FROST & SULLIVAN

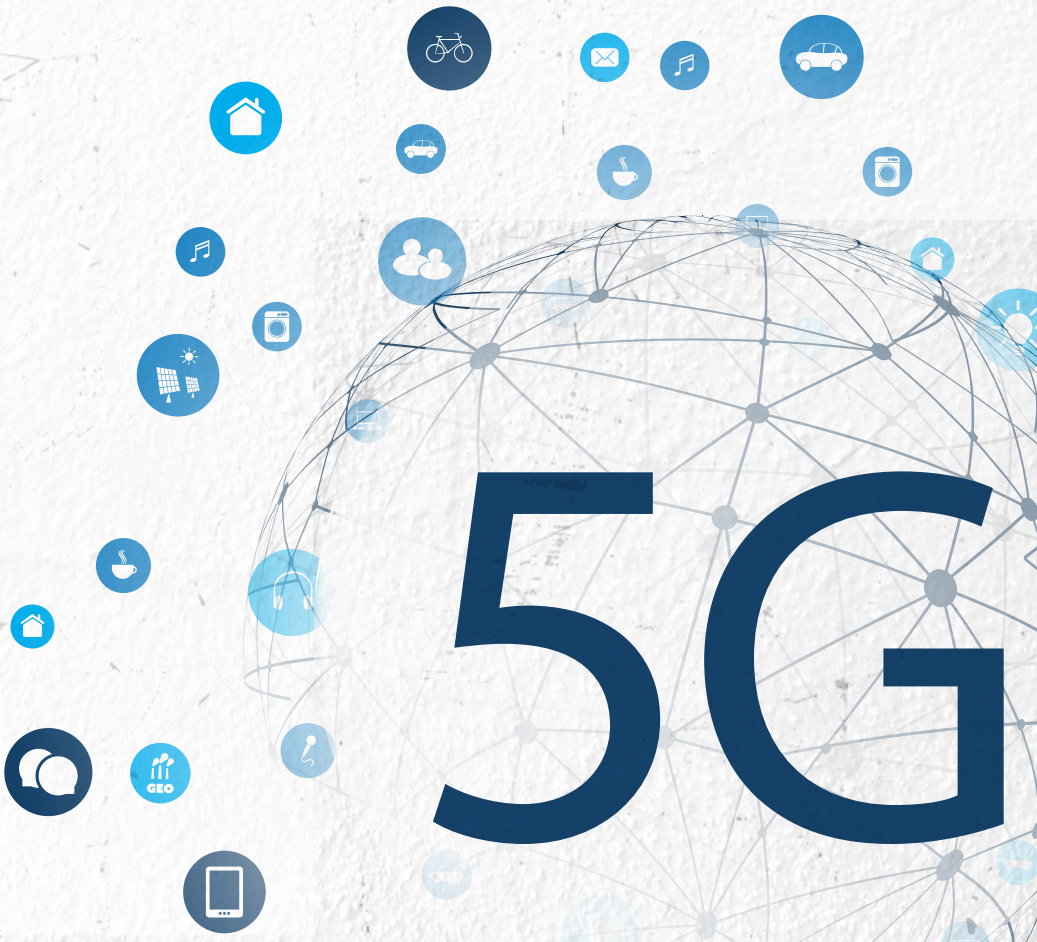
Delivering on the Promise of Private 5G

Avoiding Radio Frequency Challenges While Increasing Safety, Efficiency, and Profit

Troy M Morley, Principal Analyst

FROST & SULLIVAN WHITEPAPER

CONTENTS

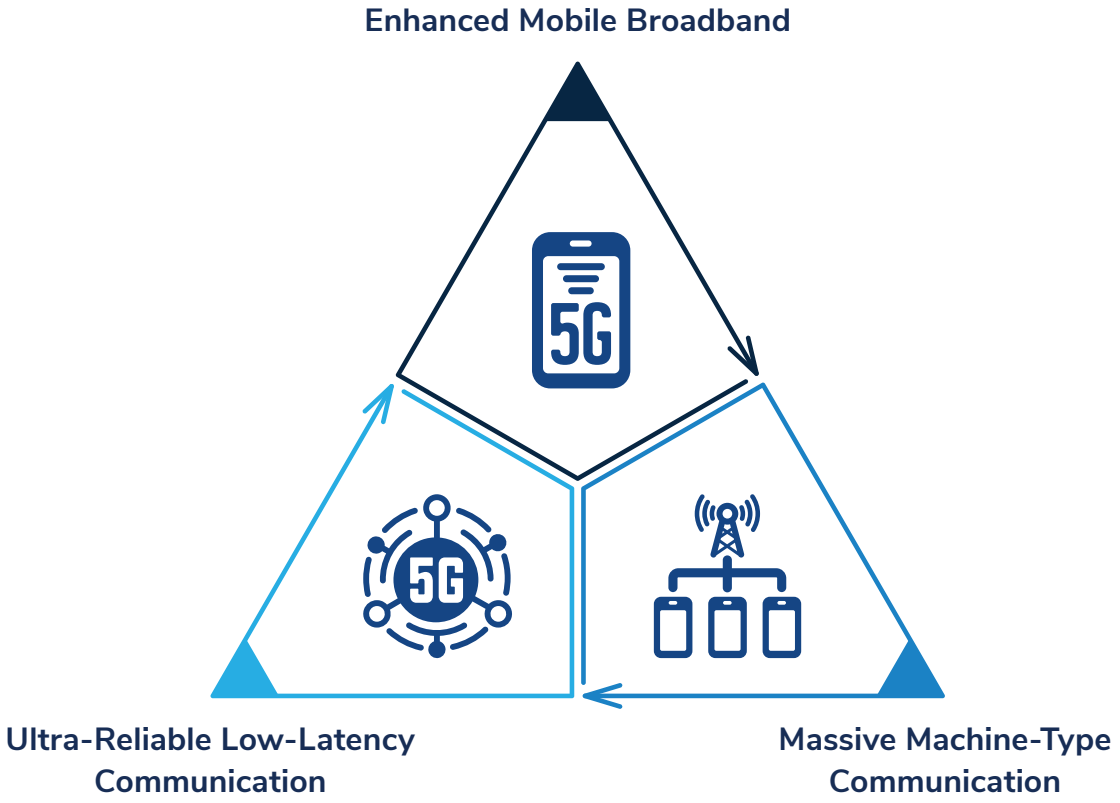


The Opportunities Presented by Private 5G Networks

Overview of 5G, private cellular networks, and enterprise connectivity needs

Enterprises, regardless of the vertical(s) within which they fit, have business problems they are trying to solve. Existing technologies, like Wi-Fi, although here to stay, were not engineered to address the new needs of enterprises.

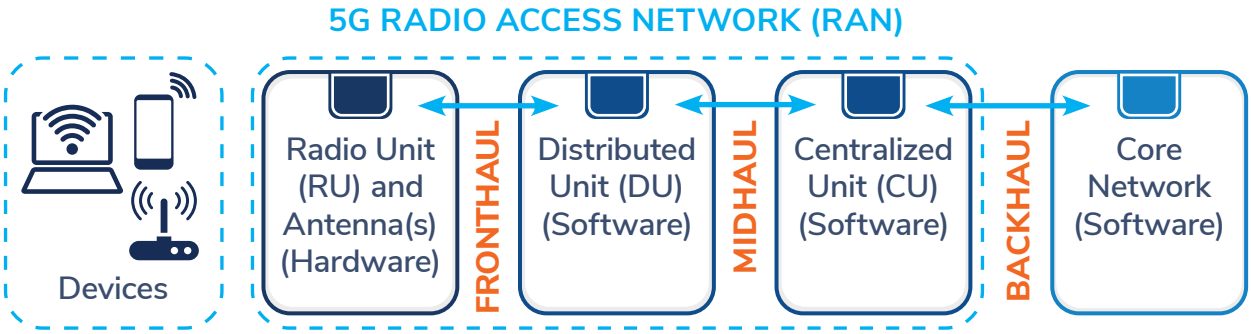
With the evolution of cellular networks to 5G, the focus has shifted from the consumer to providing new types of capabilities to support enterprise needs. The three pillars of 5G are shown below.



Source: Frost & Sullivan

The public cellular networks provided by mobile network operators (MNOs) are designed to support millions of consumers, and the primary offering is Enhanced Mobile Broadband which increases network speed and capacity.

The Components of a 5G Network (Public or Private)



Source: Frost & Sullivan

Private cellular networks have the same components and technologies as public networks, but they are tailored to the specific requirements of *that particular network*. This means each private cellular network is somewhat unique to support a particular application important to the enterprise. Private networks are now likely to use 5G to capitalize on the low-latency or massive communication pillars of the new technology in addition to enhanced mobile broadband.

The application determines the 5G benefits that are most important to the owner of the private network. For instance, a hospital using a private network will need latency requirements to be met or the patient's safety will be compromised. But a manufacturing company using a private 5G network for communication between machines on a production floor will be most concerned with supporting a massive volume of connections to improve productivity and reduce cost. In all cases, in order to meet the goals of a private cellular network, devices need to access the network when needed and retain that connection as long as necessary.

5G also expands the radio frequency (RF) spectrum used. This limited resource—that MNOs invest billions of dollars on—is key to enabling any kind of wireless connectivity. One critical factor to any wireless network is to understand the available spectrum and the challenges that might be faced in order to utilize it.

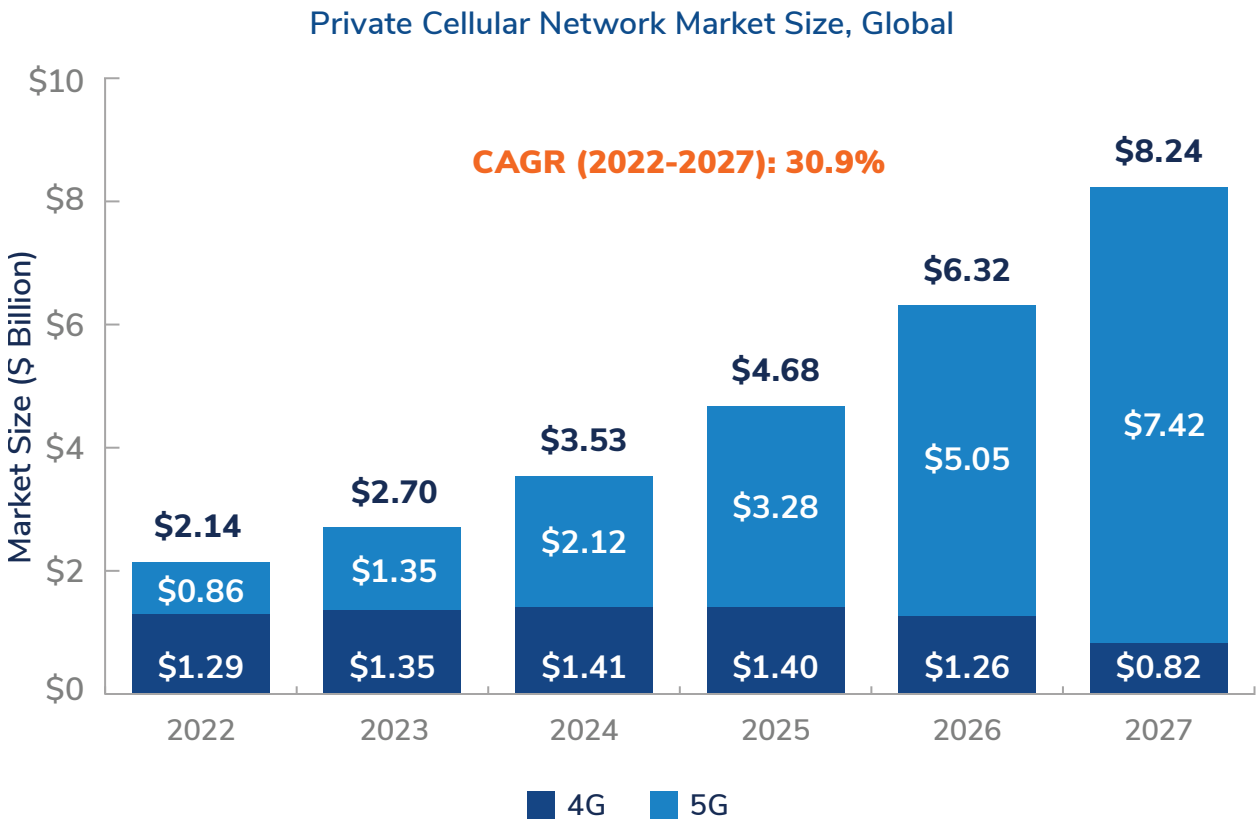
Why would an enterprise invest in a private 5G network? Simply put, they have business problems that cannot be solved efficiently with existing wired or wireless networks. The capabilities of 5G were designed with these requirements of enterprises across verticals in mind.

Opportunities abound

This presents many opportunities around private 5G networks:

- Enterprises can solve the challenges they face and increase efficiency, safety, security, and the bottom line.
- MNOs—the cellular network experts—can monetize their expertise and their spectrum holdings.
- Network infrastructure suppliers have potential new customers, expanding from hundreds of MNOs to millions of enterprises.
- System integrators and industry specialists know the needs of their customers and may be best positioned to help with their connectivity needs (working with MNOs and network suppliers.)

While the public cellular infrastructure market is quite large, it is slow growing, with annual gains in the single digits even in the best years. Conversely, the private cellular market size is currently relatively small, but Frost & Sullivan projects a compound annual growth rate (CAGR) of 30.9% over the next five years and a global market exceeding $8 billion in 2027, as shown in the chart below.



Source: Frost & Sullivan

While There Are Opportunities, There Are Also Potential Issues That MUST Be Addressed

Facing RF challenges

If one examines the cables used in a wired network, there is a significant amount of shielding involved. Why? To reduce interference.

In a wireless network, physical shielding is not possible, but the challenges in getting the RF signal to the device and back to the RAN when interference is present can be significant. Interference can reduce the capacity and reliability of the connection, increase the latency, or disrupt the connection completely, making it difficult to realize the benefits of 5G expected for the application.

The importance of the initial RF design in a private 5G network

Solving these challenges starts with the design of the network, which must be done by experienced RF experts. Maximize coverage and line of site. Minimize blockages. And much, much more.

Even with an expertly designed private 5G network, problems can (and likely will) crop up. The physical layout of the area covered can change, perhaps with a new piece of equipment that may reduce coverage. New sources of interference may be introduced, or there may be intermittent sources of interference that were not apparent during the design of the network.

These issues are not confined to private 5G networks…public cellular networks have the same issues.

> A survey of MNOs who own public RANs—*that were designed and installed by experts*—reported that **7.5% of cells experienced severe RF interference**.

If major MNOs can't design networks to completely eliminate interference, then we can't expect individual private networks to be free of interference.

RF challenges crop up in every wireless network

The point is that EVERY wireless network will encounter RF challenges at some point. All private networks need to be designed with interference in mind, and particular attention should be paid to networks in locations where interference is very high—in coastal or border locations or when signals can be affected by weather phenomena such as tropospheric ducting or a problematic combination of spectrum bands in use. Even having a lot of machinery or many wireless devices at the location of the private network can cause interference to intensify.

For a private 5G network, what are the implications? The answer is that the wireless network won't work as planned, since interference affects coverage area, the ability to make and retain wireless connections, data throughput, latency, and reliability. Since it is likely that part of the justification for having the private 5G network in the first place was to enable use cases that involved reliability, safety and/or cost savings, the implications of interference can cause the network investment to be questioned.

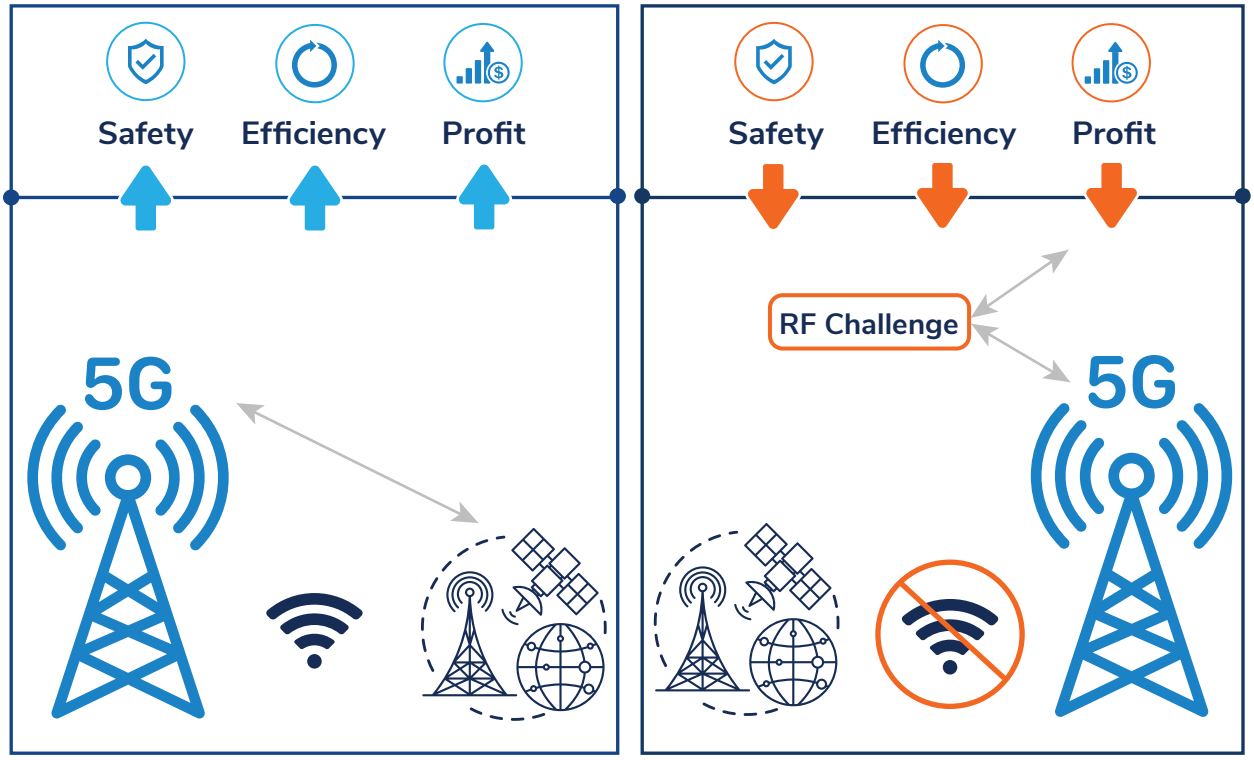
One example, autonomous mobile robots (AMRs) (shown below) can move materials around a manufacturing facility faster and more safely than a human operator AND perform inspections on them. Latency and reliability are key with this use case, as even a few second loss of communication could be deadly to workers in the facility. When RF issues arise, the AMRs must stop for safety reasons, which can quickly force the entire facility to temporarily stop. This can cost many, many thousands of dollars and impact or even reverse planned cost savings, affecting the profitability of the entire operation.

Another example revolves around security. Private 5G networks are often used with security cameras and require high data volumes for the video feed and retainability/ reliability. If interference (intentional or not) impacts the connection, would that be a perfect time for a "bad actor" to slip past the camera?

The consequences are magnified if lives are endangered when a connection is lost or degraded, or an assembly line must shut down due to connectivity issues. RF issues can impact safety, efficiency, and the bottom line.

Private 5G networks present highly viable opportunities to both enterprises and to MNOs, network infrastructure suppliers, system integrators, and industry experts *if* RF challenges are addressed. The good news is that these issues can be controlled.

5G Private Network Opportunities Can Be Impacted By RF Challenges



Source: Frost & Sullivan

ISCO International: Increasing Private 5G Network Opportunities and Reducing RF Challenges

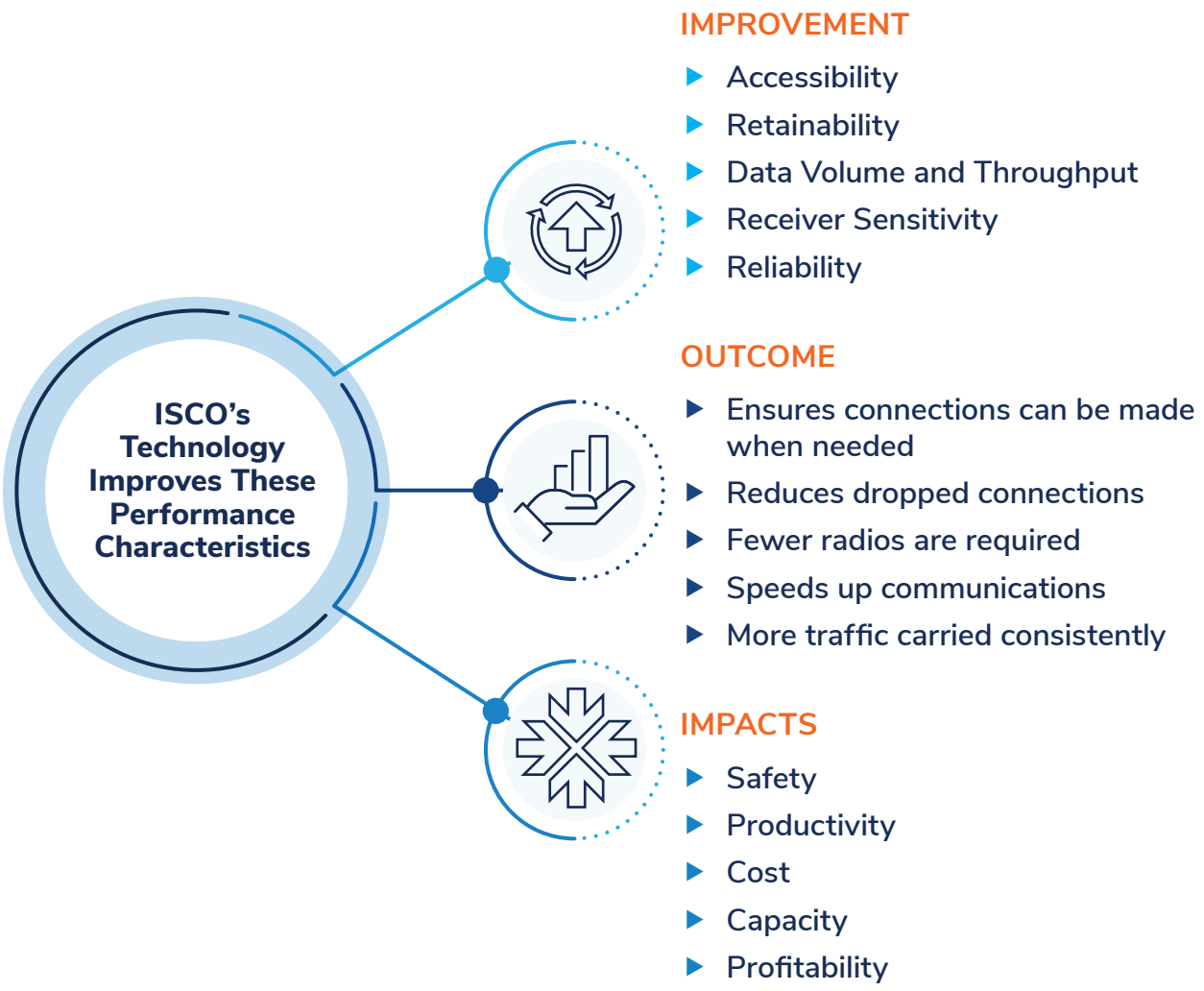
Introducing ISCO International

ISCO is a private company that develops and delivers solutions to reduce the impact of RF challenges like interference. For over 30 years, ISCO has worked with Tier 1 mobile operators to deploy interference management solutions throughout their public networks. This same technology is now available to be used in private networks to address RF challenges that can prevent these networks from meeting their goals.

RF challenges include different types of interference such as static or dynamic narrowband, wideband, cochannel LTE, cell edge, jammers, and interference created by PIM (passive intermodulation). ISCO has developed and patented software algorithms to automatically detect, identify, and remediate these different types of interference. ISCO's algorithm development evolves along with the industry; most recently ISCO's new patented Fortis™ technology was introduced which specifically capitalizes on polarization properties of radio frequency signals.

All of ISCO's solutions improve key performance characteristics in private networks to ensure the goals of the private network are met by ultimately impacting productivity, safety, and profitability. These impacts are summarized in the following table.

Private Wireless Network Performance



Source: ISCO

ISCO's Fortis™ Technology

The Fortis portfolio of patents builds upon ISCO's proven leadership in improving wireless performance in public cellular networks by favorably impacting a variety of network performance characteristics that are important to the owners of private networks. Fortis technology is effective, safe and flexible—it can be applied to antennas and radio units or in other types of discrete RAN products. Additionally, it can be applied to any device or component that facilitates the transmission and reception of radio frequencies.

The technology can be deployed standalone or embedded in a variety of devices, depending on who is using it and deciding where the interference management will be added. All of these scenarios have already been developed and tested:

1. Fortis IP integrated into a macro antenna.
2. Fortis IP implemented using digital signal processing after the RU.
3. Fortis IP embedded in an RF device before the RU.

Fortis IP Integrated into a Macro Antenna

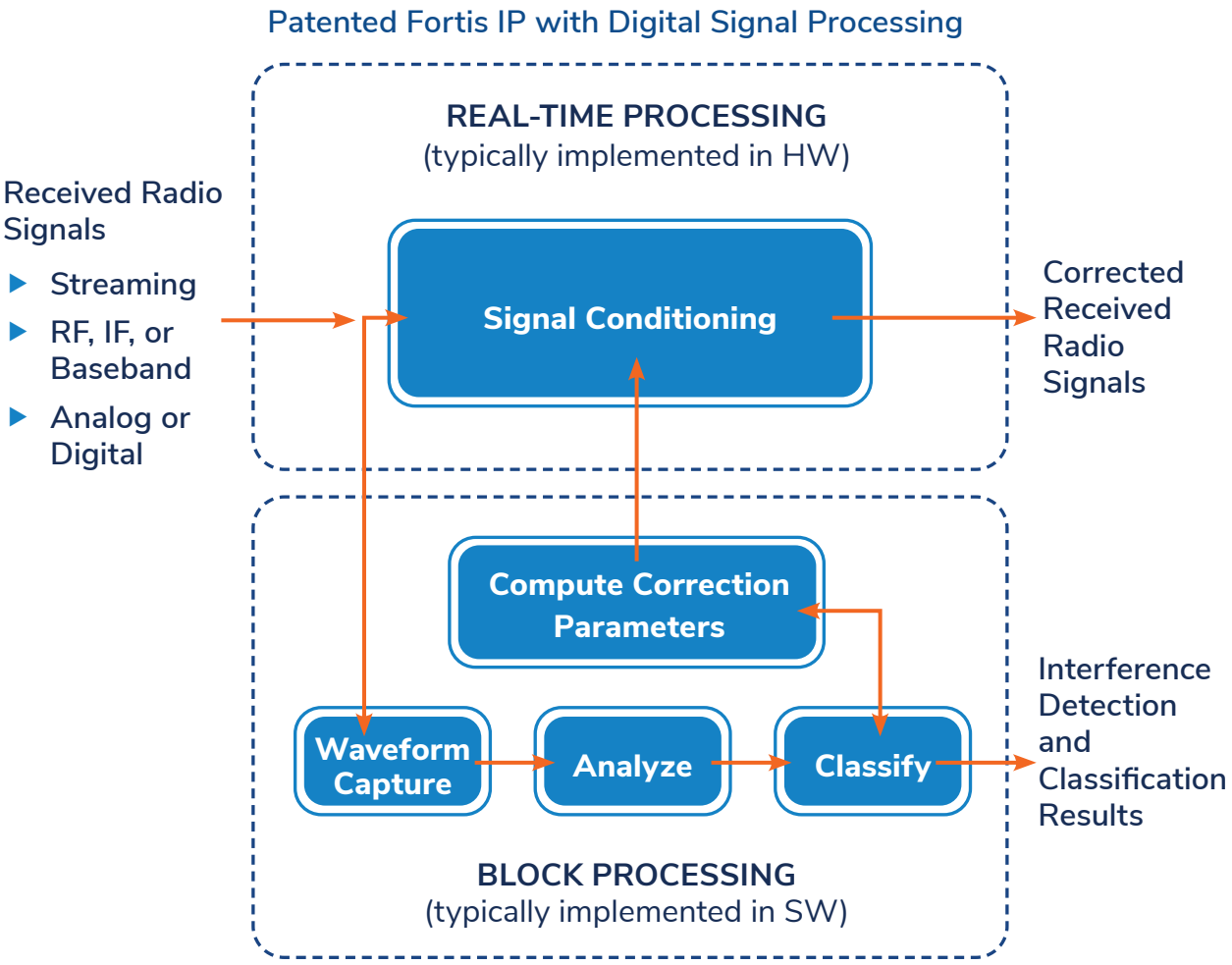
Including Fortis in a macro antenna reduces and/or eliminates many RF issues as the signal is sent or received. This eliminates the need for complicated antenna positioning and adjustment. For instance, the interference from PIM that can result from antennas located too close together is avoided by the Fortis-enhanced antenna itself.

Fortis IP with Digital Signal Processing

ISCO algorithms perform digital signal processing on the received radio signals. This starts with a segment of the received signal being captured and analyzed using a variety of different patented techniques. The analysis will detect and classify interference, if present. This information is then used to compute a set of parameters to condition the signal and reduce or remove the interference.

The analysis and classification are usually done in software because they don't need real-time processing. However, the signal conditioning, which involves making corrections to radio signals, is typically handled with hardware.

This approach has worked well in a number of large Tier 1 public networks and is illustrated below.



Source: ISCO

Fortis IP Embedded in an RF Device

Using its Fortis IP, ISCO has also packaged its technology into a simple-to-install RF product that helps reduce RF challenges, showing that interference management can be included as new devices are developed for private networks.

In addition to the above scenarios that have already been tested, ISCO's Fortis IP can be added directly to silicon chips, expanding the possibilities for use in the various components of private networks.

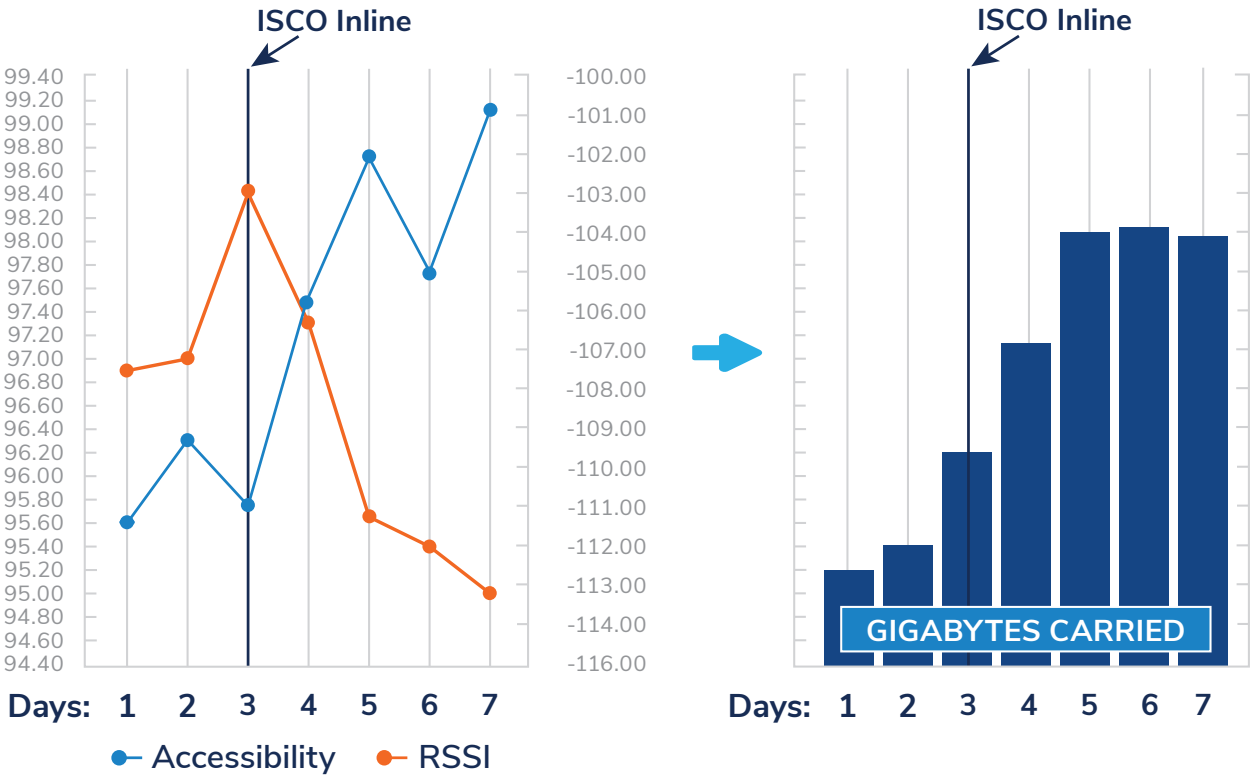
Differentiating the Private 5G Network

Frost & Sullivan projects that the market for private 5G networks will grow very quickly over the next five years. Why? Because they solve business problems for a wide range of enterprises that other options cannot solve.

However, there are many options in providing a private 5G network. Which radios (RUs), which antennas, which DU supplier(s), which CU supplier(s), which transport supplier(s), which core network supplier(s), and more.

Since RF challenges occur in EVERY wireless network, there is another important differentiator: which private 5G network minimizes the inevitable RF issues and interference? Answer: the one with ISCO's Fortis technology. When ISCO's technology is included, the private network will work better, and business risks are minimized because the network can handle more wireless connections. The following graph shows that when a solution that includes ISCO's Fortis technology is installed there is an immediate impact on important KPIs. Accessibility and Received Signal Strength Indicator (RSSI) both improve. Removing interference directly improves SINR (Signal to Interference Noise Ratio) by reducing noise rise. A user that could not be heard or device that could not be connected can now access the network. Interference management is critical for private networks to meet their goals.

Improvement in KPIs after ISCO is deployed results in more carried traffic



Source: ISCO

Who is Responsible for Interference Management?

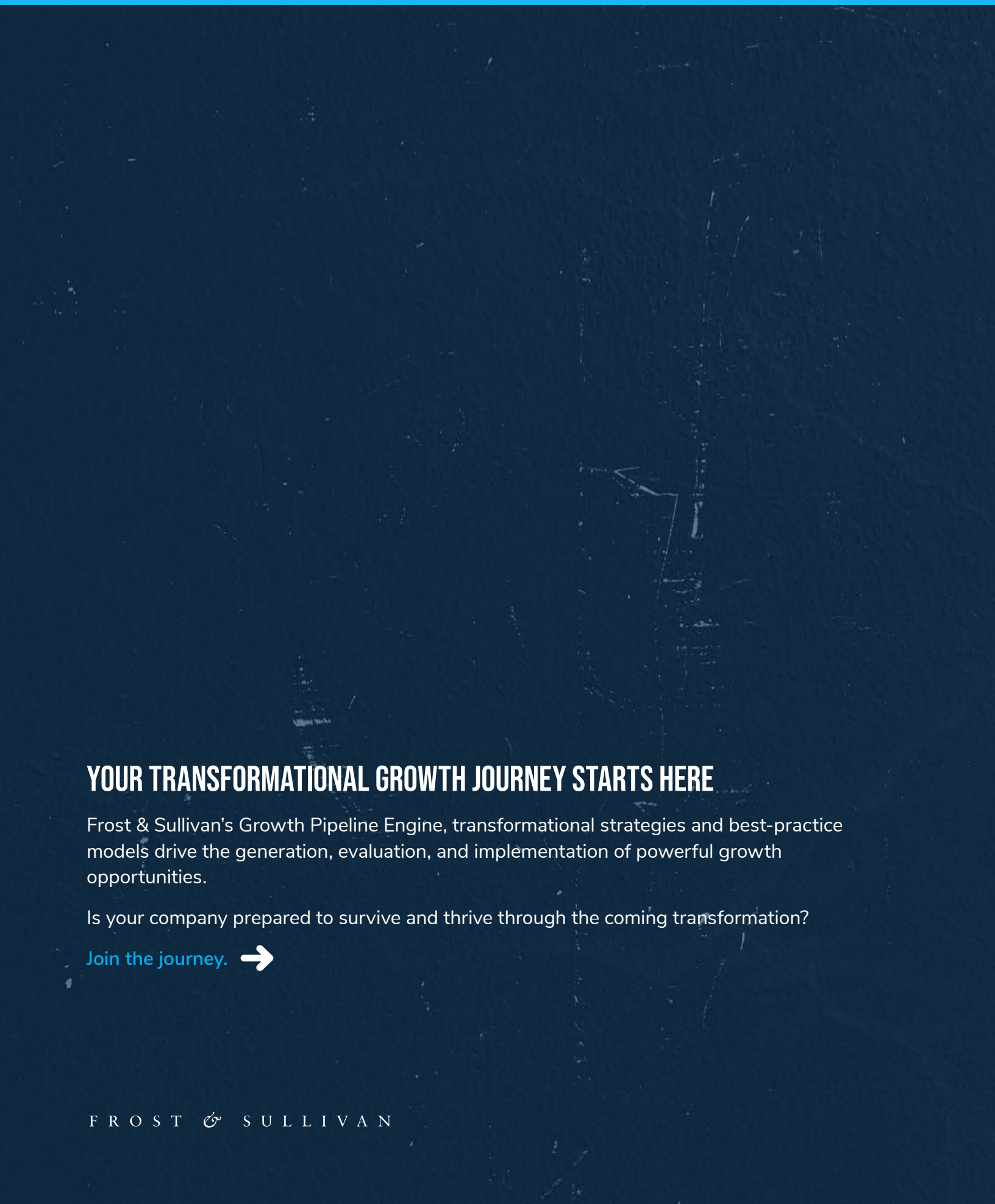
As mentioned previously, there are many ways ISCO's Fortis technology for interference management can be delivered. Therefore, every part of the private 5G network ecosystem can use it to differentiate their offerings.

MNOs are looking to expand their business with enterprises and see private 5G networks as a great opportunity. They can help with spectrum, they can help with networking expertise, and they understand the challenges associated with cellular networks. And many MNOs (particularly US-based Tier 1s) already use ISCO's technology in their public networks!

RU suppliers and antenna suppliers now have an additional way to differentiate their products by incorporating ISCO's technology within their products.

System integrators bring together a set of network suppliers along with industry expertise to help an enterprise move in this new direction.

For any of these types of companies, including ISCO's Fortis technology in their offering for new 5G private networks that are now being designed and installed helps differentiate them from their competition on day one, and in the days and years to come.



YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. ➜

FROST & SULLIVAN