WHITE PAPER

The Intel® IoT Platform

Architecture Specification White Paper
Internet of Things (IoT)

As the Internet of Things (IoT) gains momentum, there is a need for a suite of connected products and services that have awareness of each other and their surroundings. To help satisfy this need, Intel defined and released the Intel® IoT Platform, which includes reference architectures and a portfolio of products from Intel and the ecosystem. To guide the development and deployment of IoT solutions, Intel has defined reference architectures for the IoT, which addresses requirements for data and device security, device discovery, provisioning and management, data normalization, analytics, and services. These reference architectures are designed for two different use cases: one for connecting legacy infrastructure—"Connecting the Unconnected," and another for building infrastructure—"Smart and Connected Things". This white paper discusses both reference architectures and associated products from Intel.

Reference Architecture for IoT Infrastructure

By 2020, it is expected that more than 50 billion devices will be connected to the cloud and each other[1] in what is commonly called the Internet of Things (IoT). Before this can become a reality, solution providers must recognize and tackle the complexity of IoT solutions to ensure secure, scalable, and interoperable IoT deployments.

Along these lines, Intel, working with its ecosystem partners, defined a system architecture specification (SAS) for connecting nearly any type of device to the cloud, whether it has native Internet connectivity or not, as shown in Figure 1. The specification is intended to help developers, OEMs, independent software vendors (ISVs), and communications service providers (CSPs) develop and deploy IoT solutions in keeping with five key tenets:

- **Services to monetize the IoT infrastructure**
  Data and device management from things to cloud
- **Seamless data ingestion and device control to improve interoperability**
  Broad protocol normalization support with real-time, closed-loop control systems
- **World-class security to deliver the requisite data and device protection**
  Robust hardware and software-level protection
- **Analytics infrastructure to provide customer value**
  Real-time, insightful, and secure data analytics from things to cloud
- **Automated discovery and provisioning of edge devices to ease deployment**
  Device setup from box to cloud in minutes

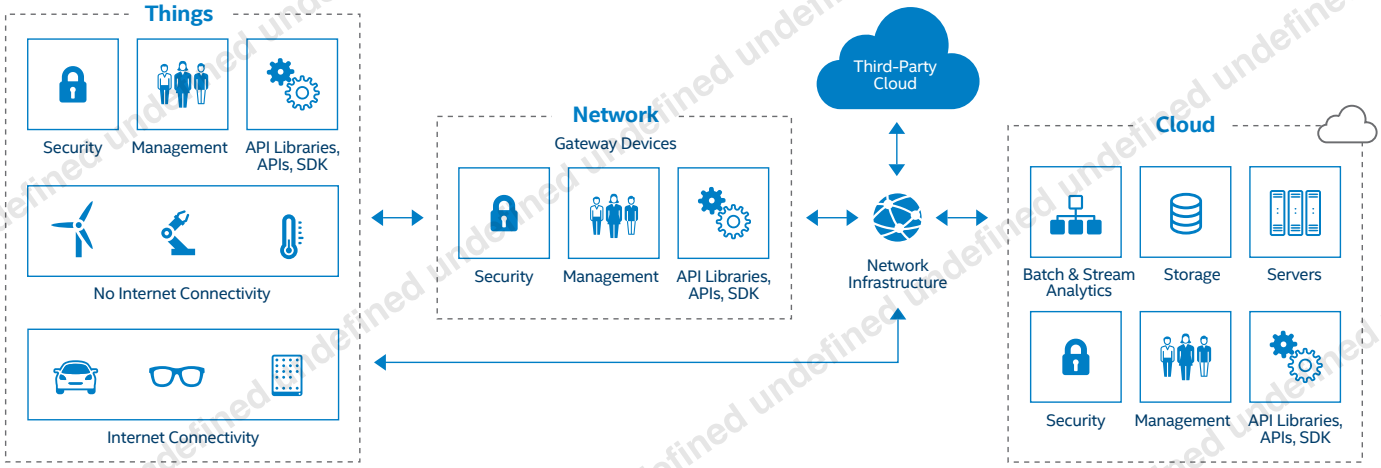

Figure 1. End-to-End IoT Solution from Things to Network to Cloud

Table of Contents

Intel Reference Architecture Overview

The Intel® system architecture specification (SAS) is a reference architecture for IoT, with two versions that co-exist and were designed to evolve as specifications for open and scalable solutions. The two versions represent concurrent reference architectures to address different partner infrastructure maturity levels, and to separate urgent and future-proofing needs. As horizontal architectures, both versions were designed with the same principles used by leading cloud providers and tested for massive loads across a range of IoT standards and business verticals.

Available under a non-disclosure agreement (NDA), the reference architecture versions are intended to accelerate partner products, requirements, and feedback.

Version 1.0 The Intel® IoT Platform Reference Architecture for Connecting the Unconnected

The Intel SAS version 1.0 specifies how solution developers and system integrators can use an IoT gateway to securely connect and manage legacy devices that were not originally built with intelligence or Internet connectivity.

Version 2.0 The Intel® IoT Platform Reference Architecture for Smart and Connected Things

Intel SAS version 2.0 specifies how to integrate a variety of smart and connected things, ranging from battery-powered through to ultra-high performance devices, which are being built today with intelligence and connectivity already integrated. In some of these configurations, an IoT gateway is not needed. However, these smart devices may lack the security, manageability, or integration capabilities necessary for real-time, closed-loop control of the data shared between smart things and the cloud. Version 2.0 describes methods to overcome these issues.

Moreover, version 2.0 is a future-looking reference architecture. It facilitates the convergence of operational technology (OT) and information technology (IT) for seamless cyber-physical systems using Universal Smart Objects (USO), which are IPSO-Alliance.org compatible. One global map provides IoT resources with a USO type and type members that have a global unique ID (GUID), and can be registered and discovered with Intel Contract Broker (iCB), which is compatible with CoRE Resource Directory from IETF.org.

The specification is future-proofed through the use of modular planes and flows for reuse across application containers, virtual machines (VM), and network functions virtualization (NFV) as developed by ETSI.org. Likewise, solution lifetimes are extended with support for software-defined networking (SDN) per the Open Networking Foundation (ONF) and other reference architectures that make it easier to manage large networks of disparate hardware and software resources.

IoT Value Proposition

Companies and organizations have been collecting and storing data for years, but now new data analytics technologies enable more productive use of this data by transforming it into information that can increase system throughput, improve efficiency, reduce downtime, and enhance customer experiences. When this data is analyzed in detail using advanced tools available on the market, it is possible to find patterns and extract meaning that ultimately lead to smarter decision making.

The IoT will deliver the infrastructure required to achieve this by making it easier to collect, analyze, and act on data generated by a wide array of endpoint devices. This is done by providing the data and device connectivity, security, interoperability, and analytics capabilities that enable greater productivity.

IoT Challenges

Before the full benefits of the IoT can be realized, the industry must address some challenges facing end customers and solution providers alike. *Data security and privacy* must be omnipresent at every endpoint and throughout the network and cloud to protect devices and users' private information as data travels from things to cloud. *Solution provider fragmentation* in many vertical market segments has resulted in vertical, purpose-built solutions that inhibit interoperability, thereby impeding the flow of data across vertical domains. The *integration of information technology (IT) and operational technology (OT) infrastructure* is vital in order to capture all the data and analyze all contextually relevant information in the company or organization in real time.

The concept of ubiquitous *device connectivity* to the Internet is still in its infancy, with 85 percent of devices yet to be connected.[2] *IoT investment justification* is hampered by underutilized data, leading to ROI calculations that fail to account for the full potential of IoT (e.g., IT and OT cost savings, new and adjacent revenue generation). *Interoperability and standards* are unavailable or globally fragmented, which slows down decision making and IoT adoption.

This Intel SAS was developed to address these challenges, and in doing so, will help accelerate growth of the IoT.

Intel Leadership in IoT

Intel has a proven history of transforming vertically fragmented, inefficient, and proprietary markets into well-organized, horizontally scalable, and open markets (as best demonstrated with the PC, laptop, workstation, server, and storage markets). Today, Intel is working to make the IoT more open and cohesive by leading the creation of two important consortia to promote a standards-based and inclusive IoT development environment. The Industrial Internet Consortium (IIC) and the Open Interconnect Consortium (OIC) were created to address the myriad of challenges that could limit growth of the IoT, including data and device security, interoperability, and scalability.

Intel's success in this effort is closely linked with the more than 250 members of the Intel® IoT Solutions Alliance, one of the world's most recognized and trusted technology ecosystems. These members offer software and hardware solutions that are fundamental to building IoT infrastructure. No single company can do this alone, which is why it is extremely important to enable a large number of vendors through open standards and platforms. Intel and its ecosystem embrace this principle, which gives end users greater vendor choice and potentially lower costs from increased competition.

Intel IoT Reference Architecture

The developer community can use Intel's IoT reference architecture to bring intelligence to endpoint things by enabling edge analytics, leading standards compliance, and direct-connect cloud control. The architecture, shown in Figure 2, is layered, where the white blocks are user layers, the dark blue blocks are the major runtime layers, and the light blue layer is for developers.

The business layer utilizes the application layer to access other layers in the solution. The vertical security layer on the right side of Figure 2 secures all layers, which is critical for satisfying the world-class security tenet mentioned previously. The following section describes the data flow through this layered architectural framework, and subsequent sections cover all the architectural layers in more detail.

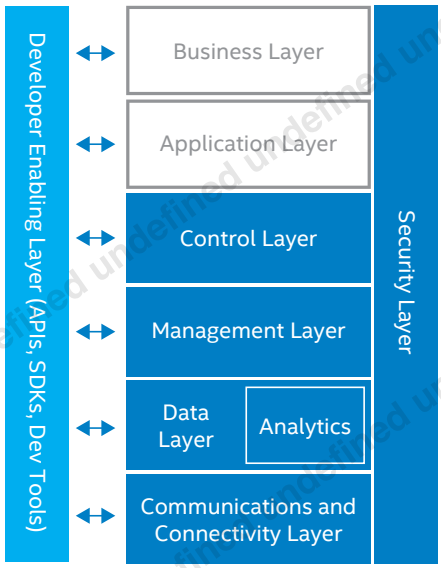

Figure 2. Layered Architecture Enables Secure, End-to-End Solutions

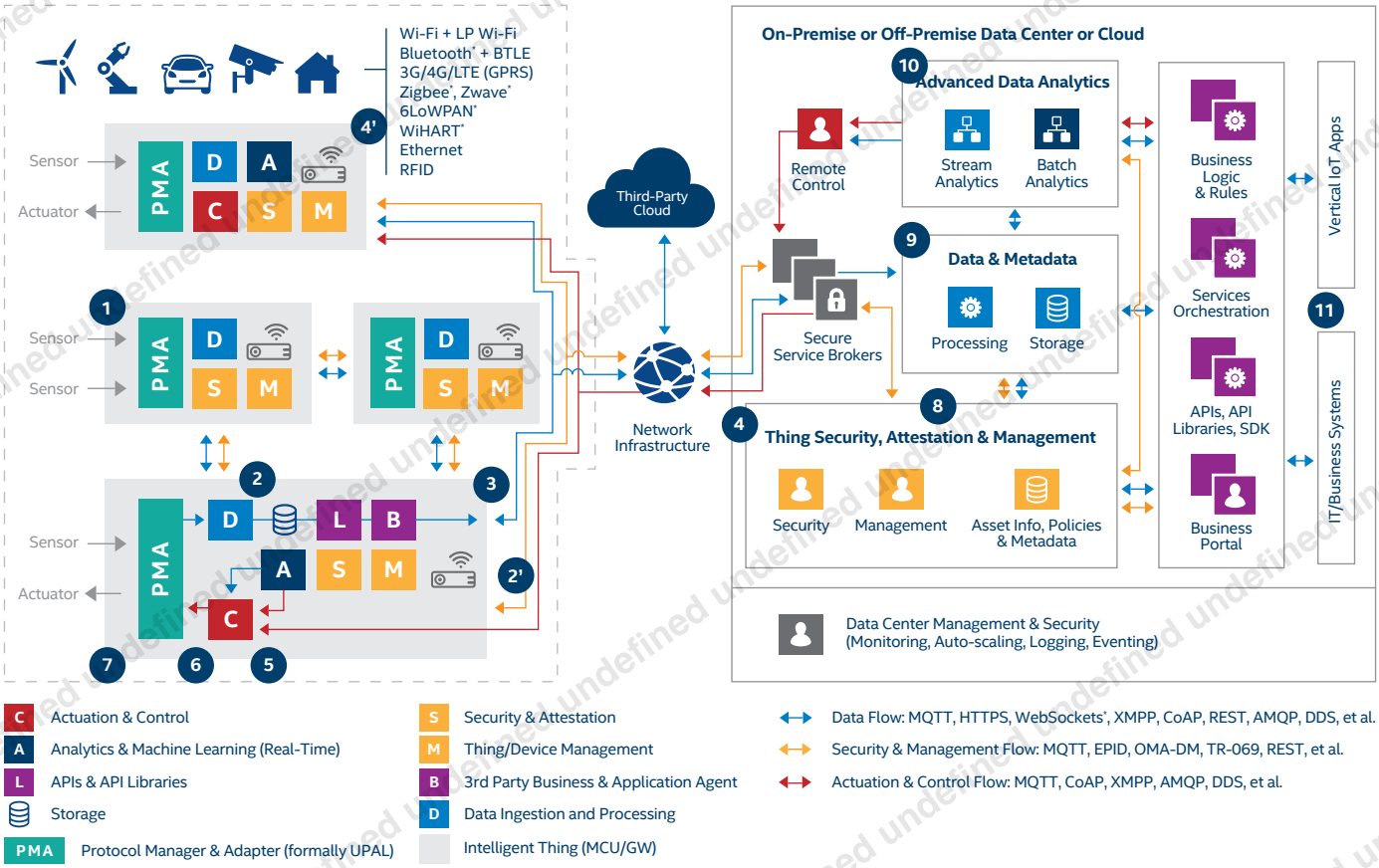

Figure 3. Data Flow for Devices without Native Internet Connectivity

Data Flow

Figure 3 depicts a typical industrial data flow through Intel's IoT reference architecture to illustrate how devices without native Internet connectivity can be intelligently controlled by the cloud.

1. Endpoint sensor devices convert analog signals to digital using an analog-to-digital converter (ADC).
2. The gateways collect data from endpoint sensors or (2' in figure) multiple sensing devices can alternatively connect directly to the data center via the Internet.
3. The gateways prepare, reduce, and aggregate data. Gateways may also include, as an example, a web server, which forwards data to the cloud via HTTPS Post to Internetwork using the MQTT protocol.
4. The data center, which may include an on-premise or Fog perimeter, is configured for low latency to provide real-time responses to the gateways via HTTPS Get/Post or (4' in figure) Fog can alternatively respond directly to endpoint sensor devices. Fog is the edge-cloud area (near 4 in figure), which is tuned for low latency with near-real-time query and analytics for on-premises value, unlike the central cloud tuned for high bandwidth and batch mode, eventually providing deep data insights for things-to-Fog, end-to-end, real-time operations.
5. The gateways forward responses (control commands) to the endpoint sensor/actuation devices.
6. The endpoint sensor devices convert digital signals to analog using a digital-to-analog converter (DAC).
7. Actuators and motors respond to the new analog input.
8. The data center transports and ingests sensor data for device security and management.
9. The data center forwards other data to runtime operations.
10. The data center also forwards data to data analytics applications.
11. Data analytics applications evaluate big data and generate analysis and operational reports.

End-to-End IoT

The major software components and interfaces in Intel's IoT reference architecture for connecting devices without native Internet connectivity are shown in Figure 4. The components are grouped by on-premises and cloud. The on-premises components are located on endpoint devices and gateways, as described in Table 1. The cloud components are responsible for data ingestion from the endpoint device, data storage, data analysis, service orchestration, and security management, as indicated in Table 2.

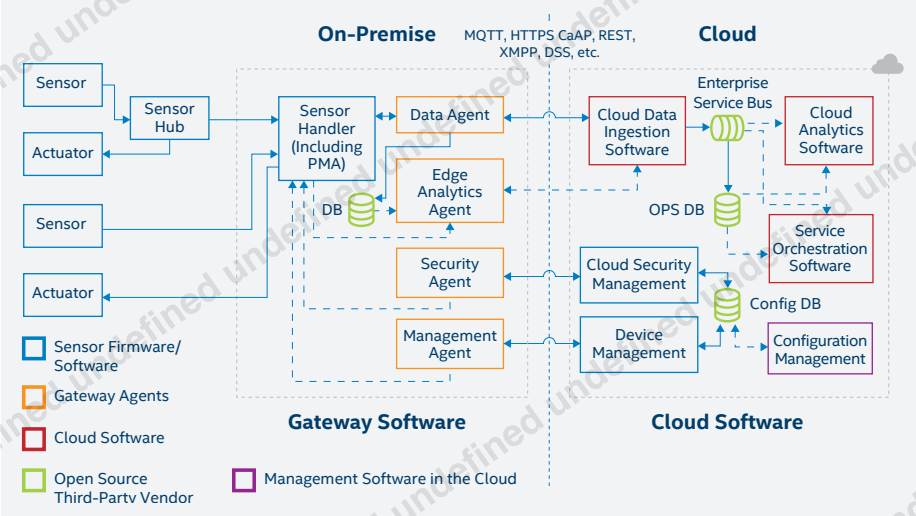

Figure 4. Software Components and Interfaces for Intel's IoT Reference Architecture

COMPONENT	SOFTWARE TYPE	FUNCTIONALITY	INTERFACES
Sensor	Hardware and firmware for intelligent things	Gathers sensory information like temperature, pressure, vibration, energy, etc.	Connects to the gateway or sensor hub via wired (e.g., I^2C, GPIO, SPI) or wireless (e.g., BTLE, ZigBee*, USB)
Actuator	Same as above	Performs actuation (e.g., turn on LED).	Same as above
Sensor Hub	Hardware and firmware	Connects to sensors and actuators, and aggregates data.	Same as above
Sensor Handler	Middleware	Interfaces with sensors using device drivers or API libraries (e.g., Protocol Abstraction or Mapping Layer (PMA) APIs).	Communicates via API calls to sensor libraries (or PMA) or directly to device drivers (in the absence of APIs).
Local Database	Third-party or open-source software	Locally stores sensor data, logging or configuring information from the cloud.	Uses REST, ODBC, JDBC, etc. on SQL, JSON, streaming, time and spatial data.
Data Agent	Software	Gathers and formats data (for the cloud) from the different sensors and controls actuators based on commands from the cloud.	Communicates with the sensor handler via API calls to sensor libraries (or PMA) or directly to device drivers (in the absence of APIs). Communicates with the cloud via different protocols, like MQTT, REST, etc.
Edge Analytics Agent	Software	Learns actionable data in local context and near real time.	Communicates with major device-to-device and device-to-cloud API for rules on data streams, their alerts, and local processing
Security Agent	Software and middleware	Handles security primitives for gateways and sensors/actuators, including authentication keys and certificates.	Communicates with the security management software component in the cloud.
Management Agent	Software and middleware	Handles manageability primitives for gateways and sensors/actuators, including provisioning, error handling, alerting, and eventing.	Communicates with the device management software component in the cloud.

Table 1. Description of On-Premises Software Components

COMPONENT	DESCRIPTION	INTERFACES
Cloud Data Ingestion Software	Interacts with the edge data agent and ingests data coming from edge devices, making it available to other cloud software via the Enterprise Service Bus (ESB).	Communicates with the data agent via different protocols, like MQTT, REST, DDS, etc., and publishes to ESB.
Cloud Security Management Software	Interacts with the edge security agent in the edge, and configures and controls security primitives of on-premise equipment.	Communicates with the edge security agent and configuration database.
Cloud Device Management software	Interacts with the edge management agent in the edge, and configures and controls manageability primitives of on-premise equipment.	Communicates with the edge device management agent and configuration database.
Enterprise Service Bus	Assists in the design and implementation of communications between mutually interacting software applications.	Supports cloud analytics and service orchestration software, and can subscribe to data from the ESB.
Operational Database	Manages dynamic data end-to-end, allowing real-time data modifications (add, change or delete). Examples include MongoDB* and Hadoop*.	Supports cloud analytics and service orchestration software, and can access the operational database.
Configuration Database	Contains all relevant information about the edge components and the relationships between those components.	Includes security and management software that can access the configuration database.
Analytics Software	Runs big data analysis on the data gathered from edge components.	Can access the operational database and data from the ESB.
Service Orchestration Software	Centrally ensures service level agreements (SLA) across resource managers workflow and provisioning applications and services	Can access the operational database and data from the ESB.
Configuration Management	Centrally ensures on-premises configuration management, including devices and security.	Updates the configuration database.

Table 2. Description of Cloud Software Components

Communications and Connectivity Layer

In support of the IoT tenet of seamless data ingestion and device control, Intel's IoT reference architecture implements broad protocol normalization and closed-loop control systems. A key aspect is enabling multi-protocol data communication between devices at the edge as well as between endpoint devices/gateways, the network, and the data center. Figure 5 depicts the three types of networks involved in this process.

Proximity networks and local area networks (PAN/LAN) connect to sensors, actuators, devices, control systems, and assets, which are collectively called edge nodes. PANs are usually wireless and more constrained by antenna distance (and sometimes battery life) than LANs.

Wide area networks (WAN) provide connectivity for data and control flows between the endpoint devices and the remote data center services. They may be corporate networks, overlays of private networks over the public Internet, 4G/5G mobile networks, or even satellite networks.

The gateways in the middle of Figure 5 are the primary on-premises devices of Intel's IoT reference architecture. They perform protocol normalization, ingest data from things, and control things based on their own application software or commands from the data center or cloud. Since the gateways both ingest data and execute commands, they are ideal for implementing closed-loop control systems. Gateways unify the broad range of endpoint things characterized by low cost, low power, purpose-built, limited, and disjoint features.

Data Layer with Analytics

The data layer plays a major role in the IoT tenet of providing customer value through valuable insights generated by data analytics and improved closed-loop control systems. Intel's IoT reference architecture addresses this need by allowing analytics to be distributed across the cloud, gateways, and smart endpoint devices (e.g., wearables), as shown in Figure 6. Likewise, control can be distributed

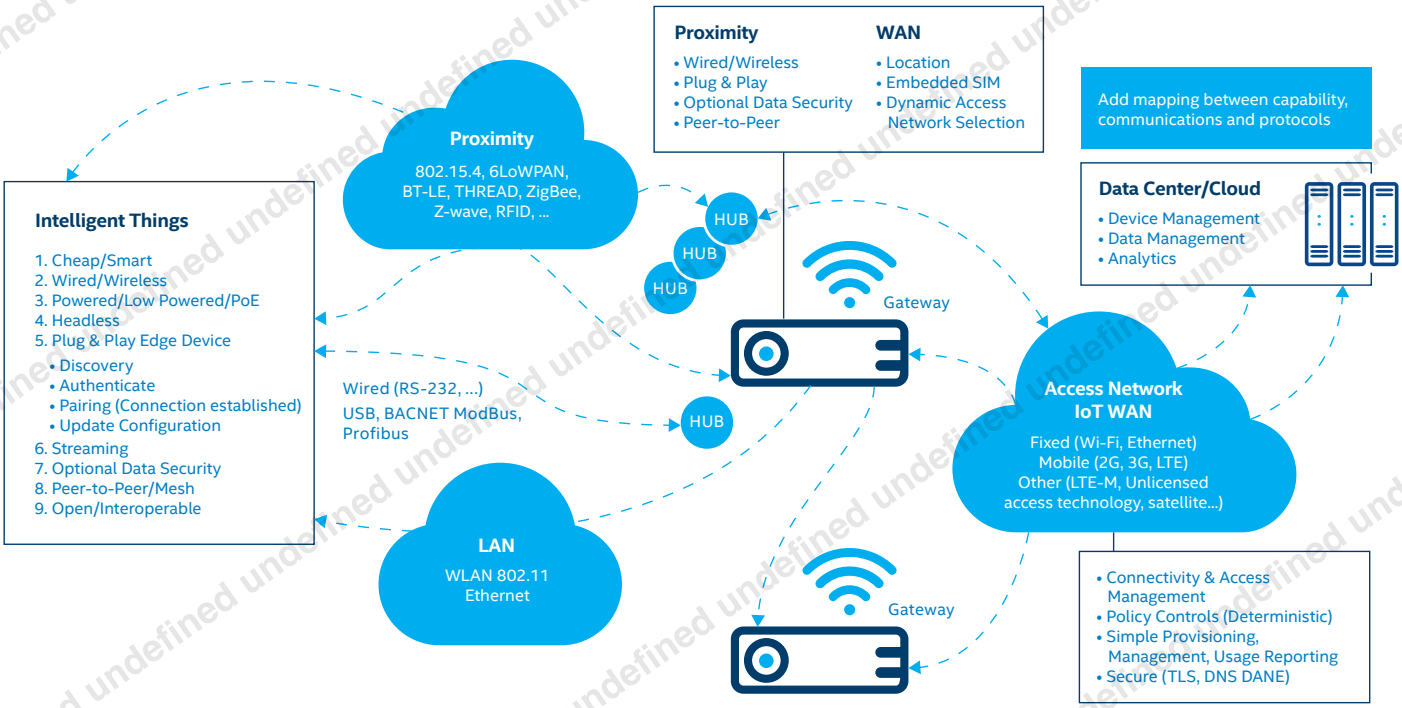

Figure 5. Detailed View of Communications

across the cloud and endpoint devices. Distributing analytics and control provides the flexibility to optimize either time-critical or computation-intensive applications.

Time-critical: The proximity of gateways allows them to respond more quickly than the cloud, which is important for real-time systems found in industrial applications or wearables in consumer markets. Gateways also have context for local resolutions, reserving central clouds for global analysis.

Central computation: The computing power and corporate-wide access to data in the cloud enables analytics to be performed on larger data sets, which is important for large transactional applications found in retail and banking. This complements the vast computation and analytics of the billions of local devices, which would flood central analysis in quantity and local context, and with noisy and aged data.

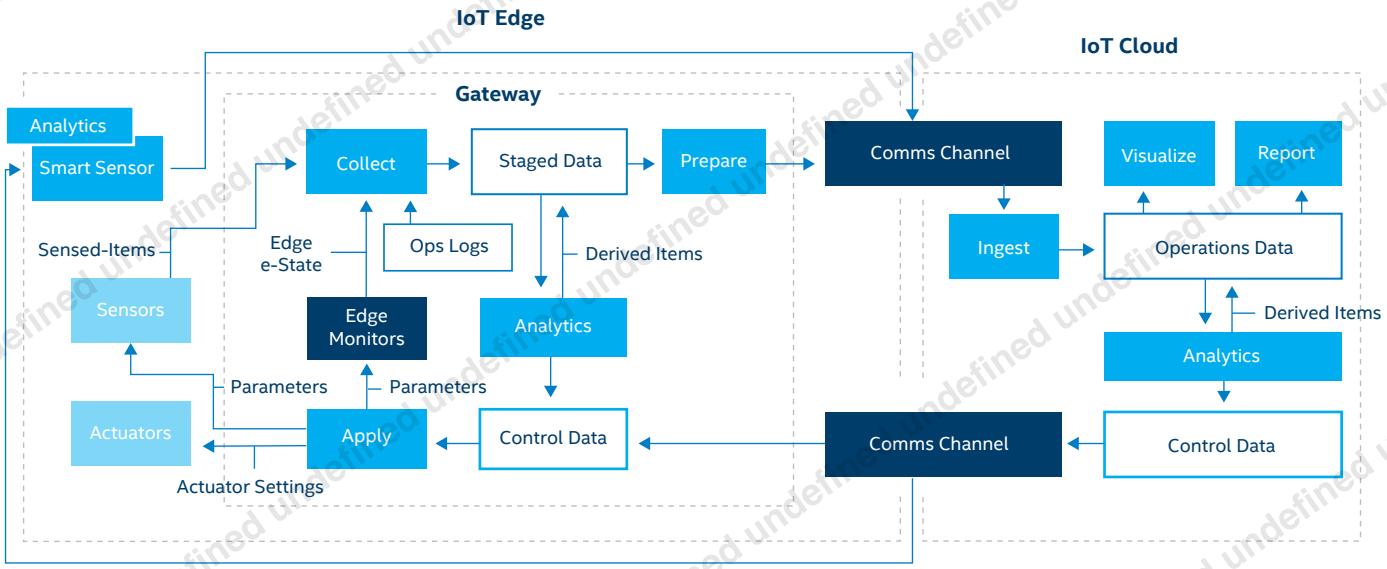

Figure 6. Data Layer Supports Distributed Analytics and Control

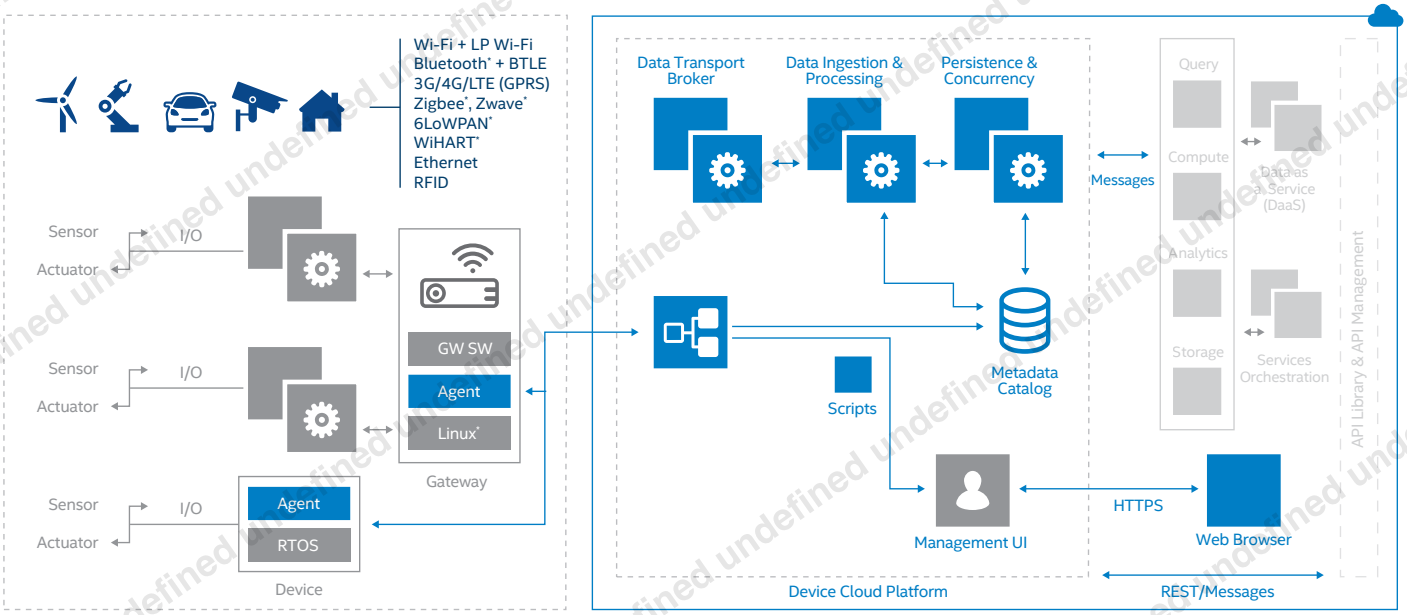

Figure 7. Management Layer Supervises Endpoint Devices

Management Layer

The management layer is important for realizing the IoT tenet of automated discovery and provisioning of endpoint devices. Intel's IoT reference architecture provides manageability functions through the Device Cloud product, whose scope is shown in Figure 7. The managed devices are on the left-hand side, and the cloud platform is on the right-hand side. Each managed device has a management agent that executes the management in its device and communicates with the cloud platform via messages. The operator manages endpoint devices via a web-based user interface.

Device Cloud is a system for managing small to very large numbers of connected endpoint devices. Its key functions are to securely connect the devices to the cloud, update device software, and supervise devices. Device Cloud can connect to gateways to manage devices that are unconnected.

Scripts can be used to write applications that use the cloud platform. Another option is to write applications somewhere else, using a REST API to take advantage of platform functions. The volume, frequency, and destination (e.g., cloud entity) of device data can be controlled.

Device Cloud has the following main device management functionality:

- Discover, register, and provision new devices
- Update applications and operating systems
- Manage data flows from devices (i.e., destination and storage policy)
- Upload or stream data via an ActiveMQ client interface
- Stop/reboot selected devices
- Define and manage events, alarms, and notifications
- Use cloud-side rules to initiate actions
- Extend platform capabilities using scripts
- Manage devices directly through its command shell
- Manage organizations, users, and access rights
- Upload and download files to/from a device

Control Layer

Intel's IoT reference architecture provides early guidance to separate the management layer into a management plane and control plane, with policy and control objects and APIs. The control layer can move off-device and off-premises for cloud or remote control, a primary requirement of software-defined network (SDN) centrally controlled programming.

Security Layer

Robust hardware- and software-level protection are essential for ensuring world-class security, which is a foundational IoT tenet. Security is more like a process than a product because it depends upon evaluating the threat model for specific use cases and addressing each possible threat. A layered security approach is highly recommended since it establishes multiple defense mechanisms against hackers.

Security in Intel's IoT reference architecture spans endpoint devices, the network, and the cloud, thus providing end-to-end protection (Figure 8). Having acquired McAfee, a world-leading security company, Intel provides a comprehensive security software product portfolio to help developers deliver interoperable and scalable solutions that span every level of the IoT.

Endpoint device level: Protect device and user identities, ensure device integrity, and protect operational and personal data on every device. Each device should guarantee authentication without jeopardizing individual privacy and have the ability to automatically self-assess and resolve any situation.

Network level: Ensure secure application, traffic, and data security in transit through every type of wired and wireless network connection. A new class of intelligent gateway solutions, developed by McAfee, Intel, and Wind River, offers secure interoperability with legacy systems while providing common interfaces and seamless communication between endpoint devices, the network, and the cloud.

Cloud level: Deliver the necessary trust for data centers and multitenant public cloud environments to unleash powerful IoT services and analytics while protecting data and ensuring privacy.

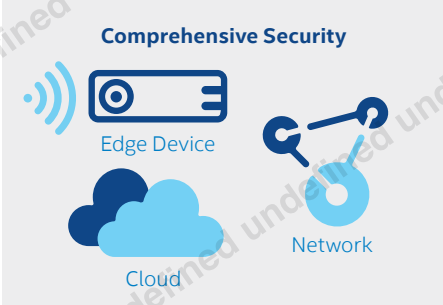

Figure 8. Security at All Levels of IoT

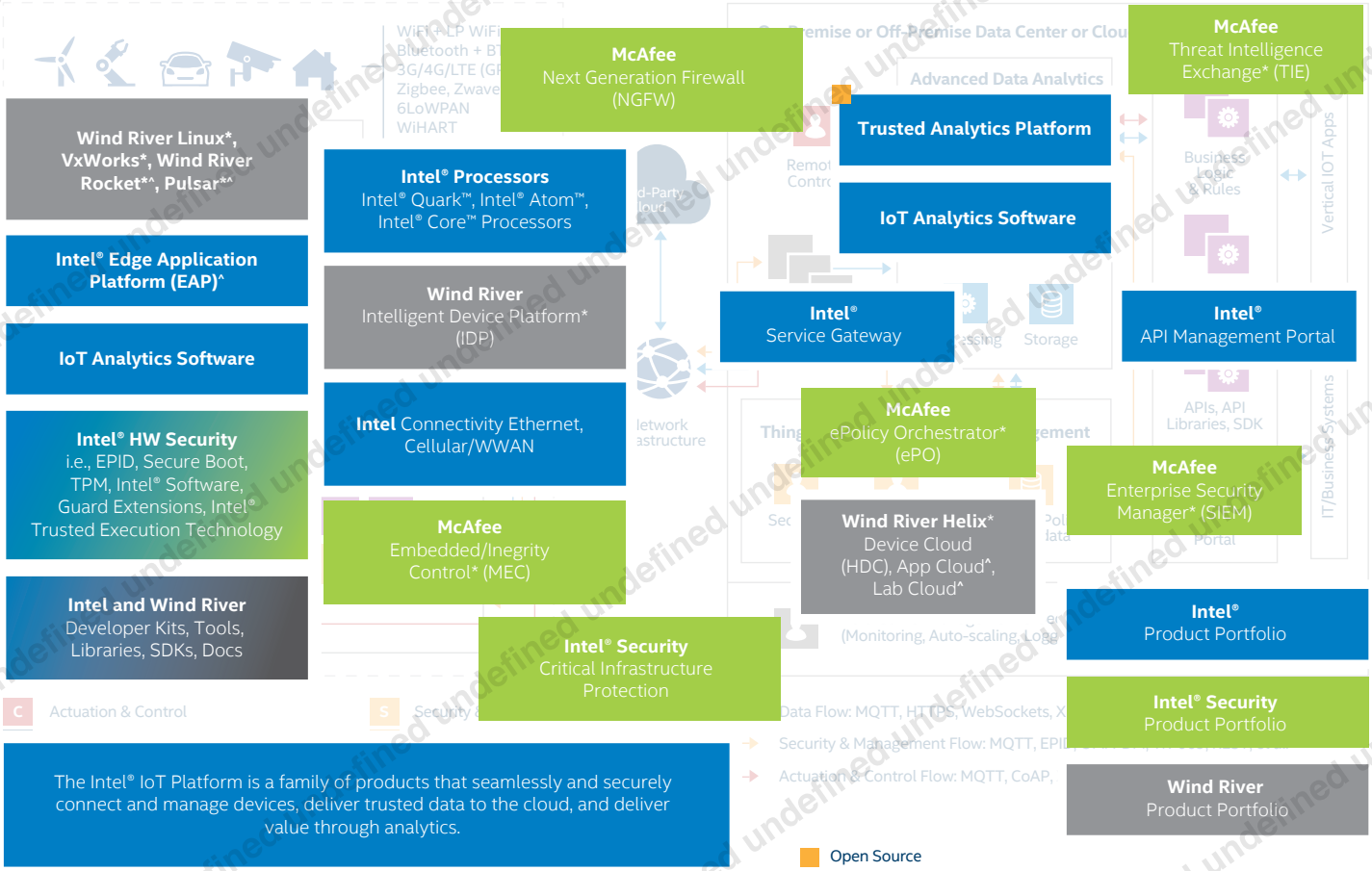

Figure 9. Building Blocks for Intel's IoT Reference Architecture

^Planned technologies for 2015-2016

Intel Building Blocks

Intel, McAfee, and Wind River have developed products that serve as IoT building blocks that developers can use to design end-to-end IoT solutions based on Intel's IoT reference architecture. The products, shown in Figure 9, are overlaid in Figure 3 and described briefly in the following.

Things

- **Wind River Linux***: Is the leading commercial embedded Linux platform and the first to bring the advantages of open source without the risks to companies in all industries.
- **Intel Hardware® Security**: Secures the platform at the hardware level with capabilities such as secure boot, Intel® Trusted Execution Technology, and trusted platform module.
- **Developer Resources**: Reduce design time with developer kits, tools, libraries, SDKs, and documentation.
- **Intel® Processors**: Provide unique performance scalability across Intel® Quark™ SoC, and Intel® Atom, Intel® Core™, and Intel® Xeon® processor families.
- **Intel® Quark™ SE SOC for IoT**: Contains Intel® Quark™ SE microcontrollers with pattern matching technologies that allow things to learn through pattern recognition and differentiate appropriate responses.
- **Wind River Rocket***: Is a tiny-footprint commercial-grade quality real-time operating system that connects directly to Wind River Helix Cloud* and is ideal for 32-bit MCUs, such as those used in small-footprint sensor hubs, wearables, and devices comprising the IoT edge.
- **Wind River Pulsar* Linux***: Is a small-footprint commercial-grade quality binary Linux* OS based on the Wind River Linux* distribution that connects directly to Wind River Helix Cloud.
- **Wind River Intelligent Device Platform XT***: Simplifies the development, integration, and deployment of IoT gateways with a customizable middleware development environment that provides security, connectivity, rich networking options, and device management.
- **Intel® Connectivity**: Supports various types of networks with interface devices for Ethernet, cellular, WWAN.
- **McAfee Integrity Control***: Performs monitoring, management, and tight security policy enforcement on edge devices.
- **McAfee Next-Generation Firewall**: Features built-in, active-active clustering that scales to 16 nodes.
- **Intel® Security Critical Infrastructure Protection**: Protects critical end-to-end infrastructure.

Network

- **Intel® Service Gateway**: Seamlessly connects edge devices to the cloud and secures their data flow.
- **McAfee ePolicy Orchestrator***: Eases the administration of distributed devices, helps automate security policy control, and simplifies compliance reporting.
- **Wind River Helix Device Cloud***: Collects and manages data from devices and machines to raise operational visibility and intelligence.
- **Trusted Analytics Platform**: Provides big data analytics on open-source Hadoop* and open-source OpenStack* for orchestration with private cloud or major public cloud providers.

Cloud

- **McAfee Threat Intelligence Exchange***: Optimizes threat prevention by narrowing the gap from malware encounter to containment from days, weeks, and months down to milliseconds.
- **McAfee Enterprise Security Manager* (SIEM)**: Delivers a real-time understanding of the world outside (e.g., threat data, reputation feeds, and vulnerability status).
- **Intel® API Management Portal**: Streamlines API access and control for organizations and developers.
- **Wind River Helix App Cloud***: Provides a cloud-based development environment for building IoT applications.
- **Wind River Helix Lab Cloud***: Includes a cloud-based virtual hardware lab for simulating and testing IoT devices and complex systems.

Secure, Scalable, and Interoperable IoT solutions

IoT solution developers and their customers need a secure and reliable IoT infrastructure, which is why Intel has defined key tenets to help ensure deployments satisfy critical requirements. Moreover, Intel's IoT reference architecture is available to help make IoT deployments more secure, scalable, and interoperable. Developers can obtain the system architecture specification for the reference design from their Intel representative.

Resources

Intel® Internet of Things Solutions Alliance

Members of the Intel® Internet of Things Solutions Alliance provide the hardware, software, firmware, tools, and systems integration that developers need to take a leading role in IoT.

Intel® IoT Gateway Development Kits

Intel® IoT Gateway Development Kits enable solution providers to quickly develop, prototype, and deploy intelligent gateways. Available for purchase from several vendors, the kits also maintain interoperability between new intelligent infrastructure and legacy systems, including sensors and data center servers.

To learn more about Intel solutions for the IoT, visit **intel.com/iot**.

1. IDC* forecast.
2. David McKinney, "Intel Champions Internet of Things Collaborations at IDF Shenzhen," April 23, 2015, https://blogs.intel.com/iot/2015/04/23/intel-champions-internet-of-things-collaborations-at-idf-shenzhen.

1115/SL/CMD/PDF ♻ Please Recycle 333452-001US