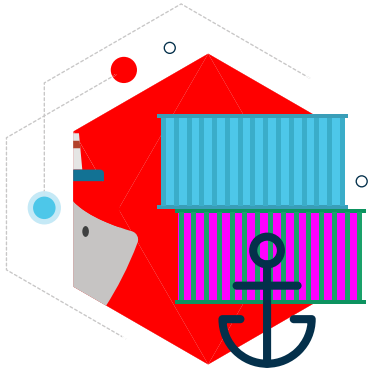


ENABLING THE

CONNECTED **PORT** OF THINGS

How a Living Network™ Addresses the
Top 5 Challenges of Port Networking Today

RAJANT

Modern ports are truly living environments—they continuously grow, change, and move.

That is why a port's network should be able to do the same.

Today's shifting technology landscape has monumentally impacted how we communicate, how we do business, and *how we trade*. Specifically, the Internet of Things (IoT) – which began mainly in consumer-oriented applications – is now being applied to create, enhance, and extend networked connectivity across industrial settings such as ports to connect to, communicate with, and control all the high-value moving assets operating within them.

This level of port connectivity has the potential to not only maximize operational efficiency and productivity, but to also truly transform port business models by giving operators the ability to predict equipment health and performance, create autonomy, and deliver new services.

Unfortunately, many ports are still limited by outdated, disparate networks that restrict expansion and make the scale and mobility needed to create a truly connected 'Port of Things' feel out of reach. This is only compounded by the fact that ports are vital hubs of international trade, and therefore key targets of both physical and cyber attacks. As greater amounts of mission-critical information traverse the network, redundancy (to mitigate communications downtime) and data security (to protect against advanced hacker threats) become even more essential.

THIS LEADS TO A DIFFICULT CONUNDRUM

How do ports evolve their existing networks...

RAPIDLY **SECURELY** **RELIABLY**

...to take advantage of the data-driven opportunities IoT provides?

5 KEY CHALLENGES
to Achieving Mission-Critical Mobile Port Connectivity

When deciding how to build out their networks to support increasingly complex operational and security functions in an ever-moving, always changing environment, most ports are confronted with a myriad of challenges. Particularly when it comes to mobile network connectivity – the kind that enables people and machines to move and communicate simultaneously and in real-time – these obstacles include:

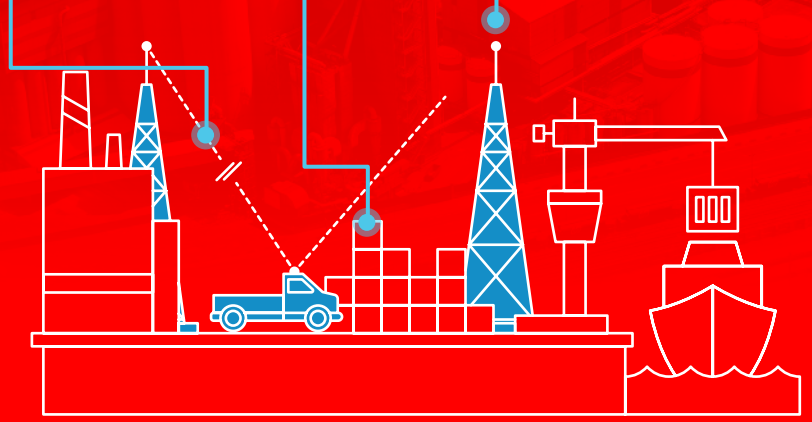
1 AGING, MOBILE-LIMITED INFRASTRUCTURE

The majority of the world's major ports have been functioning for decades. Over time, they have expanded beyond the communications capacity of their static wired network, especially as the data volume demands for SCADA, RFID, CCTV, and related applications have increased and the need for mobile communications has become essential. By adding wireless technology, whether cellular/LTE, point-to-point (PTP), or point-to-multipoint (PtMP) solutions, port operators may be able to realize incremental mobility gains, but the capabilities of such wireless solutions still fall short (see sidebar for why) when trying to achieve reliable, rapidly scalable everywhere connectivity that new IoT applications demand.

Even so, investment in these complex existing infrastructures is so significant that a full 'rip and replace' simply is not feasible. Network expansion has to efficiently build upon and integrate with the array of devices and technologies already in use, easily adding network capacity and reach whenever and wherever it is needed.

Traditional Wi-Fi and even standard mesh networks simply aren't built to thrive in mobile, dynamic port environments. Here's why:

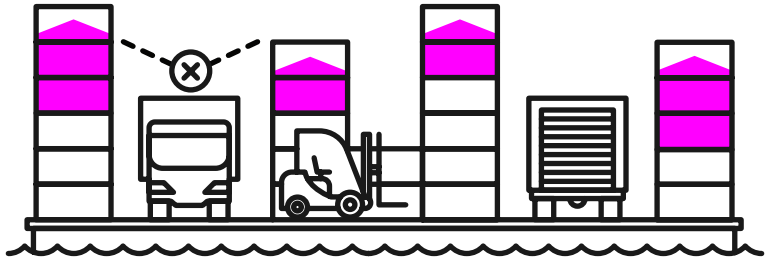
- **These networks use a "break-before-make" or "make-before-break" paradigm of connectivity.** Mobile nodes also only make one connection at a time, via a single frequency, so they therefore must continually break and re-establish connectivity as they move between access points.
  - **They also assess routes based only on RSSI,** not accounting for other significant performance factors like interference or congestion.
    - **Every break results in a temporary loss of communications.** If a node is not able to easily connect to its next closest access point due to line of sight issues or bottlenecks at the master controller node, lag time can be long enough to cause substantial operational disruption.



2 SIGNAL INTERFERENCE

The global container shipping capacity is **expected to grow by 8.4%** this year[1], with a single large merchant ship now able to carry more than 19,000 TEU containers[2]. An increasing number of ground vehicles, quay cranes, forklifts, and people are needed to move this capacity in and out of the port efficiently each day, but keeping them connected while doing so is problematic. Metal cargo containers are key culprits of signal blockage, making it very difficult to keep employees, equipment, and critical assets in communication as they move between massive container towers.

A network can be specifically arranged to avoid such signal interferences, but only in a static, predictable environment. In ports, where large metallic shipping containers are constantly in motion, configuring a traditional wireless network around interference is unrealistic.

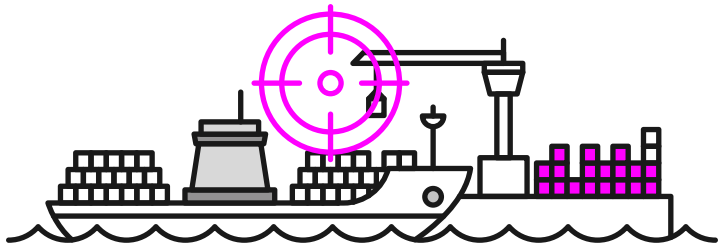


Global container shipping capacity is **expected to grow by 8.4%.**[1]

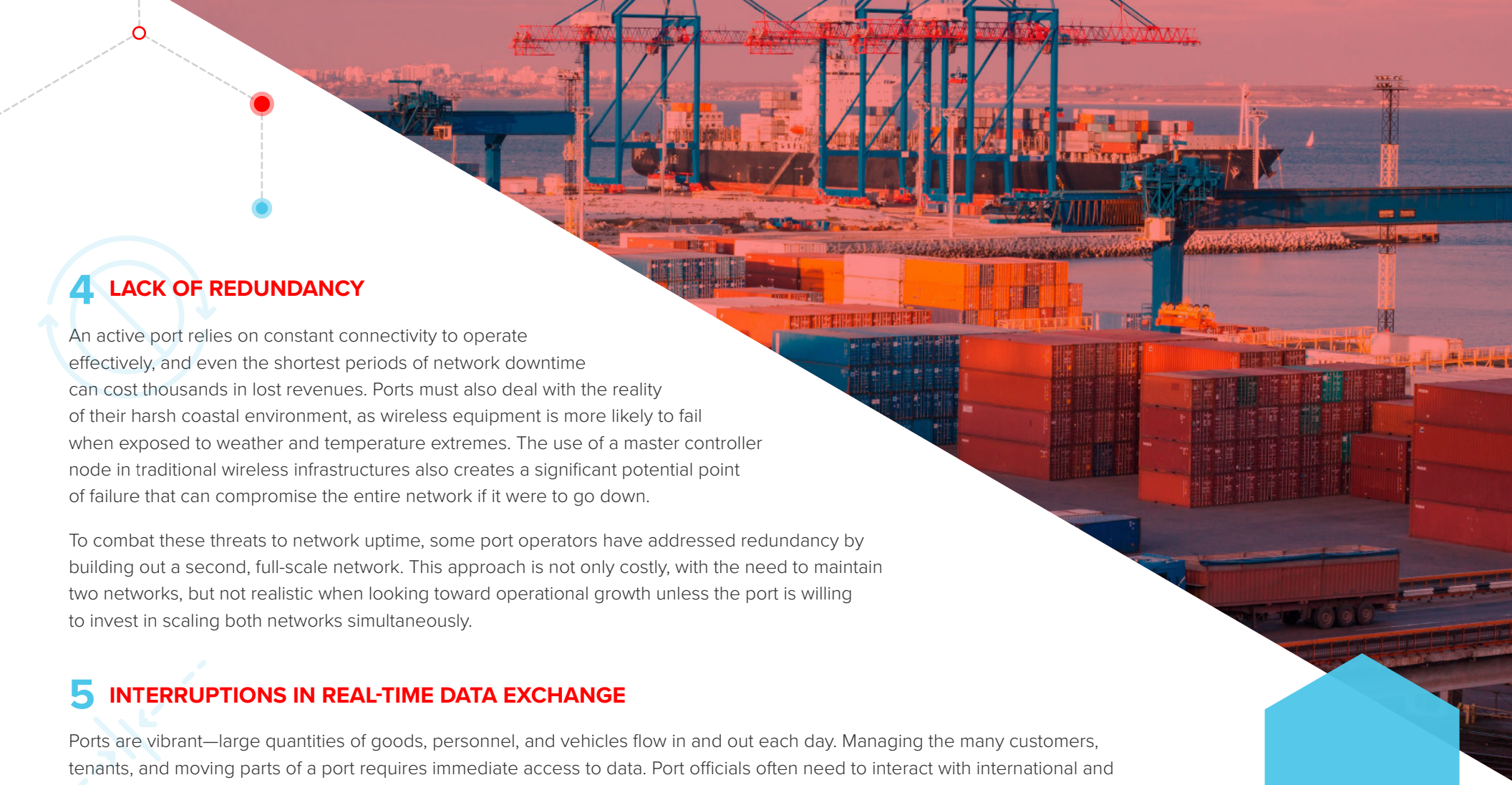
3 SECURITY

With **90% of world trade carried by the international shipping industry**[3], ports have become high-risk targets for terrorism and other malicious breaches – on both the physical and cybersecurity fronts. Many ports have already implemented layered security systems to protect the portside itself, which could include fencing, sensors, access control, CCTV, radar, sonar, and land and waterside patrols; that said, they may still be lacking the adequate network security needed to protect their data from advanced threats like ransomware attacks, which have increased in incidence by 300% since 2015.[4]

In both cases, increasing volumes of cargo and data make security more complex. Applications such as video surveillance and real-time asset tracking can help to manage the physical security of assets across a sprawling environment, but these data-intensive applications require a significant amount of bandwidth. In parallel, the network must expand its physical coverage to connect more assets moving throughout a growing port, and scale without opening up areas of weakness that cyber threats can target.



With 90% of world trade carried by the international shipping industry[3]**,** ports have become high-risk targets for terrorism and other malicious breaches.



4 LACK OF REDUNDANCY

An active port relies on constant connectivity to operate effectively, and even the shortest periods of network downtime can cost thousands in lost revenues. Ports must also deal with the reality of their harsh coastal environment, as wireless equipment is more likely to fail when exposed to weather and temperature extremes. The use of a master controller node in traditional wireless infrastructures also creates a significant potential point of failure that can compromise the entire network if it were to go down.

To combat these threats to network uptime, some port operators have addressed redundancy by building out a second, full-scale network. This approach is not only costly, with the need to maintain two networks, but not realistic when looking toward operational growth unless the port is willing to invest in scaling both networks simultaneously.

5 INTERRUPTIONS IN REAL-TIME DATA EXCHANGE

Ports are vibrant—large quantities of goods, personnel, and vehicles flow in and out each day. Managing the many customers, tenants, and moving parts of a port requires immediate access to data. Port officials often need to interact with international and country-specific agencies, supplying them with secured, authorized information when they need it. Operators must uphold safety and security with ready access to information on the location and status of people and cargo. At the same time, a plethora of operational applications must be supported to provide real-time insight into port operations, from crane management to GPS container tracking, vehicle management and automation, surveillance, and more.

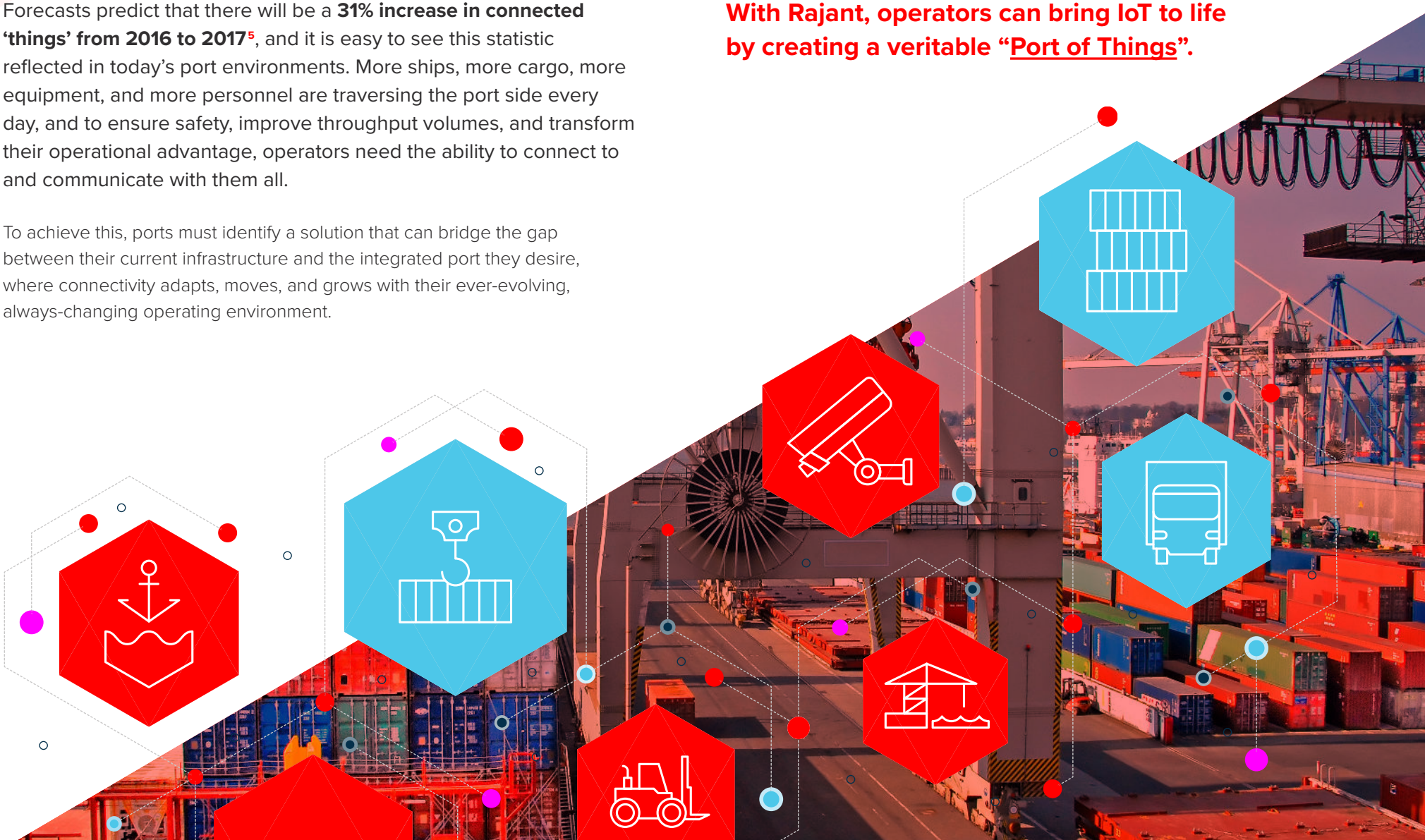
Despite all this, a network that can provide highly available, high capacity broadband connectivity across all areas of the port, and to the people and assets moving within it, can be hard to come by because most solutions are unable to effectively address interference, mobility, or scalability in a rapid and reliable manner.

LIVING CONNECTIVITY:
The Solution Living Ports Need

Forecasts predict that there will be a **31% increase in connected 'things' from 2016 to 2017**[5], and it is easy to see this statistic reflected in today's port environments. More ships, more cargo, more equipment, and more personnel are traversing the port side every day, and to ensure safety, improve throughput volumes, and transform their operational advantage, operators need the ability to connect to and communicate with them all.

To achieve this, ports must identify a solution that can bridge the gap between their current infrastructure and the integrated port they desire, where connectivity adapts, moves, and grows with their ever-evolving, always-changing operating environment.

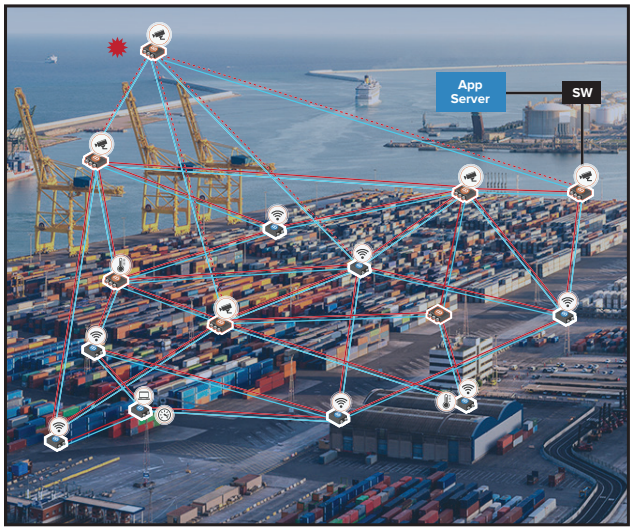
With Rajant, operators can bring IoT to life by creating a veritable "Port of Things".



Rajant Kinetic Mesh®
Powering the Living Network™

Rajant's Kinetic Mesh private wireless network gives ports the ability to rapidly deploy the fully mobile, highly adaptable, and secure connectivity they require: powering a Living Network™ that works autonomously to deliver robust applications in real-time.

Kinetic Mesh enables this by giving operators the ability to transform virtually any asset, fixed or moving, into network infrastructure. Deploying Rajant's ruggedized, multi-radio BreadCrumb® nodes, equipped with InstaMesh networking software, directly on the asset – be it a vehicle, quay crane, material handling equipment, surveillance camera, or drone – essentially turns that asset into a network node. Instead of each BreadCrumb only communicating with centralized access points, they are all able to share information back and forth in a highly interconnected web of communications.



In a Rajant Kinetic Mesh network as shown to the left, any node can receive data packets from one peer and direct them to another via multiple simultaneous connections. This example shows BreadCrumb nodes with two frequencies, although each BreadCrumb can support up to four frequencies.

BreadCrumb LX5 Wireless Nodes

BreadCrumb ME4 Wireless Nodes

5.8GHz

2.4GHz

Localized Interference on 5.8GHz

What are BreadCrumbs?

Rajant's ruggedized wireless radios can be used interchangeably as fixed or mobile nodes, and can communicate peer-to-peer via multiple simultaneous connections.

Each supports **up to four frequencies** over which traffic can be sent and received.

IP67 design is **built for extreme environments and conditions.**

Provides **configurable per-hop, per-packet data** authentication.

What is InstaMesh?

Rajant's patented peer-to-peer technology performs real-time evaluation of network links to direct traffic via the fastest pathways between any wired, wireless, or in-motion points.

- Completely distributed Layer 2 protocol eliminates controller node or single point of failure
- Instantaneously redirects traffic via the next best available link if any one path is compromised or obstructed
- Creates a fully redundant, self-healing network

5 CRITICAL BENEFITS

of a Living Network™, Powered by Rajant Kinetic Mesh

A Rajant Kinetic Mesh network is uniquely equipped to handle the complexities of today's port operations because it offers:

1 SEAMLESS INTEGRATION FOR RAPID NETWORK SCALABILITY

Kinetic Mesh is designed to flawlessly integrate with existing network infrastructure and non-Rajant technology and devices. The network supports Wi-Fi and uses Ethernet for easy integration with satellite, fiber, copper, cellular, LTE, 3G/4G, PTP, and PtMP wireless.

The network is easily scalable to hundreds of high-bandwidth nodes, giving ports the ability to leverage their legacy network investments while adding capacity and reach whenever and wherever it is needed throughout the port.

2 TOTAL NETWORK MOBILITY

Instead of retrofitting mobile-limited network technology in environments that demand total movement, Rajant's Kinetic Mesh takes a totally fresh approach with "Make-Make-Make-Never-Break" connectivity.

Through InstaMesh, each BreadCrumb node can maintain hundreds of peer connections simultaneously, even while in motion, and autonomously make new connections to other nodes as they come into range. No connections need to be broken for new ones to be made, so communications and data packets are not dropped.

If one path becomes blocked or interference is identified, InstaMesh dynamically redirects traffic over another available path, with the network automatically optimizing itself as conditions naturally change. This connectivity paradigm enables complete network mobility and ensures real-time flow of data, voice, and video at low latency and with mission-critical reliability.

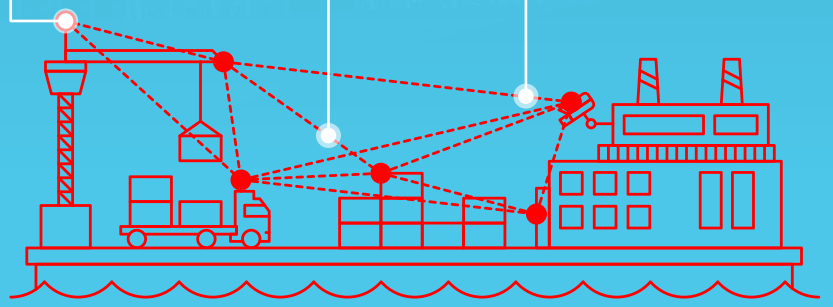
3 FULL REDUNDANCY BUILT IN

The "Make-Make-Make-Never-Break" approach also provides the Rajant network with built-in redundancy. Its ability to maintain multiple simultaneous connections removes any single point of failure and virtually eliminates downtime, and is readily scalable to hundreds of nodes. In fact, adding more nodes establishes more pathways to increase network resilience.

By adding a mobile wireless backhaul, or additional wired LAN connections as needed, the bandwidth of a Rajant Kinetic Mesh network can be readily scaled as well.

Rajant's Kinetic Mesh network achieves adaptable mobility by using a one-of-a-kind "Make-Make-Make-Never-Break" approach to connectivity. Here's how:

- **All BreadCrumb nodes are equal and all can direct traffic via multiple peer connections simultaneously,** whether fixed or moving. No connections must be broken for new ones to be made.
- InstaMesh provides **continuous path switching of wireless and wired connections** over the best available link, calculating the path that enables the fastest time to delivery in that moment.
- If one path is not available or interference is identified, the **information is dynamically redirected over a redundant available path,** upholding mission-critical reliability.

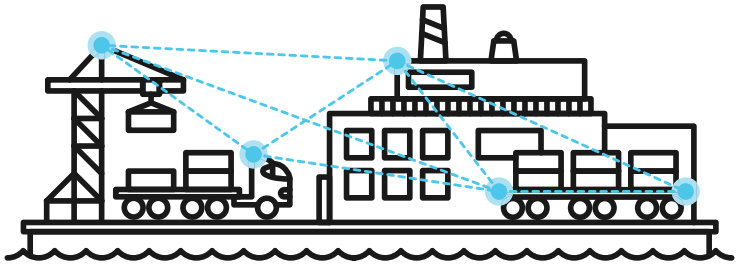


4 MILITARY-GRADE NETWORK SECURITY TO SUPPORT SAFE OPERATIONS

Rajant understands that industrial IoT networks have unique requirements that must be accounted for in the design and integration of their security. Born from military applications, Rajant's network offers robust security capabilities, including:

- Multiple cryptographic options
- Configurable data and MAC address encryption
- Configurable per-hop, per-packet authentication between BreadCrumbs
- Layer-2 and Layer-3 client/server and peer-to-peer security solutions compatibility

Rajant's Kinetic Mesh network also provides the high bandwidth needed to support video surveillance initiatives throughout a port, from streaming live remote camera video to dispatchers, security officials, and first responders to maintaining visual communications with patrolling unmanned aerial or ground vehicles.

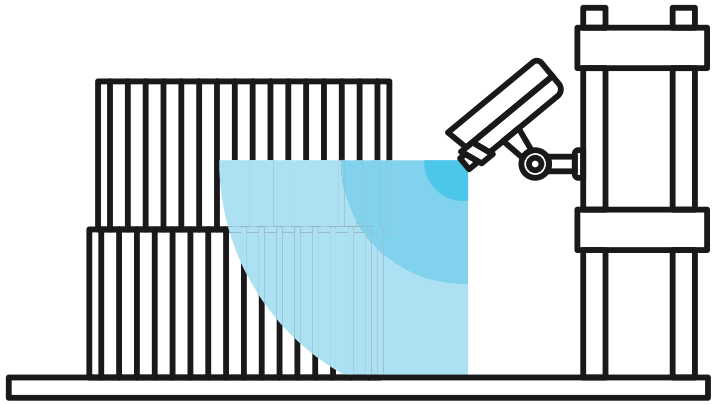


BreadCrumb nodes can **maintain hundreds of peer connections simultaneously,** even while in motion, and make new connections to other nodes.

5 EXTREMELY RELIABLE, REAL-TIME PORT-WIDE COMMUNICATIONS

With no single point of failure and self-healing capabilities, a Rajant Kinetic Mesh network guarantees uptime of mission-critical applications, anytime and anywhere they need to be accessed. With a BreadCrumb on board, each asset itself becomes a network node and has robust, redundant connectivity to other networked assets. InstaMesh can easily route data from these assets around network congestion or signal blockage using any of the multiple radio frequencies available to ensure real-time delivery rates are upheld.

Even bandwidth-intensive applications like video surveillance or remote equipment control are easily supported. Rajant's Automatic Protocol Tunneling (APT) feature enables reliable and fast off-loading into a wired Ethernet network via multiple, simultaneous bridge-mode links, avoiding Spanning Tree Loops. Having multiple ingress and egress points increases usable bandwidth and delivers data to client devices faster.



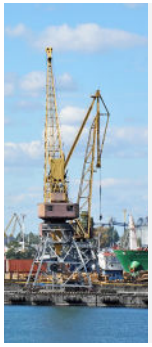
A Rajant Kinetic Mesh network **guarantees uptime of mission-critical applications, anytime and anywhere** they need to be accessed.

CREATE A CONNECTED PORT OF THINGS

and Create New Competitive Advantages

Rajant Kinetic Mesh® delivers the robust, mobile-enabled connectivity required to fully capitalize on the opportunities of IoT, because the network *is* the assets: all of the variable, valuable 'things' that must connect and communicate to power transformative insights, efficiencies, and revenue gains.

In addition to supporting efficiency and productivity gains, this technology can transform a port's network into a strategic asset by providing the port-wide access, reach, and mobility needed to support next-generation applications such as:

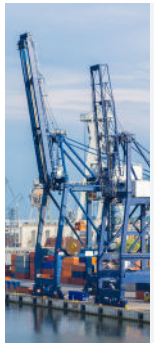


AUTONOMOUS EQUIPMENT

By equipping autonomous or semi-autonomous equipment with BreadCrumb nodes and device-specific command software, operators can communicate with and control remote equipment such as quay cranes and unmanned vehicles.

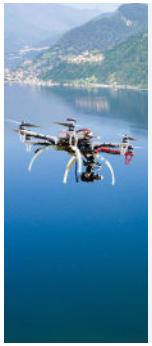
WI-FI ASSET TRACKING

Rajant enables tracking of low power Wi-Fi asset tags so that containers, equipment, and people can be located instantaneously, improving port efficiency, security, and safety.



ASSET MANAGEMENT

A Rajant network can provide real-time connectivity to enable applications for telemetry; cargo, container, and equipment tracking; and equipment health monitoring.



DRONE COMMUNICATIONS

Rajant offers a BreadCrumb module that can be attached to a single drone or a fleet of drones to collect and transfer large amounts of information securely. The drones can also be deployed in a tethered configuration to work around obstacles and operate days or weeks over long distances.

ADVANCED SURVEILLANCE AND MONITORING

The Rajant network's high bandwidth capabilities allow ports to receive real-time streaming video from unmanned ground vehicles (UGVs) and remote equipment autonomously patrolling the port's perimeter. First responder vehicles and officers can also be fitted with cameras and BreadCrumbs to receive on-scene video and emergency information while en-route to an incident, and provide real-time updates on status once they arrive.

Why Rajant?

Trailblazers Invent Paradigms Instead of Following Them

Rajant was founded to address the significant shortcomings in traditional wireless mesh technology, particularly when it came to mobile voice and data networks used by first responders. The Rajant team envisioned a new, more robust mesh technology that would allow these networks to be fully mobile and mobility-enabled, and operate reliably in even the most demanding environments. Enter the Rajant Kinetic Mesh® network.

Through Rajant's unequaled ability to turn mobile assets into network infrastructure, organizations across industries have been empowered to take private network applications and data everywhere. For more than 16 years, Rajant's networks have been successfully meeting the unique needs of customers across military, mining, oil and gas, port, transportation, and municipal environments.

To learn more about how Rajant's Kinetic Mesh network technology can become a strategic asset for your port, visit www.rajant.com/portofthings today.

RAJANT

20+ Years OF GAME-CHANGING WIRELESS

Rajant Corporation

200 Chesterfield Pkwy.
Malvern, PA 19355

P: 484.595.0233

E: info@rajant.com

www.rajant.com

References

1. Global Container Shipping Outlook 2017: Capacity discipline is needed to support & lift freight rates; increased industry concentration helps
2. Global container fleet expands by almost 1.44 million TEU in 2017
3. International Chamber of Shipping, "Shipping and World Trade," 2015
4. Ransomware attacks increase 300% in 2016
5. Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016