Leveraging Technology to Improve Safety in Confined Spaces

Advanced mesh networking solutions, certified for explosive gas environments, reduce operating costs, deliver productivity improvements, and reduce risks for workers in confined spaces.

RAJANT

Table of Contents

Introduction:
Better Communication Means Better Safety

Confined space work is inherently dangerous. Tanks, vaults, manholes, tunnels, and other areas with limited or restricted ingress and egress pose safety hazards, and despite the efforts of HSE professionals and increasingly stringent safety protocols, injuries and fatalities continue to occur.

According to the U.S. Bureau of Labor Statistics, between 2015 and 2018, there was an average of 111 deaths in confined spaces per year across the four-year period.

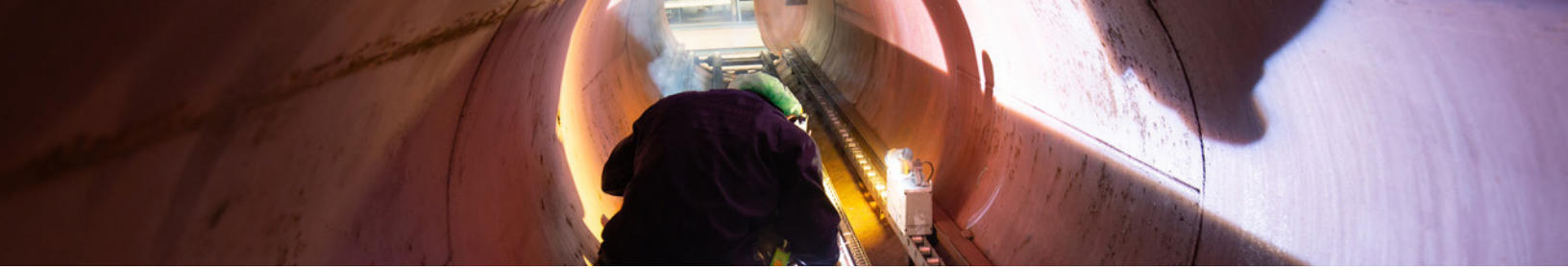
Nearly 90% of these confined space fatalities occur on jobs that had been authorized by a supervisor.

While multiple causes were cited for the confined space deaths recorded, a fair number of the fatalities resulted from exposure to fatal atmospheres. 40% of those cases, the hazard that caused the fatality was not present when the worker entered the confined space.

These are sobering statistics, and it is time for a change. Safety management must improve to reduce the number of fatalities in confined spaces significantly, and new, more effective tools must be added to the toolbox.

On average, more than **111 workers died** each year between 2015 and 2018 as a result of an accident or incident in a confined space.

Source: U.S. Bureau of Labor Statistics



Examining the Past to Improve the Future: Limitations, Vulnerabilities, Shortcomings

Historically, a qualified safety attendant managed the risks associated with confined space entry.

Authorized attendants track ingress and egress at the entrance to a confined space, making sure only authorized personnel are present in the restricted area. Because their job is to monitor situations inside and outside confined spaces, attendants must be aware of the hazards of the particular confined space and understand the physical and behavioral effects of hazard exposure. This knowledge allows them to determine if a worker is in physical danger and issue instructions for evacuation.

If an emergency arises in the confined space, it is the attendant's job is to summon emergency services and perform whatever rescue operation they have been trained and equipped to perform. Because of the criticality of this oversight role, an attendant is not permitted to leave the space until replaced by another attendant unless all entrants into the confined space have exited it.

Occupational Safety and Health Administration **(OSHA)** dictates that the **safety attendant** must:

- Continuously maintain an accurate count of personnel in the confined space
- Be able to identify all entrants to the confined space
- Monitor activities inside and outside the confined space to ensure the safety of the entrants
- Summon rescue or other emergency personnel when needed
- Perform nonentry rescues when possible
- Never leave their post when on duty.

The duties of the attendant require constant vigilance and meticulous attention to detail when collecting, collating, and managing records. Any distraction from the monitoring process could open the door to disaster, and any miscount of personnel could result in an unsupervised worker being exposed to a potentially life-threatening risk.

Because the safety attendant is positioned outside the confined space, the inability to see what is happening inside the space is a serious impediment to safety management. Another impediment is the inability to communicate work orders or information about a potentially dangerous environment, particularly when visibility is restricted, or workers are not in the line of sight.

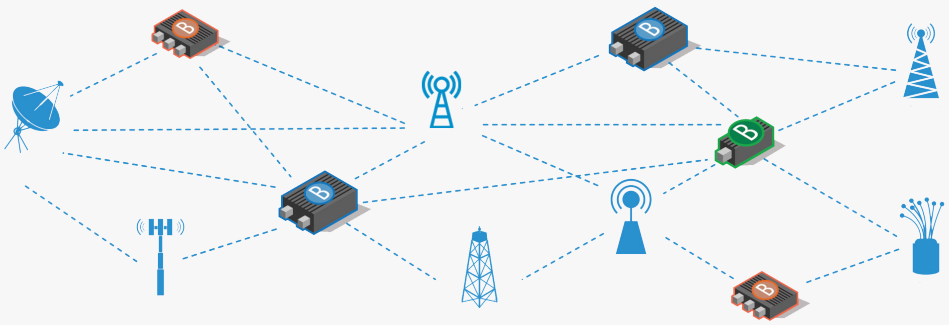
Traditional confined space safety management poses other challenges as well. A complex worksite can require multiple attendants across a large area, and it is often difficult to find qualified and experienced workers to fill this role.

In addition, as the fatality statistics demonstrate, undetected gasses lead to a large number of worker deaths. Although the attendant is required to test for gas before workers enter a confined space and to perform subsequent tests up to four times per shift to ensure that nothing has changed, it is challenging to capture subtle changes in atmospheric composition that could escalate in a confined space to create hazardous conditions for workers.

When an incident does occur, recounting how the situation developed, what happened during the event, and how the matter was resolved falls to the safety attendant. In most instances, there is no clear documentation or neutral and reliable record of the events leading to the incident or what transpired.

Technology is the key to improving worker safety. Advancements in gas detection, video surveillance, and communication can be combined to improve access control, worker monitoring, and incident resolution, improving productivity, and greatly reducing the risks associated with confined space work.

Rajant networks do not use a controller node and have no single point of failure. Using make-make-never-break technology, each radio can have multiple node connections. This any-node to any-node connectivity allows BreadCrumb® networks to scale to hundreds of interconnected mobile nodes, eliminating jitter by providing thousands of potential pathways over which data can be sent and received.



When interference or signal blockage occurs, InstaMesh dynamically routes communications via the next-best available path to guarantee performance, so there is no downtime, and network latency is minimized. The Rajant network allows three or even four times the number of retries—up to three per second—keeping information flowing and eliminating data loss. And since BreadCrumbs automatically form multiple connections with other nodes within the mesh, the network is inherently redundant.

Technology Changes the Playing Field:
Faster, Smarter, Safer

Today, it is possible to reduce the likelihood of accidents and injuries using technology to improve the visibility of workers, enhance atmospheric testing, and enable reliable communication between personnel tasked with monitoring safety and workers inside confined spaces.

Increasing interconnectivity requires a network that ensures the security and authenticity of the communications traffic moving in, out, and across it. For companies that work in ATEX environments, connectivity is even more critical. Critical applications must run on a communications network that offers reliable, agile, and adaptable connectivity and can thrive in diverse mobility-driven environments.

Rajant is helping companies address safety challenges with secure, dependable networks that enable continuous, efficient operations, and companies already are using this communications technology to enhance operational efficiencies and mitigate safety risks to achieve new levels of operational integration and performance.

The ideal solution across the board is a “living” mesh network.

Rajant Kinetic Mesh wireless networks adapt to changes in connectivity demand through a flexible, scalable, robust product that sets the standard in broadband connectivity for reliability, resilience, and adaptability.

As the exclusive provider of private Kinetic Mesh wireless networking, Rajant uses BreadCrumb network nodes powered by InstaMesh software to deliver a peerless network that is adaptable and scalable, providing real-time data on demand.

BreadCrumbs (aka radios) seamlessly integrate with any Wi-Fi or Ethernet-connected device to deliver low-latency, high-throughput data as well as voice and video applications across a meshed, self-healing network. Any information that can be sent over Ethernet can be sent over a Kinetic Mesh network.

Facing Down Network Challenges:
InstaMesh Delivers a New Standard for Performance

Companies face daunting challenges when planning and implementing a communication network that provides site-wide mobile access to vital data, voice, and video.

Work sites often cover large areas that are subject to noise, dirt, and, in some cases, weather extremes, and work conditions are subject to change. In this environment, companies strive to maintain continuous operations, without compromising safety. The design of the Rajant system improves interconnectivity by allowing devices to communicate in an ATEX environment. Automating and unifying communications across a worksite using this system streamlines operations and delivers reliable, continuous service for improved worker safety.

Patented InstaMesh software is the foundation of the Rajant Kinetic Mesh network and the primary reason Rajant networks outperform competitive systems.

Most mesh networks rely on a centralized root controller node to manage routing. Some of these system providers claim to use multiple frequencies, but what this means in the context of their systems is that they use one frequency for backhaul and another for client service. Because mobile devices lack infrastructure capabilities, they can connect to only one access point at a time. So, if an access point fails, all nodes connected to that access point are disconnected from the network (break-before-make). This means access points are potential points of failure. In the case of root controller nodes, one device manages the routing for the entire wireless network. If the root node fails, the whole wireless network goes offline.

Packets of data wait in line to be sent, and when the packet in front takes longer to be sent because the network is looking for a connection, the delay impacts all the packets behind it. If the connection takes too long, the attempt to transfer the data times out, and the packet is dropped.

`BreadCrumbs operate within a specific band of frequencies and are programmable to certain channels within that band. They support the simultaneous use of 900 MHz and 2.4, 4.9, and 5 GHz frequencies for redundancy and interference mitigation, and custom transceiver configurations and frequencies are available for development.

Most multi-radio wireless networks separate traffic into two types:

- Client access traffic, which includes communications among access points and Wi-Fi clients such as laptops, tablets, smartphones, and sensors
- Backhaul traffic, which connects access points over long distances.

Unlike many competitive wireless technologies, Rajant networks grow stronger and more resilient as nodes are added.

InstaMesh networking software is the mobility enabler for Rajant solutions and is responsible for the continuous and instantaneous forwarding of wired and wireless connections within the network. While InstaMesh uses a proprietary routing algorithm, it is fully compatible with IEEE 802.11 wireless computer networking standards.

A Rajant network transmits and receives data via satellite, point-to-point wireless, or wired links anywhere an ingress or egress point is needed. It also allows Virtual Local Area Network (VLAN) connection in a novel way, using only endpoints. This design allows up to 4,096 VLANs to be connected to the Kinetic Mesh network and eliminates the need for building precisely planned communication routes.

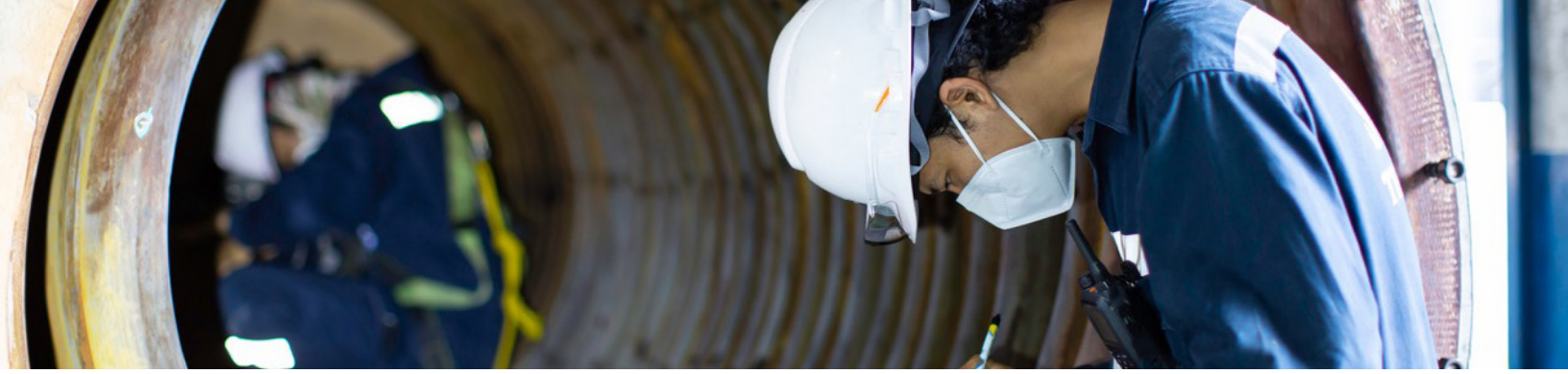
In traditional systems, a single disabled VLAN node can completely disrupt communications. The Rajant system enables continuous communication even if a FLAN is offline, delivering VLAN-tagged packets via the Kinetic Mesh exactly the way untagged packets are transmitted, using the quickest, most reliable route.

Rajant uses the VLAN to deliver Quality of Service (QoS), reduce packet loss and latency, and allow packet prioritization, essentially ranking virtual networks within the mesh. The flexibility allows data prioritization – a CCTV feed, asset tracking data, or SCADA data – to ensure critical data is transferred efficiently and prevent nonessential functions from slowing down critical operations.

As nodes are added, moved, or removed, InstaMesh adapts, establishing new links in real time while keeping the network available, intact, and secure. The software enables complete network mobility, robust fault tolerance, and high throughput with minimal maintenance and administration.

Because BreadCrumbs work peer-to-peer, each node can be fixed or mobile.

Rajant networks are designed differently. Individual network nodes can accommodate up to four radios, allowing them to simultaneously send and receive on different frequencies. This is the critical differentiator. The mesh can use any of its multiple radio frequencies anytime, allowing users to maintain access to mission-critical data and applications even in the most challenging environments.



Kinetic Mesh Enables Seamless Growth:
Removing the Impediments to Adopting New Technology

The problem with most wireless technologies is that scaling the network with additional nodes often causes performance degradation. Organizations are often forced to operate multiple networks running in parallel because new applications and updates cannot be run. Overtaxed networks can have applications running in isolation from each other, which decreases productivity and safety.

Rajant solves this problem with an architecture that allows multiple applications to run over a single network and simplifies the transition to new architecture and applications without costly downtime. The network can be scaled to include hundreds of high-bandwidth nodes. This means new, smart devices like wearable personal protective equipment (PPE) can be added and deployed easily without compromising system performance.

Once a Rajant system is configured, new BreadCrumbs introduced to the network automatically begin communicating with other nodes in the area. This capability allows the network to streamline data transfer autonomously using unique any-node to any-node capability that routes traffic over the best available path to compensate for changing network status.

The Kinetic Mesh is a living network that can be expanded easily by adding Automatic Protocol Tunneling (APT), a gateway between wired networks and the InstaMesh wireless network. APT connections eliminate bottlenecks by getting data off the wireless mesh network and onto the wired network quickly. This technology, unique to Rajant, allows APT groups to be placed wherever Ethernet access exists. APT groups create multiple network ingress points, which means there is no single point of failure for data ingress to the wired network and servers.

In an APT group, two or more APT nodes combine to form ingress/egress points without introducing the possibility of a single point of failure. Each APT group elects a master node that encapsulates and decapsulates data, enabling reliable and fast data transfer to and from a wired Ethernet network.

Rajant's SlipStream nodes, designed specifically for APT connections, speed up the data transfer process. SlipStream is a wired BreadCrumb node that provides a high-throughput interface between a wired and wireless network. With SlipStream's high-speed processor devoted to Kinetic Mesh network encapsulation and decapsulation, data moves across the wired/wireless boundary up to seven times faster than a BreadCrumb used as an APT master.

SlipStream nodes integrate seamlessly with current BreadCrumb models and are backward compatible. System flexibility makes it easy to add BreadCrumb nodes and APT connections without sacrificing the continuous connectivity required to manage complex projects in offshore environments and work on both Rajant and non-Rajant wireless networks.

Having multiple APT groups within a mesh network can:

- Prevent a single APT master from being overwhelmed with multiple data streams
- Enable more efficient load balancing
- Allow fast re-routing should a failure occur
- Greatly increase traffic throughput.

Rajant's cross-generational forward and backward compatibility integrates with existing satellite, LTE, 3G/4G, fixed wireless, and Wi-Fi networks to rapidly optimize and extend coverage.

Differentiated multi-radio architecture makes the Rajant Kinetic Mesh network the only industrial wireless solution to offer high availability for any number of real-time applications, including such things as cameras, gas monitoring equipment, and wearable PPE devices, to dramatically decrease risk exposure for confined space workers dramatically.

Overcoming IIoT Connectivity and Cybersecurity Worries: Securing Information for Safe Operations

Rajant BreadCrumb wireless nodes, powered by InstaMesh networking software, offer firmware-embedded security features, including data and MAC address encryption as well as per-hop, per-packet authentication. Rajant assures mesh networks are secure with certified secure booting and secure program updating and provides event logging and reporting to track anomalies.

Network construction prevents rogue access points, the most common threat to wireless security. An unauthorized wireless access point installed on a network permits unwanted access, exposing the network to attack by anyone with a wireless connection who is close enough to gain access.

BreadCrumb security is flexible and can integrate with network security systems that reside on non-Rajant network infrastructure. BreadCrumb nodes can be configured with multiple, powerful cryptographic options up to 256-bit AES GCM, the highest commercially available encryption standard. Security features can be configured and managed easily using BCICommander, Rajant's proprietary configuration software. This solution minimizes cyber tthreats by minimizing potential attack vectors, safeguarding people and data, and enabling continuous operations.

The network simplifies video surveillance. With multi-transceiver, multi-frequency functionality, a Rajant network ensures video streams always have available paths to the command center, which delivers 24/7 site-wide video in real time.

The Rajant network also ensures security for stored data. A data-at-rest protection mechanism and encryption schemes preserve stored data authenticity. This capability, paired with the robust security features built into the BreadCrumb nodes, enables Rajant to provide reliable radio security and encryption without impacting network efficiency and performance.

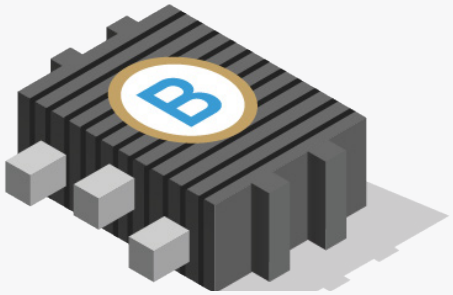
Rajant offers the **highest-grade** wireless security available commercially and is the only vendor in the world that uses **suite-B military-grade encryption** on a per-link basis with no license required and no extra costs incurred.

Improve Safety and Efficiency with Better Communications: Less Disruption, Improved Productivity

Applying advanced devices is a step in the right direction for improving worker safety. Still, the potential benefits of using this equipment are limited when technologies are implemented in a vacuum. To improve safety in confined spaces, devices must be interconnected on a reliable network that enables real-time communication.

Rajant's field-proven networks deliver the performance required to connect devices that improve confined space work.

By incorporating data feeds from cameras, smart meters, wearable PPE, and sensors, a Rajant network puts the right information in the hands of experts responsible for the critically important tasks of monitoring site conditions and identifying problematic issues. The ability to provide GPS-based locations and status tracking makes it possible to maintain communication with people anywhere on the asset for greater safety. Site-wide visibility makes it possible to identify potentially dangerous or disruptive activities before they cause accidents, injuries, or costly downtime.



Rajant technology can be applied to an **existing network**, which means, in many cases, companies can capture the benefits of advanced technology without creating a network from scratch. Kinetic Mesh networks enable continuous communications that help optimize every aspect of exploration, extraction, and production, delivering streamlined operations that increase productivity and improve the bottom line.

Future-proofing Operations:
Safeguarding Data as Technologies Advance

Rapidly changing infrastructure communication must meet the need for greater bandwidth, a higher level of security, and demand for true system resilience. Yesterday's systems for transmitting digital data for telemetry (low bit count) have been replaced with higher-bandwidth systems that can manage video images in RGB/RGBHV and IR formats.

Rajant Kinetic Mesh enables next-generation capabilities and future-proofs communications using multi-radio, multi-frequency redundancy. Wi-Fi or LTE communication can be plagued by interference and other deployment issues when operations are concentrated in a small area. The compact BreadCrumbs that form the Kinetic Mesh network compensate for that shortcoming by holding multiple connections over multiple frequencies simultaneously to create hundreds of potential paths over which to direct traffic.

Regardless of the volume or type of data, the network ensures rapid data transfer without compromising security.

Perhaps most significantly, Rajant solutions provide end users with networks that can meet changing demands, so technological advances no longer cause costly disruptions.

The interconnected future requires extremely **robust cyber-security and efficiencies** delivered via simplified networks. The Rajant solution offers the seamless and secure integration crucial to a safe and sustainable IIoT environment even in potentially hazardous environments.

RAJANT

*If it's **moving**, it's Rajant.*
*Industrial Wireless Networks **Unleashed.***

20+ Years OF GAME-CHANGING WIRELESS

Tel: 484.595.0233 | **www.rajant.com**

Learn more about Rajant's highly functional, easy-to-install BreadCrumb wireless nodes that form our Kinetic Mesh industrial wireless infrastructure. They work in concert with InstaMesh to enable voice, video, and data communications. Visit www.rajant.com or contact a representative to get started today.