Product Brief
Intel® IoT Gateway

Intel® IoT Gateway

By 2020, more than 200 billion devices will be connected to the cloud and each other[1] in what is commonly called the Internet of Things (IoT). Connectivity is imperative to realizing the power of the IoT, which can allow gaining insight from data provided by these connected devices.

There's a large amount of legacy equipment that is not connected, managed, or secured. That leaves a lot of useful data locked away in a massive array of equipment, like HVAC units, vending machines, and much more. Thus, there is a definite need to address interoperability of legacy systems in order to avoid the incredibly large cost of replacing all existing infrastructure with next generation equipment that can securely connect to the Internet.

Today's industrial devices and other systems are often designed with interconnectivity and the ability to share data. Intel® IoT Gateways enable companies to seamlessly interconnect industrial infrastructure devices and secure data flow between devices and the cloud. It also allows customers to securely aggregate, share, and filter data for analysis. It helps ensure federated data generated by devices and systems can travel securely and safely from the edge to the cloud and back—without replacing existing infrastructure. This new availability of previously hidden data can be valuable to a wide range of businesses and organizations:

- Operators, such as building maintenance personnel, can track real-time operations of various systems and optimize them for particular times of day, types of work, etc.
- Managers, such as property owners and business managers, can correlate data across entire holdings and analyze and optimize the cost of systems operations.
- Manufacturers and service agencies can analyze real-time and trended data from systems to optimize them for power efficiency, performance, operational life, and more.
- Governments and researchers can perform larger analyses on data from seemingly disparate but related systems to correlate impacts and effects of these systems on each other.

Intel® IoT Gateway

The Intel IoT Gateway offers companies a key building block to enable the connectivity of legacy industrial devices and next generation intelligent infrastructure to the IoT. It integrates technologies and protocols for networking, embedded control, enterprise-grade security, and easy manageability on which application-specific software can run.

Intel IoT Gateways enable:

- Connectivity up to the cloud and enterprises.
- Connectivity down to sensors and existing controllers embedded in the system.
- Pre-process filtering of selected data for delivery.
- Local decision making, enabling easy connectivity to legacy systems.
- A hardware root of trust, data encryption, and software lockdown for security.
- Local computing for in-device analytics.

An Integrated, Pre-Validated, and Complete Solution

Intel IoT Gateway offers a proven solution—pre-validated on industry-leading software—that delivers an application-ready platform. The solution includes:

- Choice of Intel® processors for the development kits: Intel® Quark™ SoC X1000, Intel® Quark™ SoC X1020D and Intel® Atom™ processor E3826
- Wind River* Intelligent Device Platform XT development environment
- McAfee Embedded Control* security technologies

Intel IoT Gateways are built on open architecture to ensure interoperability between systems, enable wide application development, and allow easy services deployment. Integrated and validated components allow maximum flexibility and fast application development and deployment to the field.

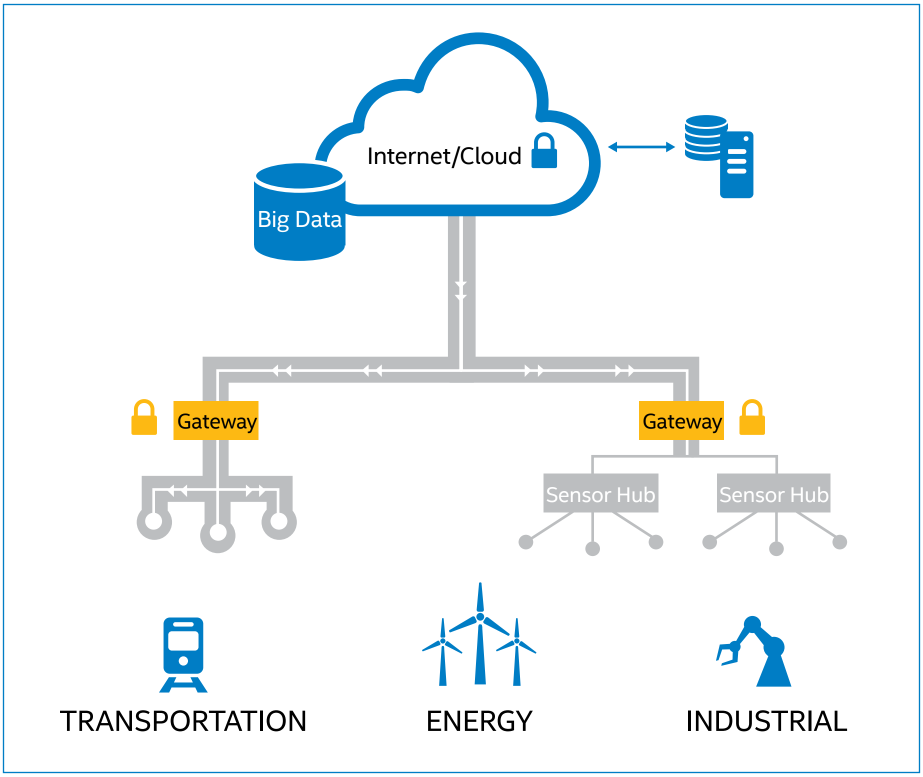
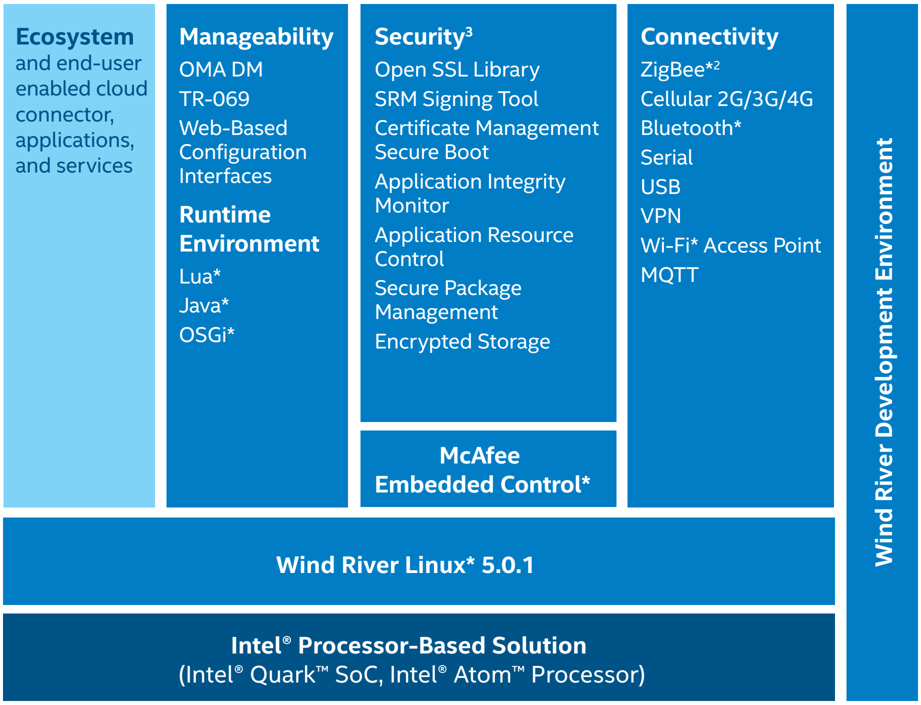


Figure 1. Addressing Endless Use Cases.



Ecosystem and end-user enabled cloud connector, applications, and services

Manageability
OMA DM
TR-069
Web-Based Configuration Interfaces

Runtime Environment
Lua*
Java*
OSGi*

Security[3]
Open SSL Library
SRM Signing Tool
Certificate Management
Secure Boot
Application Integrity Monitor
Application Resource Control
Secure Package Management
Encrypted Storage

McAfee Embedded Control*

Connectivity
ZigBee*[2]
Cellular 2G/3G/4G
Bluetooth*
Serial
USB
VPN
Wi-Fi* Access Point
MQTT

Wind River Linux* 5.0.1

Intel® Processor-Based Solution
(Intel® Quark™ SoC, Intel® Atom™ Processor)

Wind River Development Environment

Figure 2.[4] Intel® IoT Gateway Software Stack.

Wind River* Intelligent Device Platform XT

Connectivity, manageability, and security are core building blocks to IoT. Intelligent Device Platform XT provides an integrated, pre-validated stack of software, drivers for a wide range of hardware components, libraries, and tools to support these core services. The software enables flexibility for developers to quickly build enterprise-grade intelligent systems for a large number of applications. Intelligent Device Platform XT supports the following:

- **Manageability –** Intelligent Device Platform XT enables long-term secure remote manageability to simplify deployment, maintenance, and management of remote devices. The software supports industry-standard interfaces, including Open Management Alliance Device Management (OMA DM), Technical Report 069 (TR-069), and web-based configuration interfaces.
- **Communications and Connectivity** – To enable connectivity over the widest range of communications technologies, Intelligent Device Platform XT supports both wireless and wired links. The software includes drivers for a number of hardware vendors' products and software to support Cellular 2G/3G/4G, Bluetooth*, Serial, USB, Virtual Private Network (VPN), Wi-Fi* Access Point, the MQ Telemetry Transport (MQTT) messaging protocol, and ZigBee*[2].
- **Security –** Intelligent Device Platform XT provides strong support for secure image, secure data, and secure management, helping protect the device and data from boot to operations and management.[3] The software supports comprehensive device protection, from a hardware root of trust through boot and software loading, and offers a wide array of protocols and services, including secure boot, whitelisting with McAfee Embedded Control, secure storage, and more.
- **Runtime Environments –** Intelligent Device Platform XT supports applications written in a variety of environments, including Lua,* Java,* and OSGi,* to enable portable, scalable, and reusable application development for solutions based on the Intel IoT Gateway platform.

Intelligent Device Platform XT provides the foundation for fast development of intelligent system solutions on industry-standards using a proven software stack.

McAfee Embedded Control*

Integrated with the Intel IoT Gateway platform, McAfee Embedded Control maintains system integrity by allowing only authorized code to run (application whitelisting) and only authorized changes to be made (change control). It simultaneously protects embedded system integrity and automates the enforcement of software change control policies.

Application Whitelisting

The software automatically creates a dynamic whitelist of the allowed code on the platform. Once the whitelist is created and enabled, the system is locked down to the known good baseline; no program or code outside the authorized set can run, and no unauthorized changes can be made. McAfee Embedded Control shields applications and related binaries at the kernel level—protecting files on disk or in memory, helping prevent malware and zero-day exploits, and minimize the need to patch the environment.

Change Control

McAfee Embedded Control only allows policy-based changes that are expected and authorized. The software monitors files and prevents unexpected changes while logging any attempts. It provides complete visibility and accountability through the automated, continuous collection of audit data. Using the data collected by McAfee Embedded Control, one can verify that no changes have been made to critical system files, directories, or registries, and then report these findings to regulatory officials to help meet compliance requirements.

Endless Potential for Industry and Business

Designed to securely connect edge devices to the cloud, the Intel IoT Gateway is ideal for a vast array of applications including, building automation, industrial automation, and smart city infrastructure, and much more. By capturing and analyzing data

THE INTEL® IOT GATEWAY

Open, pre-validated solution

Connect, manage, and secure SW stack

Enables seamless and secure data flow

Hosts ecosystem apps and services

from new sources, it gives management, service businesses, product manufacturers, and their ecosystems new opportunities for accelerating business innovation, understanding the behavior and uses of their existing products, and a foundation for designing new products for the marketplace.

Intel IoT Gateway

Key Benefits

- Delivers an integrated, pre-validated, and flexible open-compute gateway platform, including foundational hardware, software, and security building blocks to allow fast solution development and deployment.
- Enables building scalable solutions with standards-based interfaces to securely connect and aggregate data from the edge to the cloud.
- Enables business innovation on proven technologies across compute, communications, manageability, and security.

	DK50 SERIES	DK100 SERIES**	DK200 SERIES**	DK300 SERIES
Target Markets	Developers, Enthusiasts	Industrial, Energy	Transportation	Industrial, Energy, and Transportation
SoC	Intel® Quark™ SoC X1000	Intel® Quark™ SoC X1020D	Intel® Quark™ SoC X1020D	Intel® Atom™ Processor E3826
Software	Non-production, 6 Month SW License includes, Wind River Linux* (Host), Wind River* Intelligent Device Platform XT, Wind River Workbench, McAfee Embedded Control*	Wind River Linux* (Host), Wind River* Intelligent Device Platform XT, Wind River Workbench, McAfee Embedded Control*		
Security[3]	Open SSL* Library, McAfee Embedded Control*	Open SSL* Library, SRM Signing Tool, Certificate Management, SecureBoot, Application Integrity Monitor, Application Resource Control, Secure Package Management, Encrypted Storage, McAfee Embedded Control*		
Manageability and Provisioning	OMA DM, TR-069, Web-based configuration interfaces			
Communications and Connectivity	Serial, USB, VPN, MQTT	Bluetooth,* Serial, USB, VPN, Wi-Fi* Access Point, MQTT, ZigBee*[2]		Cellular 2G/3G/4G, Bluetooth,* Serial, USB, VPN, Wi-Fi* Access Point, MQTT
Runtime Environments	Java, OSGi	Lua,* Java,* and OSGi*		
I/O	Ethernet* 10/100, USB 2.0 host & device, RS-232, full PCIe* mini card slot, UART 5V/3.3V, SPI for Arduino shield, I2C, 14 digital I/O pins, 12-bit 8 channel ADC	2x Ethernet* 10/100, USB 2.0 host & device, RS-232, RS-485, ZigBee*[2], Wi-Fi*/ Bluetooth* mini PCIe Module, 3G (data), SPI (internal), 12-bit 8 channel ADC	2x Ethernet* 10/100, USB 2.0 host & device, RS-232, Audio line in/out, CAN*, Wi-Fi*/Bluetooth* mini PCIe Module, 3 axis accelerometer (internal), 12-bit 6 channel ADC	2x Ethernet* 10/100/1000, 2x USB 2.0, 1X USB 3.0, RS-232/422/485, Line in/ out, Wi-Fi*/Bluetooth* mini PCIe Module, Cellular WAN mini PCIe module, HDMI
Memory and Storage	512KB SRAM; 256MB DDR3, onboard microSD card	512KB SRAM; 1 GB ECC DDR3, onboard microSD card	512KB SRAM; 512MB ECC DDR3, onboard microSD card	Up to 8 GB DDR3, 2.5¨ SSD via onboard SATA

Figure 3.[4]

For more information, visit intel.com/iotgateways

[**] While the DK100 & DK200 series development kits do not come with cellular built-in, they do support cellular capabilities.

[1] Intel forecast.

[2] Enabled by 3rd Party hardware.

[3] No computer system can provide absolute security. Requires an enabled Intel® processor, enabled chipset, firmware, software and may require a subscription with a capable service provider (may not be available in all countries). Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. Consult your system or service provider for availability and functionality. For more information, visit http://www.intel.com/go/anti-theft. Consult your system manufacturer and/or software vendor for more information.

[4] All products, computer systems, dates and figures specified are preliminary based on current expectations, and are subject to change without notice.

By using this document, in addition to any agreements you have with Intel, you accept the terms set forth below.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

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.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

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 here 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 go to: http://www.intel.com/design/literature.htm

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families:
go to: http://www.intel.com/products/processor_number

Printed in USA 1014/JR/HBD/PDF ♻ Please Recycle 330184-003US IBL: 546398