WHITE PAPER
DECEMBER 2015

IT@INTEL

Integrating IoT Sensor Technology into the Enterprise

Kurt H. Gaiser
Senior IoT Software Engineer
Manufacturing IT, Intel IT

Vivian P. Harrington
Technical Marketing Engineer,
Quark Solutions Division, Intel IOTG

Gary T. Loughrin
Instrumentation & Control Engineer,
Corporate Services, Intel

Steven J. Meyer
Principal Engineer,
Manufacturing IT, Intel IT

Joe M. Sartini
Intel IT Industry Engagement Manager, EMEA,
Manufacturing IT, Intel IT

We believe that publishing our best practices can help other enterprises to integrate IoT sensor technology into their environments.

Executive Overview

Intel IT recognizes the potential of using IoT sensor technology to deliver business value to the enterprise. Sensors can put valuable data into the hands of manufacturing supervisors, environmental engineers, IT managers, and other decision makers to increase efficiencies and reduce operational costs.

At the same time, integrating the technology into existing infrastructures and work processes poses many challenges, such as managing total cost of ownership, maintaining security, and designing for scalability.

During the past few years, Intel IT has integrated several IoT sensor technology solutions into our enterprise. The data collected by these sensors helps our employees more effectively perform many tasks, including these:

- Monitoring equipment performance
- Measuring air temperatures
- Gauging chemical volume levels

While implementing the IoT solutions, we developed a set of best practices that help plan, design, and integrate this increasingly important technology. We believe that publishing our best practices can help other enterprises to integrate IoT sensor technology into their environments.

Contents

Contributor

Keith Ellis
IoT System Research Lab,
Intel Labs Europe

Acronyms

HIDs	Human Interface Devices
IoT	Internet of Things
PoC	proof of concept
ROI	return on investment
SCADA	supervisory control and data acquisition
SI	system integrator

Background

As the Internet of Things (IoT) expands and IoT solutions mature, integration of sensor technology into business environments is becoming commonplace. The proliferation of sensors, which plays a key role in the IoT expansion, continually provides new possibilities for solutions in our connected world. The IT department is often the logical place to collect and aggregate granular sensor data—temperature, air flow, humidity, power demand, and so on—into a practical representation of the physical environment.

The business benefits of integrating an IoT sensor system are as varied as the industries that deploy these systems. Sensors put valuable data into the hands of manufacturing supervisors, environmental engineers, IT managers, and other decision makers. For example, sensors can monitor cooling systems to enable more efficient operation and reduce energy costs, collect air samples to help maintain ideal environments, and detect variations in a motor's vibration to reduce failure.

Intel IT recognizes that data collected from IoT sensor technology can deliver business value to the enterprise. At the same time, we understand that integrating the technology into existing infrastructures and work processes can pose new challenges to manage total cost of ownership, maintain security, and design for scalability. We learned to overcome these challenges while integrating a variety of IoT solutions, from large-scale IoT systems to smaller projects that included just a few sensors.

Solution

Throughout 2014 and 2015, Intel IT and Intel Corporate Services deployed IoT systems and 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 sensor data helps Intel employees more effectively monitor equipment performance, measure air temperatures, and gauge chemical volume levels. As a result, these production areas have seen increases in efficiency and reductions in cost. Further, we found that the IoT system does not need to comprise hundreds of sensors and alert systems to bring cost savings and benefits. A simple sensor solution can have a big impact.

Based on our experiences—and the challenges that we encountered in the process—we developed 14 best practices to address while planning and implementing an IoT solution. This methodology will help streamline future implementations of IoT systems at Intel and can help guide other organizations that plan to integrate an IoT system.

We developed 14 best practices to address while planning and implementing an IoT solution.

1. **Build an IoT team** that directly contributes to the IoT system's definition and implementation.
2. **Define the IoT system** based on customer needs and the process to be monitored.
3. **Determine the business value** of the IoT system to validate the return on investment (ROI) and the expected benefit to the organization.
4. **Acquire stakeholder agreement and funding** before planning the integration.
5. **Classify the sensor data** to determine how it will be managed, analyzed, secured, and stored.
6. **Design the network infrastructure** to operate seamlessly with current IT systems, facility operations, and business processes.
7. **Review environmental conditions** to keep the IoT system free from potential hazards.
8. **Define space and electrical power needs** to accommodate the new IoT devices and sensors.
9. **Secure the IoT devices and data** to maintain their security and integrity, as well as the security and integrity of any other enterprise networks and systems.
10. **Align with corporate data governance policies** so that the access, use, and storage of the sensor data are properly regulated.
11. **Design for scalability** so that the IoT system can be efficiently expanded or repeated across multiple locations and facilities.
12. **Integrate and manage the IoT devices** using a methodology that will result in a reliable, efficient, secure, and repeatable system.
13. **Establish a support model** that consistently and adequately maintains the IoT system.
14. **Plan the resources** to install, sustain, and manage the IoT system.

The design and integration of an end-to-end IoT system (including sensors, edge devices, gateways, firmware, software, network, data storage, and analytics) require thorough planning and coordination between the development and support teams. A concerted effort helps build an IoT system that effectively delivers the desired business solution, meets data governance policies, and secures data throughout its life cycle.

Pre-Explore the Technology and Concept

To define an IoT system and plan its integration, we assembled an IoT project team, explored the customer's needs, and defined the data collection strategies.

Best Practice #1: Build an IoT Team

We recruited business stakeholders with skillsets that directly contributed to the system's definition and implementation. A typical IoT project team includes the following:

- **Customers** from the integration site who can define the business need, provide use-case criteria, and describe what data should be collected and presented.
- **An IT department representative** who can assist with network operations and network engineering to provide infrastructure; security requirements; and tools to store, analyze, and view the data.
- **A system integrator (SI),** solution developer, or other resources that have IoT and sensor experience. They use the customers' criteria to develop or integrate software and select the appropriate sensors that will collect and deliver the data in a format that will meet the customer's requirements and is compatible with the IT infrastructure and analytical tools.
- **A finance professional** to develop project budgets and validate the potential benefit of the project.
- **A project manager** to coordinate the overall project and confirm that all installs meet local construction, electrical, and other regulatory codes.
- **External advisors**—such as network providers, device manufacturers, and SIs—might also be required.

Because the IoT systems we integrated affected more than one Intel group, a large team of stakeholders was identified to be part of the IoT project team, which includes a group of core members and support personnel (see Table 1). Although the Intel IoT project teams can be large, some members contribute only a few hours to the project. Small- to mid-size organizations might have fewer IoT team members, with some of them taking on multiple roles.

Table 1. IoT Project Team Responsibilities at Intel IT

TEAM MEMBERS	RESPONSIBILITIES
Core members	• Provide use-case criteria for the systems on which the IoT system will be integrated. • Handle the gateway software development, OS configuration, and sensor integration. • Provide the data transport solutions. • Design the data storage solution. • Provide the data visualizations and alerting mechanisms for the customer.
Supporting members	• Confirm that proper LAN/WLAN coverage models exist for the implementation. • Prepare a budget and evaluate the potential benefit of the project. • Consult on power availability at the installation site. • Evaluate the intellectual property classification of the data, and assess and prescribe proper security mechanisms and data governance policies. • Create mounting components for the sensors and gateways. • Assist with the proliferation of the IoT system.

Best Practice #2: Define the IoT System

While planning the IoT system integrations at Intel, we let the customer's business needs define the systems and drive the sensor and data collection strategies. For example, if a customer needed to determine the chemical volume levels of a bottle, a scale or strain gauge sensor to measure the weight of the chemical bottle was deployed. If an alert was required to identify when a temperature differential existed between components, then the appropriate temperature sensors were installed.

Data Collection

Data collection strategies are driven by the following: customer needs, the process to be monitored or improved, hardware and infrastructure that are available in the environment surrounding the equipment, accuracy requirements, regulatory and code requirements, and ROI.

We consult with the customers regarding a sensor-collection/scanning rate that is optimal for data storage and retention levels. Data collection can be extremely fast, in the KHz range if necessary, for parameters like machine vibration or conveyor belt photo-cell monitoring. In other instances, interrupt-driven data collection is used where new data is sent only when a change occurs beyond a pre-defined threshold. Edge analytics can also be used to filter very high data samples to send alerts only on significant changes in the data. Even though it is possible to collect excessive amounts of data, we try to avoid doing so because we do not want to amass unnecessary data management costs.

Data Analysis

Our data analysis strategies are also based on customer needs. For example, we ask if the customer needs real-time notification of out-of-spec conditions? Do customers want to analyze the data over days, weeks, or months, or do they simply need a daily average? In our implementations, some data is averaged over recent scans and notifications are sent if threshold limits are exceeded. We also graphically display real-time values and capture the data in historical data logs for analysis.

Data Governance

It is important to establish policies and processes for governing (capturing, managing, storing, and securing) collected data to protect the business and meet legal obligations.

We only allow data access to essential users and delete the data when there is no longer a business need or legal retention requirement. To protect the sensor data—and learn which policies should govern how it will be collected and managed in the enterprise—we consult with a data governance manager.

Standards and Scalability

While defining how to collect and govern sensor data, we create architectural (software and hardware) guidelines and standards so that IoT project teams do not duplicate efforts in other integration projects. These are some examples:

- Create a standard for IoT gateway hardware that can be applied to other projects.
- Develop standard operating-system builds for the IoT gateways that cover several project possibilities and the required security protocols.
- Create a base layer of software on the devices, which enables data collection and transport across different IoT system implementations.

Explore the Project Feasibility and Value

Before an organization makes a capital budget decision, it weighs expected costs against the expected benefits. For example, we might consider implementing a fan-vibration sensor that notifies customers in real time when the vibration gets too high so that they can immediately shut down the equipment and prevent a possible catastrophic failure. Such an IoT system may improve safety and reduce equipment repair costs. Further, this solution can eliminate the need for staff to physically check vibration on a weekly or monthly basis, which also improves efficiency and reduces long-term costs.

Once we determine the IoT system will reduce costs and improve efficiency, stakeholder agreement and funding are approved.

The IoT system does not need to comprise hundreds of sensors and alert systems to bring cost savings and benefits. A simple sensor solution can have a big impact.

Best Practice #3: Determine the Business Value

To show the business value of this proposed IoT system, we would ask the IoT project team's finance professional to quantify (using cost-benefit analyses, net present value calculations, and so on) the IoT system's potential for reducing costs and enhancing efficiency. This kind of projection shows how Intel can benefit as a whole and helps align senior management with the business decision to move forward.

Best Practice #4: Acquire Stakeholder Agreement and Funding

While defining an IoT project budget at Intel, we develop funding levels that support phasing in the solution. We usually begin with a small-scale pilot project, expand to a wider implementation, and then deploy a large-scale rollout as the value of the technology is realized.

First, a finance professional develops budgets that include both capital implementation and long-term maintenance costs to show the total cost of ownership for each phase of the IoT system. We might use a net-present-value calculation to determine business value because it takes into account the time value of the investment.

Second, we vet the business value statement and ROI calculations with implementation experts to minimize the risk of making inappropriate or inaccurate assumptions.

Finally, after reviewing and approving the budgets, the IoT team seeks stakeholder agreement of the budget from senior managers, engineers, and operational managers before initiating the IoT integration.

Plan and Scope the Project

To plan and scope the IoT system, we classify the sensor data, design the network infrastructure and choose the IoT devices, review environmental conditions, and define space and electrical needs.

Best Practice #5: Classify the Sensor Data

At Intel, we assign three levels of importance (see Table 2) to the collected data that dictate how the data is managed, analyzed, secured, and retained. We establish security and encryption requirements and controls based on the business value (intellectual property). We also set privacy requirements for the data, including where it will be transported and stored—inside firewalls or into the cloud (see Best Practice #9: Secure the IoT Devices and Data).

Table 2. Collected Sensor Data: Levels of Importance

DATA TYPE	DESCRIPTION
Nice to have	Typically supplements existing data, is not used for process control, and will not impact business or operations if it is lost for a long time. This data type is used to increase efficiency or make tasks easier, but it is not required. Example: Air-temperature readings from a cafeteria
Could impact a process (or equipment), if lost	Needed to maintain normal operation of a process or a system. The loss of this data may eventually create some financial impact, loss of product, or shut down a process for a period of time. Example: Data indicating a vibration that, left unchecked, would disrupt a process or shorten the life span of equipment
Critical	Loss of this data may impact equipment or process control after a short time and could have financial impact. Generally, operations cannot maintain process control within limits or a business group cannot deliver its expected output without critical data. Example: A severe rise in air-sample measurements, indicating possible imminent equipment damage

Best Practice #6: Design the Network Infrastructure and Choose IoT Devices

Our goal is to design IoT systems that operate seamlessly with current IT systems, facility operations, and business processes. Further, the IoT systems should not adversely impact other network users.

Defining the IoT system's hardware and software requirements involves the entire IoT team. If the data being collected is for operations outside of the team's expertise, we recruit an expert to review the strategies and hardware/software specifications to confirm compatibility. For example, during the design phase of a recently integrated IoT system, we worked with experts to mock up data-transfer experiments to verify that the data could be transferred as planned. Early on, we discovered some security challenges. As a result, we adjusted both our data-transfer methods and the gateway software to improve efficiency and security.

IoT Devices

Determining how many gateways and sensors/actuators to install relates directly to the number of systems that need monitoring and the existing infrastructure. If only a few network drops, electrical outlets, or circuits exist in an area, the number of devices that can be installed might be limited. However, if the data being collected is critical, network drops and electrical outlets can be added to increase data-collection reliability.

When choosing IoT devices, we consider these points:

- **Gateways.** We base the selection on the use-case criteria and understand the network, physical environment, sensor and equipment interfaces, device and data security considerations, performance, and power requirements. For example, if the IoT system will use a serial communications protocol, then the chosen gateway needs to accommodate that protocol.
- **Sensors.** We base the selection on accuracy requirements, data type (digital or analog), power needs, communication method (wired and/or wireless), protocol, physical size, mounting location, and material compatibility with the process to be scanned or monitored.

To date, Intel IT has found that USB-interfaced sensors are well suited for IoT deployments because they are robust and have simple plug-and-play interfaces. Using readily available USB libraries on the gateway (combined with a multiport USB hub), we can attach multiple sensors to a single gateway device. In one IoT system, a driver library on the gateway enabled us to seamlessly connect USB sensors as Human Interface Devices (HIDs). This enabled us to deploy common software that can read and process the data values from the sensor. Although these USB-interfaced sensors cost more than others (for example, the I2C or analog sensors), we believe they justify the extra cost. In addition to using USB sensor technology, there are also a variety of off-the-shelf analog and digital sensors available that will work equally as well with Intel® IoT gateways. We have also explored the use of wireless sensors (802.11, 802.15.4 [ZigBee or 6LoWPAN], Bluetooth* LE, and cellular), which have advantages in hard-to-reach areas, as well as locations further from the nearest gateway than can be easily managed with wired sensors. For wireless sensors, additional power and/or battery requirements as well as connection and protocol details need to be considered.

Network

Network connectivity is a foundational element across the system (Figure 1). To confirm that the existing network will support the IoT system, we review the following questions:

- For LAN installations, are there enough network ports/drops?
- For Wi-Fi* installations (802.11x), will the IoT system interfere with mission-critical equipment? Will the scalability, bandwidth, and IP range of the Wi-Fi network support the IoT devices? And depending on the criticality of the data, does the existing network infrastructure need to be updated or augmented if its Wi-Fi coverage cannot currently accommodate the IoT devices?

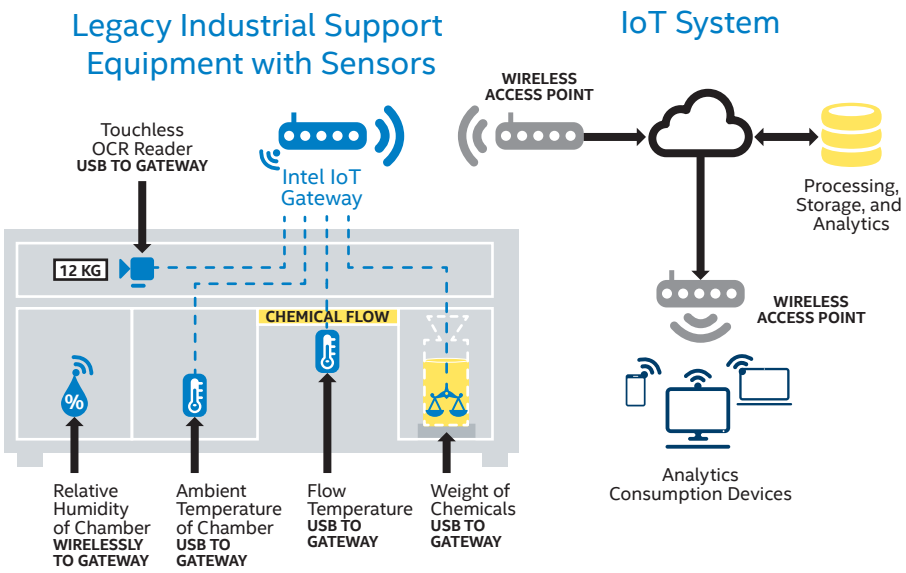

Figure 1. An example of a legacy industrial equipment cabinet with an integrated IoT system that includes sensors, gateways, access points, storage devices, and analysis devices. This flexible design provides easy data access and helps ensure that the existing network will support the IoT system.

Share:

Intel® IoT Platform Solutions

The Intel® IoT platform is an end-to-end reference model and family of products.[1]

Intel® IoT gateway[2]

The Intel IoT gateway is a critical component within this framework and the result of collaboration with Intel® Security and Wind River. Intel IoT gateways connect legacy and new systems to enable seamless and secure data flow between edge devices (sensors and actuators) and the cloud through preintegrated, prevalidated hardware and software building blocks. Intel IoT gateways offer a choice of Intel® processors for different application needs, support for multiple operating systems (Wind River and Ubuntu Linux*, Microsoft Windows* 10, etc.), and robust device management capabilities. The Intel IoT gateways also include Intel Security with whitelisting, secure boot, and deep-packet inspection features.

Intel® Quark™ microcontrollers

Microcontrollers (MCUs) are general-purpose computing/IO devices at the low end of the compute spectrum. Intel® Quark™ microcontrollers D1000 and D2000 are the first products to extend the Intel IoT capabilities to the deep edge. A software development kit supports application and product development on these devices. Additional information is available at www.intel.com/quark/mcu.

[1] See www.intel.com/content/www/us/en/internet-of-things/iot-platform.html for detailed explanation and video by Brian McCarson about the components of this framework and their interaction.

[2] See intel.com/content/www/us/en/embedded/solutions/iot-gateway/overview.html for details on the Intel IoT gateways.

- What type of traffic flow will occur (outbound data only, inbound command/control, or both)? We use this information to plan how the data and devices will be secured (Best Practice #9: Secure the IoT Devices and Data) and managed (Best Practice #12: Integrate and Manage the IoT Devices).
- Is it necessary to integrate the IoT system on a network that is separate from mission-critical or office networks? (We use a software-defined network designed specifically for IoT devices.)

We find it is best to invest in a company-wide network architecture to accommodate IoT devices. Intel IT is investing in the infrastructure in three phases: getting the correct network to the available deployment of wireless access points; optimizing the placement of access points to obtain a minimum low-density coverage layout in deployment areas; and establishing a gateway-management service inside IT that will procure, secure, patch, and manage IoT gateway devices with proper network-access provisioning.

Data Communication Protocols

An IoT system can use one of two communication protocols:

- **Open-standard protocols** use internationally accepted standard protocols and published APIs. Examples of these protocols include SIP (Sessions Initiation Protocol), SOAP (Simple Object Access Protocol), MQTT (Message Queuing Telemetry Transport), HTTP, and FTP. These protocols use TCP/IP at the transport level. They typically allow data to be transferred within common infrastructures, such as supervisory control and data acquisition (SCADA) systems, cloud locations, big data platforms, custom data shares, and historical data-logging databases. Further, these protocols allow users to select the analytical tools they prefer.
- **Proprietary protocols** (also called closed or private protocols) require users to install and use a specific vendor's hardware, sensors, tools, network types, data storage, and analytical tools. Hardware and software developed by other vendors may not function with proprietary protocols.

In our experience, open-standard protocols simplify the IoT integration effort, keep costs low, and facilitate future scalability.

Best Practice #7: Review Environmental Conditions

To keep the IoT system free from potential hazards in the environment—and keep customers safe—we address the following issues when relevant:

- Install interior sensor devices in locations that meet operational requirements (heat/cold thresholds, humidity, temperature fluctuations, static electricity).
- Consider properly protecting exterior sensor devices from weather elements, theft, and incidental damage.
- Consider the process to be monitored and verify that the sensor materials are compatible or can withstand the environment in which they will be placed. For example, if the sensor is monitoring an acidic chemical, confirm that it is designed to do so.
- Confirm that the IoT devices will be clear of other planned installs and located in places where they cannot be damaged.
- Watch for other potential hazards:
  - Place sensors and gateways away from areas that may become wet or flooded due to condensation, liquid leaks, rain, or overflows.
  - Protect electrical wiring from physical damage, liquids, or chemicals.

IoT Device Checklist

- **Assess device power needs**
- **Consider type of power required**
- **Check network's power**
- **Verify space requirements**
- **Consider electrical noise**
- **Evaluate impact of power outage**

Best Practice #8: Define Space and Electrical Power Needs

The IoT system will put additional demands on an environment and network. To safely accommodate the new IoT devices—and data they generate—we use the following checklist:

- Assess the possible need for adequate electrical power at each IoT data-collection location. (Note that some sensors require their own power sources.)
- Consider the type of power required. If the data is considered "nice to have," then normal power will suffice; however, if the data is critical to a process, system, or business group, then an uninterrupted power supply (UPS) may be more appropriate.
- Check the network's electrical power to determine whether upgrades or new installation will be necessary.
- Verify that the installation environment has the necessary space for mounting the IoT devices; confirm that sufficient space exists for maintenance or future replacement.
- Consider the electrical noise in the area; high electrical noise may interfere with wireless communications.
- Evaluate the impact of a power outage and how to recover from it. Determine whether a localized outage would impact multiple IoT devices and if they can automatically recover.

Develop and Deploy the IoT System

During this last phase, we define the security requirements, develop a data privacy plan, design the system for scalability, integrate the IoT devices, establish a support model, obtain financial commitment, and define how the IoT system will be maintained.

Best Practice #9: Secure the IoT Devices and Data

Because an IoT system can potentially expand the perimeter of an enterprise's attack surface, defense-in-depth security is essential to protect the devices, networks, and the integrity of the sensor data.

Network and IoT Device Security

While defining the security requirements, we complete the following tasks related to the network and the IoT devices:

- Use a directory services account and wireless LAN-access authentication servers (for example, RADIUS) to manage device network access.
- Develop a patching process.
- Centrally manage and audit the endpoint access logs, which includes installing virus scanning and a hardware-intrusion protection system on endpoints and/or gateways.
- Deploy an Integrity Management Architecture to ensure integrity of software on remote gateways.

- Secure the IoT devices with password and authentication measures. The local IT group can provide minimum requirements.
- Manage the IoT devices through a remote management system, with managed access controls and auditing that align with the data classifications set in Best Practice #5: Classify the Sensor Data.
- Limit access to IoT gateways solely to administrators who have appropriate control mechanisms in place. We use "least privilege" methodologies for interactive log-ons to the device over protocol connections like Secure Shell.
- Provision devices as out-of-band so that they require a separate security process outside of the normal data-access path.
- Disable unnecessary access services and ports (for example, HTTP, TELNET, and FTP) on IoT gateways.
- Use endpoint and data-source authentication to check that the data comes from known sources.
- Avoid storing credentials on removable media.

Data Security

While defining the security requirements, we complete the following tasks related to data security:

- Choose the type of data storage based on the nature of the database use (transactional vs. nontransactional) as well as the amount (big data or small data) and type (structured or unstructured) of data being collected.
- Establish a need-to-know access methodology and security policy for the data based on its classification. Employees who need the data can access it through a secure system, and those who do not need the data will not have access.
- Depending on where the data will be transported and stored (inside firewalls or into the cloud) and the intellectual property value and/or privacy requirements, we establish the encryption required for the data.
- To reduce data transportation and storage burden, we perform analytics/data filtering and processing at the edge (gateways). For example, the Wind River Edge Management System[3] enables customers to aggregate data at the edge.

Best Practice #10: Align with Privacy and Corporate Governance Policies

Most privacy policies focus on who accesses the data, how it is stored, how it is being used, and the retention period. For example, if a sensor is attached to a person (for example, on a name badge), it may identify the individual and his or her workplace behavior. This potentially raises several privacy and labor-law concerns. In some jurisdictions, workplace monitoring must be reviewed by the Works Council (or a similar organization that represents employees' rights) and can be implemented only after accepting the specific practices.

Intel requires that a privacy plan be developed and approved before deploying new workplace monitoring activities. Planned sensor implementations might need to be reviewed with the privacy, HR, and legal staffs. Additionally, organizations typically have data-governance models that cover policies and regulatory compliance of their enterprise data. We consult with the data-governance manager to verify that the established classification and security levels of the sensor data meet the policy requirements.

[3] See www.windriver.com/products/product-overviews/wind-river_edge-management-system_product-overview.pdf

Best Practice #11: Design for Scalability

It is important to understand the potential scalability of the IoT system. How many devices could end up on similar equipment or across other types of use cases? How will the organization support those devices?

We design the IoT infrastructure so that it can efficiently scale across multiple facilities. This means adhering to industry standards and using a "copy exactly" principle to make a scalable model for hundreds—or thousands—of gateways across the enterprise. (This practice is similar to copy-exactly methodologies used when deploying laptops, desktops, and mobile devices across our enterprise.) The fewer differences between the devices, the easier they will be to support.

Other benefits gained from standardizing the hardware, software, and communication protocols include a lower bill of materials, decreased need for support staff, reduced negative impact on customers over time, reduced mean time to repair, and less time spent provisioning new devices.

Best Practice #12: Integrate and Manage the IoT Devices

Our IoT team develops an integration and management methodology that will result in a reliable, efficient, secure, and repeatable IoT system.

Deploy in Phases

Early on, we implement positive-business-value IoT systems that are low risk and not mission-critical to daily operations. Example starter projects might include installing sensors to detect whether lights need to be shut off or the temperature adjusted. After integrating a relatively simple IoT system—and confirming its success—the team is better prepared to proceed with integrating a higher-end IoT system.

To avoid scope expansion, we built a business-value roadmap (Figure 2) with small, quick succession deployments. Similarly, we aim to integrate IoT systems gradually at a crawl-walk-run cadence:

- **Crawl.** As a proof of concept (PoC), we install a small set of devices to verify the idea and feasibility, and test connections. Because this PoC install is experimental, a full-fledged support model is not required.
- **Walk.** We integrate the PoC into a local site or environment, make improvements to the initial design, and develop a production version for deployment to several areas. This includes hardening the code, integrating remote-management software, documenting procedures, developing a support model, and adding web-based analytics.
- **Run.** We deploy the full IoT system at many sites or locations. This includes making incremental improvements, integrating a long-term support model, and updating the database to support scalability.

Figure 2. Intel IT uses a roadmap while planning, designing, and integrating IoT systems. This method helps us streamline future implementations of IoT systems and can guide other organizations that plan to do the same.

Integrate the IoT Devices

While determining where and how to integrate the IoT system devices, we use the checklist in Figure 3. Although this list is not all-inclusive, it offers basic points to review before plotting the integration.

After determining how to integrate the IoT devices, we establish a secure method to route and deliver sensor data. We base the method on how customers will use the data by learning how they use currently collected data and determining what their ideal delivery state is for the new sensor data.

For example, we consider the need for personnel to monitor chemical levels in industrial-equipment cabinets. To learn how they collect and use the data, we observe users as they collect, record, and archive the data. We note how the customers interact with the equipment and their monitoring frequency, and ask them how often they might check chemical levels if unlimited resources were available. We also observe how customers consumed the data and how they determined when to replenish a chemical based on the collected data. Finally, we review how the overall process could be improved if the data-collection process were streamlined with an IoT sensor system.

If data will be analyzed after delivery, we select the format in which it will be delivered: SQL, CSV, or HTML, for example. (Web pages and statistical analytic programs can provide visual analytics of the data, if desired.) With data that will trigger threshold or change-detection alerts, we need to provide the associated message text and how the alert should be sent. Examples of alert delivery methods include text-messaging, email, SCADA screen, or an audible alert.

Manage the IoT Devices

The fleet of IoT devices and software that constitute the IoT system need to be maintained. It is important to determine what skillsets and resources are needed to make OS upgrades, install security patches, repair sensor failures, and monitor gateway health to check for issues such as loss of sensor or Wi-Fi connection. (For large organizations, we sought help from an existing network support team, adding "IoT device support" as a new service of that team.)

To manage the devices, either third-party remote management software can be used or internal skilled resources can build a dashboard. We currently use a variety of solutions—from home-grown tools to vendor solutions to custom scripting—and plan to standardize our IoT management efforts using Wind River Helix* Device Cloud. Custom management agents or Intel® Security IoT management tools are additional options.

Sensor Integration Checklist

- ☐ Choose the sensor connection to the IoT gateway: wired (USB, I2C, analog) or wireless (ZigBee, Bluetooth* LE, cellular).
- ☐ Choose the IoT gateway connection to the data center: wired (Ethernet) or wireless (Zigbee, Wi-Fi*, 3G).
- ☐ Determine that the network, gateways, database, and servers can support the sensor data throughput.
- ☐ Establish the minimum-security network requirements.
- ☐ Decide where the sensor data will be routed.
- ☐ Decide whether the sensor data will cause an automatic action to occur in the environment or will simply be monitored and analyzed for possible human response.
- ☐ If capturing digital images, determine where the video or still images will be sent, who will see them, how privacy will be maintained, and how the video or images will be monitored or recorded (local vs. remote).

Figure 3. The sensor integration checklist provides basic review points to plan the integration. The list helps to determine where and how to integrate the IoT system devices.

Finally, we perform these maintenance-related tasks:

- Create a list of peer contacts from support organizations, the cloud provider, and device suppliers for assistance with maintenance issues; we formalize these engagements with service-level agreements.
- Develop backup IoT devices.
- Compile a list of alternate suppliers for key IoT system components.
- Define the upgrade path to manage hardware end-of-life.
- Maintain and back up any software configurations and/or customized software or scripts in an appropriate software management system and repository.

Best Practice #13: Establish a Support Model

To reliably benefit its customers, the IoT system requires an effective support model. Intel IT integrated the following support levels in its service-management-support structure:

- **Level 1 (touch) support.** Touch services handle initial gateway provisioning as well as the physical installation and replacement (quick swaps) of failed units. Trouble tickets are handled by the call center, and procedures are defined via knowledge articles created by second- and third-level support.
- **Level 2 (diagnostic) support.** Using centralized management tools for connection and troubleshooting, the client-management group provides diagnostic services.
- **Level 3 (sustaining) support.** The engineering team that designs and implements the integrated solution performs sustaining support.

This multilevel support model is effective with large-scale deployments that have the potential for high call volumes. For small- to mid-sized organizations, all levels of support might be performed by one or two groups, depending on available resources.

Best Practice #14: Plan the Resources

To determine who will purchase the IoT system components (sensors, gateways, software, network upgrades, monitoring dashboard program, and so on), we align with senior management and obtain financial commitment for the budget. These funds may come from the IT department or from the business unit that requires the IoT solution.

We then decide how much support the IoT team will need to integrate and maintain the system. If sufficient internal resources exist, the team determines who will perform the installation, debug, test, and maintenance tasks.

How Intel IT Monitors Industrial Consumables

In our chemical monitoring IoT use case, we do the following:

- Collect data from a scale measuring the weight of bottles to determine the volumes of remaining chemical.
- Provide web-based analytics with that data to help the equipment owners forecast when chemicals must be replenished.
- If chemical levels reach threshold levels, the system generates a text-message alert to support personnel so that they can intervene before the equipment is impacted.

The Global Impact of IoT

On a local level, Intel has realized the business value of the IoT after it deployed well-planned sensor systems. From a broader perspective, once sensor technology integrations reach global proportions, it is predicted that the economic impact will be unprecedented.

In June 2015, McKinsey & Company[4] reported on their analysis of 150 IoT use cases to determine the IoT's potential benefits. Those use cases ranged from personal health-monitoring devices to manufacturers that use sensors to optimize equipment maintenance. They estimate that the IoT has a total potential economic impact of USD 3.9 trillion to about USD 11.1 trillion per year by 2025. At the top end, that financial value would equal about 11 percent of the world's economy. Specifically, industrial and manufacturing environments make up most of that global value.

[4] Manyika, James. "Unlocking the Potential of the Internet of Things." McKinsey & Company: Insights and Publications, June 2015.

If internal resources are not available for the project, a reputable system integrator (SI) who can either assist with part of the integration or provide a complete turn-key solution can be retained by the IoT team. An SI that has experience working with the desired technologies and implementation methodologies is important. Also, reviewing examples of successful IoT projects that the SI built on Intel® technologies is helpful in choosing an SI.

Conclusion

Through our IoT integration efforts, Intel has realized productivity benefits and cost savings. Our goal is to achieve even higher increases in productivity, cost savings, and security as we integrate future IoT systems. At Intel IT, we formalized a set of best practices to follow while integrating an IoT system into the enterprise. We believe that by publishing these best practices, other enterprises will find it easier to integrate IoT sensor technology into their environments.

For more information on Intel IT best practices, visit **www.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

Visit **intel.com/IT** to find content on related topics:

- The Intel® IoT Platform: Secure, Scalable, Interoperable Intel site
- Exploring the Internet of Things in the Enterprise paper
- Harnessing the Power of IoT brief
- Joining IoT with Advanced Data Analytics to Improve Manufacturing Results paper

Printed in USA. Please Recycle. 1215/JGLU/KC/PDF