WHITE PAPER
FEBRUARY 2017

IT@INTEL

Horizontal IoT Platform Paves the Way to Enterprise IoT Success

Robert Colby
Wireless Sensor Architect, Intel IT

Paul Donohue
Systems Integrator, Intel IT

Steven J. Meyer
Sr. Principal Engineer, Intel IT

Ramchandra Patel
Network Engineer, Intel IT

Sunita P. Shenoy
Director of IoT Products, Smart Building Solutions, Intel IoT Group

Steve Willoughby
Sr. Information Security Specialist, Intel IT

Enterprise IoT is poised to generate USD 2 trillion in economic benefit by 2020.

Executive Overview

Internet of Things (IoT) solution providers will see enormous opportunities for enterprise IoT solutions in the coming years. By 2020, 25 billion enterprise-owned Internet-connected things across the globe stand to generate up to USD 2 trillion in economic benefit according to Gartner Research.[1] But these are not consumer devices, such as smartphones and PCs; enterprise-owned Internet-connected things include smart spaces, digital ceilings, smart lighting, and industrial equipment.

These opportunities for IoT solution providers come with significant challenges since enterprise IoT is much more complex than consumer IoT.

Intel IT, along with our internal partners, has implemented several IoT solutions in our offices and factories. We have experienced challenges associated with cost, organizational alignment, security, and changes to business processes.

We believe IoT standards that help enable a horizontal platform bring these benefits:

- **End-to-end integration.** A single enterprise IoT network reduces cost and complexity.
- **More solutions.** Suppliers designing to common standards bring products to market more quickly.
- **Improved security.** Clearly defined, standard security requirements across industries ensure important built-in security methods from the beginning.
- **Better quality.** Open standards increase peer review, which leads to higher quality solutions.
- **Lower cost.** With all IoT solutions coexisting on a single infrastructure, technology duplication is eliminated, increasing operational efficiency and decreasing total cost of ownership (TCO).

IT departments are in a unique position to lead the transition to open standards-based IoT, helping organizations reduce time to market, improve security, and align expectations with the company.

[1] gartner.com/smarterwithgartner/the-internet-of-things-and-the-enterprise

Contents

Acronyms

ACL	Access Control List
IoT	Internet of Things
OCF	Open Connectivity Foundation
OIC	Open Internet Consortium
OT	operational technology
ROI	return on investment
SaaS	software as a service
TCO	total cost of ownership
VLAN	virtual LAN

Background

Gartner Research expects the number of enterprise-owned Internet-connected things to reach 25 billion globally by 2020, generating nearly USD 2 trillion in economic benefit.[1] These are not consumer devices, such as smartphones and PCs, but dedicated enterprise objects, such as smart lights, temperature monitors, and industrial sensors. There is an enormous opportunity for Internet of Things (IoT) solution providers—an opportunity that brings with it significant challenges since developing and implementing enterprise IoT solutions is much more complex than consumer IoT.

Successful enterprise IoT solutions require a deeper understanding of infrastructure, security, integration, and interoperability than consumer IoT solutions.

Intel IT has worked with various Intel business-unit partners to implement several enterprise IoT solutions in our offices and factories. We faced challenges in the areas of cost, people, processes, and technology. What we have learned has helped us develop guidelines for having productive conversations with third-party IoT solution providers.

Here are three of our most important high-level insights:

- Initial costs make it difficult to justify investment.
- IoT changes existing business processes.
- IoT requires organizational alignment and common standards.

Initial Costs Make it Difficult to Justify Investment

Enterprise IoT solutions—which cost more than consumer solutions, especially in the initial investment—can potentially transform how business is done to promote operational efficiency and reduce long-term costs. These solutions are often implemented for specific use cases, creating information silos and duplicate infrastructure (see Figure 1).

[1] www.gartner.com/smarterwithgartner/the-internet-of-things-and-the-enterprise

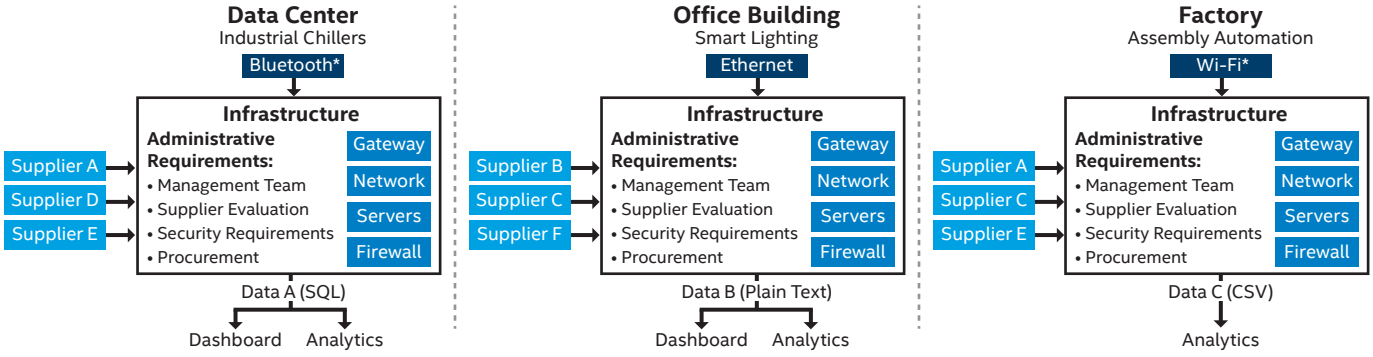
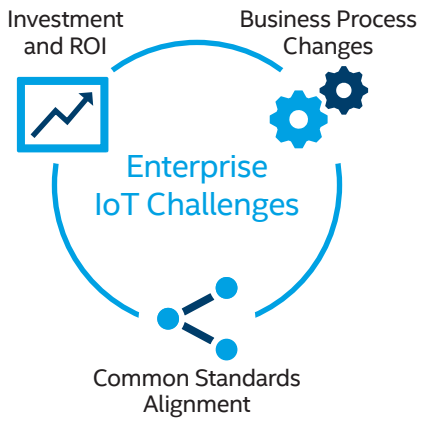


Figure 1. IoT solutions are often implemented in silos within the enterprise, duplicating technology and data management, which can ultimately increase the overall cost of the solution.



Cost concerns most often center on these areas:

- **High initial investment.** Enterprise IoT often requires costly investment in infrastructure that includes multiple products from a variety of suppliers.
- **Inefficiencies.** Siloed IoT implementations duplicate much of the infrastructure, increasing the overall cost and creating inefficiencies.
- **Return on investment (ROI).** Illustrating ROI can be difficult because cost savings derived from IoT implementations—such as improved product quality, reduced rework, and increased customer satisfaction and brand loyalty—do not always follow a straight, measurable path back to processes.

IoT Changes Existing Business Processes

Enterprise IoT often requires fundamental changes in business processes, and process changes impact people. Success of the overall implementation depends on meeting the following process challenges, which are sometimes overlooked in planning:

- **Ownership becomes collaborative.** Business units—such as Facilities Management Services, who deploy operational technology (OT) that manages equipment like lighting, heating, cooling, and ventilation—have not previously needed to work closely with IT regarding these assets. But when lighting and other equipment are connected to the Internet and begin collecting data that triggers other actions—such as turning off lights in vacant rooms or changing the temperature in sensitive manufacturing processes—the ownership lines between IT and Facilities Management become blurred.
- **Shifting process focus.** Where process automation was once relatively independent and designed around people, enterprise IoT solutions connect multiple complex processes to dynamic digital tasks. These tasks may be simple, such as notifying drivers of empty parking spaces through a smartphone app, or complex, such as sorting and routing millions of bags at a major airport.

IoT Requires Alignment and Common Standards

The technical challenges of enterprise IoT implementations often stem from the existence of multiple IoT solutions dedicated to separate use cases within one organization. For example, one IoT solution may monitor temperature-susceptible manufacturing processes while another may monitor occupancy-dependent lighting—with both solutions connecting to the same infrastructure. The variety of devices and solutions can cause implementation and process problems.

When multiple groups across the enterprise work with a variety of third-party IoT solution providers, we typically encounter difficulty in these two areas:

- **Lack of interoperability.** Many implementations lack interoperability; devices and equipment are made by different manufacturers and run on different systems. The lack of standards means that devices do not operate using the same communications specifications.
- **Failure to meet requirements.** Devices and equipment have varying requirements and capabilities. The diverse use cases of multiple IoT solutions within an enterprise can lead to mismatched requirements and capabilities, such as implementing nonsecure edge devices. These devices also may not be proxy-aware; may not operate with network segregation; may have proprietary interfaces; or may not meet standard, acceptable installation requirements.

Intel IT believes that the best way to overcome these challenges is to implement a horizontal platform, which will make it easier for OEMs and solution providers to connect and integrate in enterprise environments. A horizontal platform also requires consistent, open standards for end-to-end security rather than proprietary approaches.

Solution

Intel IT and many leading IoT solution providers recognize that enterprise IoT integration can be achieved when all parties involved adopt a standards-based approach—moving away from siloed solutions toward enterprise integration based on a horizontal architecture. A standards-based IoT solution requires strong IT leadership and a change in the way IT leaders think about IoT.

Open Standards and a Horizontal Architecture

Developing open standards leads to a horizontal architecture for IoT solution providers and device suppliers to build on. A standard, IoT industry-wide architecture leads to compatibility and end-to-end integration because solution providers, IT organizations, and device manufacturers can expect common requirements when developing and implementing solutions (see Figure 2).

The benefits include:

- **End-to-end integration.** Rather than approaching each IoT solution individually, all aspects of the enterprise IoT network—sensors, edge devices, wireless controllers, access points, switches, routers—can be tightly integrated, reducing duplication.
- **More solutions.** As new solutions become available, implementation is faster, more secure, and easier. Edge-device manufacturers adopt plug-and-play designs, and software providers can better meet data-related needs, such as normalization, analytics, and streaming.

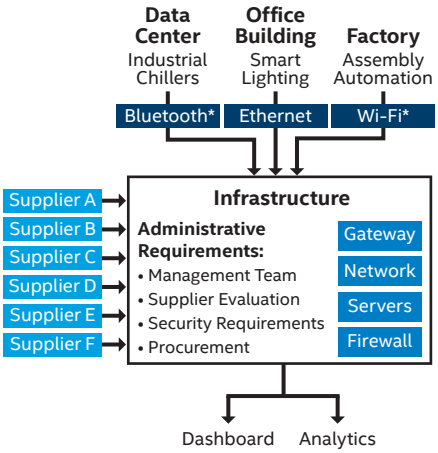


Figure 2. Investing in a horizontal architecture provides open connectivity, improved security, scalability, and flexibility.

- **Better privacy and security.** Rather than implementing multiple solutions with varying (and sometimes inconsistent or lacking) security expectations, standards-based IoT clearly defines requirements up front. Standardized IoT solutions and products require solution providers to adopt privacy-by-design and security-by-design processes as well as to collaborate with privacy and security professionals at each stage of the product lifecycle.
- **Higher quality.** With a single device-agnostic infrastructure that uses common protocols and messaging, silos are eliminated, new devices can connect more easily, and data integrity is improved. Open standards also result in increased peer review, which leads to higher quality solutions.
- **Lower cost.** When all IoT solutions coexist on a single infrastructure, duplicate equipment, policies, and data are eliminated, leading to increased operational efficiency and decreased total cost of ownership (TCO). A single platform also provides IT organizations with a more efficient, sustainable model.

IT organizations, in particular, are at the heart of enterprise IoT implementations and can help lead the transition to a standards-based horizontal architecture.

IT Leadership

To help with Intel's transition, Intel IT focused on integrating security and technology and on evaluating suppliers.

Security and Networking

To help our solution providers bring enterprise-ready products to market, Intel IT created the following requirements:

- **Use existing infrastructure.** Historically, enterprises have isolated IoT solutions on separate networks to mitigate security concerns. By defining strong security and system requirements up front, IoT solutions can use existing networks. Security can be managed by segregating applications within the same infrastructure—for example, using dedicated virtual LANs (VLANs) with Access Control Lists (ACLs).
- **Restrict Internet access.** Enterprises face numerous challenges which expose their IoT devices to the Internet. These include the vast number of IoT devices in use, network protocols that are often not properly authenticated or encrypted, lack of support for proxy servers, insecure IoT software update mechanisms, and the common problem of device passwords remaining set to manufacturers' default values. We bring solutions on-premises to eliminate direct Internet access to backend systems or the cloud when the data classification requires us to do so.

Platforms On-Premises or in the Public Cloud?

Enabling an enterprise Internet of Things (IoT) horizontal architecture includes defining clear standards for what applications and data are best to keep on-premises and what applications and data can be accessed from a cloud-based SaaS. As solutions evolve toward a blend of on-premises and public-cloud implementations, security concerns arise and IT organizations are faced with the task of coordinating workloads across technologies. To protect the integrity and security of intellectual property as well as to maintain customer privacy, we have found that we must develop clear guidelines and strategies for individual industries and solutions.

- **Flow data outward.** When using applications that cross the firewall, such as software as a service (SaaS), connections originate inside and flow outward as needed. For example, a dedicated port, such as 443, might be used for secure web service calls through the proxy. With varying levels of security on edge devices, such as cameras, it is important protect privacy.
- **Design for security and privacy.** Teams work together in the early phases to identify requirements: data encryption, secure provisioning through authenticated device IDs, privacy guidelines that exclude personally identifiable information, data collection without consent, and other areas of concern.

Evaluating Suppliers

Whether the supplier is an enterprise solution provider, a hardware or software developer, or a device manufacturer, it is important to understand how each supplier approaches business processes. For example, do they consistently maintain products over time and provide security patches when vulnerabilities arise? Intel IT evaluates every supplier, in part, on these areas:

- **Compatible sensors.** We look for suppliers with sensors that are compatible with horizontal IoT architecture. We created a technical working group that governs and standardizes the use of IoT sensors. This group also heavily focuses on standardizing wireless connectivity to mitigate radio interference, supportability, and plug-and-play infrastructure.
- **Open standards.** We seek software providers who have solutions that easily share data with other applications.
- **Scalability and manageability.** All suppliers, especially cloud-based SaaS providers, must be able to scale globally. It is important that the devices can be managed through the horizontal platform. If devices use proprietary gateways, we must segregate them to mitigate security risks. We also consider the continuity of the supplier's business, as well as their approach to change management, security, and privacy.
- **Security requirements.** We use the standard security requirements discussed in the Security and Networking section as requirements for suppliers.

Standards Are Defining the IoT Ecosystem

A horizontal Internet of Things (IoT) architecture improves consistency and security for enterprise IoT implementations, leading to easier, more affordable solutions. The following IoT standards organizations have emerged from consumer device usage, which has defined plug-and-play, to advance these goals:

- **Open Connectivity Foundation (OCF).** OCF, formerly the Open Interconnect Consortium (OIC), is an entity whose goal is to help unify IoT standards so solutions and devices can be developed to work seamlessly together. It unites the entirety of the OIC with companies from silicon, software, hardware, and finished-goods industries. With OCF specifications, protocols, and open source projects, a range of enterprise and embedded devices and sensors from a variety of manufacturers can securely and seamlessly interact with one another.
- **IoTivity.** The IoTivity project is sponsored by OCF to organize the open source community and accelerate the development of the frameworks, reference implementations, and services required to connect billions of IoT devices.
- **OIC Specifications.** The OIC Specification 1.1 includes detailed requirements for four primary implementation areas: core framework, security, smart-home devices, industrial devices, and resource types.

Integrating IoT into the Enterprise at Intel

In 2014 and 2015, Intel IT and Facilities Management deployed several IoT systems that gathered data from flow meters, fan- and motor-vibration monitors, temperature and humidity sensors, weight scales, and webcams using a variety of off-the-shelf analog and digital sensors. The collected data helps Intel employees more effectively monitor equipment performance, measure air temperatures, and gauge chemical-volume levels.

We experienced common challenges while integrating the technology into our existing infrastructure and processes. We also had challenges managing TCO, maintaining security, and providing scalability. From this experience we developed several standard processes for implementing IoT systems:

1. **Define the IoT system** based on customer needs and the process to be monitored.
2. **Classify sensor data** to determine how it will be managed, analyzed, secured, and stored.
3. **Design the network infrastructure** to operate seamlessly with current IT systems, facility operations, and business processes.
4. **Align with corporate data-governance policies** so that the access, use, and storage of the sensor data are properly regulated.
5. **Integrate and manage the IoT devices** using a method that will result in a reliable, efficient, secure, and repeatable system.
6. **Design the IoT system** to comply with privacy requirements that safeguard and protect personal and sensitive data.
7. **Establish a support model** that consistently and adequately maintains the IoT system.

We also deployed an IoT experience lab to install, test, and assess IoT solutions prior to the actual implementation. This allows us to identify issues early and better understand the costs associated with fixing them. For example, we might install a few light fixtures in the lab ahead of a planned office-floor upgrade to test the solution.

As a result of our processes, individual production areas collecting and using IoT data have seen increased efficiency and cost reductions. We also found that the IoT system can use fewer sensors and alert systems than previously to produce cost savings and benefits.

Intel® IoT Platform

The Intel® Internet of Things (Intel® IoT) Platform connects smart devices, taking advantage of many of Intel's core competencies, such as these:

- **Breadth and scale.** Intel's scalable silicon platforms—from Intel® Quark to Intel® Atom to Intel® Xeon processors—have compute, connectivity, and security built in to enable operational technology (OT) and IT systems integration.
- **Analytics.** Intel's high-performance processors can run compute-heavy analytics functions on a multitenant hardware platform.
- **Solutions.** Intel's world-renowned ecosystem of developers and solution providers is integral to developing an IoT industry-wide horizontal architecture.
- **Security and device management.** With Intel's security-focused software applications from trusted brands like McAfee® and Wind River*, IoT platforms, such as Intel® Building Management Platform (Intel® BMP), provide built-in security and manageability features from edge to cloud.

Conclusion

While enterprise IoT is vastly more complex than consumer IoT, there are huge opportunities for solution providers to meet the growing demand. Enterprise solutions require a deeper understanding of infrastructure, security, integration, and interoperability. Historically, enterprise implementations have resulted in information silos with duplicate infrastructure and management, making it difficult to justify the initial expense or illustrate sufficient ROI.

Intel IT has faced the challenges of cost justification as well as changes in business processes, an increased need for organizational alignment, and the need for different IT leadership. We believe that a horizontal platform along with strong IT leadership, will deliver a broader range of solutions, more secure implementations, end-to-end integration, and higher quality. As we deploy IoT in the enterprise, we anticipate that we will see reduced TCO in various areas. Using a standards-based approach, Intel IT is better able to integrate new capabilities into our standard IoT platform, and what once took months to connect can often be completed in a fraction of that time.

For more information on Intel IT best practices, visit **intel.com/IT**.

Receive objective and personalized advice from unbiased professionals at **advisors.intel.com**. Fill out a simple form and one of our experienced experts will contact you within 5 business days.

IT@Intel

We connect IT professionals with their IT peers inside Intel. Our IT department solves some of today's most demanding and complex technology issues, and we want to share these lessons directly with our fellow IT professionals in an open peer-to-peer forum.

Our goal is simple: improve efficiency throughout the organization and enhance the business value of IT investments.

Follow us and join the conversation:

- Twitter
- #IntelIT
- LinkedIn
- IT Center Community

Visit us today at **intel.com/IT** or contact your local Intel representative if you would like to learn more.

Related Content

If you liked this paper, you may also be interested in these IT@Intel White Papers:

- IoT Data Standards Provide the Foundation for Smart Buildings Paper
- Improving Manufacturing with Advanced Data Analytics Paper
- Integrating IoT Sensor Technology into the Enterprise Paper

Printed in USA Please Recycle 0217/JGLU/KC/PDF