WHITE PAPER

Logistics and Asset Management
Intel IoT

Intel® Connected Logistics Platform (ICLP) Solution Architecture: Securely Transforming Data to Action

Solution providers use Intel and Microsoft Azure* IoT to gain a competitive advantage in edge-to-cloud integration and deliver key customer insights with faster time to market

Authors

Savitha Gandikota
Intel Corporation

Nandakishor Basavanthappa
Microsoft Corporation

Contents

Background

The target audience of this document is both end users and solution providers who are interested in next-level details for implementing a scalable logistics Internet of Things (IoT) solution from Intel and Microsoft.

The implementation overview section provides details of the Intel® Connected Logistics Platform (ICLP), which is based on Microsoft Azure and aligned with the Microsoft Reference Architecture 2.1. This document builds on the foundational principles and architecture subsystems detailed in the Microsoft Reference Architecture to provide a basic implementation of ICLP, which system integrators can use to customize and scale while meeting customer requirements gathering insights using the data sent by IoT devices, and developing applications to take necessary actions. It also features control and data flows, device onboarding and management, and operations associated with domain-specific insights.

The Intel Connected Logistics Platform (ICLP) is a pre-certified and ready-to-deploy track & trace solution. Through the use of IoT Sensors, Gateways, and a proprietary Wireless Sensor Network (WSN), ICLP enables near real time condition and location monitoring of freight across the supply chain.

Companies can use this data to mitigate risk, perform trend analytics, and automate decision-making in the supply chain. Further, with the insights and freight tracking granularity that ICLP provides, companies can also improve their operational efficiencies and reduce supply chain cost.

The Intel Connected Logistics Platform provides system integrators with a ready-to-deploy, scalable, edge-to-cloud infrastructure that enables them to securely connect and analyze end-to-end logistics data through the Azure Cloud.

Executive Summary

To maintain a competitive advantage, organizations no longer have the option of operating “things” in silos. Connecting, capturing, and analyzing data improves business insights, and the Internet of Things has become critical for business success. A fully integrated edge-to-cloud solution will allow businesses to consolidate their process data, eliminate duplicate infrastructure, and reduce security risks. Working with ecosystem partners to deploy proven end-to-end solutions will reduce complexity and achieve faster time to market than with a customized solution. Furthermore, the insights gained through analytics can help businesses expand their product portfolios and empower them to create new opportunities.

Whether it is to improve industrial efficiencies, track inventory, monitor business performance, or predict maintenance needs in real time, using a well-defined IoT solution accelerator that is built on established platforms can streamline the process of authenticating devices, supporting standard and custom protocols, and establishing reliable communication between billions of IoT devices and the cloud. Such an IoT solution can provide real-time analytics capabilities that companies can use to transform their businesses.

Built on a strong and longstanding partnership, Intel and Microsoft* are continuing to extend their comprehensive solutions portfolio to provide mature offerings to the IoT industry. Their combined solutions enable IoT developers and ecosystem partners, including original equipment manufacturers (OEMs), independent software vendors (ISVs), and system integrators (SI), to create differentiated, scalable and efficient vertical solutions. With a joint-reference implementation built on the Intel edge platform and Microsoft Azure, IoT solution providers will be able to seamlessly integrate sensors with their domain-specific cloud applications, using device management, edge analytics, standard security, and data-cleansing application programming interfaces (APIs).

The Intel Connected Logistics Platform (ICLP) and Microsoft Azure joint solution architecture serves as an example and provides a holistic approach for connecting devices to the cloud, gathering data, and effectively analyzing the data to create actionable insights.

Introduction

The Internet of Things is ready to go mainstream and will no longer be confined to early adopters. An expected 25 billion enterprise-owned things are expected to be connected by 2020, potentially generating up to USD$2 trillion in economic benefit globally.[1] While some pieces of the edge-to-cloud solution puzzle exist, putting them all together in a reliable way to enable a customer to sell a differentiated product can be a complex task.

The Intel Connected Logistics Platform provides system integrators with a ready-to-deploy, scalable, edge-to-cloud infrastructure that enables them to securely connect and analyze end-to-end logistics data through the Azure Cloud.

With the global logistics market alone expected to register a compound annual growth rate (CAGR) of 3.48 percent from 2016 to 2022, and to reach a market size of about USD$12.2 billion by 2022, the challenges and opportunities are unmistakable.[2] The market challenge is global and covers damaged, lost, stolen, and delayed shipments, and the challenge is even more profound when it comes to perishable items. Roughly one-third of global fresh fruits and vegetables are thrown away, because their quality has dropped below an acceptable limit before they reach their destination.[3] Losses in the pharmaceuticals business account for more than USD$35 billion per annum, strictly related to temperature excursions, with about 30 percent of those losses attributed to logistics issues alone.[4]

IoT implementation challenges can be multifaceted. Although using previously collected data to gain insights is the primary goal, technical challenges may arise when an organization tries to implement a secured, scalable solution that is specific to vertical use cases. The challenge does not end there, however, because the multiple implementations still need interoperability between devices and equipment from independent manufacturers. Building an IoT solution on a strong infrastructure that has the ability to quickly integrate devices from edge to cloud, and using pre-validated solutions, can reduce the risk to any organization that is trying to transform itself to gain a competitive edge.

An integrated, pre-validated, flexible, and robust platform from Intel and Microsoft can help simplify implementation and enable organizations to deploy their IoT solutions at a faster rate. Azure solution accelerators developed using Microsoft Reference Architecture 2.0 provide solutions to quickly address specific scenarios and business needs. One such example is the Intel Connected Logistics Platform on Azure. A solution originally built to solve Intel's own challenge of tracking high-value assets, ICLP is now being deployed to the entire shipping industry. Please refer to Figure 2 for a high level view of Intel Connected Logistics Platform on Azure.

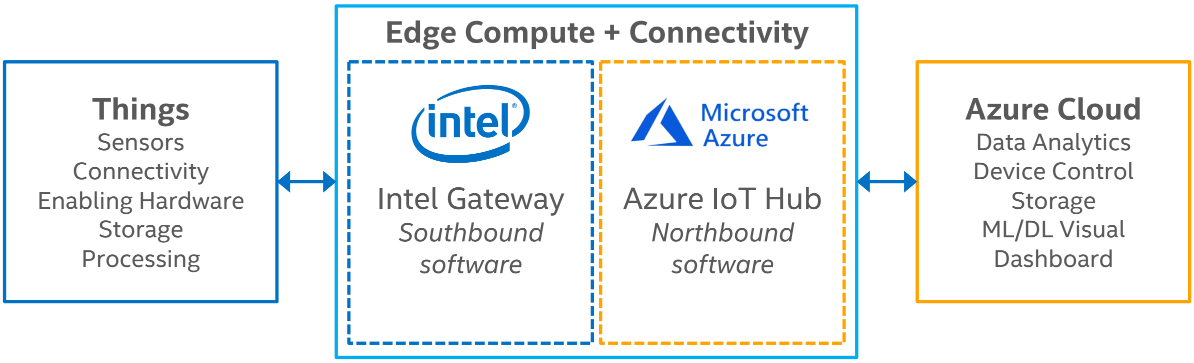

Figure 1: Edge-to-Cloud flow

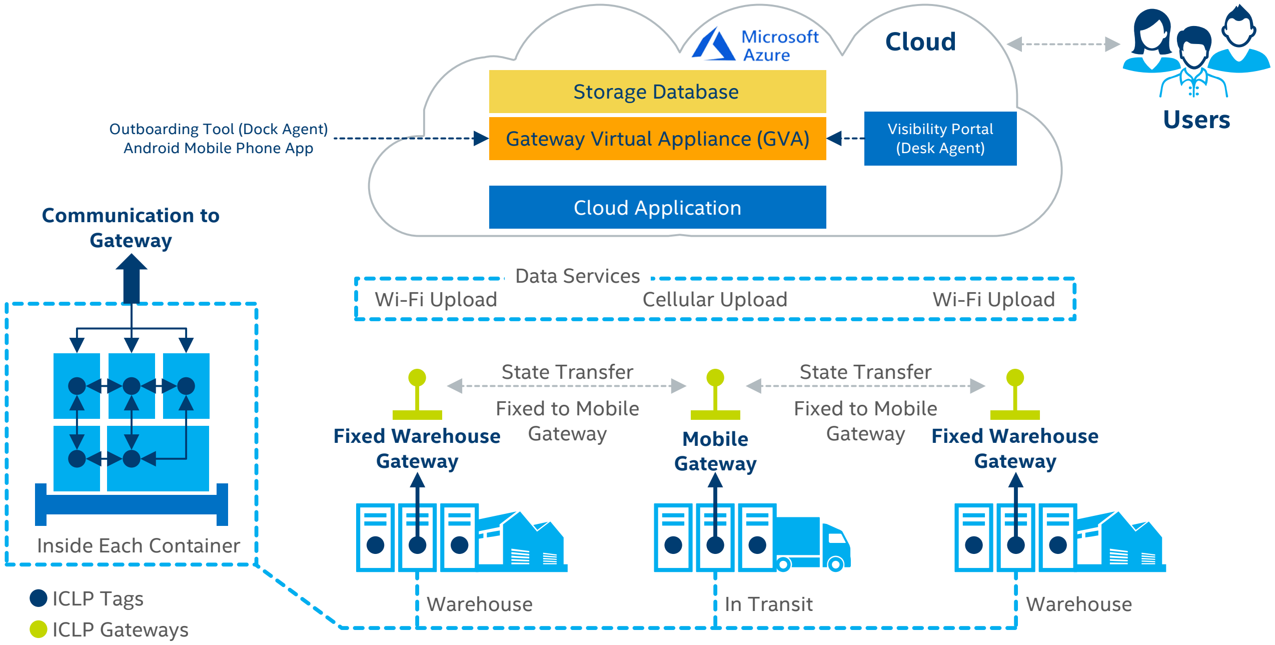

Figure 2: Intel® Connected Logistics Platform (high level view)

Benefits

Together, the Intel IoT and Microsoft Azure joint reference implementation seamlessly transmits data from sensors, actuators, and other endpoint devices to the Azure cloud. It provides the structure to use preconfigured, pre-validated components to generate a scalable solution. A clearly defined standard reference implementation, which details edge, network, and cloud components, provides the following:

- **Collect and control data and devices seamlessly.** Standards-based reference implementation will improve visibility and makes it easier for seamless data ingestion and device control from edge to cloud.
- **Power at the edge.** Intel-powered gateways and devices with Azure IoT Device SDK software extends the power of the cloud to the edge.
- **Cost effectiveness.** Helps control costs by offering the ability to track an individual package or a large volume of assets, and low-cost sensors provide an option to eliminate reverse logistics.
- **Built to scale.** Robust and ready to scale to keep pace with demand, and built to support multiple IoT implementations.
- **Easy device onboarding.** Zero touch onboarding of devices at power-on, and simplified bulk provisioning with Azure IoT Hub, improve security.
- **Manage devices.** Monitor device status, modify device access, and apply over-the-air updates with IoT Hub.
- **Domain-specific insights.** Azure Stream Analytics and Azure ML will provide critical insights to help organizations make informed business decisions and open the door to new opportunities.
- **Wide range of application services.** Azure IoT Service SDKs and App Services support development on many platforms for building applications that directly interact with an IoT solution.

IoT Solution Development

The first step in developing a joint solution involves understanding the building blocks needed to assemble the solution. These include both hardware and software components at the edge as well as in the cloud. The Intel edge platform and the Microsoft Azure IoT solution accelerators each provide capabilities and benefits that help IoT developers, OEMs, ISVs, and SIs develop industry-standard, seamless solutions. This section covers some of the Intel and Microsoft IoT components used for building a logistics solution. Figure 3 illustrates how these components work together.

Intel IoT Components	
Edge components	**Hardware components.** The Gateway (GW) and ICLP sensors (sometimes referred to as tags). The GW is a general edge compute device with either Intel® Atom®, Core™ or Xeon® processors. The second component is the ICLP sensor hardware that contains the detecting functions needed to track the condition parameters. The GW collects the data from the sensors and provides the local intelligence to run edge analytics. The GW also provides the cloud connectivity for Azure IoT Hub. **Intel hardware-based security technologies.** Hardware-level security on the platform through Secure Boot, Trusted Execution Environment (TEE), and Intel® Enhanced Privacy Identifier (Intel® EPID).
Device and security management	**Sensor protocol adapters.** These are southbound protocols to connect to ICLP sensors and include management of Sensor Data, Communications, Status, Device Security, Device Diagnostics, Device Monitoring, and Functional Safety. This layer includes peer-to-peer (P2P) protocols.
Device and security management	**Onboarding Tool (OBT).** The Onboarding Tool can be initiated using an Android device equipped with NFC (Near Field Communication). This device mediates the shipping creation process between the GW and the cloud. On the Gateway, it uses GW APIs to provision hardware profiles (GW Network IDs, Sensor Thresholds, etc.) and initiates the shipment creation/completion process. Additionally, on the Gateway end, it retrieves the information related to the sensor devices (Sensor UUID, GW UUID, Sensor Network IDs, and Sensor/GW battery levels) and passes them on to the cloud. On the cloud end, it uses shipping APIs to (a) retrieve the information necessary to provision the GW, and (b) transfer the information retrieved from the GW and Sensor Devices to the cloud after verifying the necessary credentials, where the cloud binds this information to the shipping IDs and stores the complete information in a database. **Enhanced services.** Security Abstraction Layer APIs covering Secure Data, Secure Transport, Secure Discovery, Secure Provisioning, Secure ID, Secure Log, and Crypto. The Secure Data API is the protection of data at rest and in use by enforcing security policies defined by the data creator. Data can be provisioned locally or remotely. The Secure Transport API establishes a direct channel via mutual authentication, with client credentials protected by hardware. The Secure Discovery API allows remote backend to determine the security capabilities available on devices. The Secure Provisioning API enables devices to provision secrets, data or policies locally or from a remote backend, and performs device attestation as part of the provisioning process. The Secure ID API will provision and use identity secret credentials for remote authentication. The Secure Log API generates a protected log. The Crypto API abstracts crypto usages for non-expert developers and enables the innovation of security services that are not provided by this set of Security Abstraction Layer APIs.
Device Software	**Feature/Capabilities as a Service Module.** This layer will help with metering the gateway hardware (HW). It includes call-home capabilities for provisioning, and “on-the-fly” turbo boosts and HW scaling with back-end integration for billing. **Data Hub and Cleansing APIs.** Data Hub can provide libraries for data cleansing, and basic data services for aggregation, normalization and filtering. Data Poisoning is a critical issue in IoT, and this layer can host the business logic to defend against that. This layer can be tapped to provide Data-as-a-Service (DaaS) as well. The Intel® Data Analytics Acceleration Library (Intel® DAAL) is the library of Intel Architecture optimized building blocks that cover all stages of data analytics: data acquisition from a data source; preprocessing; transformation; data mining; modeling; validation; and decision making. To achieve best performance on a range of Intel® processors, Intel DAAL uses optimized algorithms from the Intel® Math Kernel Library and Intel® Integrated Performance Primitives. **Events, Notification, Mgmt. Engine.** This layer is responsible for detecting, extracting, and tagging the incoming sensor data. It responds to commands and uploads the data appropriately.

(continued on next page)

(continued from previous page)

Azure Components

Azure IoT Hub. Establishes bi-directional communication with billions of IoT devices. Customers can rely on Azure IoT Hub to easily and securely connect their IoT assets. It offers device-to-cloud telemetry data to help customers understand the state of their IoT devices and assets, and enables them to be ready to take action when an IoT device needs attention. In cloud-to-device messages, it reliably sends commands and notifications to connected devices and tracks message delivery with acknowledgement receipts. Device messages are sent in a durable way to accommodate intermittently connected devices.

Azure IoT Edge. Enables hybrid cloud and IoT solutions through a fully managed service that delivers cloud intelligence at the edge.

Azure Stream Analytics. Provides seamless integration of stream analytics with Azure IoT Hub and Azure IoT solution accelerators to enable powerful real-time analytics on data from IoT devices and applications.

Azure Event Hub. A hyperscale telemetry ingestion service that collects, transforms, and stores millions of events. As a distributed streaming platform, it provides low latency and configurable time retention, which enables customers to ingress massive amounts of telemetry into the cloud and read the data from multiple applications using publish-subscribe semantics.

Azure Machine Learning. Enables customers to deploy machine learning models into production as a web service in minutes.

Azure Logic Apps. Enables customers to connect business-critical apps and services with Azure Logic Apps, automating workflows without writing a single line of code.

Azure Container Service. Eliminates the complicated planning and deployment of fully orchestrated containerized applications with Kubernetes. It enables quick provision clusters to be up and running in no time, while simplifying monitoring and cluster management through auto upgrades and a built-in operations console.

Azure Cosmos DB. A globally distributed, multi-model database. With the click of a button, Azure Cosmos DB enables elastic scale throughput and storage across any number of Azure's geographic regions.

Azure Web Apps. A service for hosting web applications, REST APIs, and mobile back ends.

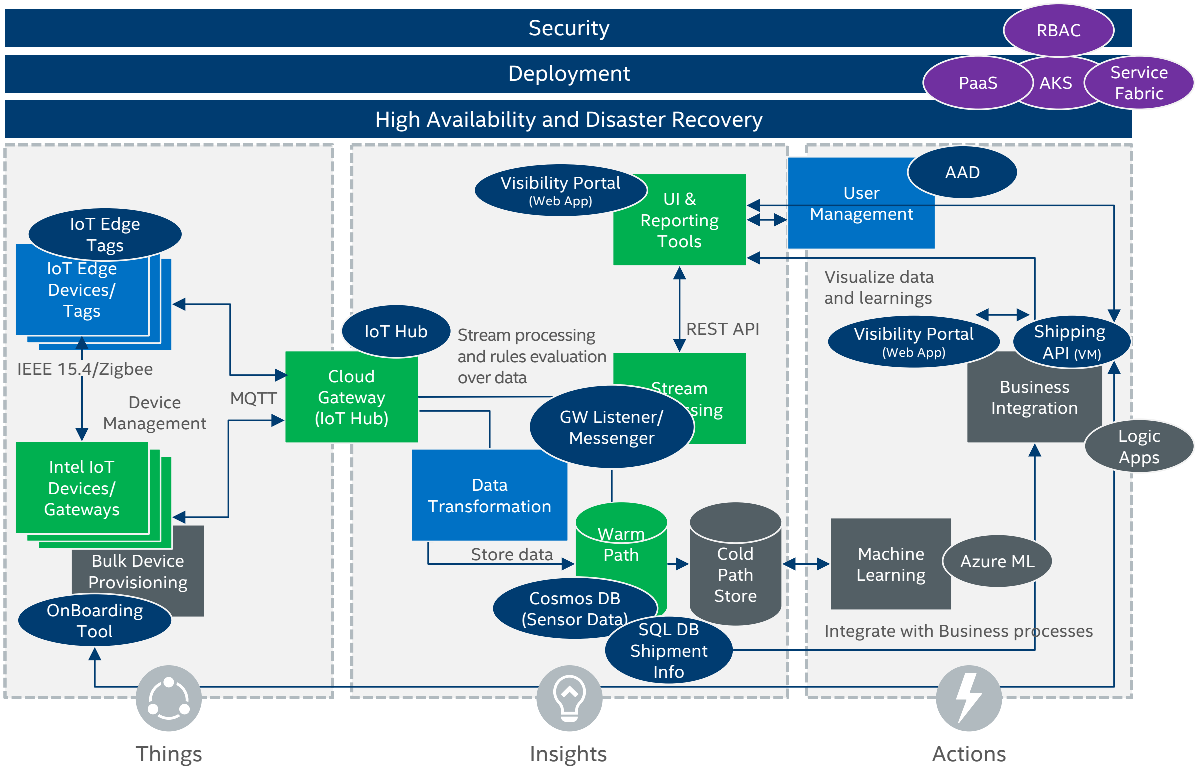

Figure 3: The joint Intel® and Microsoft* reference implementation makes deploying an end-to-end Internet of Things solution easy, with a focus on security at every layer

Implementation Overview

The Intel Connected Logistics Platform is an asset tracking logistics platform that uses a combination of a Gateway and Tags to provide near real-time visibility into location, condition and security of packages at the Cloud. The Temperature, Humidity, Light, Accelerometer, Pressure sensors inside both Gateways/Tags. The Tags communicate to the GW, while the GW communicates to the Azure Cloud at (pre-configured) regular intervals.

The Onboarding Tool is an Android device with an Android application in conjunction with the Gateway to facilitate the customer's workflow at the warehouse.

Figure 3 describes the Intel Connected Logistics Platform and Microsoft Azure IoT joint reference implementation across various domains and shows the connection of edge devices to the Azure cloud. In this implementation, the Gateway is treated as a single device to which sensors report. It uses Azure IoT Device SDK software in the GW domain to connect and communicate with the IoT Hub in the cloud domain, where the data can be further processed for predictive analytics. The edge software filters the sensor data, performs necessary analytics, and packages it securely before forwarding it to the cloud connector. Users also have to option to directly send the encrypted sensor data to the cloud where it can be decrypted and processed. While the joint reference implementation points out the art of the possible, the final solution will depend on the vertical use case and the needs of the end user. It is assumed that additional hardware and software will be added, based on the application. The architecture also assumes the availability of sensor drivers and additional software for sensor integration for the specific vertical market.

Appendix A demonstrates the significant benefits provided by this architecture for a connected logistics use case. Although this architecture is agnostic to the GW operating system (OS), an implementation of the Intel IoT Gateway stack is provided for the Android* OS. The GW can be treated as a single device on Azure's IoT Hub, and as such will connect to the cloud through an Android application and the Azure IoT Device SDK. The GW for this use case will be Wi-Fi capable to connect to the cloud as well as other gateways. Using the Intel Gateway stack, devices can perform device management, collect sensor data, and filter/analyze this data locally, relying on the cloud to relay status messages for events and data synchronization. Note that even though this reference implementation has been implemented as a PaaS offering, systems integrators have a choice to implement a Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS) solution specific to customer requirements. By using Azure IoT Central, customer will be able to utilize a fully managed global SaaS solution that makes it easy to connect, monitor, and manage IoT assets at scale.

A quick Edge-to-Azure connectivity can be achieved with onboarding and system flow steps.

System Flow

The following section describes the steps involved with the system flow, and is illustrated in Figure 4.

1. Create initial shipment request, which includes source and destinations, thresholds, alerts, etc. (done by the desk agent).
2. Download the shipping information from Step 1 to the OBT (done by the dock worker).

ICLP Reference Implementation using Microsoft Reference Architecture 2.0 – All Subsystems and Cross-Cutting needs

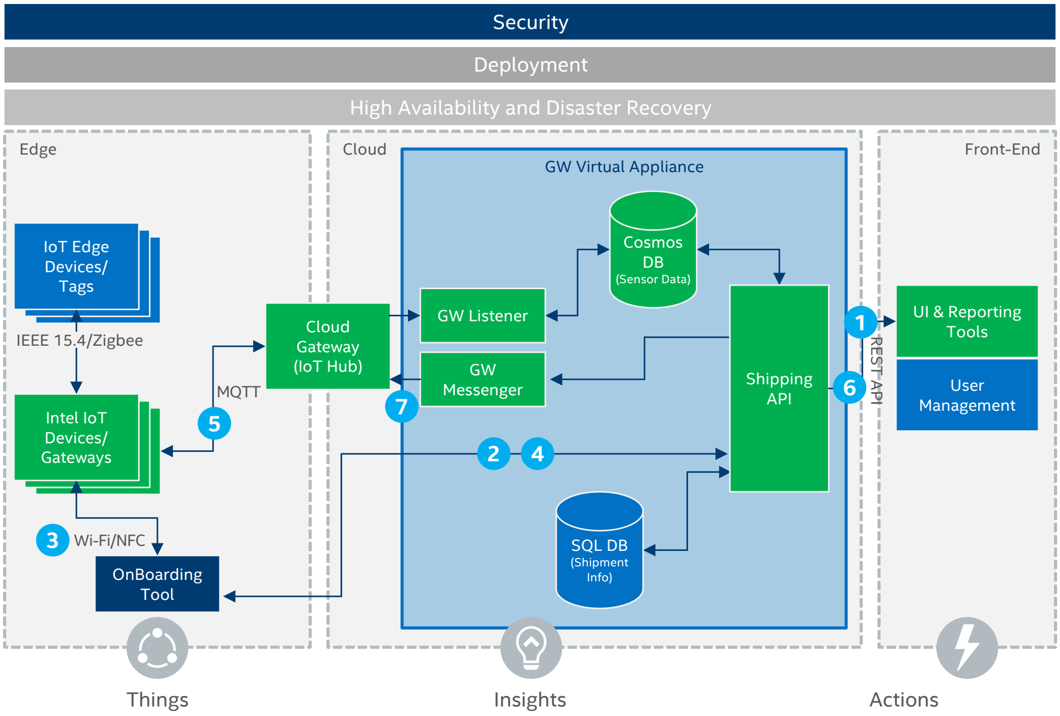

Figure 4: The Intel® IoT Platform and Microsoft Azure* joint reference implementation details the connections for seamless device onboarding and ownership privacy.

3. Associate sensors, Gateway, Shipment ID); pass on threshold values to the Gateway (done by the dock worker).
4. Make it an active shipment after successful provisioning (done by the dock worker).
5. Transmit sensor data (autonomously via cellular).
6. Get sensor data to the dashboard.
7. Receive shipment. Active shipment is closed by Visibility Portal user.

Pre-Provisioning the Gateway Devices

- The original design manufacturer (ODM) uses an Intel toolkit to create a Global Unique Identifier (GUID) and installs it into the device (either Gateway or sensor) as a QR Codes Label. This universally unique identifier (UUID) can also be retrieved programmatically by running the UUID-creation program.
- Each device is installed with its public/private key-pair in a secured storage area. Each UUID is associated with the private key and a corresponding certificate signed by the Device Signing Authority. The user of a device with a known UUID can verify the device by searching its public key, and then validating the public key using a signed certificate.
- The purchaser of the GW imports the device UUIDs into Azure's IoT identity registry to associate the GW device with their account. The owner then receives a connection string using the secured provisioning process, which allows the GW to connect and communicate with the cloud upon completion of the shipment-creation process.
- The purchaser of the sensors, or tags, pre-register the device UUIDs into Sensor Device Management Services to prevent spurious, unaccounted or unverifiable devices from participating in the shipping process.
- A data path is established between the GW device (UUID) and the Azure IoT Hub. The Gateway Virtual Appliance (GVA) subscribes to the Azure IoT Hub and directs messages to the Microsoft Azure IoT solution accelerator after extracting and validating the sensor-specific data from the GW message.

The joint reference implementation points out the art of the possible. The final solution can be created to serve the vertical use case and end-user needs.

On-Boarding the Gateway Devices

- The GW is provisioned for shipment using the OBT to install the necessary attributes required for the GW to become operational and construct a wireless sensor network.
- Sensors are onboarded to the GW through an NFC sequence that involves data exchange between sensors and the GW.
- The Onboarding Tool receives the GW and sensor-specific data (GW UUID, Sensor UUID) programmatically, using GW APIs and verifying these IDs by scanning the QR codes and reading the tracking numbers before sending them to the cloud using the shipping APIs.
- Once the hardware and tracking data are received by the cloud (via the OBT), they are associated with the shipment (in progress) and stored in the SQL database using the data abstraction layer (DAL). Upon completion of the onboarding process, this specific shipment moves into the monitoring phase. Preconfigured sensors that are related to this shipment are activated and associated with the completed shipment. Any data received from these sensors in the cloud, via Gateway Messages to the Azure IoT Hub, will be allowed to pass to the Microsoft Azure IoT solution accelerator by the GVA after the messages are validated.

Collecting and Integrating Data

- Business applications on the GW acquire data from connected sensors through a number of supported protocols.
- Intel edge software aggregates sensor data and performs analytics on it to determine when certain thresholds are breached. The data is then marked with an anomaly tag and triggers an event specific to the vertical application.
- The GW sends messages containing data and important event information to the Azure cloud. The data is intercepted by the GVA and dispatched to various endpoints (after data and sensor source verification) to give notifications and perform data analysis.
- Managing Devices and Software Updates
- Application software managers modify a device's access or can trigger a software update through the provisioning API.
- The provisioning API makes changes to the device twin, informing the device through the cloud gateway that an update is ready.
- The device recognizes a change in its twin, which invokes a direct method to apply the software update.

End-to-End Security

Keeping the sensor data secured is critical to any IoT solution. While the Intel Gateway comes with built-in hardware security, with Root of Trust and secure boot and update, additional edge software will authenticate as well as encrypt data at appropriate node points to transport it securely to the cloud. This will include industry-standard symmetric (HMAC) and asymmetric (ECDSA) methods. All keys will be stored in a secured location.

Summary

By implementing IoT solutions using Intel and Microsoft Azure IoT solution accelerators, industries can fully manage devices and establish bi-directional communications between millions of devices and the cloud to gain insights that will enable them to grow their business and go-to-market quickly. The joint reference implementation:

- Provides a method to extensively monitor IoT devices.
- Captures data in a reliable and secured way.
- Streams and analyzes data to meet business needs.
- Provides tools to scale and develop cutting-edge applications.
- Explore Partner Solution Accelerators on the www.azureiotsolutions.com/accelerators web portal or click here to try ICLP now.

Find the solution that is right for your organization. Contact your Intel representative or visit intel.com/iot.

Learn More

You may also find the following resources useful:

- Intel ® Connected Logistics Platform
- Intel IoT Gateway Technology
- Intel IoT Solutions
- Intel® Connected Logistics Platform animation
- Intel Distribution of OpenVINO™ Toolkit
- Intel® IoT RFP Ready Kits

Learn more about Microsoft's offerings:

- Azure* Internet of Things (IoT)
- Azure* IoT Reference Architecture
- Azure* IoT Solution Accelerators
- Azure* Cloud Computing Platform & Services
- Azure* IoT Central

Appendix A:
Logistics and Asset Management Use Case (Proof of Concept (PoC) with Curry & Co.)

Any business that manages a complex supply chain suffers from a lack of visibility as to where their valuable assets are at any given time. Industry experts estimate that cargo thefts are responsible for up to $30 billion in losses each year.[5] Thieves are also becoming smarter, targeting food, beverages, and pharmaceuticals—cargo that is typically expensive, difficult to track, and very sensitive to the environment in which they are being stored and transported.[6] A solution that allows businesses to monitor the location and status of valuable or perishable goods in real-time can transform how assets are managed, tracked, and secured through logistics. The Intel IoT and Microsoft Azure IoT asset-management solution is shown in Figure A1 and detailed in Table A1.

Intel's supply chain team worked with Oregon blueberry distributor Curry & Co., using blockchain technology to help the company improve its supply chain and delivering a farm-to-fork solution through ICLP. The POC involved tracking one truck of blueberries from harvest in the field to the customer distribution center, over a 72 hour time period (please refer to Figure A2 for all the steps). Three key parameters—temperature, location (using GPS), and humidity—were monitored throughout the entire journey.

Challenges in food tracking:

- Path to the GW is limited due to moisture content of the fruit and positioning of the sensor relative to the pallets and facility layout.
- Sensors should be food grade quality and must be placed in plastic jackets for food safety.
- Once picked, fruit begins to ripen quickly, and overripe berries are prone to damage and disease.

The sensor dashboard recorded all of these parameters and generated alerts about the temperature and humidity of the berries being transported.

Intel worked with Curry & Co. to employ an integrated blockchain-based IoT solution to help the company solve several business problems related to its supply chain and product distribution. This proof-of-concept project was the first time that blockchain technology was used to track a shipment of berries and provide visibility about the location and condition of the fruit and how it was handled, thus setting the stage for increased trust with consumers by meeting a higher level of food safety.

Blockchain is a distributed ledger technology that has the potential to transform the way enterprises, governments, and consumers exchange data. By eliminating the need for a central authority, blockchain technology simplifies transactions, mitigates transaction risk, and increases efficiency and transparency. The technology is based on an open source, fully distributed network, enabling pure peer-to-peer communication. Transactional information is stored in a publicly distributed ledger, which is arranged in blocks. Each block is then connected (chained) to the previous block and has a cryptographic signature that is dependent on all the previous blocks.

There are many benefits to using blockchain in a perishable goods supply chain, including:

- **Provenance:** stronger assurance of the origin and chain of custody of blueberries throughout the supply chain, which in turn reinforces brand reputation
- **Food Safety:** allows for near real-time monitoring of fruit, leading to a more proactive approach in terms of safety, quality and recalls while minimizing food waste
- **Distributed Ledger:** transforms manual recordkeeping to digital and establishes a trustworthy exchange of data across supply-chain partners. The blockchain acts as a record of financial transactions, events, or even environmental data capture.
- **Security:** Blockchain technology ensures that data cannot be tampered with or modified.
- **Supply Chain Network Optimization:** better visibility into the supply chain network might allow companies to improve their

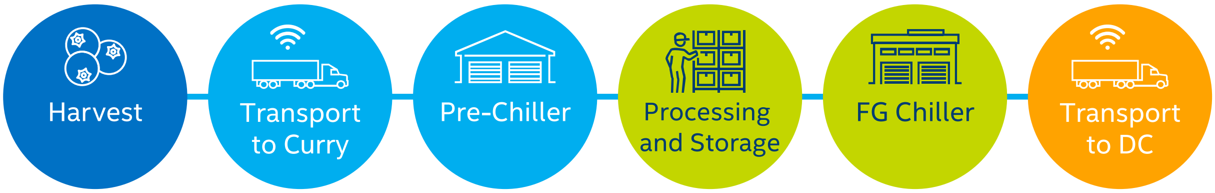

Figure A1. As demonstrated by the Curry & Co. blockchain- and IoT-based supply-chain proof-of-concept project, the Intel® IoT Platform and Microsoft Azure IoT joint reference implementation provides visibility into the location and status of perishable goods — blueberries — while they are in transit, helping businesses reduce losses and deliver more products to market in good condition.

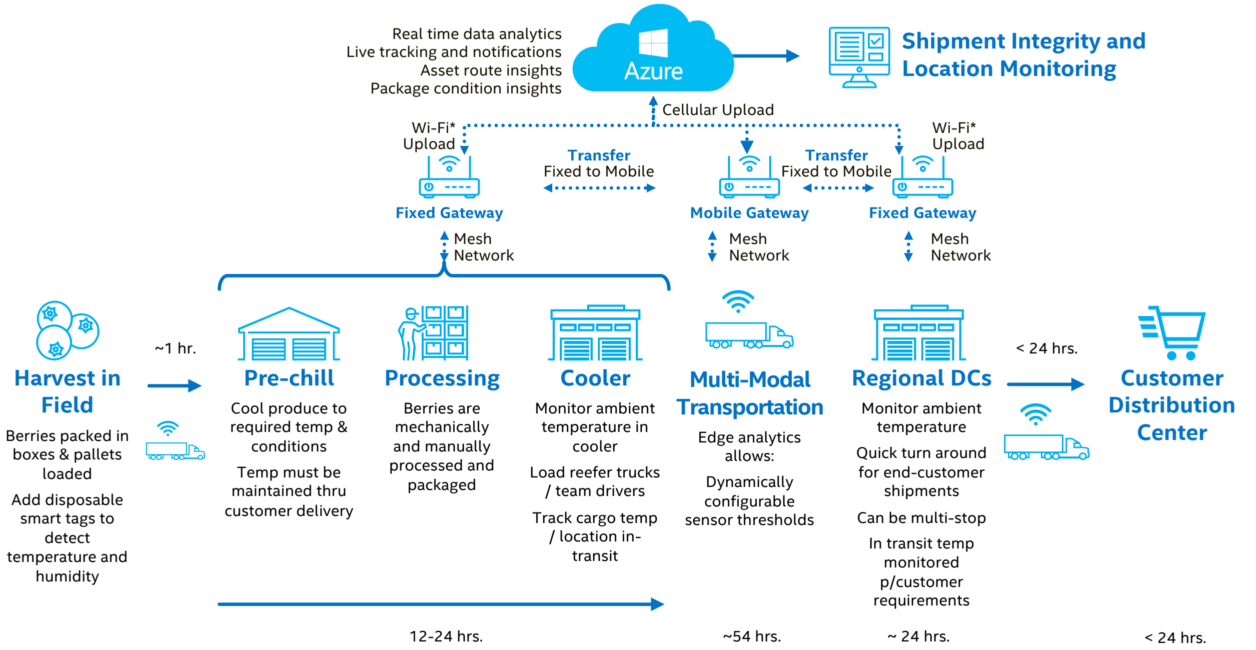
Real time data analytics
Live tracking and notifications
Asset route insights
Package condition insights
Azure
Shipment Integrity and Location Monitoring
Cellular Upload
Wi-Fi* Upload
Transfer
Fixed to Mobile
Transfer
Fixed to Mobile
Wi-Fi* Upload
Fixed Gateway
Mobile Gateway
Fixed Gateway
Mesh Network
Mesh Network
Mesh Network
Harvest in Field
Berries packed in boxes & pallets loaded
Add disposable smart tags to detect temperature and humidity
~1 hr.
Pre-chill
Cool produce to required temp & conditions
Temp must be maintained thru customer delivery
Processing
Berries are mechanically and manually processed and packaged
Cooler
Monitor ambient temperature in cooler
Load reefer trucks / team drivers
Track cargo temp / location in-transit
Multi-Modal Transportation
Edge analytics allows:
Dynamically configurable sensor thresholds
Regional DCs
Monitor ambient temperature
Quick turn around for end-customer shipments
Can be multi-stop
In transit temp monitored p/customer requirements
< 24 hrs.
Customer Distribution Center
12-24 hrs.
~54 hrs.
~ 24 hrs.
< 24 hrs.

Figure A2. The Intel® IoT Platform and Microsoft Azure IoT joint reference implementation provides visibility into the location of goods while in transit, helping transportation businesses reduce lost cargo.

logistics network and inventory turnover.

Summary: Connecting Physical to Digital

This pilot was instrumental in connecting the physical and digital worlds, using ICLP and the Hyperledger Sawtooth blockchain. Intel technology enabled Curry & Co. to gain valuable insights into their existing system of moving produce from harvest to processing to distribution through real-time environmental and transit monitoring, thereby paving the way for a smarter supply chain. Read more about the pilot in this case study.

The integrated solution that Intel piloted with Curry & Co. directly address and helps to mitigate the challenges associated with shipping perishable goods, by using the ICLP and Intel's Hyperledger Sawtooth Blockchain to create a connected supply chain. The ICLP enables the monitoring and tracking of environmental conditions for a variety of products and ensures that items arrive at their destination in optimal condition. The ICLP communicates live data to the cloud while simultaneously creating an immutable record on the blockchain.

Among its many features, the ICLP:

- Allows near real-time monitoring of environmental data, including temperature, humidity, light, tilt, shock, and location with a tag/gateway sensor solution.
- Enables pallet-level monitoring of shipped goods to facilitate course correction as needed.
- Delivers near real-time location tracking and programmable notifications (i.e. for temperature excursions).
- Collects all of this information and pushes it to the blockchain to establish supply-chain transparency and create an

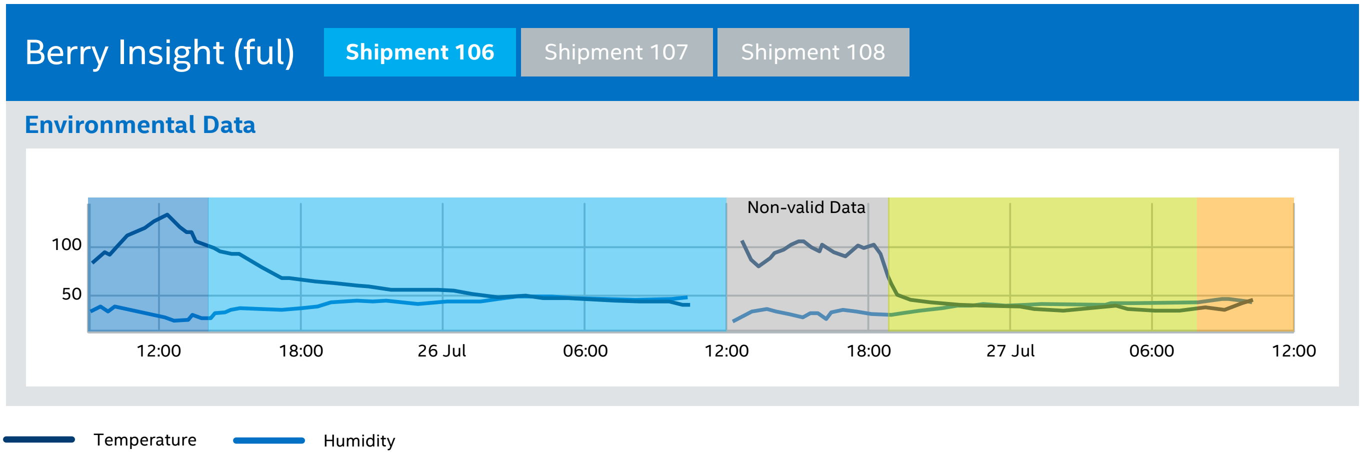

Figure A3: Blockchain Dashboard

Appendix B: Additional Resource Capabilities

- **Intel® processors.** Several families of Intel processors are available to meet the needs of the end use cases. These include the Intel Atom® processor for low-power solutions as well as the Intel® Xeon® and Intel® Core™ processor families, which provide high performance and scalability. For example, Intel Xeon and Intel Core processors can be used for manufacturing/industrial and artificial intelligence (AI)-based solutions that involve a lot of data and need high-compute capability. To meet the specific needs of customers across vertical use cases, additional SKUs within each family are available to satisfy requirements such as high temperature (industrial/manufacturing) and graphics (video). These processors come with a 15-year life expectancy and are suitable for rugged environments.

  With respect to the Microsoft Reference Architecture, the processors are the IoT devices, also referred to as field gateways, and fall under "things" in the core subsystem.

- **Hardware Accelerators.** These include the integrated GPU (iGPU), application-specific integrated circuit (ASIC), and Field Programmable Gate Array (FPGA). These accelerators are used along with the Field Gateway to significantly improve the performance of targeted, specialized, and complex tasks. Some of these tasks include video processing and executing deep learning/machine learning algorithms.

  The iGPUs are typically used for video acceleration, offloading the main CPU for performance boost. Similarly, FPGAs IoT devices can offload the processor for video or inference use cases. For flexibility and scalability, FGPAs can come as discrete CPUs that provide the highest performance per watt, integrated CPUs for low-latency and low-power and, finally, soft CPUs for maximum flexibility. Finally, Intel®Movidius™ VPUs (visual processing units) are specifically designed for computer vision and AI workloads, and provide high performance with ultra-low power consumption.

Myriad™ VPU2	Industry-defining always-on vision processor, and second generation VPU from Movidius™
Myriad™ XVPU	3rd generation VPU, firt of its class to feature the Neural Compute Engine — a dedicated hardware accelerator for deep neural network inferences.
Neural Compute Stick	Tiny fanless deep learning device that you can use to learn AI programming at the edge.

- **Computer Vision SDK.** Development of multi-platform computer-vision solutions can be simplified using the Open Visual Inference & Neural Network Optimization (OpenVINO™) toolkit. This toolkit enables convolutional neural networks (CNN) based on deep-learning inference at the edge. It supports heterogeneous execution across computer-vision accelerators—CPU, GPU, Intel® Movidius™ Neural Compute Stick, and FPGA—using a common API. Furthermore, the OpenVINO toolkit contains library functions and pre-optimized kernels, optimized calls for OpenCV and OpenVX that ultimately accelerate deep neural networks and AI workloads.

- **Intel RFP Ready Kits.** Provide a ready-out-of-the-box experience to demonstrate hardware-to-cloud capability. These ready-for-order kits are rugged and connect to the cloud as soon as the power is on.

[1] *The Internet of Things and the Enterprise*, Gartner, August 31, 2015 (Reference: https://www.gartner.com/smarterwithgartner/the-internet-of-things-and-the-enterprise/)

[2] *Logistics Market by Mode of Transport and End-user—Opportunity Analysis and Industry Forecast,* 2014 – 2022, Allied Market Research, February 2017 (Reference: https://www.alliedmarketresearch.com/logistics-market)

[3] *Reducing Food Losses by Intelligent Food Logistics,* National Library of Medicine, National Institutes of Health, June 13, 2014 (Reference: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4006167/)

[4] *The Perils of Perishable Airfreight Shipments,* American Journal of Transportation, March 26, 2018 (Reference: https://www.ajot.com/premium/ajot-the-perils-of-perishable-airfreight-shipments)

[5] *Inside Cargo Theft: A Growing, Multi-Billion-Dollar Problem,* Federal Bureau of Investigation, November 12, 2010 (Reference: https://archives.fbi.gov/archives/news/stories/2010/november/cargo_111210/cargo_111210)

[6] *Cargo theft now a tougher nut to crack,* FleetOwner, June 1, 2016 (Reference: https://www.fleetowner.com/fleet-management/cargo-theft-now-tougher-nut-crack)

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

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

Printed in USA 0419/MS/MIM/PDF ♻ Please Recycle 340013-001US