WHITE PAPER

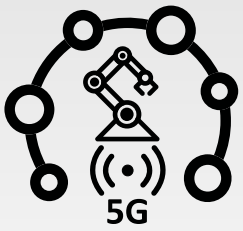
Security Considerations in Industrial 5G Environments

Executive Summary

The convergence of market demand and new digital capabilities is helping companies transform their operations. Industry 4.0—which includes connectivity, advanced analytics, automation, and advanced-manufacturing technologies—was gaining momentum before the recent market effects of the global pandemic. Organizations utilizing digital solutions have moved faster and further than their peers during the crisis, in everything from production efficiency to product customization, with improvements in speed to market, service effectiveness, and new business-model creation.

Using digital technologies such as 5G is top of mind for many, and this nascent demand is creating new 5G supply players, ecosystems, services, and business models to capitalize on this unique opportunity.

5G survivors and winners in this supply-and-demand environment will be the ones that can best meet, deliver, adopt, and implement the technology and services as an integral part of an ecosystem that is the core of enterprises' and industry verticals' transformation and innovation.



The adoption of 5G technology by enterprises will support and accelerate Industry 4.0, but enhanced security considerations and architecture are required in 5G-enabled industrial environments.

From the demand side, there is a major evolution from just consumer and enterprise employees' mobility driving growth to 5G's integration into enterprises' core technological, operational, and business aspects, becoming the main growth engine for 5G. And within this enterprise landscape, industrial verticals are the early adopters.

The 5G market brings new stakeholders and dynamics to bear with the potential to significantly reshape competition and the balance of power in this market.

And when it comes to core technology in critical enterprise use cases, security is fundamental. Security can be a barrier or an enabler for 5G adoption in enterprise verticals. A Verizon 5G business report places security and compliance concerns as the second challenge or barrier to 5G adoption by enterprises.[1] Security is top of mind on the enterprise demand side, and therefore must be top of mind in the industrial 5G supply-side and incorporate security solutions and service offerings.

5G Value and Place in Industrial Environments

5G can significantly enable and accelerate industrial transformation and innovation like no other communications and networking technology:

- Enhanced Mobile Broadband (eMBB) delivers high data rates, enabling data-driven applications and industrial use cases, such as augmented reality-based maintenance.
- Massive Machine-Type Communications (mMTC) supports highly scalable sensor networks and provides high indoor penetration and position accuracy, allowing for a high degree of mobility and flexibility in demanding industrial environments while delivering the required quality of service (QoS) and asset tracking.
- Ultra-Reliable Low-Latency Communications (URLLC) enables the critical nature of wireless connectivity in critical industrial use cases with ultralow latency required for real-time applications such as mobile robots and closed-loop process control.
- 5G New Radio (NR) high-positioning performance enables asset-tracking use cases in multiple verticals, both indoor and outdoor applications.
- Control and User Plane Separation (CUPS) enables better control of data flows to applications and locations so that sensitive data can stay on-premises.
- Network Exposure Functions (NEF) provides an interface for applications to program some aspects of the 5G network and services to meet dynamic requirements of mobile and critical industrial environments and use cases.

Combining these capabilities as a networking platform, 5G is seen as the network of the future for industrial environments, as it enables a significant number of industrial innovations.

5G Consumption in Industry Verticals

5G can be consumed by enterprises as required by their needs. A private 5G network empowers enterprises to have complete control and customization, better transparency, data privacy, and flexibility. On the other hand, a private 5G can be expansive, complex, and lengthy to implement and maintain. Consuming public 5G is significantly more cost-effective and rapid but offers lesser control and customization. It seems that private and hybrid (a combination of private and public 5G consumption) 5G networks will be the popular 5G enterprise consumption form. However, recent studies show that enterprises considering 5G would rather use private 5G networks than public, due to the critical and sensitive nature of industrial environments, processes, and operations.

Security in Pre-5G Industrial Environments

Operational technology (OT) is a vital component of many functioning enterprise verticals, such as manufacturing, energy, utilities, transportation, and logistics. OT consists of hardware and software that detects or causes a change by monitoring and controlling industrial equipment, assets, processes, and events. Much OT spending is related to the convergence of OT infrastructure, such as supervisory control and data acquisition (SCADA) systems with IT networks, extracting, understanding, and applying information to boost operational efficiency and profitability. Historically air-gapped from the internet, OT systems now depend on information from enterprise and third-party IT systems to effectively manage operations in real time. However, this improved agility and effectiveness come at the cost of increased risk. Many of today's OT systems face all the threats that IT systems face.

Security in these environments has been mostly implemented based on the classical ISA99 Purdue Enterprise Reference Architecture, which outlines the key infrastructure layers used in ICS environments and the boundaries between them where security is required, as outlined in Figure 1.

A key to Purdue reference architecture is its hierarchical nature, whereby each layer within the segments can only interface and communicate with the layer above and below it. Therefore, the establishment of horizontal enforcement boundaries between segments and layers.

Figure 1: ISA99 Purdue reference architecture..

5G Mandates an Enhanced Purdue Reference Architecture

When introducing 5G in an industrial environment with 5G-capable devices and platforms in the different Purdue model layers, the hierarchical nature of data flow between the layers is no longer valid.

5G-connected devices, platforms, and applications can now send and receive data directly via flows that do not necessarily pass through the Purdue model-defined enforcement boundaries, as demonstrated in Figure 2. This mandates the addition of an additional security boundary at the 5G domain with the following high-level functionalities:

- OT/Industrial Internet of Things (IIoT) security visibility and control
- 5G network security
- Industrial applications security

Deploying 5G use cases in production will take time as devices, applications, 5G technology, experience, and know-how are mature and reliable enough to be deployed. It is essential that alongside this evolution of 5G deployments in enterprise verticals, the appropriate security considerations are taken and implemented throughout the industrial environment, including the 5G network, services, and overall use cases.

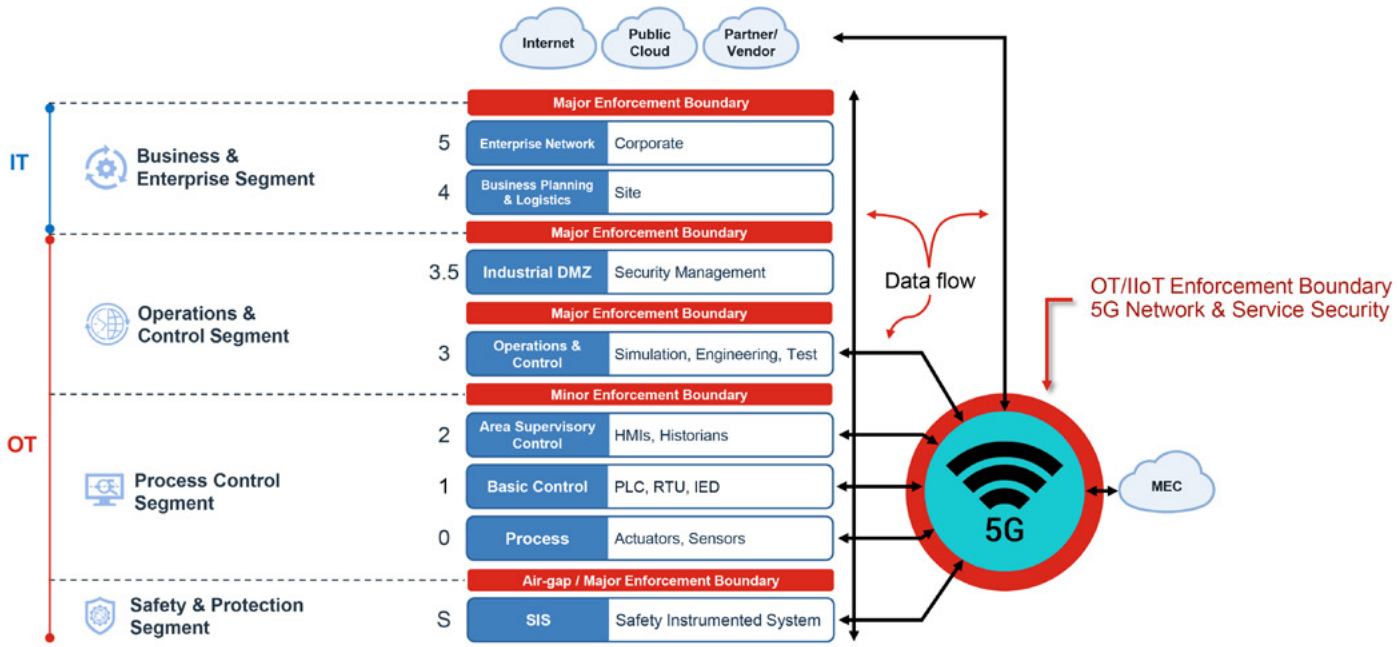


Figure 2: Enhancement to ISA99 Purdue reference architecture in a 5G industrial environment.

Holistic Security in 5G-enabled Industrial Environments

5G is only an enabler for many new industry verticals use cases. Delivering these use cases requires an integrated ecosystem of technologies and partners: OT/IIoT vendors, ICS vendors, 5G vendors/providers, industrial applications providers, hyperscalers, and integrators.

Many organizations assume that a private 5G network will inherently keep them safe, which is not necessarily the case. 5G private networks are rarely entirely isolated from the enterprise IT environment and external environments (partners, integrator, public cloud, etc.) and may be exposed to internal and external attacks and risks resulting in productivity and production degradation, compromised physical safety, and brand degradation. An increase in OT and IIoT exposure, the mobility of users and devices on the network, and the interplay among the enterprise, mobile network operators, IoT manufacturers, and OT vendors and suppliers all also contribute to 5G security challenges, whether the network is private or not.

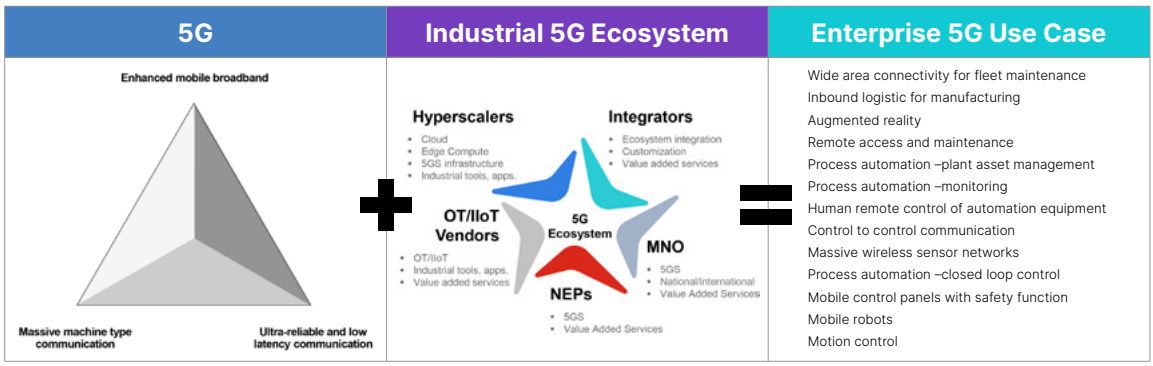


Figure 3: 5G part of a larger ecosystem to deliver 5G-enabled use cases.

When considering security in industry verticals for years to come, the security of such an end-to-end supply chain and ecosystem must be considered. And not just the security of its components and in the context of a hybrid industrial environment where traditional and 5G-enabled components, processes, and use cases exist. Furthermore, organizations must consider the capacity and knowledge required to manage the rapidly expanding landscape of connected OT.

Fortinet Security Fabric Platform as an Enabler for Industrial 5G

The security of an industrial environment is only as strong as its weakest link. With the ongoing OT-IT convergence, assets digitization, and digital transformation initiatives, **the introduction of 5G into industrial environments represents a complex technology that expands the industrial attack surface.** The above and other security considerations should be structurally, methodologically, and proactively implemented as enablers for impactful 5G adoption in enterprise verticals.

The Fortinet Security Fabric is a unique security platform that encapsulates IT, OT, IIoT, and 5G security with broad visibility, control, and value-add services, empowering 5G providers, industrial enterprises, and system integrators to secure critical traditional and 5G-enabled use cases over private, public, and hybrid 5G networks and services.

- Integrated and automated end-to-end cybersecurity mesh architecture that covers IT, OT-specific capabilities, ICS, and 5G across multiple locations and architectures
- Security visibility and control for 5G user and control planes, and multi-access edge compute (MEC) infrastructure and applications
- Consolidate networking, cybersecurity, and surveillance functions in an industrial environment into a single system, with complete visibility and control on a single pane of glass
- A broad selection of ruggedized security appliances to fit all environmental needs and to support business continuity in the most punishing industrial environments
- A comprehensive solution to guard against insider threats, including intent-based segmentation, deception technology, and user and entity behavior analytics (UEBA)
- FortiGuard labs robust threat intelligence specific to OT, ICS, and 5G systems

In addition to the broad portfolio of Fortinet security tools, specialized OT and 5G solutions can be integrated seamlessly with the Fortinet Security Fabric through the ecosystem of Fortinet Fabric Partners.

[1] Verizon 5G Business Report, Verizon, December 2020.

March 24, 2022 8:20 AM

1394108-0-0-EN