TECHNICAL BRIEF
Public Sector Applications

DELIVERING LEADING-EDGE COMPUTING TECHNOLOGY TO THE PUBLIC SECTOR

Solutions from Intel and its partners help system developers address emerging challenges regarding performance, security, and cost in the public sector.

System Design Challenges in the Public Sector

The fast pace of technological innovation is having a tremendous impact on the public sector market (e.g., military, aerospace, and government), providing new opportunities for system developers to increase performance, security, and predictability while reducing overall cost. To meet public sector requirements, it takes leading-edge technologies and a vibrant ecosystem that deliver cost-effective solutions with lifecycle management.

To satisfy these needs, Intel and the Intel® Internet of Things (IoT) Solutions Alliance (with more than 400 members) provide long lifecycle hardware and software products. Intel works with federal agencies and its contractor/sub-contractor ecosystem partners to create end-to-end solutions that public sector system developers can deploy to solve their real-world challenges, such as:

Greater Computing Performance

Public sector applications, such as military command and control (C5 ISR), aircraft predictive maintenance, and license plate readers in government vehicles need much greater computing horsepower in order to adopt state-of-the-art tools and technologies, including artificial intelligence (AI), machine learning, and image processing.

Better Security

Public sector systems must have multiple layers of security in order to better protect sensitive data, prevent intellectual property

(IP) theft, help thwart cyber and physical attacks, and establish trusted data that can be more safely shared across defense networks.

Lower System Cost

Developers can lower system cost by migrating and consolidating workloads on commercial, off-the-shelf (COTS) solutions that also employ open standards, improve interoperability, and ease system maintainability.

More Predictable Performance

Some safety-critical public sector applications, such as avionics, must support real-time and deterministic performance. Flight-critical systems require the delivery of predictable outcomes in a specified period of time in order to demonstrate air-worthiness and achieve flight certification at the system level.

High Performance Computing

Whether developers require the highest performance-per-watt or raw performance, they can choose from a large family of Intel® architecture processors featuring a backward compatible instruction set. Figure 1 shows Intel® processors for mobile devices, embedded computing, server applications, and almost anything in between. This broad product portfolio enables suppliers to build end-to-end solutions that bridge field personnel, remote embedded systems, and high performance servers used for command and control and flight systems.

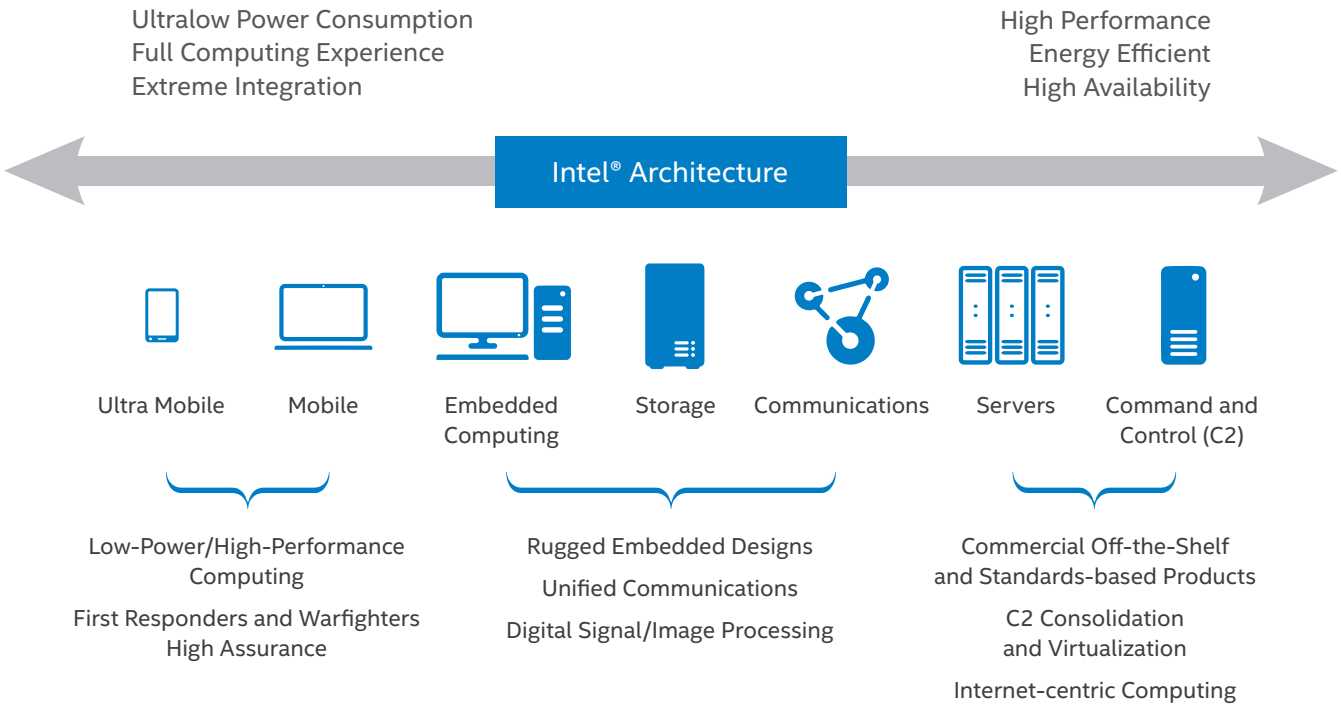

Figure 1_Intel® solutions serve a wide range of public sector systems

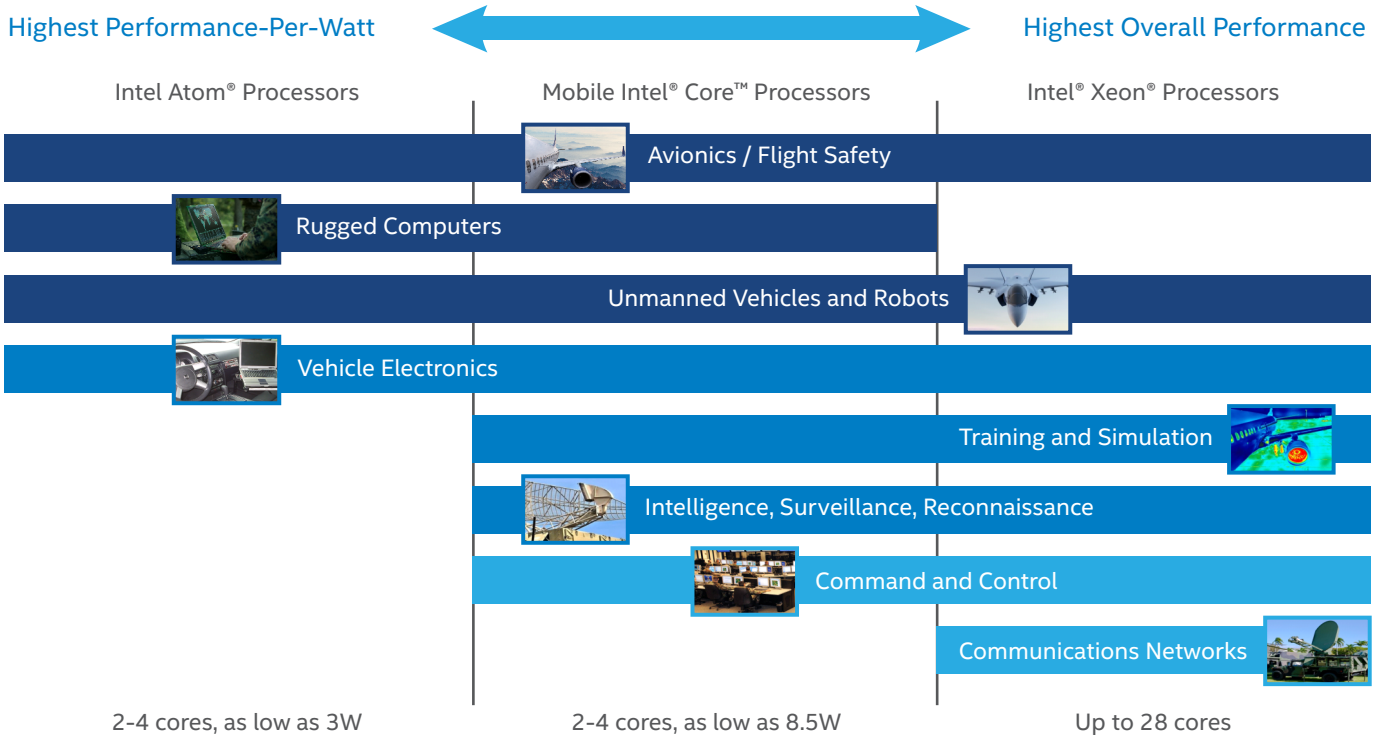

Figure 2_Intel® architecture processors power many types of public sector systems

Intel's broad processor roadmap, including Intel Atom®, Intel® Core™, and Intel® Xeon® processors, satisfies a wide range of performance objectives, as shown in Figure 2. Select SKUs of Intel processors and chipsets support an extended temperature range (-40°C to 85°C ambient and higher) and are backed by seven or fifteen year availability. As a result, these processors are well-suited for many public sector applications, including ruggedized computers, vehicle electronics, handheld/wearable devices, avionics, command and control solutions, surveillance and reconnaissance solutions, and training and simulation systems.

System developers can optimize performance through the use of a large number of Intel technologies and products, including:

Intel® Turbo Boost Technology[1]

This technology enables the processor to automatically run faster than its rated frequency when the processor is operating below power, current, and temperature specification limits. This results in increased performance for both single and multithreaded applications. There is no need to install any additional software to take advantage of this technology.

Intel® Advanced Vector Extensions 512 (Intel® AVX-512)[2]

These instructions perform ultra-wide 512-bit vector/single instruction, multiple data (SIMD) operations, thus accelerating performance for workloads such as signal

processing for radar/electronic warfare, scientific simulations, AI/deep learning, 3D modeling and analysis, image and audio/video processing, cryptography, and data compression. Applications can pack 32 double precision and 64 single precision floating point operations per second per clock cycle within the 512-bit vectors, as well as eight 64-bit and sixteen 32-bit integers, with up to two 512-bit fused-multiply add (FMA) units on select processors.

Deep Learning and Computer Vision

Intel offers a wide range of advanced silicon – from CPUs and graphics processing units (GPU) to Intel® Movidius™ vision processing units (VPUs) and Intel® FPGAs – to match the performance, cost, and power efficiency required at any AI-enabled node. Intel has developed a product line of add-in PCIe* cards, designed for applications that require real-time or offline video/image recognition, classification, and segmentation. The cards work seamlessly with Intel Atom, Intel Core, and Intel Xeon family processors, plugging into host systems via a standard PCIe connector and accelerating computationally-intensive neural network (CNN) workloads.

Layered Security

Due to the wide range of public sector systems, applications, and stakeholders, there is no single security product that will deliver comprehensive protection. A well-designed, layered defense is needed to safeguard public sector networking and communications infrastructure from identifiable, emerging, or even unknown threats. Supporting a layered approach, Intel offers a wide range of security technologies, which can be the foundation for enabling the highest levels of security, including:

Intel® AES New Instructions (Intel® AES NI)

Encryption is frequently recommended as the best way to secure business-critical data, and the Advanced Encryption Standard (AES) is widely-used to protect network traffic and IT infrastructure.[3] Software developers can accelerate AES encryption/decryption and key generation by executing Intel® AES NI instructions on the CPU. These specialized instructions help to better protect confidential data at rest and in flight without incurring the typical performance penalty associated with software-only security solutions or without the need for specialized engines that increase cost and power consumption.

Intel® Platform Trust Technology (Intel® PTT)[4]

Offering the capabilities of a discrete trusted platform module (TPM) 2.0, Intel® PTT is a platform functionality for credential storage and key management used by Windows* 8 and Windows 10. Through the use of Intel PTT, system developers can reduce the BOM cost of an external TPM chip and the form factor of the solution. TPM 2.0 is a microcontroller that stores keys, passwords, and digital certificates. Intel PTT supports BitLocker* for hard drive encryption and supports all Microsoft requirements for firmware TPM 2.0. This technology is also supported on certain Linux* distributions.

Intel® Device Protection Technology with Boot Guard[5]

It is critical to protect a system while it boots through immutable hardware-based root of trust, which can be extended all the way to the application software to protect against any malware. Boot guard utilizes an authenticated code module to provide this functionality.

Benefits from Consolidation

By consolidating system functions using virtualization technology, solution vendors can provide substantial benefits to their customers, such as:

- Lower overall solution cost: A consolidated device should cost less to manufacture than the combined subsystems because it has a smaller bill of materials (BOM).
- Reduced integration cost: Integration is simplified since the networking, cabling, shielding, and configuration, etc. that connect multiple subsystems together are handled within the system.
- Smaller factory footprint: Consolidated equipment takes up less factory floor space than the individual systems it replaces.
- Reduced overall energy consumption: The power efficiency of Intel® processors, combined with system consolidation, can yield a solution that consumes less power than the individual systems combined.
- Simpler to secure: There are fewer systems to secure; the system attack surface is reduced; and potentially, there are fewer security solutions to support.
- Higher reliability: A consolidated system should have a better mean time between failures (MTBF) than a combination of subsystems it replaces because there are fewer points of failure.
- Easier system management: IT personnel have a smaller number of devices to install, provision, manage, and carry inventory.

Intel® Software Guard Extensions (Intel® SGX)[6]

This technology allows software developers to protect selected code and data from disclosure or modification from the OS kernel or other virtual machines or virtual machine monitors themselves. Intel® SGX creates protected areas of execution, called enclaves, in which application code can be stored via special instructions and the Intel® SGX SDK. The SDK is a collection of APIs, libraries, documentation, sample source code, and tools that assist in the creation and debug of Intel SGX-enabled applications in C/C++.

System Cost Savings

Designers developing with Intel processors can reduce overall system cost by taking advantage of workload consolidation, commercial, off-the-shelf (COTS) solutions, and select Intel processors with extended availability.

Workload Consolidation

A growing trend in the public sector is to use virtualization technology to combine what were previously discrete subsystems into a single system, called workload consolidation. By consolidating functions, vendors can reduce system footprint, energy consumption, and support effort.

Helping to maximize the benefits from workload consolidation, Intel® Virtualization Technology (Intel® VT)[7] makes virtualization practical by minimizing performance overheads and improving security. Intel VT provides hardware assist to the virtualization software, reducing its size, cost, and complexity. Special attention is also given to reducing the virtualization overhead associated with cache, I/O, and memory. Over the last decade or so, a significant number of hypervisor vendors, solution developers, and users have been enabled with Intel VT.

Intel VT represents a growing portfolio of technologies and features, such as:

- CPU virtualization – assigns a dedicated Intel processor core to a virtual machine (VM). All software in the VM runs natively on the core, thus it incurs negligible or no performance penalty.
- Memory virtualization – abstracts and monitors a VM's memory and facilitates live VM migration, fault tolerance, and security.
- I/O virtualization – offloads packet processing to network adapters and assigns VMs to I/O ports, thus minimizing latency and the load on the CPU.
- Intel® Graphics Virtualization Technology (Intel® GVT) - allows VMs to have full and/or shared assignment of the GPU as well as the video transcode accelerator engines integrated in Intel system-on-chip products.

Intel Ecosystem COTS Solutions

Public sector system vendors can reduce development time and cost by adopting commercial, off-the-shelf (COTS) solutions. The solutions can provide hardware scalability and flexibility, as well as improve interoperability and simplify system upgrades through the use of open standards.

Public sector suppliers can choose from a wide range of Intel technology-based COTS solutions in a variety of standard form factors. Information about the standard boards offered by the members of the Intel IoT Solutions Alliance can be found on the web. As one of the most trusted ecosystems, the alliance can help with the design and deployment of end-to-end solutions.

Extended Use Conditions and Lifecycles

Select Intel silicon products are designed to support harsh temperature and weather conditions. The use conditions supported by select Intel processors are detailed in Figure 3.

Figure 3_Use conditions supported by Intel® processors

Use Conditions	Temp Range	Reliability
Automotive ▪ Advanced Driver Assistance Systems (ADAS) ▪ Software Defined Cockpit (SDC)	Automotive Grade 2, T_{la} = -40° to 105° C	15Y Reliability up to 11.4% Active, Tj-max = 110° - 125° C
Industrial	CT - Commercial Temp: T_{la} = 0° to 70° C ET - Extended Temp: T_{la} = -40° to 85° C	10Y Reliability up to 100% Active, Tj-max = 100° - 110° C Base Frequency only - No core or graphics turbo
Communications	CT - Commercial Temp: T_{la} = 0° to 70° C ET - Extended Temp: T_{la} = -40° to 85° C	10Y Reliability up to 100% Active, Tj-max = 100° - 105° C
Embedded Broad Market	CT - Commercial Temp: T_{la} = 0° to 70° C	5Y Reliability up to 80% Active, Tj-max = 100° - 105° C
Server/Enterprise	CT - Commercial Temp: T_{la} = 0° to 70° C	5Y Reliability up to 80% Active, Tj-max sku dependent
PC/Client/Tablet	CT - Commercial Temp: T_{la} = 0° to 70° C	5Y Reliability up to 30% Active, Tj-max sku dependent

NOTES:

- Spec Temperature ranges provided are based on Tla (local ambient temperature) - see definitions foil for descriptions
- The Temperature and Active % values referenced above are to be used for general planning/information purposes only - product specific Temperature and Active % may vary
- The most stringent use conditions can support lesser use condition requirements in many but not all cases
- Specific product tested use conditions and thermal ranges as well as Reliability failure rates calculated/published are based on a weighted temperature distribution for a given use condition - not at the temperature limits stated above. Refer to the Product PRQ report in QCDB for specific details by product family
- Product EDS and Thermal Design Guides can be found on developer.intel.com once product is launched
- Industrial Use Condition established ranges are based on Base Frequency only - No core or graphics turbo

Select Intel silicon products are supported for extended lifecycles:

- Available for fifteen years or longer if the processor and chipset are manufactured on 22 nanometer process or smaller.
- Available for seven years or longer if the processor or chipset is manufactured on processes larger than 22 nanometers.

The Intel product availability management process is described in Figure 4.

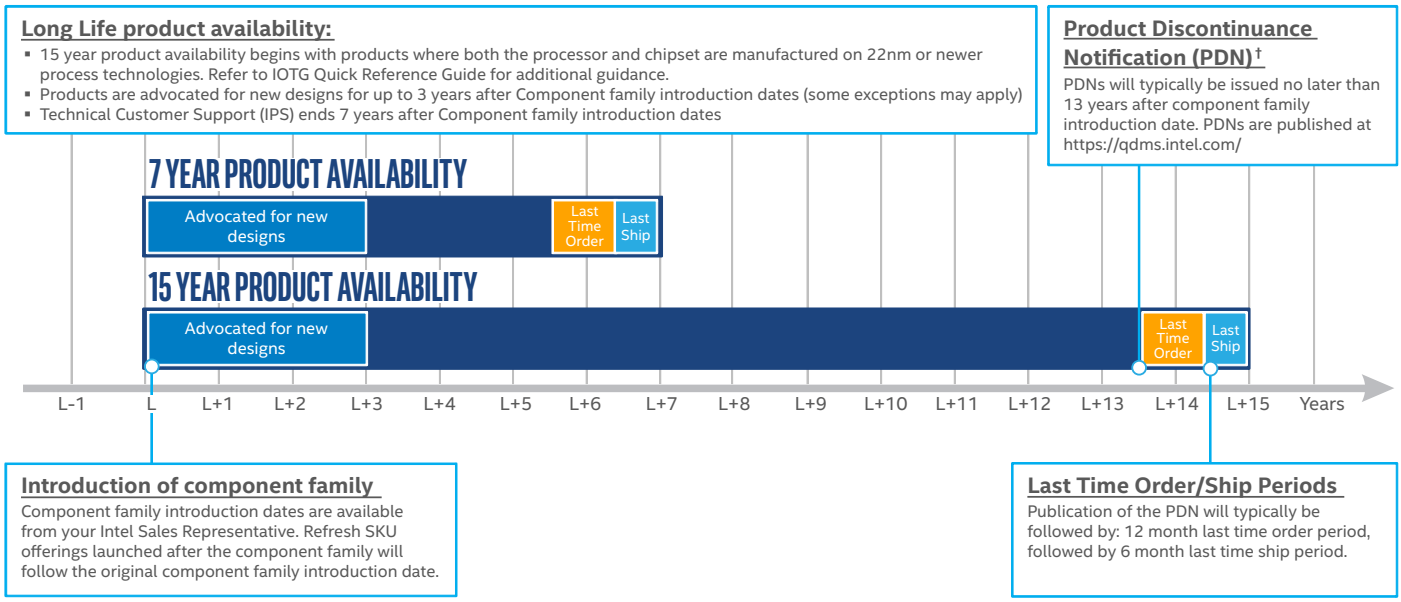

Figure 4_Product availability management processes for select Intel® processors

Predictable Performance and Flight Certification

For time-critical applications in the public sector systems, Intel and its partner solutions provide several ways to help achieve deterministic, real-time performance or the ability to service all critical events within an allotted time. Real-time performance is a relative metric because it depends on the frequency of events; the higher the event frequency, the higher the performance requirement.

For safety critical applications, like aerospace, it may be necessary to demonstrate a system can handle events in real time before it can be flight certified. Select Intel processors support a number of technologies that help improve deterministic, real-time performance, such as:

Intel Cache Allocation Technology

Software developers can allocate data to specific regions of last-level cache, enabling the isolation and prioritization of key applications. This capability enhances runtime

determinism by protecting the resources used by time-critical applications running in VMs, such as virtual switches and packet processing applications. The technology helps minimize resource contention and noisy neighbor interference across various classes of workloads.

Intel Cache Monitoring Technology
Last-level cache utilization can be monitored on an individual thread, application, or VM basis, thus providing greater insight that is useful when tuning application performance via resource-aware scheduling decisions.

Memory Bandwidth Monitoring
Memory bandwidth can be monitored for each running thread at the VM or application level. Capabilities include detection of noisy neighbors that over-utilize memory bandwidth, characterization and debugging of performance for bandwidth-sensitive applications, and more effective non-uniform memory access (NUMA)-aware scheduling.

Code and Data Prioritization
Software developers have separate control over code and data placement in the last-level cache. Certain specialized types of workloads may benefit from increased runtime determinism, enabling greater predictability in application performance.

Multi-Core Processors
As the avionics industry transitions to multi-core processors, the EASA.2011/6 "MULCORS" Project is offering particular guidance for developers of airborne systems.[8] Intel has become familiar with the requirements placed on embedded systems using multi-core Intel processors, and is offering guidance to avionics system developers.

Flight Safety
Intel is helping developers satisfy a system's intended function, meet safety objectives, and sustain foreseeable conditions. Recognizing the complexities of flight safety certification requirements, Intel is working to enable system providers to build Intel processor-based systems with D0-254 certification to a Design Assurance Level A.

Addressing Public Sector Challenges

Intel and its ecosystem of hardware and software vendors offer standards-based, modular, rugged, network-ready solutions for public sector applications, backed by Intel's 30+ years of experience in delivering world-class computing and communications solutions. System developers and integrators can benefit from this broad selection of interoperable, COTS solutions at multiple levels of integration and from software tools designed to shorten development time and cost.

Those tasked with addressing emerging challenges in the public sector can satisfy their need for greater computing performance, better security, lower system cost, and more predictable performance when they design with Intel solutions.

For more information about public sector solutions from Intel, please contact your Intel account owner or distributor partner.

1. Requires a system with Intel® Turbo Boost Technology. Intel® Turbo Boost Technology and Intel® Turbo Boost Technology 2.0 are only available on select Intel® processors. Consult your PC manufacturer. Performance varies depending on hardware, software, and system configuration. For more information, visit www.intel.com/content/www/us/en/architecture-and-technology/turbo-boost/turbo-boost-technology.html.

2. Intel® technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at https://www.intel.com.

3. Intel® Data Protection Technology with AES-NI and Secure Key, https://www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard-aes/data-protection-aes-general-technology.html.

4. Trusted Platform Module Information, https://www.intel.com/content/www/us/en/support/articles/000007452/mini-pcs.html.

5. "Hardware-Enhanced Security Strengthens Anti-Malware Defenses," 2014, https://www.intel.la/content/dam/www/public/us/en/documents/white-papers/hardware-enhanced-security-anti-malware-pillar-paper.pdf.

6. Intel® Software Guard Extensions SDK for Linux*, https://01.org/intel-softwareguard-extensions.

7. Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, and virtual machine monitor (VMM). Functionality, performance or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit http://www.intel.com/go/virtualization.

8. EASA 2011.C31"MULCORS" Project, "The Use of MULticoreproCessORS in Airborne Systems," 2012, https://www.easa.europa.eu/sites/default/files/dfu/CCC_12_006898-REV07%20-%20MULCORS%20Final%20Report.pdf.

† Intel may support this extended manufacturing using reasonably feasible means deemed by Intel to be appropriate. Future business, manufacturing, or market conditions may change, which may cause Intel to revisit the EOL/PDN timing. Intel may make changes to dates and schedule at any time without notice.