



Private Wireless Networks for Industrial Campus Sites

A closer look at the growing role of 4G/5G in the Enterprise.
A Disruptive Analysis thought-leadership eBook.

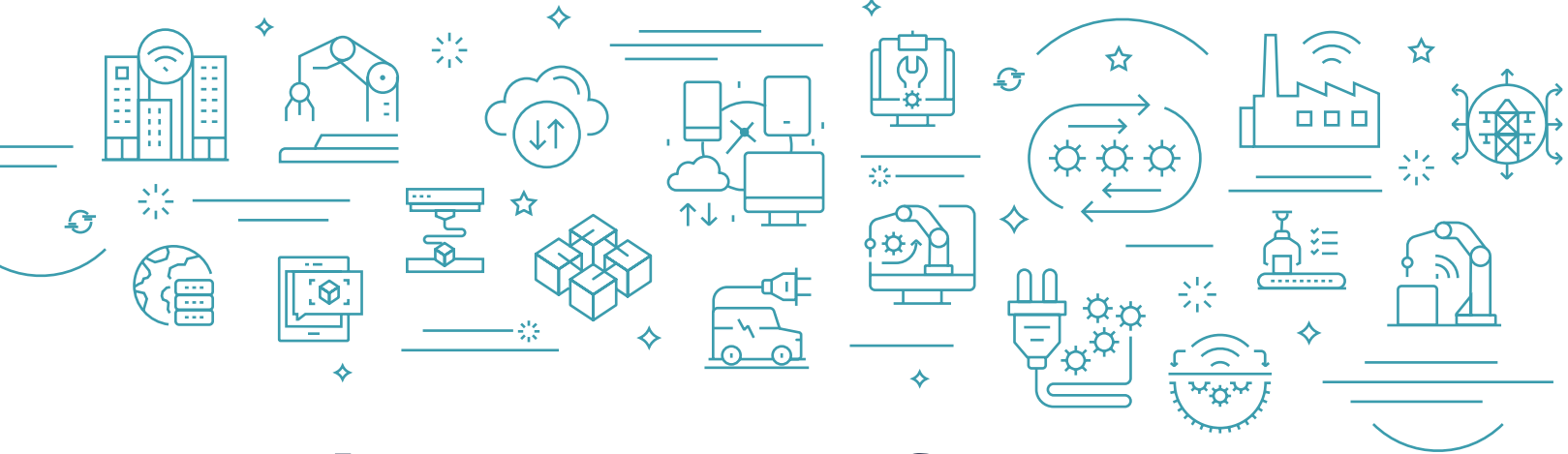


Disruptive Analysis



Table of Contents

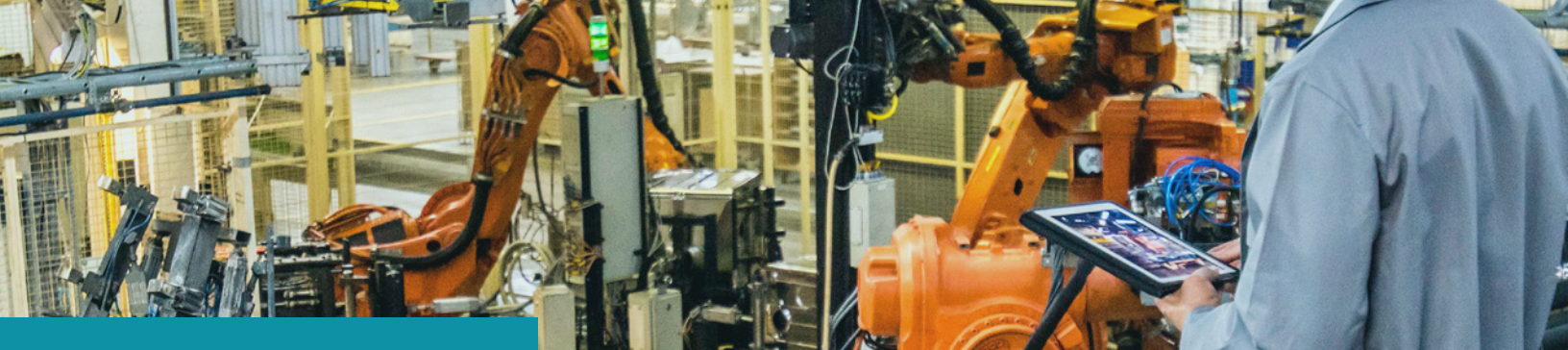
Looking at 4G/5G for industrial campus networks.....	3
Industrial transformation driving wireless	4
Use-cases for private wireless in industrial settings	5
Why private 5G? And how?.....	9
Public vs. private 5G	10
Practical challenges for industrial campus 5G	12
5G-only vs. Hybrid wireless environments	13
Conclusions	15



This eBook is an overview of the trends occurring in wireless applications and technologies for industrial campus sites. In particular, it examines the growing role of 4G/5G cellular, either delivered via public carrier services or local private network deployments specifically for the enterprise.

- Descriptions of typical industrial settings and their uniqueness compared to other wireless environments.
- The broader context of industrial transformation, safety and sustainability that underpins new networking / IT / OT (Operational Technology) requirements.
- A selection of use-cases and applications that are putting more demanding requirements on wireless connectivity and drive demand for higher performance.
- The specific rationales and drivers for deployment of private 4G/5G networks, such as direct control of network operation and configuration, helped by local / shared spectrum and cloud-delivered core networks.
- Co-existence of multiple technologies on industrial sites, such as 5G and Wi-Fi 6.
- Challenges involved in the design and deployment of wireless on industrial campuses.
- The roles of CSPs, systems integrators, industrial solutions vendors and other stakeholders in delivering private wireless systems.

Business,
economic, social
& political top-
level drivers &
"megatrends" of
industrial change
(eg. sustainability)



Industrial transformation driving wireless

Many heavy industries are midway through transformation projects – enhancing productivity, safety and flexibility through new technologies, IoT and automation. This is occurring across the broad range of different industrial settings, from mines to power-stations, or from manufacturing facilities to chemical plants.

Some sites combine multiple industries, for instance a port which has a large oil storage-tank depot, as well as warehouses and railway yards.

While they differ widely in size and operation types, there are several consistent themes driving the greater use of networked technology, and new ways in which it gets deployed / operated. These, in turn, are driving campus deployments of new wireless technologies, including public and private 4G/5G cellular, as well as new generations of Wi-Fi and low-power IoT connectivity.

Among the key universal trends are:

- More use of industrial automation, robotics, remote-operation and closed-loop control. In general, there is a desire to use wireless connections to enable greater flexibility and to shift from legacy/proprietary technologies to more standardized alternatives.
- Greater adoption of telemetry and sensors for mass-scale collection of operational data, feeding into both realtime monitoring systems, and longer-term “digital twins” and machine-learning tools to improve productivity and performance.
- Integration of individual plants or sub-systems into broader global supply chains, allowing for optimized flows of products, staff and components – and to get early warnings of delays or downtime, to aid decision-making and oversight.
- Assuring regulatory compliance with rules on pollution, hazardous materials, working practices and sustainability requires ever-greater collection of data, images and process automation.
- Growing emphasis on ensuring safety and security, for both workers and assets.
- Desire for improved human communications and collaboration, including voice and video optimized for field-workers, as well as good connectivity in onsite offices, control-rooms and other indoor spaces.
- Ability to support the communications and interconnection of multiple stakeholders and partners on the same site such as external companies involved in maintenance, equipment supply, transport and security.

All of these general business trends require improved connectivity, across all parts of an industrial site, and often beyond to other locations or the cloud. Reliable wireless links are increasingly important – and require careful planning and skilled operation/management.

The details of the wireless connectivity needs for each specific use-case are considered in the next section.

Many different classes of industrial campus environments



Process Plant



Mining



Ports



Oil & Gas



Energy



Warehouse & Logistics



Multi-use Complexes

Use-cases for private wireless in industrial settings

Drilling down from these top-level trends for industry transformation and IT/OT upgrade, we see these shifts are strongly correlated with new uses for wireless connectivity. These need to be capable of dealing with ever-higher levels of data throughput, higher reliability and lower latencies – as well as the ability (and design emphasis) on ubiquitous coverage despite numerous real-world challenges.

Many of the private wireless use-cases relate to one or more of the following underlying technology capabilities:

- Use of high-definition video communications – either uplinked from cameras, or for two-way communications.
- Requirements for low (and often deterministic) end-to-end latency, both for the network itself and the compute/application environment.
- Ability to connect a high density of “lightweight” endpoints such as sensors, combining regular data uploads with low connectivity costs and (where possible) long-life battery power.
- Good handling of mobility, onsite and sometimes over wider areas / nationally.
- Potential to integrate with diverse other network and IT systems used on-site, which may endure (or be migrated slowly) over a long period of time.
- Limited dependency on external suppliers and providers, except where covered by excellent service-level agreements, or tightly coupled with specific devices and systems.

These capabilities are then combined into one or more of these networked industrial application-types:

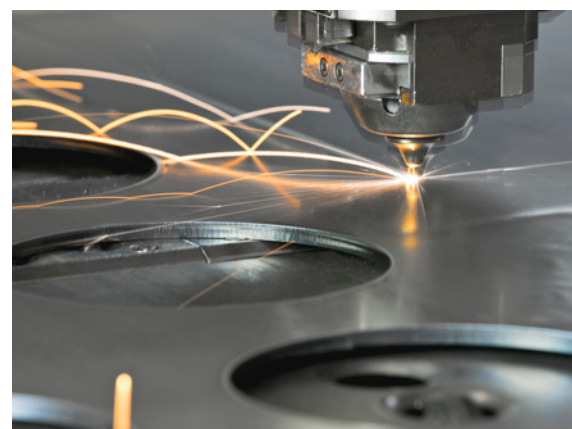
- **Safety-Critical Communications:** Push-to-talk (PTT) communications, alerting systems and increasingly video-based communications are essential for safe and productive industrial operations. They are used to communicate actions, problems and coordinate teams, as well as deal with emergency situations that may also need telemetry of workers' vital health data. They may also inter-operate with normal telephony networks or collaboration applications as well. Local wireless connectivity and call-control is essential, as plants may be in areas with no reliable connection to national mobile networks.
- **SCADA (Supervisory Control & Data Acquisition) and Closed-Loop Communications:** SCADA systems of different types are common throughout industry, used for industrial monitoring and operational control applications. They link sensors, displays, analytical systems and actuators in real-time, allowing for both human and automated control ("closed loop" automation). Wireless links improve efficiency and minimise downtime for re-wiring, compared to Fiber. Future SCADA systems will need reliable "hard real-time" deterministic latency for the most time-sensitive machines – and synchronized hand-offs between machines. Robots, humans with devices such as tablets or AR headsets, or vehicles and materials are mobile, and thus cannot be "instrumented" without wireless connections. Each sector will have its own niche applications – such as smart ventilation in mining, or active water-management in oil and gas sectors. Technologies such as 5G can include ultra-low latencies, TSN (Time Sensitive Networking) for deterministic latency needs.
- **Mobile Control Panels:** Industrial control panels (or HMIs – Human-Machine Interfaces) are digital dashboards that allow human operators to see and control a machine or system. They usually support safety-stop buttons for instant reaction to dangers. Often, HMIs are wired-in to the automation systems directly. Wireless connectivity enables them to be untethered, in a similar fashion to ruggedized tablets, or even run as apps on general-purpose hardware.
- **IoT Sensors for Process Automation & Telemetry:** Process industries have a huge requirement for sensors, monitoring temperature, pressure, flow rates, chemical presence, vibration and so on. They may be distributed across fairly wide areas – for instance multiple wells in an oil field, while other systems are highly localized, such as equipment for detecting gases and anomalous temperatures in refineries or chemical plants. Operators want to aggregate IoT data flows centrally to make decisions, automate processes (eg closing valves remotely) and inform operational planning and strategy. Over time, sensors will generate more granular data, so future-proofing for higher traffic volumes is important.

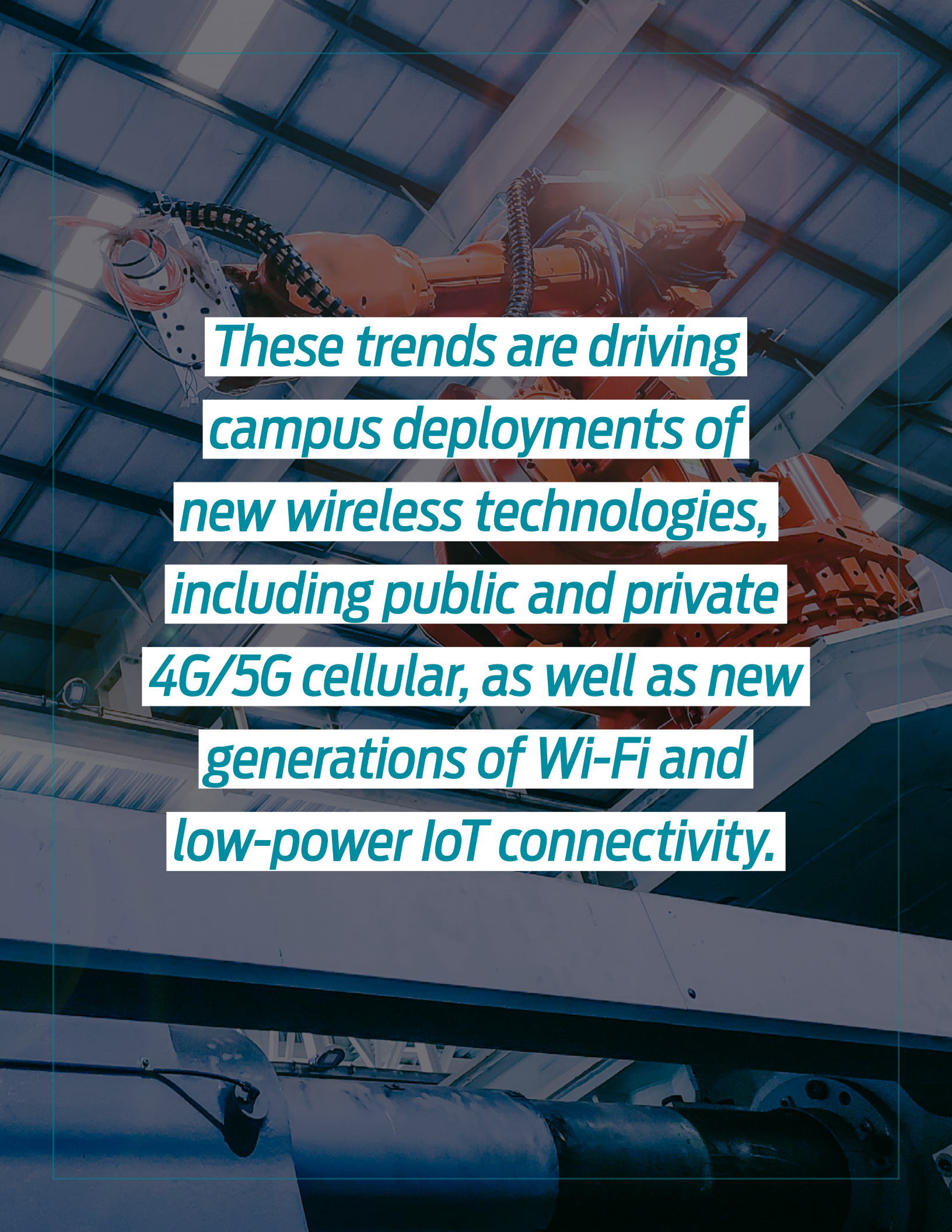


- **Mobile Robots and AGVs:** Industrial robots are used to move material or components, conduct inspections, or for other tasks. They are often separated from human workers for safety reasons. A sub-class of mobile robots – automated guided vehicles or AGVs – are used for transporting material around the plant. Wireless guidance control can help robots and AGVs move safely and interact with other machines such as conveyor belts, lifting systems or static storage. Inspection robots can use gas-detectors, machine vision or thermal cameras for checking pipes, tanks and other equipment. Again, high-reliability wireless is essential.
- **Video Surveillance & Security Systems:** Monitoring security and safety risks, whether related to fire, intrusion, terrorism, leaks or process-monitoring, are critical in many industrial settings. Video – both normal imagery and using thermal cameras – is used for both human and machine observation. In some cases, terrestrial connectivity may be supplemented with drone or satellite imagery.
- **Wireless AR/VR Applications:** Industrial uses of immersive augmented and virtual reality are emerging rapidly. VR-based training can give a significant improvement of occupational health and safety knowledge, especially for new employees. AR/VR can enable practicing of complex, multi-task operations, or hands-free instructions and directions to be given in the field. Millisecond latencies reduce the risk of “VR sickness”.
- **Predictive Maintenance:** Equipment malfunction and unscheduled downtime is costly, especially at remote or unmanned sites. If operations cease, fixing equipment - and ordering and replacing parts – can be very disruptive. There may also be serious environmental harms resulting from failures. Preventative maintenance aims to reduce these risk, by using analytics to predict imminent failures. Data built up across the wider population of assets, can be used alongside digital twins to create customized servicing schedules for each installation.
- **Machine Vision-Based Tasks:** Techniques such as 3D-printing and precision-welding need close attention to quality during the process, enabling mistakes to be corrected instantly, or part-finished products to be rejected quickly, without waste of further time or materials. Wireless cameras, connected to on-premise or nearby edge-computing functions can analyse video feeds for badly-formed welds, cracks or infra-red thermal signatures of other problems.

Not every industrial sector will need all of these use-cases. In addition, many individual companies will have additional specialist and niche applications, as well as unique blends of legacy systems and networks, and differing relationships with key solution suppliers for them.

Depending on the specific requirements of each application – and the site as a whole – campus network managers will select one or more network types and topologies.



A low-angle, upward-looking shot of a large orange industrial robotic arm in a factory. The arm is positioned in the center, with its joints and cables visible. The background shows the complex steel structure of the factory ceiling, with various beams and supports. The lighting is somewhat dim, with a blueish tint, giving it a high-tech, industrial feel. The text is overlaid on the right side of the image, following the curve of the robotic arm.

*These trends are driving
campus deployments of
new wireless technologies,
including public and private
4G/5G cellular, as well as new
generations of Wi-Fi and
low-power IoT connectivity.*



Why private 5G? And how?

From the previous discussion, it is clear that in the future there will be many more wireless use-cases at modern industrial sites than in the past, and that they are becoming far more demanding in terms of performance, coverage and flexibility.

There are numerous potential advanced network options becoming available:

- Use of Wi-Fi, especially as it evolves to Wi-Fi 6 and soon 6E (using the new 6 GHz band), with version 7 about 3-4 years away. These bring progressively more capacity and control / QoS options. (A number of industrial companies have proprietary enhancements to their “industrial WLAN” solutions, which are cousins of certified Wi-Fi).
- 4G and 5G cellular networks, delivered either from the public (MNO) infrastructure, or with dedicated private on-site deployments. (see below for details)
- Fixed-wireless links, for connection to specific buildings or structures. These can be based on a variety of standards-based and proprietary technologies, with varying performance and cost parameters. 5G and Wi-Fi are among the FWA options.
- LPWAN (Low Power Wide Area Networks) such as LoRa and SigFox, as well as narrowband versions of 4G/5G.
- Satellite-based solutions, which are also evolving rapidly with the emergence of constellations of low-orbit satellites, such as SpaceX’s StarLink.

Each of these technologies have their strengths, weaknesses and future evolution trajectories. While some overlap and effectively compete for specific uses, others are complementary or distinct. There will be no “one-size fits all” approach on typical industrial sites. Connectivity choices are not made in isolation – they will also often be combined with other decisions about cloud, edge-computing, cybersecurity and artificial intelligence.

What is becoming clearer is that cellular technologies will definitely increase in importance – initially 4G (which is proven, mature and comparatively simple), but then more 5G over time (earlier and costlier) – but with much more long-term potential).

Private 5G will be an important part of industrial wireless

Business, economic, social & political top-level drivers & “megatrends” of industrial change (eg. sustainability)

Systemic shifts in transformational technology (closed-loop, AI, digital twins, etc.)

Networked capabilities on-site (eg video upload, critical IoT, SCADA, etc.)

Wireless network choices, requirements & challenges (eg. fiber, public/private 5G, Wi-Fi, LPWAN, etc.)

There are three reasons why 5G will be used broadly in the future, in industrial settings:

- › Support for full mobility, and good for covering areas of many square kilometres and above.
- › Growing range options for supply and delivery, either with a service-based model, or private ownership / control directly by the enterprise.
- › Strong roadmap for supporting industrial needs for low/deterministic latency, along with performance assurances from use of licensed spectrum. Accurate positioning/location-awareness may become useful as well.

This does not mean that 5G will “win” – the supposed “battles” which other technologies (notably Wi-Fi) are just convenient marketing fiction and hype. As discussed below, most sites will continue to invest in multiple networks. Various purported extra benefits such as on-site / off-site roaming are questionable.

A particular issue is that 5G capabilities are arriving in stages, aligned with 3GPP Release 15/16/17 and vendor product support, as well as availability of spectrum. Features like ultra-low latency remain some years away. In particular, early 5G networks using non-standalone cores cannot support most of the high-performance capabilities.

The evolution and implied timing lags add complexity in terms of commercial B2B offers, planning and design, trials, proofs-of-concept (PoCs) etc. Interim solutions and roadmaps are needed, as enterprises seem unwilling to wait until 2023 for improved connectivity for current transformation projects.



Public vs. private 5G

The second point above is an important one. Industrial 5G (and also 4G) networks can be provided via multiple paths. In particular, enterprises do not need to rely on traditional MNOs to deploy, run and own the local mobile infrastructure, or even the underlying spectrum it uses.

Although the mobile industry initially expected the sectors covered in this paper to drive demand – and extra revenue – for MNOs’ 5G networks and services, there has been a rapid shift of focus since 2018/19.

Many enterprises – while indeed interested in 5G applications and capabilities – are not convinced that MNOs are the best providers of the advanced connectivity they require, on the terms and timelines that they are prepared to accept. There are differences of opinion over control, cost, coverage and fine-grained functionality.

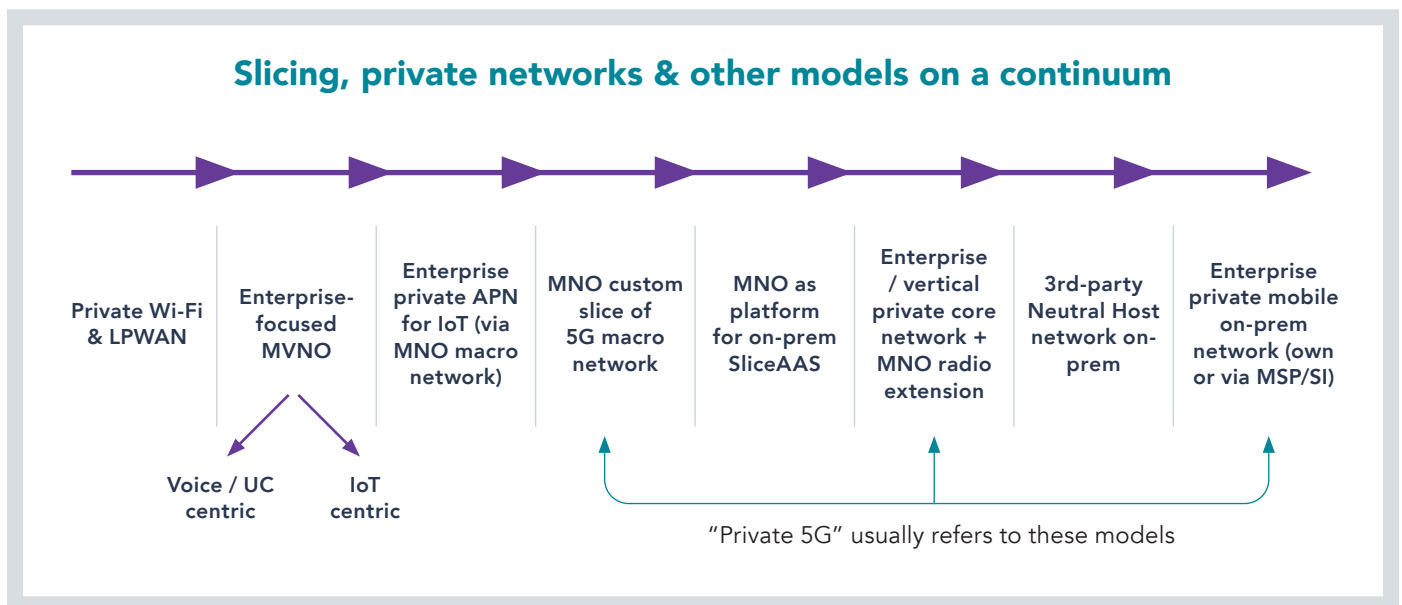
Heavy-industry sites have traditionally run networks in-house: ethernet, Wi-Fi or private two-way radio systems – integrated tightly into IT and OT platforms. They have specific requirements for management, security, cloud integration and service-levels. Private / industrial 5G cannot be deployed in isolation – it will need to be integrated into the incumbent systems.

Most national public 4G/5G networks have limited coverage in industrial locations anyway – such low-population areas have not typically been priorities for MNOs’ build-outs.

In fact, there will actually be four main groups of stakeholders involved in deploying and managing connectivity for industrial sites' needs:

- **MNOs:** Traditional MNOs can provide wide-area or specialized on-premise 5G networks, using tools such as network-slicing. They may extend their national "macro" networks, or supplement them with additional on-premise radio capacity and edge-compute. They may develop expertise in some industrial verticals, or work with sector-specific integration partners, but the network is essentially linked to the "mothership" in some fashion. Examples include AT&T, T-Mobile and China Mobile.
- **Enterprise:** Industrial companies can build and run their own connectivity and campus 4G/5G networks – just as some utilities, rail networks, military agencies and remote oil/mining facilities have done for years. They can take advantage of new localized spectrum such as the US CBRS band or German 3.7 GHz industrial spectrum, alongside cloud-based functions to reduce cost and complexity.
- **Other CSPs:** New classes of service provider beyond traditional MNOs are deploying private 4G/5G networks – mostly on specific sites, but in some cases across wide areas. These include certain towerco's, fixed telcos building private networks for select clients, or specialized "industrial mobile operators". For instance, several providers (eg RigNet and Edzcom, owned by ViaSat and Cellnex respectively) offer cellular connections to oil/gas or offshore wind facilities, or onshore mines and ports. They can focus directly on enterprises, and may bring innovative approaches to financing network builds such as leasing.
- **Solution Integrators:** Various IT and industrial system providers may build 5G (or other connectivity) directly into solutions for enterprise, "under the hood". Robots, cranes, warehouse automation systems – or a broader IoT or supply-chain software XaaS player could own – or just control – the networks they need. They may even acquire localized spectrum on behalf of their industry customers.

Numerous hybrids are emerging as well, with MNOs now setting up dedicated integration and partnership efforts for verticals from mining to manufacturing and agriculture. Others are entering the market from adjacency – cloud providers, traditional critical-communications specialists and others. We can expect continued evolution – and probably acquisitions – in the future.



There are also interesting enterprise-oriented proposals from the new breed of national MNOs that are deploying Open RAN-based 5G networks, such as Dish in the US, Rakuten in Japan, and Jio in India. These disruptors are likely to bring new styles of partnership to the market compared to their more-established peers.

Practical challenges for industrial campus 5G

The general capabilities of 5G for industrial sites are attractive, while the arrival of private-deployed options expand the levels of control and operational flexibility for enterprises. However, there remain significant practical challenges to designing and building effective campus-wide cellular networks.

Industrial sites such as chemical plants and oil refineries can span a range of several kilometres in size – sometimes much more, in the case of the extractive and energy industries.

Some present a wide range of challenges for network design and planning, which requires careful focus and attention. These include:

- › Metal structures and pipework, with curving surfaces and sensors placed near joints or under overhangs.
- › Health and safety challenges for installation, worker accreditation and RF propagation – sometimes including requirements to protect control infrastructure against explosions.
- › Heavy moving objects, from cranes to trucks to temporary cabins.
- › Unusual indoor spaces for wireless usage, such as the insides of silos and vessels.
- › Sources of unshielded RF interference and noise, such as electric motors and arc-welding torches.
- › Potentially multiple overlapping private cellular networks, for instance where machinery or production systems have their own in-built wireless networks.
- › Legacy integration and migration from older proprietary wireless systems. Conservative infrastructure managers may look to run these in parallel to the new 4G/5G/Wi-Fi systems for some time.
- › Underground areas and structures.
- › Where possible, there is a desire to limit the number of radios / access points to cover a given area, in order to minimize Fiber or fixed-wireless links used for backhaul, as well as containing upfront investment.

These considerations are not show-stoppers, but they will occupy time and resources to solve and plan. Upfront thought about both current applications' physical environment, and future options should reduce long-term costs. This does not just relate to a proposed 4G/5G industrial network, but also to the supporting Fiber infrastructure and other wireless platforms which may be able to share some elements.

Unique challenges in industrial environments



Metalwork & Complex Topologies



Indoor / Outdoor Hybrids



5G-only vs. Hybrid wireless environments

The last point is important. Despite a lot of rhetoric positioning 5G as a sort of universal “one-size fits all” network technology, that can cover all use-cases simply with “network slicing”, the truth is much more nuanced.

Essentially all sites will feature a variety of different network technologies, addressing separate needs and applications. While there are always overlaps and opportunities for substitution, there are also unique requirements.

Thus on a typical industrial site, there may end up being a variety of wireless and wired systems:

- Private 4G/5G networks for the types of industrial automation, robotics and video-based use-cases described in detail above.
- Public 4G/5G networks for visitors and vehicles coming onto site.
- Wi-Fi in office areas for laptops, screens and other IT-type devices, or for less-critical automation systems, laboratory equipment, tools and many other classes of device.
- Existing two-way radio systems, which may get phased out slowly in favour of cellular.
- 60 GHz fixed-wireless access between buildings.
- Other fixed-wireless links (perhaps based on 5G or Wi-Fi) for connecting remote structures or IoT installations.
- Satellite connectivity to ships, trucks – or perhaps for backhaul, if the site is in a remote area.
- Fiber for connecting buildings, datacentres, specific critical equipment, wireless backhaul / fronthaul etc.
- LPWAN technologies – perhaps LoRa or SigFox – for remote sensors or smart-building systems.

There are multiple touch-points between these systems, both in terms of design and implementation / operation. Some may just be entered into the same geographic inventory and planning software, while others may share physical mountings or Fiber connections. Over time, there may be more unified and integrated operation and security, for instance using a private 5G core network to control Wi-Fi access points, or an IT security platform to manage 5G eSIMs and other secure credentials.

2024 Industrial networks will be multi-technology

	Wi-Fi	Public 4G / 5G	Private 4G / 5G	Other
MNO indoor coverage / offload (esp. phones)		mmWave		
Local/Guest IT LAN (laptops, phones, etc.)				Fiber, ethernet - still important
Local IoT (static)	Wi-Fi 6 / 6E / 7			FWA, BLE, Zigbee, Ethernet
Local IoT (moving)	Limited	Opportunity	Opportunity	Niche wireless
Local OT (industrial)	Critical - Wi-Fi7? Wi-Fi6E	Needs partners, vertical focus	Opportunity	Fiber, FWA, niche wireless
Local voice radio				DECT, TETRA
Sector-specific uses				

MARKET ADOPTION FORECAST

Ubiquitous	Common	Rare	Very Rare
------------	--------	------	-----------

NOTE: Many variables by industry, site, operator, country, detailed use-cases. Some overlap between categories.

Conclusions

Industrial sites are undergoing a revolution in terms of their technology adoption. The ongoing transformation of systems and processes is broad – and still expanding.

Automation, the application of AI and digital twins, improved monitoring of assets and employees, and a growing focus on security and sustainability all imply much more “connectedness” – whether that is for a port, a chemical plant or a manufacturing complex.

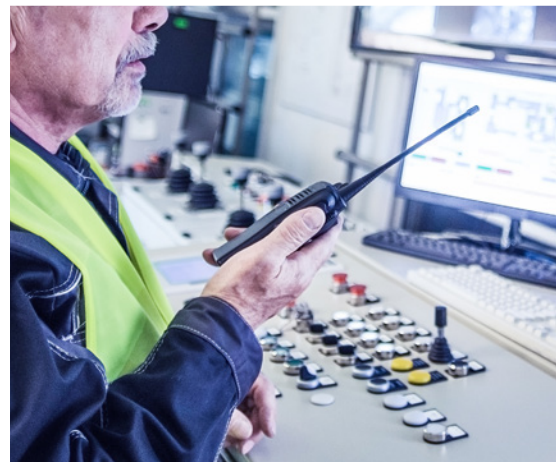
Wireless use-cases are proliferating, and are expected to continue to evolve in reach, performance requirements and criticality. Networks will be expected to have complete and reliable coverage on industrial campuses, despite the complex practicalities of huge and heterogeneous sites.

While 5G mobile technology is likely to be hugely important in industrial settings, its deployment and operation is not as easy as for consumer/national MNO networks. It will require careful design and optimisation to map onto current and future applications, and deal with the evolution of both the plant environment, and also the shifting generations and releases of the technology itself. Some companies may stick with 4G cellular until stability and maturity improves.

There are multiple paths for creating private/campus 5G. MNOs can “slice” national public networks or provide local coverage enhancements, although not all can deliver the right wireless capabilities, at the right time/cost, with appropriate levels of control for the business. It can be hard to deploy and manage public networks on private property.

This is leading to demand for, and supply of, customized or private 4G/5G networks for enterprises, but the exact measures vary widely by country. Germany, Japan, US, UK and a few others are showing early “best practice” in terms of spectrum availability. There is a growing range of options for on-site small cells, cloud/on-premise cores, and other components of the overall solutions. Enterprises can now build their own 5G networks independently. New classes of niche service provider and integrator are emerging to fill the gaps.

Most industrial environments will remain multi-network. Wi-Fi is evolving in tandem with 5G and will remain essential for many use-cases. Fiber is often preferred. Legacy wired and wireless systems cannot be removed overnight. Fixed-wireless has many use cases, some of which can be enabled by 5G, but also alternatives such as 60 GHz meshes. Industrial site operators should expect – and exploit – such heterogeneous mixtures of technology. Wireless is like a well-stocked toolbox – simply using a 5G hammer is not enough.



About iBwave

iBwave Solutions, the standard for converged indoor network planning is the power behind great in-building wireless experience, enabling billions of end users and devices to connect inside a wide range of venues. As the global industry reference, our software solutions allow for smarter planning, design and deployment of any project regardless of size, complexity or technology. Along with innovative software, we are recognized for world class support in 100 countries, industry's most comprehensive components database and a well established certification program. For more information visit: www.ibwave.com.

About Disruptive Analysis

Disruptive Analysis is a UK-based research and advisory firm, founded and run by Dean Bubley, an independent industry analyst and futurist with a long background in consulting and commentary on the telecoms industry. It provides consulting and advisory services on technology evolution, regulatory policy, market and competitive dynamics, with a particular focus on 5G, Wi-Fi and private networks arenas.

Disruptive Analysis has clients across the telecoms, cloud, regulatory and investment universe and has followed private and enterprise cellular networks since 2001.

Mr Bubley is also widely-known as @disruptivedean & is on LinkedIn

<https://www.linkedin.com/in/deanbubley/>

Intellectual Property Rights / Disclaimer

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher, Disruptive Analysis Ltd.

Every reasonable effort has been made to verify research undertaken during the work on this document. Findings, conclusions and recommendations are based on information gathered in good faith from both primary and secondary sources, whose accuracy it is not always possible to guarantee. Disruptive Analysis Ltd. disclaims all warranties as to the accuracy, completeness or adequacy of such information. As such no liability whatever can be accepted for actions taken based on any information that may subsequently prove to be incorrect. The opinions expressed here are subject to change without notice.

