Solution Brief

Any Device, App, Cloud and Network – Changing the Game for Factory Industrial Internet of Things (IIoT)

Deploy a private wireless network over a 40+ acre industrial site and quickly and securely standup devices at scale

Executive Summary

Intel, Dell, and an aviation company partnered on the deployment of a transformational edge to cloud solution for a 42-acre industrial site. The Intel® Smart Edge solution leverages Intel® Secure Device Onboard (SDO) to establish a zero-trust network where devices can be quickly on-boarded and authenticated, spectrum parsed for multi-tenancy, and end users can easily and securely access engineering/data center data on the factory floor. The solution takes advantage of Long-Term Evolution (LTE) spectrum to enable a private LTE network with improved coverage, lower latency, and higher bandwidth. This solution allows for cell phones, tablets/PCs, and Internet of Things (IoT) devices to use web-based engineering tools and Industrial Internet of Things (IIoT) applications, such as tools and foreign object debris tracking.

Business Challenge

Manufacturers with large factory and production areas face unique challenges in deploying edge/IoT capabilities. Hardwiring instrumentation and sensors are time consuming and expensive. Setting up a traditional wireless network (Wi-Fi) requires very skilled network designers, can be cost prohibitive, pose a security risk, and still result in a network with insufficient coverage because of interference from moving parts and equipment. These connectivity challenges have slowed the adoption of new edge functionality like asset tracking, machine vision, augmented reality and predictive maintenance. Even more fundamentally, they have limited employees' ability to access engineering and manufacturing data via tablet and laptop on the factory floor/yard. Without this connectivity, an employee must anticipate his or her needs before leaving the office, which often results in lost productivity.

It is not sufficient to provide robust connectivity and coverage to enable data flow from the factory floor. Manufacturers have stringent security standards and need to ensure that increased connectivity does not increase data vulnerability. To reach the full potential of edge applications, it is likely that 1,000s to 10,000s of devices will need to be connected, managed, updated, and secured. To be economical, scaling to this level must be achieved with minimal IT support staff. Finally, any solution aimed at pulling data from the factory floor must work with legacy sensors and systems. For example, getting factory floor tools qualified can be a multi-month process, making it infeasible to replace existing edge capabilities simply because the new network is not compatible. Seamless integration with existing tools and capabilities increases the total value offered by the solution.

The Intel Smart Edge solution addresses all of these pain points and makes it easy for companies to access and acquire data from the factory floor. Also, the entire solution is network agnostic and can use Mobile Network Operator (MNO) LTE, private LTE, other carrier LTE, Citizens Broadband Radio Service (CBRS) spectrum, 5G, WiFi or a combination of these.

Use Cases

The initial use cases are:

Use Case 1: Data access from engineering laptops (Dell LTE-enabled laptop or Dell laptop using LTE dongle) on the factory floor

Use Case 2: Data collection from multiple Radio-Frequency Identification (RFID) readers from an existing RFID asset tracking solution routed through a Dell 3000 Gateway

Use Case 1 – Laptop Access on Factory Floor

The industrial customer shares the manufacturing space in the 42-acre site with multiple competitors. Managing the wireless network on-site and providing security for multiple companies has been extremely challenging. The Intel Smart Edge solution made it possible to parse the private LTE network so that each company can access their own spectrum, but not anyone else's. Additionally, Intel Smart Edge forces authentication of each device so that only known and validated devices can connect and pass data over the network (see "Security Section" for greater detail). A new laptop or device can be brought online and in use within minutes using company-specific spectrum. This simple provisioning simplifies IT operations and results in a lower total cost of ownership. Operationally, the high bandwidth and robust coverage of the private LTE network means that engineers and technicians can pull up engineering drawings wherever and whenever they need them when working on the factory floor.

Use Case 2 – Asset Tracking

The industrial customer already made a substantial investment in a RFID based asset tracking solution. This solution was successful but limited in value because the data was stranded on local RFID readers where it could not be accessed remotely in near real time. By treating the RFID readers as IoT devices on the Intel Smart Edge system, it was possible to load the asset tracking data from the readers to a central data center for dashboarding across the entire facility. This allowed the customer to derive even greater value from their current asset tracking solution without having to qualify a new tracking solution that would have driven incremental investment and taken months of testing and approvals.

Given the success of these two use cases, the industrial customer is planning to expand their usage of this solution to include digital signage, predictive maintenance, machine vision, virtual reality for remote expert support, and many other IIoT functions.

Solution Value

The Intel Smart Edge platform provides complete application lifecycle services for the premise edge. This enables simple one-click deployment of applications as well as the zero-trust security paradigm required to on-board devices and protect resources from undesired access. When Intel Smart Edge is implemented along with Intel SDO capabilities, IoT devices can operate in a trusted manner and they cannot be recruited as platforms for distributed denial-of-service (DDoS) attacks.

Through a comprehensive set of deployment and management tools, this software enables any manufacturer to stand up a private LTE/5G network inside their factory premises. Only identified devices associated with the factory have access to these facilities thereby ensuring performance and security. Local hosting of applications provides sub-millisecond access to compute and storage within the premises by authorized devices.

Key high-level benefits of the Intel Smart Edge solution include:

- More secure operational environment
- Higher performing compute and storage
- Ease of deployment and use
- Faster responses and lower latencies
- Scalability of devices to 1000s

Solution Architecture

Intel® Smart Edge Software (SW)

The multi-access edge compute (MEC) is a new services architecture that delivers overlay IT and cloud-computing capabilities from servers deployed for mobile base stations, small cells, eNodeBs, and cloud radio access network (RAN)—including on-premises in an enterprise. The MEC specifications from ETSI's Industry Specification Group (https://www.etsi.org/committee/1425-mec) call for an open compute-edge node platform based on network functions virtualization (NFV) that can be installed in base stations and small-cell locations. This NFV Infrastructure (NFVI) uses a general-purpose server and leverages an open-source operating system combined with NFVI software. Intel Smart Edge builds on this foundation with additional features such as content delivery network (CDN) nodes, enterprise applications, security-enabled connectivity, ability to run third party virtualized network functions (VNF)/cloud native network functions (CNF) [e.g. software-defined wide area networking (SD-WAN)] and analytics probes to deliver a low-latency edge to cloud services architecture for next-generation mobile data services and applications. Intel Smart Edge has two primary components (see Figure 1):

Intel® Smart Edge: An Edge Native Converged Platform

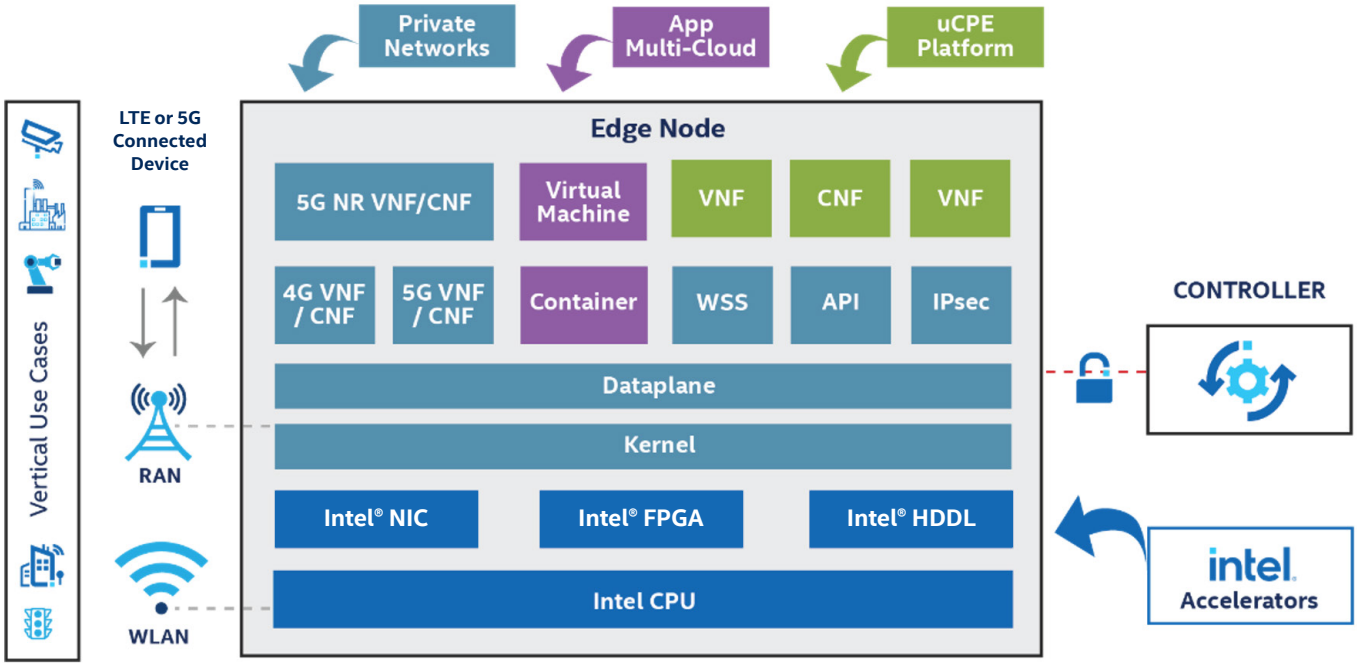

Figure 1. High level architecture of the Intel® Smart Edge platform

1. Intel Smart Edge Controller - The Controller gives administrators the ability to manage thousands of edge nodes from a centralized location at scale. The Controller may operate from a private data center or public cloud facility and includes several important services:
    a. Lifecycle and configuration management of the Edge Node firmware and software (including operating environment).
    b. Management and provisioning of Edge Node software features.
    c. Full application lifecycle management for third party applications.
    d. Centralized reporting and capacity planning.
    e. Management of 4G and 5G network services.
    f. Communication between all Edge Nodes and Controllers uses Internet Protocol Security (IPsec) and mutual Transport Layer Security (TLS) for network communication, leveraging native Controller Public Key Infrastructure (PKI) services and X.509 client and server authentication for all endpoints.
2. Intel Smart Edge Node - The Edge Node software is installed on Dell servers, leveraging Intel central processing units (CPU), that are deployed to any location with an edge computing workload requirement. Under the direction and control of the Controller, the Edge Node software provides:
    a. Application lifecycle management
    b. Comprehensive zero-trust security
    c. Operational telemetry
    d. Policy enforcement
    e. Data routing and filtering
    f. Hardware management for applications, virtual machines and containers

The Intel Smart Edge node software supports multiple access topologies including wired and wireless. This flexibility enables a broad array of environments including WiFi6, Private LTE, or 5G.

The Controller and Edge Node are enabled in an all-in-one hardware and software solution to decentralize the network and the cloud, enabling computation at the on-premise edge of the network. The software was built with security as the primary foundation while emphasizing an effortless user experience. The platform empowers enterprises to simplify implementation of new services, such as optimized, high priority content or applications. It also enables software defined functions and network context to localized edge deployments of applications, excelling in enterprise environments that heavily leverage and depend upon mobile devices.

Intel® Smart Edge Security

Intel Smart Edge security capabilities use a zero-trust model for all connections, users, and applications (including internal microservices), which reduces attack surfaces therefore reduces attack opportunities by only enabling data flows from authenticated devices. If traditional security is analogous to the locks of the exterior door of a house, the Intel Smart Edge platform extends the traditional boundary threat protection with locks and surveillance on every door, hallway and room. This provides a new, powerful control point to help manage malicious adversaries, allowing interception, blocking, and control before traffic is allowed beyond the first network hop.

- Privacy: all control traffic is encrypted
- Authenticity: all communication is between agents authenticated against an internal PKI trust
- Integrity: all communication is cryptographically signed using asymmetric keys
- Strict Whitelist: authorization is only granted with explicit roles and permissions to authenticated actors
- External Security Assertions: third party network authentication for local MEC networks and MEC unique metadata, such as location
- Proxy Authentication: leverage existing LTE authentication sources for external applications or networks
- Secure Edge Services: only authorized applications can run to process User traffic or provide services to connected devices

Intel® Secure Device Onboarding (SDO)

Intel® Secure Device Onboard is an automated "Zero-Touch" onboarding service. To more securely and automatically onboard and provision a device, it only needs to be drop shipped to the point of installation, connected to the network and powered up, SDO does the rest. This zero-touch model simplifies the installer's role, reduces costs and helps eliminate poor security practices, such as shipping default passwords.

SDO Benefits:

- Zero touch onboarding – integrates readily with existing zero touch solutions
- Fast and more secure – ~1 minute
- Hardware flexibility – any hardware [from ARM micro-controlled unit (MCU) to Intel® Xeon® processors]
- Any cloud – internet and on-premise
- Late binding – of device to cloud greatly reduces number of SKUs vs. other zero touch offerings
- Open – LF-Edge SDO project up and running, SDO code now on GitHub
- Industry standard – FIDO Alliance has released 1st spec draft based on SDO
- Download target software – Install the desired Operating System (OS or Hypervisor) at the Point of commissioning with SDO plus Bare Metal on Board option.

Configuration

The architecture deployed for this industrial customer is given in Figure 2. Intel Smart Edge software is written to work with any device that can be connected into a network (note that there may be need for middleware for protocol conversion based on application requirements). As the ecosystem evolves there are more and more options for LTE and for 5G enabled devices. For legacy devices, there are many universal serial bus (USB) dongle options available. Since Intel Smart Edge is designed for a virtualized environment, applications can be run in either containers or virtual machines (VM). For this customer, the solution was run entirely on-prem; however, Intel Smart Edge is designed to work with all major cloud service providers (CSP).

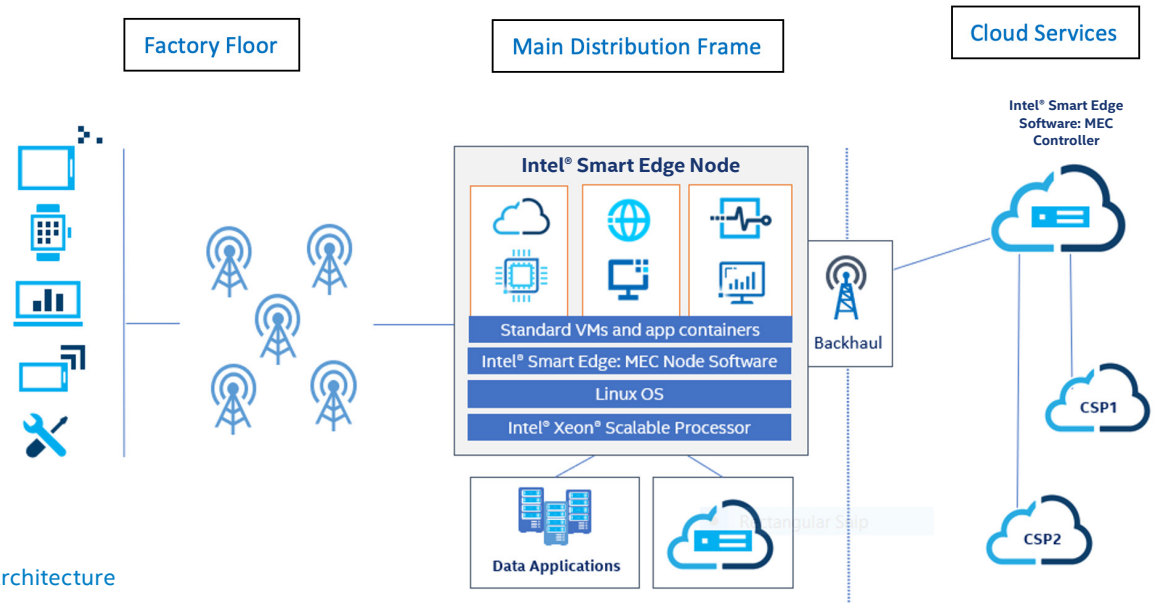

Figure 2. Architecture

Value of Dell/Intel Hardware

The Intel Smart Edge Software was implemented on Dell PowerEdge R740 servers featuring Intel® Xeon® processors. The Dell R740 provides a robust way to operationalize and secure the network and compute edge. The R740 is designed for use close to the factory floor. For the work with this customer, the server was located in a rack in a storage room close to the factory floor.

Conclusion

The factory floor no longer needs to be hard wired to facilitate data access. Given the capabilities of private LTE and 5G coupled with Intel Smart Edge, it is now possible to wirelessly, easily and securely access data on the factory floor.

For more information, email us at smartedge@intel.com or visit Intel.com/smartedge.

Acronyms

API	Application Programming Interface
CBRS	Citizens Broadband Radio Service
CDN	Content Delivery Network
CNF	Cloud Native Network Functions
CPU	Central Processing Units
CSP	Cloud Services Platform
DDoS	Distributed Denial-of-Service
eNodeB	Evolved NodeB
HSS	Home Subscriber Server
HW	Hardware
IoT	Internet of Things
IIoT	Industrial Internet of Things
IPsec	Internet Protocol Security
LTE	Long-Term Evolution
MCU	Microcontroller Unit
MDF	Main Distribution Frame
MEC	Multi-access Edge Compute
MNO	Mobile Network Operator
MME	Mobility Management Entity
NFV	Network Functions Virtualization
NFVI	NFV Infrastructure
PKI	Public Key Infrastructure
RAN	Radio Access Network
REST	Representational State Transfer
RFID	Radio-frequency Identification
SDN	Software Defined Networking
SDO	Intel Secure Device Onboarding
SD-WAN	Software-defined Wide Area Networking
SIM	Subscriber Identity Module
SKU	Stock Keeping Unit
SW	Software
TLS	Transport Layer Security
USB	Universal Serial Bus
VM	Virtual Machine
VNF	Virtualized Network Functions
Wi-Fi	Wireless Fidelity (Wireless Network)

0621/DL/ICKK/PDF 347021-001 EN