Reference Architecture

IoT Joint Reference Architecture from Intel and SAP

How the joint reference architecture applies to connected assets and logistics use cases

Executive Summary

The Internet of Things (IoT) helps enterprises gather granular, machine-generated data at the edge and then synthesize that data into actionable insights when combined with near-real-time operational and supply-chain information. IoT enables new capabilities around data collection, data storage, analytics, and digital business processes, which in turn can help businesses combine real-time operations technology (OT) data with information technology (IT) business processes. These new capabilities can help redefine the way companies operate by transforming both their processes and their products.

Intel and SAP are working together to fulfill the promise of IoT. By bringing together the Intel® IoT Platform with SAP® Leonardo IoT capabilities running on SAP Cloud Platform, enterprises can enjoy the wide-ranging benefits of IoT data collection and analysis while easing the burden of IoT management.

This paper, the first in a series that showcases IoT in specific vertical industries, describes the building blocks of a combined IoT solution from Intel and SAP within a connected assets environment in the manufacturing industry. It also describes an end-to-end joint Intel and SAP reference architecture to help enterprises transform their core processes and differentiate the quality of the services and products they produce.

The Value of an End-To-End IoT Solution

According to research by McKinsey Global Institute, the total value created by deploying IoT solutions is expected to approach a potential combined US$2 trillion by 2025.[1] To unlock this potential, enterprises within these industries are projected to spend $55 billion to $150 billion in 2025 on value-added applications and hardware, including sensors that target asset management, the supply chain, and operational visibility and optimization.[1]

Despite the potential of IoT, organizations face significant challenges for deploying IoT infrastructures and discovering insights from the vast amounts of device-generated data. Intel and SAP bring together the building blocks of an IoT solution that provides the functionality and deployment flexibility needed to support and monitor individual assets and execute automated cross-company transactions.

Intel, a leader in infrastructure-management software, provides the hardware foundation of an IoT solution. This foundation lets enterprises:

- Acquire and manage the devices that create data
- Strengthen security for the data from sensor to gateway
- Execute hands-free onboarding of devices
- Ingest, collect, store, and analyze data at the edge

SAP, a leader in business and enterprise applications and analytics, provides the software capabilities to synthesize sensor data, visualize the data in meaningful ways, and then combine the data with operational data, such as customer information, inventory, pricing and promotions, demand management, order response, and integrated business planning. In addition to these traditional data-management capabilities, SAP provides the SAP Leonardo digital innovation system, an innovative platform that delivers software and microservices that give enterprises the capability to take advantage of technologies such as IoT, machine learning, blockchain, analytics, and Big Data.

This partnership is unique in that it brings together two industry leaders that can deliver an end-to-end solution from sensor to the cloud and can then integrate that solution into an end-to-end enterprise business process that is robust, flexible, and open for future enhancements driven by either new technologies or business applications.

The joint Intel and SAP solution can be monitored, controlled, and optimized, allowing for autonomous functionality in interaction with other smart objects. Its flexibility allows for cross-system optimization across an ecosystem of partners, software services, and solutions that are integrated in a more secured and manageable way and driven by a variety of use cases and vertical industries.

Solution Overview

Solutions from Intel and SAP help enterprises realize the potential of IoT by more securely managing networks of IoT devices; collecting, managing, and analyzing the data generated by those devices; and then combining that data with the business intelligence of SAP S/4HANA® and SAP Cloud Platform. This type of IoT deployment has the potential to impact businesses by:

- Lowering costs
- Increasing uptime and efficiency
- Creating new products or services
- Optimizing productivity and production capacity
- Minimizing waste
- Improving turnaround
- Enabling new business models, such as usage-based pricing

For example, enterprises can realize the greatest benefits by combining device-generated data at the edge with near-real-time operational and supply-chain information to create actionable insights. These businesses can deploy security-enabled IoT devices across disparate manufacturing and distribution sites to monitor and analyze data. They can then combine this operational sensor data with tactical information, such as customer demand, inventory, supply-chain data, pricing, and raw-material flow to improve processes across the organization. Dynamic pricing on popular items can help boost revenue, while machines within warehouses can coordinate with each other to fulfill orders and maintain inventory levels.

With the advanced data gathering and analytical capabilities of a joint IoT solution from Intel and SAP, enterprises can get a clearer view of their operations. Figure 1 illustrates how changes or decisions made in one operational area can now be viewed

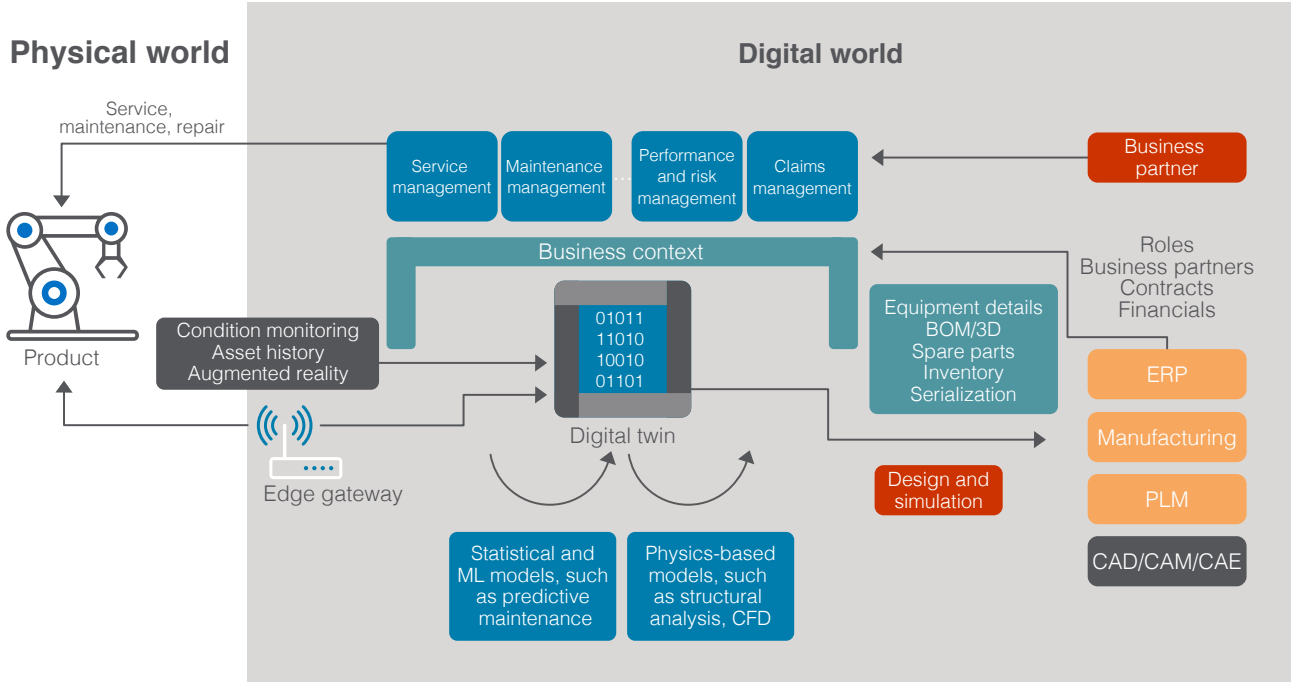

Figure 1. With an IoT solution, business decisions can be viewed across an enterprise's entire network of plants, warehouses, and suppliers

across the entire manufacturing plant or network of plants and optimized either with human intervention or autonomously over time. The business can be viewed holistically, rather than as isolated plants, warehouses, and suppliers.

Reference Architecture View and Functional Elements

The joint reference architecture, including Intel IoT Platform, SAP Leonardo IoT Edge, and SAP Cloud Platform, depicts edge computing, network, and cloud components, and it provides the framework for deploying the hardware and software. It depicts not only the functional building blocks, but also the steps to connect the sensors, actuators, and other endpoint devices to SAP Cloud Platform and SAP S/4HANA. Using this architecture, enterprises can:

- Host their private containers at the edge
- Host gateway proxies in the cloud
- More securely onboard devices with minimal human interaction
- Run implementations on different edge configurations

Enterprises can deploy the joint solution to meet their own unique needs—the actual deployment for any specific use case might use all or only a subset of the capabilities.

The joint reference architecture and the key functional blocks used by the use case examined in this paper are shown in Figure 2. The architecture demonstrates IoT use cases across the domains of devices, infrastructure, edge computing, cloud, and applications, with the goal of enabling rapid deployment of scalable IoT projects.

The current reference architecture from Intel and SAP includes the following features:

- **Data acquisition and device control:** The architecture allows data acquisition and ingestion from various sources—such as industrial sensors that are part of the operational domains—and provides control from a single dashboard. Data from these various sources is ingested into the controlling entities using various protocols.
- **Data security features between sensors, gateways, and the cloud:** The architecture provides security-enabled capabilities along the entire data path with key, certificate, and identity management using Intel® hardware–based technologies, including Intel® Platform Trust Technology (Intel® PTT), Intel® Trusted Execution Engine (Intel® TXE), and Intel® Software Guard Extensions (Intel® SGX), in addition to Intel® Enhanced Privacy ID (Intel® EPID). The security features allow devices to differentiate data as private or shared. The security-enabled flow can allow data to reach only the device for which it is intended.
- **More secure, hands-free device onboarding:** New devices, such as physical gateways and qualified sensors, can be automatically onboarded and provisioned, eliminating extra deployment tasks while improving security using Intel® Secure Device Onboard (Intel® SDO).
- **Edge-data collection, storage, and analysis:** Enterprise IoT solutions need an edge platform with robust offline capabilities to collect, store, and analyze data. SAP Leonardo IoT Edge provides domain-specific insights, real-time events and actions, reliable dashboards, and local business-process execution at the edge.

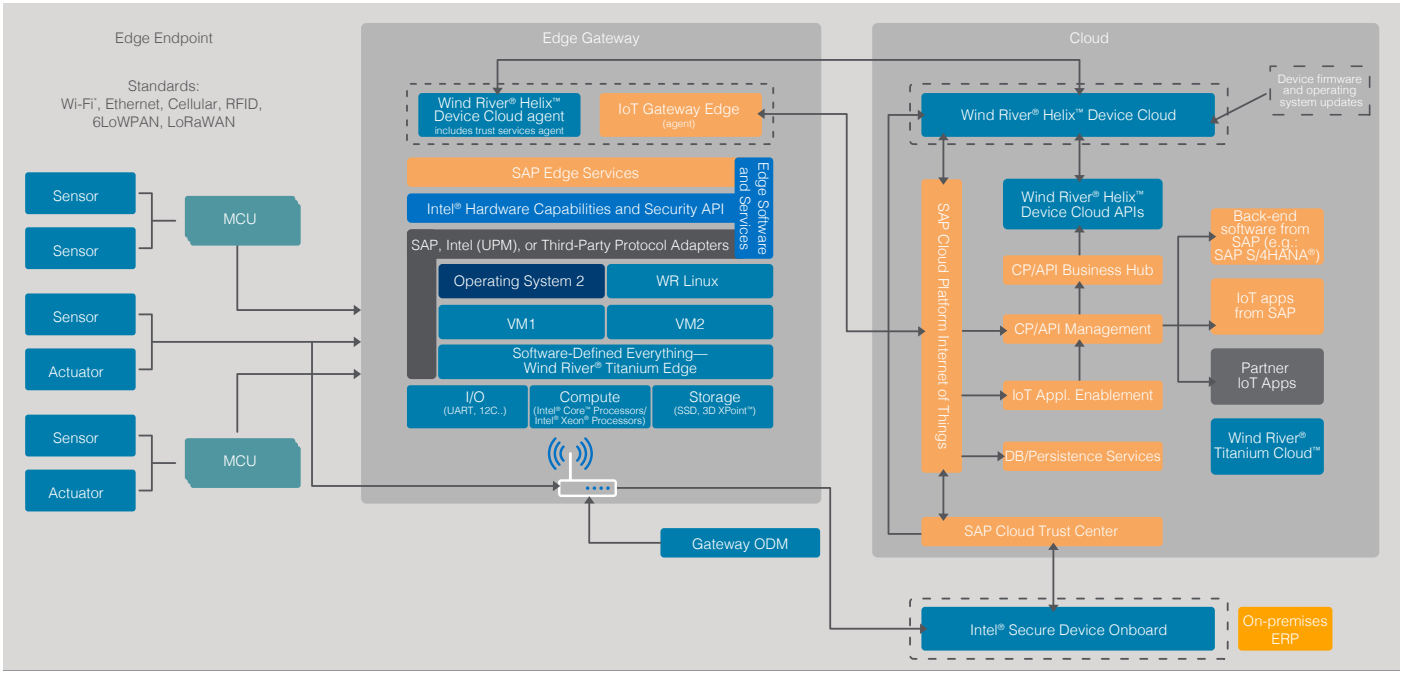

Figure 2. The joint reference architecture from Intel and SAP

- **Real-time business intelligence for optimized decision support, autonomous decision-making, and optimized interaction and decision-making across devices:** This functionality is achieved using IoT applications from SAP, SAP Cloud Platform, SAP Leonardo IoT capabilities, and Intel device- and security-management technologies, in addition to other IoT solutions. The joint solution provides streamlined infrastructure management by securely onboarding, configuring, and monitoring IoT devices.
- **Edge-platform flexibility and scalability**: The architecture supports multiple edge gateway configurations, ranging from systems powered by minimal-compute Intel Atom® processors to those powered by high-compute Intel® Xeon® processors, and running software suitable for small and large enterprises. The joint solution can be deployed in the cloud, on-premises, or using hybrid scenarios, and it supports cloud-to-cloud and cloud-to-on-premises integrations.

Solution Architecture Details

The joint reference architecture utilizes the following components and solutions.

Intel® IoT Platform

The Intel IoT Platform is an end-to-end reference model and family of products from Intel that works with third-party solutions to provide a foundation for seamless, security-enabled connection of devices. The model delivers trusted data to the cloud and ongoing value through analytics. It provides an end-to-end platform that allows data from billions of devices, sensors, and databases to be securely gathered, exchanged, stored, and analyzed. It helps bring innovations to market faster, reduces complexity, and delivers actionable intelligence by offering a defined, repeatable foundation for how devices will connect and deliver trusted data to the cloud.

The platform includes:

- Edge components
- Processors and accelerators targeting the 15-year life of IoT environments
- A ruggedized platform that can withstand extreme temperatures and vibration
- Certifications for embedded, industrial, and automotive hardware-based security, in addition to device provisioning, monitoring, and control
- Scaling through virtualization
- Carrier-grade reliability

The platform includes virtualization and software-defined everything (SDE). This architecture introduces virtualization at the edge through Wind River® Titanium Edge, where multiple virtual machines (VMs) can be deployed to divide workloads for different functional areas, such as operations, asset management, factory floor, and inventory management. Virtualization can provide several benefits:

- Decouples compute and storage resources
- Redirects and enables dedicated resources when needed
- Provides the ability to independently manage brownfield machines, which enables integration of different classes of equipment

Each VM can, as required, run on a different operating system and can still connect through a single cloud connector. A one-to-one security-enabled server-pair configuration can be used to increase high availability, which can reach six-nines reliability, depending on the configuration.[2]

Edge Components

The joint reference architecture's edge components use the following Intel technologies.

Intel® Processors

Intel Xeon processors provide high performance, scalability, and artificial-intelligence (AI) inference algorithms. These processors are applicable for industries such as industrial manufacturing that must process significant amounts of data. Other uses, such as monitoring refrigerators in retail settings, can take advantage of other Intel hardware options, such as the Intel Atom processor family for low-power solutions and Intel® Core™ processors for workload consolidation. Software, accelerators, or field-programmable gate arrays (FPGAs) working in conjunction with the processor offer additional performance gains.

Selecting the processor for an edge gateway device depends on several factors:

- The type of workload the gateway will be required to accommodate
- The environment the device will operate in, such as harsh industrial areas with severe operating temperatures, clean rooms, and so forth
- Hardware requirements, such as power, core, and thread count, video technology, expansion options, memory, and networking capabilities

To handle a large amount of data generated at the edge, high compute processors that can run analytics to process this data and take corrective action are recommended—such as Intel Core processors or Intel Xeon processors. Software solutions certified by SAP take advantage of the Intel strategic order-document-management (ODM) ecosystem to provide appropriate gateway-implementation designs.

Intel Next-Generation Storage Solutions

Intel storage solutions can provide targeted storage, from non-volatile memory to Intel® Solid State Drives (SSDs), both at the edge and in the cloud. Intel® Optane™ technology can provide high performance and low latency for Big Data processing, and Intel® 3D NAND Technology can provide high density at low cost.

Intel Hardware–Based Security Technologies

To combat IoT threats, Intel enables security layers at all levels—data ingestion, data in use, data in motion, and data in action. Security starts at the hardware level, with security-enabled boot and storage, a trusted execution environment (TEE), and Intel EPID. While the operating system itself utilizes many of these built-in security features, developers can further utilize some of these features by employing application programming interfaces (APIs) that tap into hardware features such as Secure Boot, TEE, Protected Storage, Unified Extensible Firmware Interface (UEFI), Trusted Platform Module, Intel PTT, Intel SGX, Intel® Dynamic Application Loader (Intel® DAL), and explicit parallel instruction computing. Using these APIs, developers can better ensure security-enabled connections, data- and key-protection features, security-enabled credential provisioning, IP-protection features, and code-privileges separation in the applications they develop.

Device Management Components

The joint reference architecture uses the following components to onboard and manage IoT devices.

Intel® Secure Device Onboard (Intel® SDO)

This function is a zero-touch onboarding service that accelerates trusted onboarding of Intel EPID technology–based hardware. Zero-touch onboarding is used for device onboarding attestation. The process uses Intel EPID technology to reduce overhead by eliminating workflows on device installation.

Wind River® Helix™ Device Cloud

This product provides gateway and device-management capabilities, in addition to a mechanism for performing operating system and firmware upgrades from the cloud. Device management involves several steps, as illustrated in Figure 3. These steps include deploying devices; monitoring, servicing, and managing devices against security threats and field expenses; ongoing operating system and firmware upgrades; and finally, successfully decommissioning devices to eliminate any security threats in the case of theft. One of the most important platform features is the management console. Built using RESTful APIs, the console lets customers manage services remotely from a single platform, and it can filter device data by metadata, list order, or other criteria.

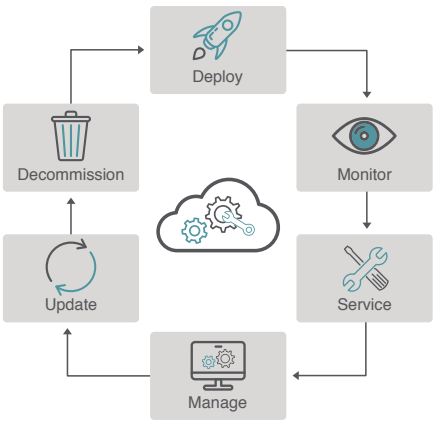

Figure 3. Wind River® Helix™ Device Cloud helps enterprises manage devices throughout the entire device lifecycle

Edge Applications and Services

The joint reference architecture uses the following edge applications and services to deliver high reliability and support for multiple sensor protocols.

Wind River® Titanium Edge

Titanium Edge provides a dual-server configuration with a small footprint that enables virtualizing compute and storage and delivers the reliability and performance of virtual clouds. Because not all implementations need virtualization, Titanium Edge is an optional layer.

Titanium Edge contains three nodes:

- The control node, which contains the virtualization infrastructure manager (VIM)
- The compute node, which includes a carrier-grade accelerated vSwitch and a carrier-grade Kernel-based Virtual Machine (KVM) hypervisor
- The storage node, which provides a carrier-grade storage cluster

Sensor Protocol Adapters

These are southbound protocols used to connect to sensors, and they include sensor data management, communications, status, device security, device diagnostics, device monitoring, and functional safety. This layer includes peer protocols and can be extended with securely signed third-party drivers and software libraries. Intel and SAP have several offerings that address these protocols.

Additional Packages and Libraries

Depending on the use case, customers can select from several firmware support and development packages; communication kits such as Data Plane Development Kit (DPDK); embedded system debuggers; and development libraries, analysis libraries, and kits. Support is available for various operating systems, such as Linux* distributions and Android*. The platform also provides virtualization support (with a hypervisor) and containers (with a container engine), in addition to standard API interfaces.

SAP Solutions

SAP has supported the digitization of business processes for more than 45 years through its business applications. By utilizing low-cost sensors, affordable bandwidth for data transportation, the Internet, and the ability to manage Big Data, SAP solutions can make use of real-time data created by smart products and assets.

SAP Leonardo IoT Capabilities

SAP Leonardo IoT capabilities are one of the key elements in enabling digital transformation. They connect the OT world of physical devices with the IT world of software.

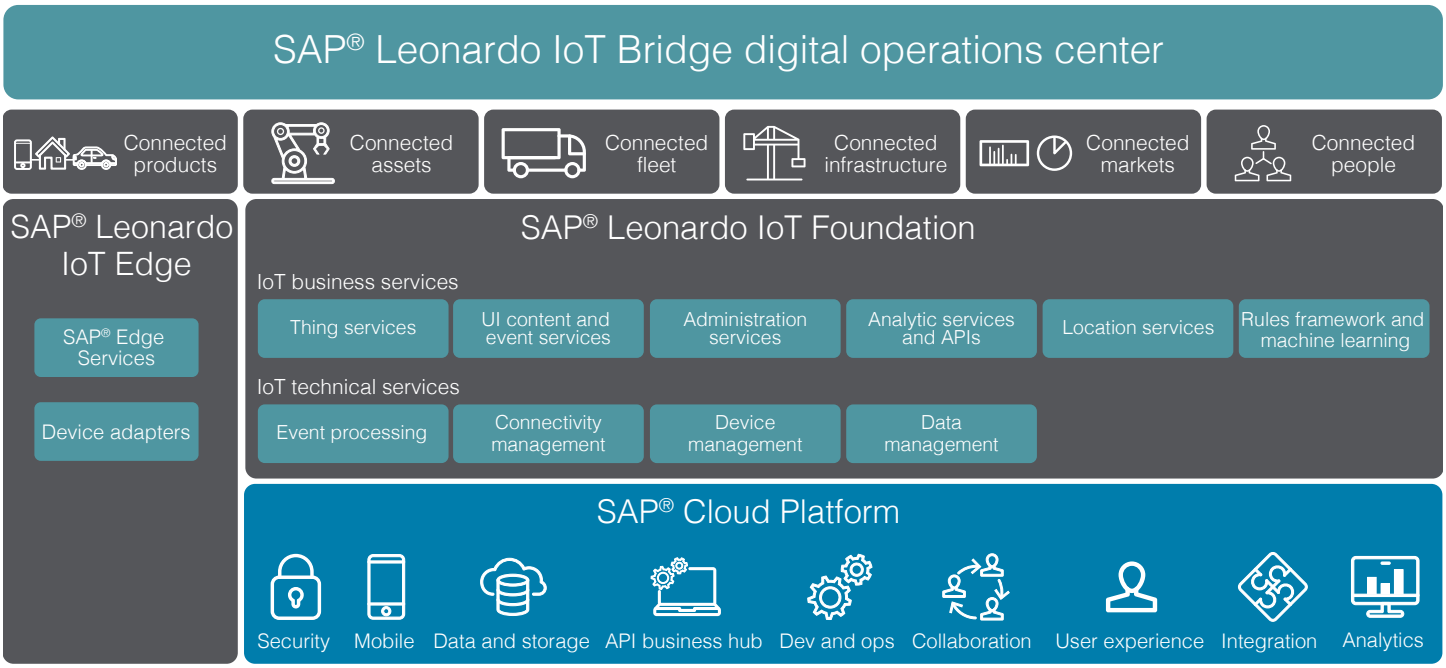

Figure 4. Overview of SAP® Leonardo IoT capabilities

SAP Leonardo IoT capabilities are based on technology solutions from SAP, including SAP Cloud Platform and the SAP Data Hub solution. These solutions provide a proven and scalable offering that focuses on:

- Connecting and managing IoT devices via the cloud
- Processing IoT streaming data at the edge and in the cloud
- Storing data in a cost-efficient Big Data lake
- Allowing interactive and deep analysis of the data with machine learning algorithms
- Enabling the development of integrated IoT applications based on reusable, semantically rich microservices

SAP Leonardo IoT Bridge

The SAP Leonardo IoT Bridge digital operations center addresses customer expectations for deeply integrated scenarios across IoT-connected applications, as shown in Figure 4. It provides a holistic view across inter-application scenarios, providing immediate insights in the case of machine- or plant-specific issues. SAP Leonardo IoT Bridge uses SAP Fiori® user-experience (UX) concepts for a user-interface (UI) integration with SAP Cloud Platform to easily connect to various business systems. It is also open for partners and customers to extend and build custom scenarios.

Solutions Related to SAP Leonardo

Solution offerings related to SAP Leonardo and IoT technology provide value by addressing the specific needs of enterprises and also provide integration with SAP business solutions, such as SAP S/4HANA.

Examples include:

- SAP Connected Goods software
- SAP Predictive Maintenance and Service solution
- SAP Asset Intelligence Network
- SAP Vehicle Insights application
- SAP Global Track and Trace solution

SAP Leonardo IoT Foundation

SAP Leonardo IoT Foundation is built on SAP Cloud Platform as a multi-cloud platform-as-a-service (PaaS) solution. It includes both business services that enable users to rapidly build IoT applications and technical services that let businesses manage devices securely and connect them using a wide variety of industry-standard protocols.

To support the rapid development of applications on SAP Cloud Platform by either partners or customers, the SAP IoT Application Enablement toolkit provides business services and developer-focused tools that provide easier time-series data handling, rules enablement, reusable UI controls for SAP Fiori apps, and development tools embedded into SAP Web IDE. SAP IoT Application Enablement also supports the digital-twin concept, which enables mapping the physical world of connected things to their digital “operational” or “business” representation. It supports lifecycle management for modeled entities (from onboarding to decommissioning), analytical use cases, and programming models for distributed data management and application development.

The SAP Cloud Platform IoT service provides integration capabilities for connecting and communicating with physical devices either directly or through an edge gateway. It enables bidirectional, secure communication between devices at the edge and SAP Cloud Platform, which provides secure and scalable entry into SAP Cloud Platform with support for the most important IoT-related protocols, like Message Queuing Telemetry Transport (MQTT). It also provides a device model that defines the technical view on the incoming data.

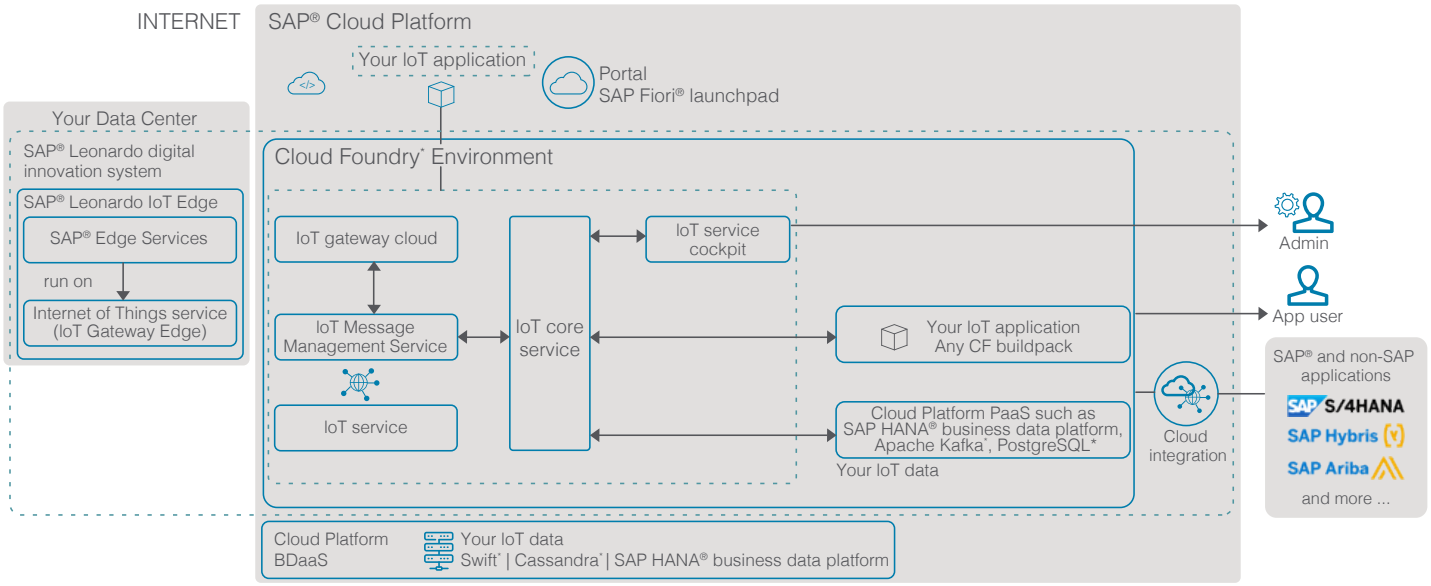

Figure 5. Overview of the SAP® Leonardo digital innovation system architecture

SAP Leonardo IoT Edge

As the amount of data generated by IoT devices continues to grow exponentially, enterprises increasingly require data processing at the edge. For example, in large-scale manufacturing environments, it is often more effective to connect a single manufacturing device to a locally installed edge gateway rather than connecting the device directly to a cloud service. This setup allows the gateway to manage the data, which reduces network traffic and cost.

SAP Leonardo IoT Edge, as described in Table 1 and Figure 6, provides the foundation for this type of scenario. It combines the capabilities offered by the SAP Cloud Platform IoT service with additional SAP Edge Services to persist IoT data for local data storage, in addition to providing run rules and streaming analytics algorithms. SAP Leonardo IoT Edge extends business functions from SAP software systems to the edge and supports operations in intermittently connected environments. These services are centrally defined, managed, and distributed from the cloud to the local edge node.

A flexible plug-in concept manages local connections to devices and provides secure data transfer to and from the cloud, in addition to direct processing of IoT data streams. The plug-in concept also enables a variety of communication protocols, such as MQTT, Constrained Application Protocol (CoAP), Modbus*, Simple Network Management Protocol (SNMP), and OPC Unified Architecture (OPC UA*), which enables connection to many types of devices on the edge.

SAP Cloud Platform

SAP Cloud Platform provides a foundation for SAP Leonardo IoT offerings and is based on Cloud Foundry*, an open initiative to provide an industry-recognized platform for the development of microservices-based solutions. It supports a multi-cloud approach that provides an abstraction layer for SAP applications. This layer allows IoT applications to run on either public cloud platforms, such as Google Cloud Platform*, Amazon Web Services* (AWS*), and Microsoft Azure*, or in SAP data centers.

Table 1. Overview of SAP® Leonardo IoT Edge

Feature	Description
Persistence services	Stores data locally on IoT gateways
Streaming analytics	Analyzes IoT data streams for exceptions and patterns and creates alerts and events based on pattern matching
Business-essential functions	Provides business processes at the edge for business continuity when the edge is disconnected from core services
Predictive modeling	Provides predictive models for analyzing IoT data; the predictive algorithm is trained in the core based on all available data, and the resulting predictive model is then applied to the edge devices
Machine learning	Applies machine learning algorithms at the edge specifically for image and video analysis
Device adapters	Provides data-format conversion across a multitude of IoT device protocols, and securely transmits data to and from SAP® Cloud Platform

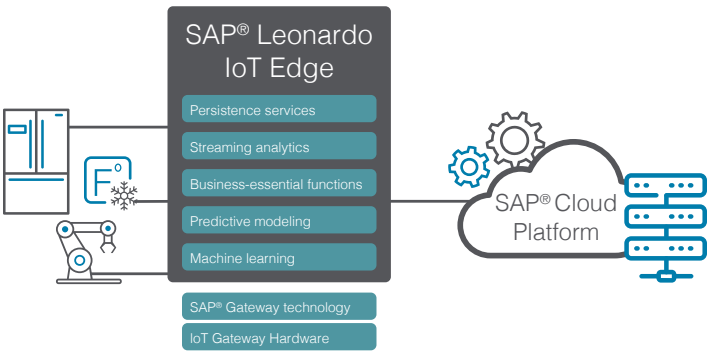

Figure 6. SAP® Leonardo IoT Edge provides data persistence and processing capabilities at the edge

SAP Cloud Platform provides a large set of technical platform services that support IoT and digital-transformation scenarios, and it provides flexible process integration between various SAP and third-party business systems.

Control and Data Flows

This section describes three stages of the IoT device lifecycle that enterprises must securely manage throughout an IoT deployment.

Onboarding Devices

Onboarding is the physical deployment of IoT devices—such as gateways or sensors—into a network. Device onboarding historically has been a time-consuming task because it involves coordination between IT and operational teams for proper installation and security-enabled setup. By using Intel SDO zero-touch, device identification, and data privacy, ownership and communication setup from the edge to the cloud can be better secured.

Devices must have Intel EPID capabilities to be enabled for Intel SDO. The process of connecting devices, integrating data, and managing software upgrades is displayed in Figure 7 and summarized in the "Device Onboarding" steps below.

Device Onboarding

Steps 1 through 6, in addition to step S, describe the device onboarding process.

1. During the manufacturing phase, the Intel EPID credentials are embedded in the TEE of the processor. The gateway then creates a globally unique identifier (GUID) using an Intel toolkit. The gateway also creates a URL that the device uses to connect to the rendezvous server, which allows the device to get its new owner information.

2. The device owner receives an ownership proxy for the device over the network. This information is then imported into the cloud service provider and associates the device with the device's owner. The Intel cloud trust broker, or rendezvous server, provides the rendezvous service IP address to direct the device to the new owner—in this case, IoT services from SAP—via the SAP Cloud Trust Center site.

3. Once the device is powered on, it "phones home" to the Intel cloud trust broker to locate its new owner. The broker provides the IP address and redirects the device to SAP Cloud Trust Center.

4. SAP Cloud Trust Center is responsible for verifying the Intel EPID signature and ownership of the device, and then registering the device. It forwards the connection certificate for further configuration and communication to Wind River® Helix™ Device Cloud. SAP Cloud Trust Center is also responsible for maintaining the list of valid devices.

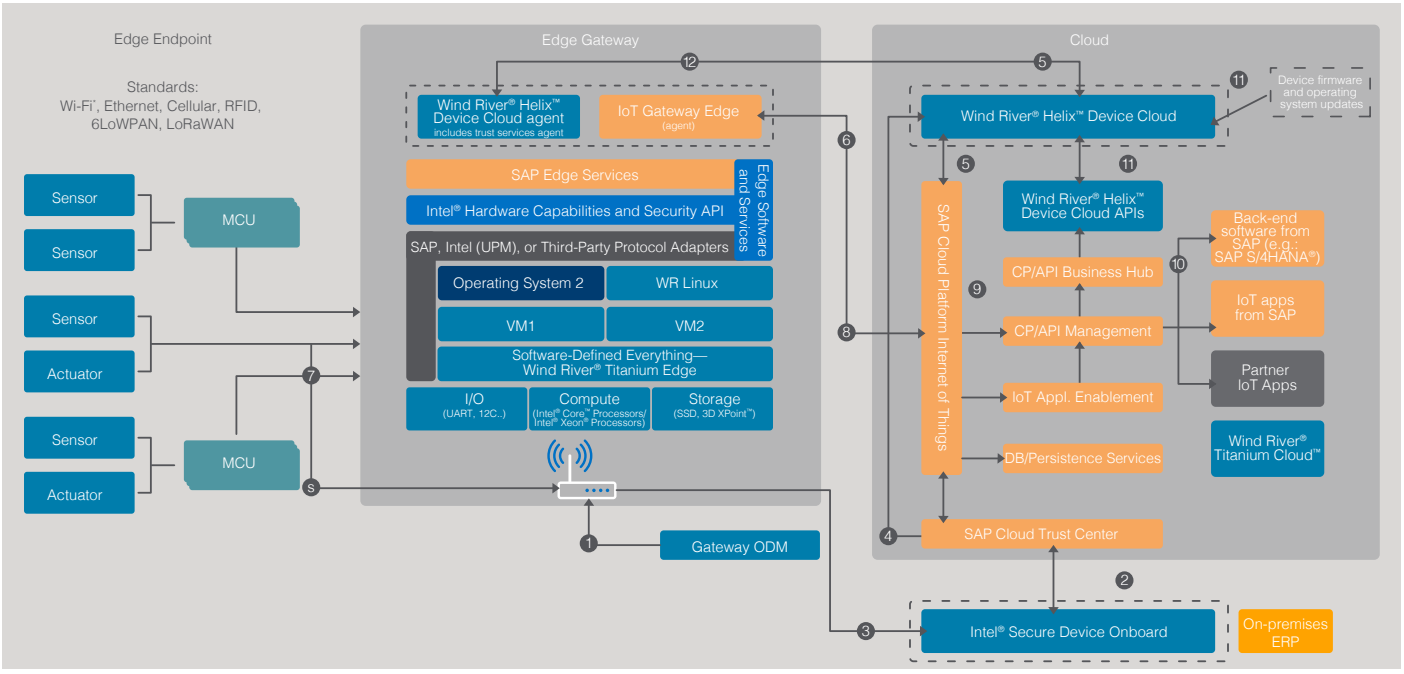

Figure 7. The joint reference architecture from Intel and SAP; the individual data flows are described in the following steps

5. Once the connectivity path is established between the device and Wind River Helix Device Cloud, the device certificates are forwarded by the owner followed by the device configuration, including publish-subscribe topic subscriptions on the gateway.

6. SAP Gateway technology provides a simple way to connect devices, environments, and platforms to SAP software based on market standards. SAP Gateway authenticates using the device certificate, and it then establishes a data path to the cloud provider.

   At this stage, the device onboarding is complete and data control and data path flows have been established. The device is capable of collecting data and processing it according to defined business rules. The collection and implementation of data is looked at in the following "Collecting and Integrating Data" section.

S Sensors or microcontrollers that are Intel EPID technology–enabled can use steps 1 through 4 for onboarding. However, legacy sensors connected to the gateway might be detected and authenticated by using a simple sensor directory.

Collecting and Integrating Data

Steps 7 through 10 describe the process of collecting and integrating device data.

7. Business applications on the gateway acquire data from connected sensors through a number of supported protocols. The data from registered sensors can directly flow to the gateway, or the data can be encrypted by the edge devices and then sent to the gateway if the owners of the gateway and sensors are different.

8. SAP Leonardo IoT Edge software modules receive messages from devices and perform actions on them, ultimately sending messages to the cloud gateway to be dispatched to cloud services.

   SAP Leonardo IoT Edge invokes the persistence service and streaming analytics to locally store IoT data on the gateways. These analytics analyze the IoT data streams for exceptions and patterns, and they then create events and alerts in accordance with the specific rules set up to reflect custom industrial use cases and operational needs. In addition, business-essential functions run business processes at the edge to provide continuity for critical business functions, even when the edge is disconnected from the core.

9. Cloud services then disseminate the data to enterprise cloud software for further processing.

10. Data is also forwarded to back-end applications as necessary.

Managing Devices and Software Updates

Steps 11 and 12 describe the device management and software update process.

11. Application software managers modify a device's access or can trigger a software update through the provisioning API.

12. Wind River Helix Device Cloud pushes the necessary software packages to the gateway. The device-management agent on the gateway takes appropriate action either by installing or upgrading existing software.

Use Case: Connected Assets and Logistics

This connected assets and logistics use case demonstrates the value of applying portions of the joint reference architecture to a real-world example. This use case illustrates the simplified view of the combined physical and digital world linked to the business processes as shown in Figure 1, where business decisions can be viewed across an enterprise's network of distributors, warehouses, and suppliers.

Although this use case focuses on an IoT deployment of connected assets in a discrete manufacturing environment, the joint reference architecture can be applied to other industry sectors, such as retail, industrial, energy, biotech, pharmaceuticals, chemicals, or electronics, where data from physical machinery or devices is generated and can be combined with business data, such as inventory, production, and maintenance scheduling, to create insights that lead to better business decisions.

In this use case, the example company is a leading manufacturer of innovative protective packaging materials and systems for medium-to-large manufacturers and distributors. Rather than selling machines, the company provides them under a consignment model.

Historically, inventory replenishment for the machines was performed by company technicians on a biweekly schedule where the machines were also inspected and serviced as needed. The company is launching a new "smart" model that provides data streams that allow for inventory replenishment, management, condition monitoring, and performance optimization. Collecting and monitoring these data streams across all of the machines deployed will allow the company to:

- Decrease replenishment costs for consumables
- Optimize service routing and scheduling based on actual usage patterns and analytics
- Improve machine uptime and decrease machine downtime alerts through remote condition monitoring
- Improve overall customer satisfaction

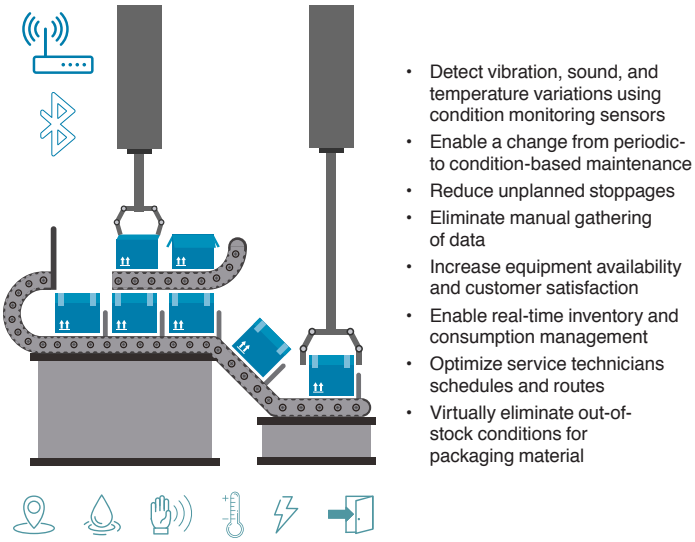

Figure 8. Functionality overview of "smart" packaging machines

For other industries, a similar solution might require a different selection of modular components described in the joint reference architecture than is shown in this specific use case.

Storyline: Digital Transformation to Product-as-a-Service

This section focuses on applying the joint reference architecture to a set of connected packaging machines at a factory location. The use case includes an example of the logistics involved.

Manufacturing Packaging Machine Digitization

1. A small automotive parts manufacturer orders five "smart" packaging machines from the packaging machine company, with the functionality shown in Figure 8. Because the packaging machines will be located together at one plant, one packaging machine requires connectivity and acts as a gateway, and the remaining four communicate through it. The machines are shipped directly to the manufacturer and are installed by the packaging machine company technicians.

2. The packaging machine company preconfigures the gateway on the machines with appropriate security profiles, certificates, language packs, and communications functionality.

3. The packaging machine company provides a tracking number and notifies the manufacturer of the scheduled delivery date, and then provides updates using SAP Global Track and Trace. These updates include production start, completion, palletization, loading, customs clearance, delivery, and unloading, as shown in Figure 9.

Packaging Machine Initial Setup

1. A service technician unpacks and powers-on the packaging machines.

2. The gateway attached to the machine uses its on-board subscriber identity module (SIM) to connect to the cloud and register its location, availability, and capability.

3. Security certificates and profiles are validated and applied as necessary. Once the gateway packaging machine is powered on, it "phones home" to the Intel cloud trust broker to locate its new owner. The Intel cloud trust broker provides an IP address and redirects the device to its new owner, SAP Cloud Trust Center. SAP Cloud Trust Center verifies the Intel EPID signature and ownership of the device, and it then registers the device. It forwards the connection certificate for further configuration and communication to Wind River Helix Device Cloud.

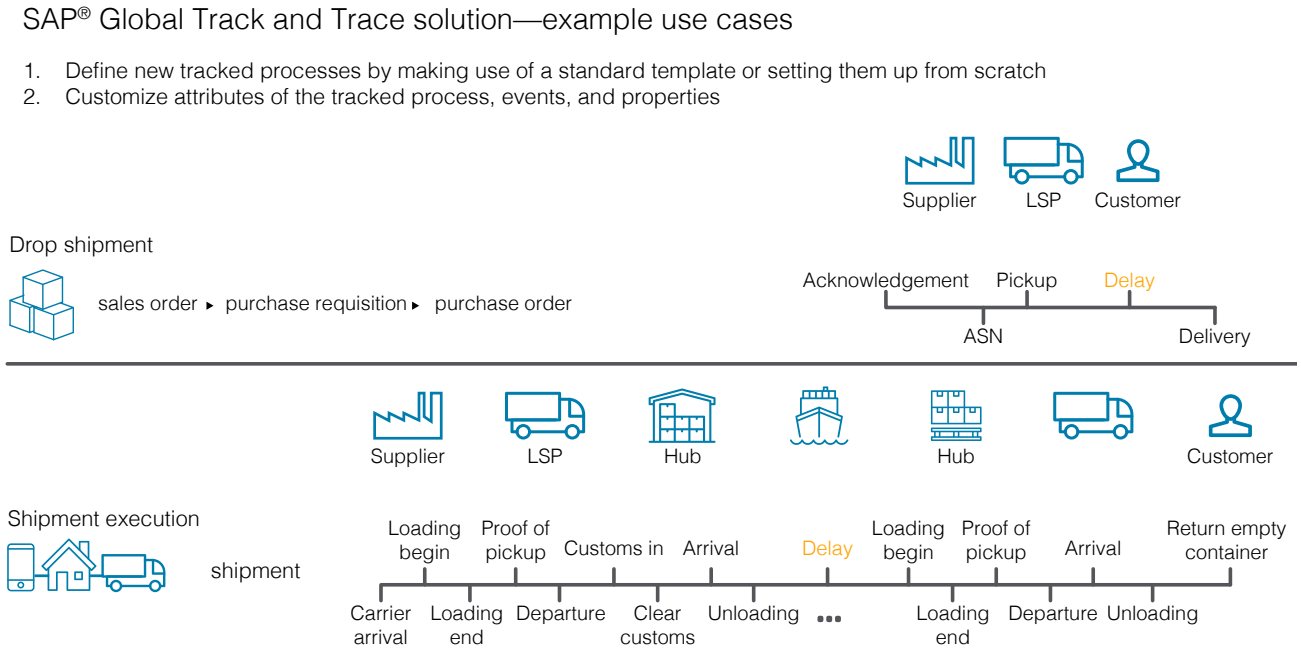

Figure 9. SAP® Global Track and Trace object tracking scenario

4. The packaging machine can be assigned to groups for ease of administration. Once the connectivity path is established between the device and Wind River Helix Device Cloud, the device certificates are forwarded and the device is configured, including publish-subscribe topic subscriptions, on the gateway. SAP Leonardo IoT Edge and SAP Cloud Platform on the gateway authenticate SAP Cloud Platform using the device certificate, and they then establish a data path to the cloud.

   At this stage, the device onboarding is complete, and the data control and data path flows have been established. The device is capable of collecting and processing data.

5. The packaging machine is installed and stocked with packing material, and it is now operational.

Packaging Machine Production

1. **Real-time inventory tracking:** An SAP business application on the gateway acquires data from connected sensors through a number of supported protocols. This data is used for real-time inventory tracking. The data from registered sensors flows directly to the gateway. If the gateway and sensor owners are different, the data can first be encrypted and then sent to the gateway.

2. **Product replenishment:** SAP Leonardo IoT Edge receives messages from devices and performs actions on them, ultimately sending messages to the cloud gateway to be dispatched to cloud services. SAP Leonardo IoT Edge invokes the persistence tools and streaming analytics to store and analyze the data on the gateway. Real-time monitoring of consumables combined with historical consumption patterns let the packaging machine company optimize its service schedules and routes within a given market area.

3. **Operational monitoring:** Real-time condition monitoring of the packaging machine allows the packaging machine company to dynamically schedule maintenance based upon the visible condition of critical components, rather than depend on statically scheduled maintenance that had been performed in the past. Creating a historical store of data across all machines in operation allows the packaging machine company to, over time, refine the modeling techniques used to quantify the condition of critical components to improve equipment availability.

4. **Intermittent connectivity:** Business-essential functions can provide business processes at the edge to enable continuity for critical business functions, even when the edge device is disconnected from the core. Once connectivity is reestablished, SAP Cloud Platform can then forward data to enterprise cloud software for further processing. Data is also forwarded to back-end applications as necessary.

When device maintenance, performance issues, or security breaches are detected, or when overall configuration updates are required, application software managers can modify a device's configuration or can trigger a software update through the provisioning API. A device can be taken offline, or, in case of a software or firmware upgrade, Wind River Helix Device Cloud can push the necessary software packages to the gateway. The device-management agent on the gateway then takes appropriate action either by installing or upgrading existing software. Once installation is complete, control for the device is passed to SAP Leonardo IoT Edge.

Conclusion

Intel and SAP have collaborated to develop an end-to-end solution that helps meet the digital business-transformation needs of enterprises worldwide. With this joint reference architecture, enterprises can now make use of data collection and analysis at the edge while still benefiting from the core business intelligence and overall performance of SAP S/4HANA and SAP Cloud Platform.

This joint reference architecture brings together Intel IoT Platform performance, SAP Leonardo IoT capabilities, and SAP Cloud Platform to securely onboard and manage a network of devices, collect and manage machine data, and perform analytics—and then combines these functions with the business processes running on SAP S/4HANA to fully enable the digital transformation of a business.

This paper provides a use case of connected assets in a manufacturing environment, which demonstrates how machine-generated data at the edge can be synthesized into manageable insights in combination with the near-real-time operational and inventory information available from within the business. By using this data, an enterprise can optimize its business of consigning a machine as a service to decrease cost while increasing customer satisfaction. The joint reference architecture can also support multiple use cases across a variety of industries with an end-to-end view of the data collection, storage, and analysis that drives digital business transformation.

For more information about the joint reference architecture, or to discuss specific use-case implementations, please contact your Intel or SAP sales representative.

[1] McKinsey & Company. "The Internet of Things: Mapping the Value Beyond the Hype." June 2015. *mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx*.

[2] Wind River. "Titanium Cloud." *windriver.com/products/titanium-cloud/*.

Printed in USA 0418/TA/PRW/PDF Please Recycle 337119-001US