Towards the Resilient Factory of the Future

Telefónica and Fortinet value proposition
The whole industrial sector is living a deep transformation process that involves embracing digital technologies to boost productivity and to respond to competitive threats. In our view, connectivity and mobility are key components of the Factory of the Future and we believe that only the combination of private 5G and edge cloud can meet the stringent requirements that the wave of automated industrial processes need in terms of low latency, high bandwidth, and massive number of connected devices.

At the same time, massive connectivity and cloud computing mean exposing assets and systems that have been traditionally isolated, which raises the relevance of the cybersecurity risks. Typical factory assets such as sensors, engines or robots have traditionally remained in air-gap environments. But now, these devices are being connected with remote systems and platforms. Although new 5G access networks come with robust security mechanisms, protecting the services underpinned by these networks requires analyzing its cybersecurity requirements with an end-to-end approach including the devices, platforms and applications that are part of the services. In addition, these new factories will be connected to legacy infrastructures and, therefore, we also need to consider their specific requirements. These topics are developed in this document.

Section 2 details how 5G and edge cloud can be combined to implement new disruptive use cases for factories to enable business transformation. Section 3 presents the cybersecurity challenges that industrial organizations face, especially when cellular private networks are present. As 5G is still actively evolving, this specific topic is a work in progress and this document describes our current vision and approach on this topic. Finally, Section 4 presents our cybersecurity proposal followed by the conclusions section.
02 Telefónica-Tech’s 5G & private cellular network approach

The next wave of digitalization is appearing at the convergence massive of IoT, Big Data and Artificial intelligence enabled by seamless mobility and the new generation of infrastructure platforms including edge and cloud computing. Some examples of the new use cases emerging now are: Automated Guided Vehicles (AGV) carrying goods around factories, fully integrated logistics and production chains that reduce the time components and goods remain idle, flying drones with computer-aided vision for surveillance and inspection, robotic arms that carry preventive maintenance during scheduled pauses of the production chain. Innovation in this space is moving fast and a myriad of new use cases will continue to appear fueled by new connectivity and computing capabilities.

5G sits at the heart of this transformation by bringing secure, Gbps, low latency and wireless connectivity with deterministic QoS control that can connect a massive number of IoT devices ranging from basic sensors and meters to advanced robots and vehicles. All these advanced characteristics cannot be met by other technologies like Wi-Fi or Ethernet. 5G is the best choice for the industry sector to implement use cases with strict security, performance and/or control needs. Private 5G edge cloud – defined as dedicated connectivity, coupled with edge compute – will enable business transformation with an estimated impact of 60 billions of euros worldwide according to Arthur D. Little1, with much of these volume centered around industry 4.0.

Implementations today of Private 5G Cloud are being driven by use cases that have strict and advanced requirements that traditional technologies cannot meet:

- **Wireless connectivity**: to adapt to increasingly flexible enterprise environments with non-static objects cutting the cord becomes critical. Wireless connectivity is used to connect tools and devices, i.e. Automated Guided Vehicles (AGV) and to simplify the relocation of equipment inside the factory floor for evolving manufacturing processes.

- **High performance connectivity**: Guaranteed and secure Gbps connectivity for devices that generate great amounts of data. Drone-aided video surveillance or quality control based on computer vision require transmitting high quality video in real-time uplink. QoS control and high throughput is fundamental.

- **Low latency**: We are entering the ms era. Real-time automated decisions is becoming increasingly important. 5G and edge computing improve latency by two orders of magnitude versus traditional solutions. This enables real-time remote control of robotic arms and worker safety controls.

- **Data sovereignty**: Complete control on where data is stored and processed is increasingly important due to security/privacy requirements from enterprises and/or regulatory compliance. Not all data can be taken to the cloud, but must be securely stored locally.

- **Seamless multi branch operation**: Enterprises have their productive processes run at different heterogeneous sites and facilities, making it difficult to manage them by IT/OT teams. Secure connectivity is required amongst branches, private and public clouds and external services.

- **Disaster recovery procedures**: including fallback connectivity using the operator public cellular network to guarantee service continuity and application and data store redundancy.

- **Cloud Continuity**: Digitalization processes have pushed enterprises to increase the number of cloud environments and even migrate in some cases to the public cloud. Homogenizing the technology stack, tools and processes throughout the distributed environments becomes critical to reduce operating costs and experience.

---

Delivering Private 5G use cases requires constructing a complex puzzle with specific integrations between all the solution components (connectivity, cloud, devices and applications). This results in special purpose-built projects with high complexity and delivery costs without any economies of scale.

Telefónica’s approach focuses on three components: 5G communications, edge computing and value added services.

### Connectivity
Business grade connectivity ready to support customer solutions.
- **On-premises connectivity**
  - Local connectivity fully dedicated to a final customer
- **Public connectivity**
  - Connectivity provided by Telefónica public network

### Computing
Computing power dedicated to run the SW applications, either networking (VNF, CNF) or SVA (business applications).
- **On-premises computing**
  - Local computing environment fully dedicated to a final customer
- **Shared computing**
  - Computing infrastructure out of customer premises

### VAS (Value added service)
Full end to solutions for vertical business. Ready to purchase and plug and play.
- **Business App**
  - Specific vertical business solutions
- **Business Equipment**
  - Customer equipment associated with specific SVA solution

Figure 1. Telefónica’s approach components

The approach can have specific flavors to tailor performance, security, control and business models required. The two more extreme visions for this space are shown below, the on-premises flavor with all elements deployed on the customer premises and the as a service flavor that leverages the Telefónica public cellular network and edge computing.
**Option 1: On-premises**

For those businesses that demand the best performance, ownership and control over their production processes, the on-premises flavor offers a full on-premises 5G radio network with a 5G Core network to keep all the information of the company on-premises. It also features a managed computing environment to host the applications of the company that require the highest performance.

**Option 2: As a service**

Other companies may prefer a simpler approach that doesn’t require to deploy new pieces of equipment nor having dedicated computing elements on their premises. The as a service flavor leverages Telefónica’s public 5G network and edge computing by defining a dedicated virtual space for the customer, that includes some dedicated resources on the cellular network and a virtual data center in the Telefónica’s Edge to run the applications of the company.
The following table compares the two visions:

<table>
<thead>
<tr>
<th></th>
<th>On premises flavor</th>
<th>As a service flavor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TCO</strong></td>
<td>Higher</td>
<td>Lower</td>
</tr>
<tr>
<td><strong>Recurrent fee</strong></td>
<td>Lower</td>
<td>Higher</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td>Highest possible</td>
<td>Business critical</td>
</tr>
<tr>
<td><strong>Latency</strong></td>
<td>Single digit milliseconds</td>
<td>Tens of milliseconds</td>
</tr>
<tr>
<td><strong>Capacity</strong></td>
<td>Tens of Gbps</td>
<td>Hundreds of Mbps</td>
</tr>
<tr>
<td><strong>Time to deploy</strong></td>
<td>Weeks</td>
<td>Days</td>
</tr>
<tr>
<td><strong>On-premises facilities</strong></td>
<td>Server room with A/C and wall/ceiling mounts for RAN</td>
<td>None</td>
</tr>
</tbody>
</table>
3.1. Overview of the general challenges

Although this paper is specifically focused on the cybersecurity challenges of the Factory of the Future where private cellular networks have a key role, it is worth to start by providing context on the current challenges that the industrial sector already face.

Next generation factories will include assets, networks and services that are still being defined, but they will need to coexist with legacy environments and, hence, the cybersecurity challenges of the existing environments need to be considered, too. As a result, any industrial company faces cybersecurity challenges that we can arrange in three stages, as depicted in Figure 4.

Most companies with legacy plants that have been built over many years lack an updated and accurate inventory of their networks and assets. As this infrastructure underpins the organization productive processes, it is extremely important to guarantee the business continuity. An initial cybersecurity assessment provides visibility on the assets, services and network architecture as well as an identification of the potential risks. Typical findings of those assessments are uncontrolled remote accesses, weak passwords in platforms and devices or evidences of malware activity. Afterwards, a cybersecurity master plan to addresses its mitigation must be defined.

Once an organization has identified the risks and prioritized the corrective actions, it is in a good position to start deploying more advanced cybersecurity solutions as represented by the mid-term group of challenges in Figure 4. The three components of cybersecurity solutions need to be considered:

- **Processes**: some actions will need to be changed to be more resilient. E.g., remote access will add robust authentication, monitoring of malicious actions and recording of relevant information in case a later investigation is required.
- **People**: As they are the users of the infrastructure and the services, awareness and training about the new solutions will need to be provided.
- **Technology**: meaning the specific solution that will need to be deployed in the selected environment.

The most innovative industrial organizations are already starting to design, build and deploy new services that leverage the capabilities provided by 4G and 5G cellular private networks. Security needs to be implemented from the beginning as it simplifies and reduces the cost in the long run. This is already represented in the last picture of the Figure 4.
3.2. **Focus on use cases underpinned by private cellular networks**

Private cellular networks, understood as the bundle of high-performance connectivity plus managed computing environments, are one of the key elements for the digital transformation of the industrial sector in the following years. They are cutting the cord in the production environment and can provide a seamless and predictable mobility inside and outside the production facilities. This will enable a technical revolution similar to the one the phone industry faced when cellular technology was introduced first and then came the smartphone, where numerous applications have appeared that were unthinkable in the good times of the Plain Old Telephone Service (POTS).

Private cellular networks are critical systems that must be secure by design. On the one hand, they are key for keeping the daily business operations running and, on the other hand, they manage and store some of the most critical and sensitive pieces of information of the company.

### 3.2.1 Connectivity challenges

Wireless technologies can be both a blessing and a curse, as they provide connectivity from anywhere, but they can also increase the exposure of the company assets to potential threats compared to a wired network scenario. Fortunately, 5G cellular networks provide the most secure radio technology because they leverage all the knowledge acquired throughout the last decades in the public mobile networks, including network access control and auditory, usage metering, quality management and control, and proper assignment and prioritization of resources. The 5G Radio Interface makes use of the most advanced cryptographic algorithms for device admission control and traffic encryption. The 5G Core Network makes use of mTLS to secure its control traffic plane and can be split so that its elements critical for performance are deployed on premises while the rest are centralized. This split core uses carrier-grade VPNs, ACL and traffic flow filters to isolate and secure the traffic.

Finally, the traffic coming out of the radio access network needs to be seamlessly integrated into end-customer’s network. For this purpose, SD-WAN technology can help with its intelligent routing, rich failover mechanisms and VPN stitching.

### 3.2.2 Computing and applications challenges

The computing platform is critical, as all the applications of the industrial companies run on it. The security of the computing infrastructure must take into account the strictest guidelines both for classical servers or hyperscaler public clouds. The approach by Telefónica is to guarantee that each application is run in a virtual environment fully isolated, safe and secured from external parties.

Firstly, each application image must be pre-validated, to search for any security vulnerability, library security issue or any hidden malware before it is made available to customers.

Then, the computing must guarantee complete isolation amongst applications –CPU, memory and disk– and amongst the networks where the applications connect to. This is made possible by the most restrictive possible base scenario where all the communications, inter-process communications and system interactions are forbidden by default with explicit description of those that are allowed.

Finally, the factory applications and services must be updated quickly after their vendors release new versions so that the latest security fixes are applied.
4.1. General approach to industrial cybersecurity projects

In order to provide visibility on the assets, networks and security risks in any industrial environment, Telefónica Tech has developed a methodology called METEO that is further explained in a previously published document\(^2\) and that we use here to explain the general approach for industrial cybersecurity projects.

![Figure 5. Methodology for Operational Technologies and Environments (METEO)](image)

The two first stages of METEO describe the proposal for facing the short-term challenges. Firstly, the current cybersecurity profile has to be assessed. This assessment is based on several activities aimed at determining the compliance level of the selected targets and on a technical assessment in which the network traffic of key plants and factories is analyzed and some controlled cybersecurity exercises are performed. Secondly, based on the conclusions of this report, a cybersecurity master plan is defined, where the enterprise sets the goals and the desired target profile.

One of the best practices for the security assessment is to use a well proven cyber-security model as a reference. This enables a structured and systematic analysis of the security requirements and challenges of 5G private networks. In this document, we use an evolved version of the Purdue Model that has successfully been applied to OT Security and that is represented in the following figure.

---

Industrial IoT (IIoT), wireless, 5G, and other trends have implications for OT environments that are frequently built on the Purdue Enterprise Reference Architecture (PERA). This model provides a good structure for the security analysis and design, as it describes a hierarchical set of levels for applications and controls.

- **Levels 0, 1, and 2** (the process control zone) define physical processes, sensors, actuators, and related instrumentation as well as the systems that supervise these implementations.

- **Levels 3 and 3.5** (the operations and control zone) describes overall manufacturing operations across multiple processes. Together, Levels 0-3.5 comprise an OT environment.

- **Levels 4 and 5** are collectively known as the business zone, comprised of enterprise IT systems and applications. First conceived in the early 1990s, the original Purdue model did not anticipate IIoT, wireless, or cloud connectivity. Fortinet has been promoting an enhanced Purdue model over the past several years. To be architecturally agnostic, the IIoT device and platforms as well as wireless devices are represented laterally in an unlayered "Zone 6" that physically resides in the security perimeter within OT.

---

**Figure 6. Purdue Security Model applied to 5G private networks**

<table>
<thead>
<tr>
<th>Purdue Levels</th>
<th>Major Enforcement Boundary</th>
<th>Wireless Boundary</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Enterprise Network</td>
<td>Corporate</td>
</tr>
<tr>
<td>4</td>
<td>Business Planning &amp; Logistics</td>
<td>Site</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Levels</th>
<th>Major Enforcement Boundary</th>
<th>Wireless Boundary</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5</td>
<td>Industrial DMZ</td>
<td>Security Management</td>
</tr>
<tr>
<td>3</td>
<td>Operations &amp; Control</td>
<td>Simulation, Engineering, Test</td>
</tr>
<tr>
<td>2</td>
<td>Area Supervisory Control</td>
<td>HMI, Historians</td>
</tr>
<tr>
<td>1</td>
<td>Basic Control</td>
<td>PLC, RTU, IED</td>
</tr>
<tr>
<td>0</td>
<td>Process</td>
<td>Actuators, Sensors</td>
</tr>
</tbody>
</table>

**Digital Assets**

- **SIS**
  - Safety Instrumented System

**Enforcement Boundaries**

- Cloud
- Wireless (Wi-Fi, 5G)
- Industrial Wireless (RAN, Wi-Fi, 5G)
- Major Enforcement Boundary
- Major Enforcement Boundary
- Major Enforcement Boundary
- Major Enforcement Boundary
- Major Enforcement Boundary
The third stage of the METEO approach involves implementing cybersecurity solutions and initiatives according to the previous master plan. We will focus on those that apply to the cellular private networks in the next section, but the solution also involves adapting processes and training personnel to make them aware of the changes.

Finally, as security is a process and not a state, the cybersecurity solutions implemented following the METEO methodology need to be managed and integrated with the rest of the cybersecurity controls. We leverage on our Security Operations Centers (SOCs) in order to provide managed security services that cover the IT, OT and IoT infrastructure of our customers (Figure 7).

Managed detection and response for OT and IoT infrastructures is a good example of this kind of service in which specific knowledge and experience is required. On one hand, the security monitoring solution needs to be deployed in the customer’s infrastructure. It requires a thorough preparation process to define its architecture, which includes deciding the points where the sensors are to be deployed and how the network traffic will be captured.

On the other hand, as any other security monitoring technology, it will generate tons of events that need to be properly aggregated, correlated and analyzed to be transformed into meaningful alerts. It can be accomplished with tools and technologies available in our SOCs (e.g. SIEMs, SOAR), but requires the definition of detection and response use cases that meet customer’s needs.

For those readers interested in this kind of services, a specific document has recently been published³.

---

4.2. Focus on use cases underpinned by private cellular networks

As mentioned before, private cellular networks enable a broad range of services with high requirements in terms of bandwidth, latency or mobility. These services are based on a set of elements that can be classified according to the following groups:

- **OT & IoT devices** are spread all over the factory. They produce information (sensors...) and/or consume information (robotic arms) and therefore they have communication needs.

- **End-user apps** are mobile and computer applications used by the factory personnel.

- **5G access** is the radio access network that connects devices with the rest of network. It is in the factory.

- **5G core** is the core network that is responsible for the mobility, access control, connection management of the devices. It can be on premise of the factory, in Telefonica’s edge or in Telefonica’s central data centers.

- **Value added services (VAS)** for the devices, the factory personnel or other VAS. They can be in the factory or in a public external location. They can use a shared computing.

- **Third party interfaces** are used to expose specific functionality to partners and other parties.

Figure 8 shows an example of the use of a framework in order to analyze and identify the security risks and requirements for each valued added service. The example is used to protect a set of robotic arms, their control process and its monitoring service. The factory operators can monitor and control remotely the robotic arms using specific applications. Finally, an API (application program interface) provides data for predictive maintenance support to the robotic arm manufacturer.

![Figure 8. Robot control and monitoring service.](image-url)
There are several references that can be used to identify the security capabilities that are required for protecting this specific IIoT service, such as the ISA/IEC 62443 standard or the NIST Cybersecurity Framework (CSF), although they need to be adapted to this new context. What follows is a list of the most relevant ones:

- **Endpoint (Robot) Protection.** Typically, OT/IIoT devices have been in air-gap networks isolated from other networks. With 5G, these devices will connect to remote platforms to increase their functionality and simplify their maintenance. Many of these new devices require agent-based solutions to detect and prevent attacks directly in the endpoint computing platform.

- **Signaling Protection:** With a large number of IIoT endpoints there is always a risk of signaling storms—either intentional (as a result of a cyberattack) or unintentional (as a result of key element restarting). The 5G infrastructure has to be protected against any denial of service.

- **Network Segmentation and micro-segmentation:** Many OT assets have limited cybersecurity capabilities across a longer life cycle than traditional IT devices. As such, OT devices will need to rely on strong network perimeters by segmenting critical OT networks from corporate communication networks. OT network segments leverage on Demilitarized zones (DMZ’s) and security zones.

- **Network Access Control (NAC):** NAC decides whether a device can access a network or not. It is applicable for all communication network boundaries. The NAC solution integrates different authentication and authorization capabilities, including the SIM and 802.1X. In Wi-Fi networks, the NAC has to cover the AP, the switch and the firewall for a granular access control for IIoT.

- **Asset Management:** consists of understanding the devices within a specific environment through a current device inventory that includes parameters for securing those devices, such as associated software and firmware versions, known security controls and criticality of the asset itself.

- **Intrusion Detection and Prevention:** IIoT devices are prime candidates for attack, mainly because they can “short circuit” multiple layers of the Purdue model and provide direct access to devices at the lowest layers. This security capability allows detecting these activities by analyzing network traffic and detecting specific malicious activity using signature-based mechanisms but also by detecting anomalies such as unusual values of process variables.

- **Application Visibility and Control:** The operators of the factory can monitor or limit which protocols can be used by the device as well as the applications with which it can communicate. Commonly used Industrial and IoT protocols (such as MQTT, AMQP, HTTP, and CoAP) are covered, and transport layer security (TLS) inspection can be performed. An analyzer provides a high-level security-operations-center (SOC) view, with the ability to drill down to specific events.

- **Software Defined-WAN (SD-WAN):** intelligent routing is applied to egress traffic so that the optimal route is taken and traffic flows are seamlessly integrated into the rest of the network of the end customer.

- **Virtual patching:** when a vulnerability is found in one device, it can take days or weeks until the production line goes into maintenance mode and it can be patched. In the meantime, the device needs to be isolated from all network access except for its regular communication needs.

- **Logging and Monitoring:** Monitoring and reviewing logs across assets and networks is a critical capability for responding to cybersecurity incidents and helps identify what went wrong. Although system logs within OT environments will vary, centralized log monitoring helps to identify the root cause of an event.

- **SOC & Managed Security Services:** Finally, it is worth to add that those security capabilities need to be properly manage to ensure that they remain useful and to respond to specific security incidents and respond properly.
Production environments are going through tremendous transformations thanks to the digitalization, mobility, automation and adoption of artificial intelligence for productive processes. 5G Private Networks are cutting the cord in OT and enabling new use cases based on seamless mobility, high performance and the integration with the public networks. These changes are ushering in a new era of flexibility, productivity, and control for OT-based organizations. At the same time, these innovations are opening up new attack vectors for bad actors who prey on any factory component whose disruption can have a major impact on the business of the enterprise or the safety of its employees and facilities. These threats are real today and are continuously evolving. It is therefore critically important to put in place a flexible security infrastructure that can adapt to the ever-changing wired and wireless OT environments.

Telefonica and Fortinet offer a full portfolio of integrated security solutions and design processes that interconnect and protect products from hundreds of suppliers in OT, IT and 5G mobile networks. This includes all of the major 4G/5G network equipment, ICS and supervisory control and data acquisition (SCADA) offerings, visibility products for industrial asset and network systems, and the services of industrial systems integrators. We use proven methodology and security models to identify the places where security functions need to be placed. With our joint offering, as production and operational technology evolves, organizations can be sure that the security investment made today will adapt and grow to meet future requirements.
About Telefónica Tech

Telefónica Tech is a key holding of the Telefónica Group. The company offers a wide range of integrated technology services and solutions in Cyber Security, Cloud, IoT, Big Data and Blockchain. Telefónica Tech’s capabilities reach more than 300,000 customers in 175 countries every day.

More information

telefonicatech.com