOLUTION PROVIDED BY:



- Improve the security and stability of safety-critical code

Many industrial systems, like programmable logic controllers and motion controllers, require a combination of low-latency, deterministic response and full-featured user interfaces. Virtualization enables systems to simultaneously run real-time and general-purpose operating systems, each on dedicated processor cores of an Intel® multicore processor. This configuration can increase the speed and determinism of time-critical applications, because they operate unencumbered by non-real-time tasks that otherwise compete for CPU resources. Furthermore, virtualization enables equipment manufacturers to combine functions running on multiple boards onto one board, which lowers platform cost and reduces system size.

LEARN MORE ABOUT INTEL IN INDUSTRY

For more information on 4th generation Intel® Core™ processors in intelligent systems for industrial applications, visit <http://intel.ly/1dbs0xl>.

HOW INTEL® VT WORKS

Intel® VT performs various virtualization tasks in hardware, like memory address translation, which reduces the overhead and footprint of virtualization software and improves its performance.

In fact, Intel developed a complete set of hardware-based virtualization features designed to improve performance and security for virtualized applications. These 4th generation Intel® Core™ processors include:

- Intel® Trusted Execution Technology⁵ (Intel® TXT) provides a hardware-based root-of-trust.
- Intel® Virtualization Technology⁴ (Intel® VT) hardware assists improve application performance.
- Intel® Virtualization Technology for Directed I/O (Intel® VT-d) improves I/O efficiency.
- Intel® Virtual Machine Control Structure Shadowing (Intel® VMCS Shadowing) improves performance for multi-VMM usage models.

1. Intel® vPro™ technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environments. To learn more, visit: www.intel.com/content/www/us/en/architecture-and-technology/vpro/vpro-technology-general.html.

2. Requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware, and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating, or powered off. Results dependent upon hardware, setup, and configuration. For more information, visit www.intel.com/technology/vpro/index.htm.

3. KVM Remote Control (Keyboard, Video, Mouse) is only available with the Intel® Xeon® processor family, Intel® Core™ i5 vPro™ processor, and Intel® Core™ i7 vPro™ processor running activated and configured Intel® Active Management Technology with integrated graphics. Discrete graphics are not supported.

4. Intel® Virtualization Technology (Intel® VT) 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.

5. No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules, and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.2. For more information, visit www.intel.com/content/www/us/en/data-security/security-overview-general-technology.html.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information herein is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's website at www.intel.com.

© 2013, Intel Corporation. All rights reserved. Intel, the Intel logo, the Intel Inside logo, Intel Core, Intel vPro, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.