

Intel® Smart Edge : Manufacturing

Executive Summary

Manufacturers seeking the benefits of Digital Transformation are grappling with many of the same issues as it relates to digital transformation within factory and manufacturing operations. Increasingly, infrastructure based on the public wireless spectrum does not provide the same level of reliability and robustness of carrier-class wireless technology like LTE or 5G, which is built for uninterrupted operation in the harshest environments. In addition to reliability of communications, the factory floor and applications in use, necessitate fast response times and timely access to data that are not readily available with far distant public cloud offers. Intel® Smart Edge solutions provide robust communications services as well as on premises compute, network and storage for legacy and emerging compute requirements.



Manufacturing Needs

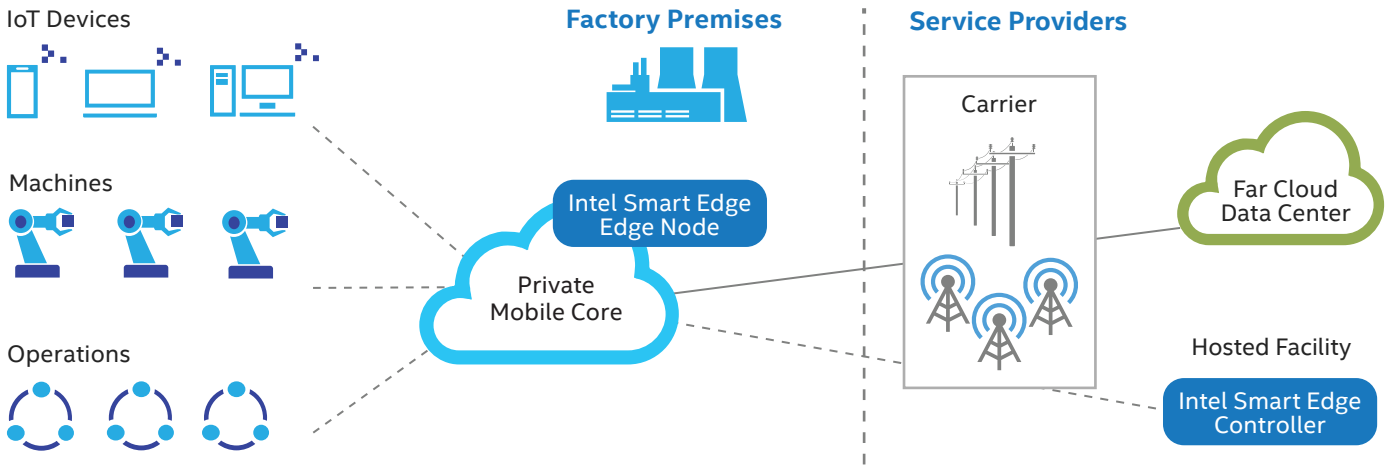
The advent of cloud computing has created tremendous advantages and opportunities. This evolution has impacted nearly every industry in varying orders of magnitude. Still, the bulk of manufacturing applications run inside the enterprise network. Increasingly, the requirement to collapse adjacent technologies into a single form factor—in both software and silicon—has come to the forefront. On the factory floor, a close integration with communications facilities built on LTE, and recently expanded to include Citizens Broadband Radio Service (CBRS), combined with high-performance, virtualized compute and modular storage, provides many benefits. These include:

- **Privately Managed Mobility and Automation.** Carrier-class wireless connectivity using managed or licensed spectrum must be easily deployable and simply operated on an ongoing basis. Private LTE, encompassing leased-licensed and CBRS spectrum, provides the comprehensive consistency and control that mission critical applications require. In addition, carrier-class wireless in the form of LTE reduces network downtime and provides a robust communications service that consumer-grade unlicensed wireless technologies do not. A private network as described supports the “factory of the future”—further enabling progress toward comprehensive automation throughout a manufacturing facility.
- **Local Application Access for Lower Latency.** Traditional carrier services used a structured networking approach that often introduced latency between device and application. Based on secure policy, an edge compute solution with analytics that are tightly integrated with wireless connectivity selectively directs desired traffic to the correct local resources. This cuts round trip delays and overall latency, thereby ensuring instantaneous access to local applications and data storage.
- **Zero Trust Security Model.** The software of any contemplated solution must ensure that remotely deployed edge compute comprehensively protects the increase in “attack surface”. Leveraging asymmetric cryptography and strict mutual authentication for control interfaces is a critical requirement. In addition, policy-driven operation combined with centrally controlled permissions ensure that only legitimate traffic flows between applications and devices.

Proposed Solution

The Internet of Things (IoT) arena includes the ability to securely and automatically onboard and enable entire classes of devices, or things. Intel® Secure Device Onboard (Intel® SDO) is a capability that when used with Intel Smart Edge can enable endpoints to communicate securely with Intel® Smart Edge software without the threat of potential “man-in-the-middle” attacks. Intel SDO helps prevent the hijacking of devices in a distributed denial of service (DDoS) attacks by creating a trust relationship between the Intel Smart Edge software and all manner of IoT devices.

Intel Smart Edge is a multi-access edge computing (MEC) platform and has the ability to connect all premises devices and applications over a robust carrier-class private wireless network to local compute and storage on the premises. Should far cloud resources or public carrier services be required solution elements, access to those service providers is further enabled and governed by the Intel® Smart Edge node. The diagram below provides a simple reference for the topology:



Benefits & Outcomes

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

- Secured operational environment
- Higher performing compute and storage
- Ease of deployment and use
- Faster responses and lower latencies

The Intel Smart Edge platform provides complete application life-cycle services for the network 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 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.

The Intel Smart Edge software can be implemented on Intel® Xeon® processors-based servers to offer a robust way to operationalize and secure the network and compute edge. Additionally, Intel SDO ensures automated deployment of endpoint devices enabling a chain of trust between them and other resources. Intel® Software Guard Extensions, enable secure enclaves with the Xeon processor, which can also help increase the security of application code and data, giving them more protection from disclosure or modification. With this portfolio of Intel technology, manufacturing environments can implement a secure, high-performance edge compute frameworks for manufacturing floor applications.

Find more information

To learn more about the Intel Smart Edge solution, please contact us at smartedge@intel.com.

Disclaimers

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

344048-001US 0820/FS/JAG/PDF

