

White Paper

**Protect Critical Assets
with Ultra Rugged,
Team Intelligent Devices
for Security and
Facilities Management**

Protect Critical Assets with Ultra Rugged, Connected Team Intelligent Devices for Security and Facilities Management

For today's mobile workers, a communication device represents a standard tool of the trade. However, for security operations and facilities management personnel – often lone workers -- that device is both a power tool and critical lifeline. From an IT/Operations perspective, not only does it need to be cost-effective, rugged and engineered with intelligence to maximize worker productivity, but also embedded with the safety features and reliable connectivity to protect lives. The stakes for companies and managers responsible for these workers have never been higher.

In fact, the Corporate Manslaughter and Corporate Homicide Act issued in 2007 has added another layer of liability for organisations and their managers when it comes to lone worker safety. And big fines are now being levied for companies who fail to demonstrate that they are doing everything possible to protect the Health and Safety of their employees. Ensuring these workers have access to reliable communications is key to keeping them safe. With numerous network and mobile device options available on the market – from two-way radios to Smart phones -- the evaluation process can be complex at best.

Understanding your workers' needs, their environment and the circumstances that define how they work is an imperative first step in device selection. This paper will address the critical communications requirements of security and facilities management personnel, review available technologies and the impact of that investment on IT, Health & Safety managers and Operations.

Progressive organisations are demanding solutions that deliver scalable, reliable and intelligent connectivity and a lower total cost of Ownership (TCO). Ensuring compliance to all relevant safety regulations and risk mitigation are important considerations as well, along with demon-

Keeping Operations Safe and Secure

Security guarding presents numerous challenges, for those who choose that line of work and the companies and managers responsible for them. Tasked with protecting people and property, security personnel usually work alone and in environments that put them in potentially dangerous situations. Reliable communications help keep these workers safe and are an important part of that responsibility.

Securitas Trades PMR for Ultra Rugged GSM

Securitas is a leading, global security solutions company with more than 260,000 employees in 40 different countries. To provide its clients and guards with the highest degree of safety, Securitas requires reliable and tough mobile handsets to keep employees protected and connected at all times. In the past, the company relied on portable Private Mobile Radios (PMR) for communications. But after ongoing coverage issues, numerous false alarms and lengthy and costly repairs, the company invested in a rugged GSM solution with advanced lone worker capabilities and the flexibility to match their existing safety processes. The result? Guard safety and productivity have improved with always on, reliable connectivity; the number of false maydays and man-down alerts has decreased; and, their overall costs are significantly reduced.

A critical lifeline, security guards function as the front line in emergencies. They are charged with managing access and ongoing risk assessment, thus require rugged communications devices that can withstand adverse environmental conditions, such as water, temperature extremes and maintain coverage no matter their location. They also need an intelligent device that can track user location and dynamically support team collaboration between multiple workgroups or outside public safety agencies.

Device safety and security

Smart phones have embedded security features to protect data, but require continuous updates to operate reliably and aren't designed for use in demanding or hazardous environments. Other limitations include limited battery life with GPS usage, usability challenges with gloves and audio levels in noisy, outdoor environments.

New rugged GSM technologies combine the best of both worlds with devices that not only feature native software applications, but also visible and tactile panic buttons, accelerometers that immediately detect falls or other accidents and GPS tracking specifically designed for lone worker scenarios.

When lives are on the line, communications count. Ensuring your enterprise, employees, business partners and customers are safe is a daunting responsibility. Arming security personnel with the right device not only protects their safety, but allows them to more effectively and efficiently protect the operation as a whole. Investing in reliable, rugged and smart connectivity will allow you to cost-effectively achieve both goals.

Improving Facilities Management Communications

According to a study by The British Institute of Facilities Management, facilities management – whether an internal function or outsourced service -- receives a significant portion of an organisation's budget, up to 20 percent of its total annual spend.

features can vary widely between communications devices. Private Mobile Radios (PMR) typically have dedicated tactile controls that trigger "man down" alarms when necessary. However, due to where they are physically located on the device, users can inadvertently trigger false alarms. Coverage issues can also impact a guard's connectivity to an operations center, thus leaving him unprotected and increasing the number of unnecessary alerts.

Defining Trends

Recent trends and statistics have raised the importance of security guarding to an urgent new level:

- The 2008-2009 British Crime Survey indicates that during the preceding 12 months, there were approximately 305,000 threats of violence and 321,000 physical assaults by members of the public on British workers.
- Business downsizing has resulted in an increase in lone workers, who are particularly susceptible to violence and assaults.
- The Management of Health and Safety at Work Regulations require employers to conduct a “suitable and sufficient” assessment of the risks employees face while at work. Employers who fail to recognize a foreseeable risk or address a significant potential risk can be found negligent.
- The Corporate Manslaughter and Corporate Homicide Act of 2007 is enabling prosecutors to go after corporate senior management straight up the management chain. This law makes an employers’ Duty of Care a legal requirement and very costly if not demonstrated. The first corporate manslaughter conviction saw a fine of £385,000 and sets the stage for greater corporate liability.

Despite this funding, facilities managers are under growing pressure to maximize expenditures and implement cost-effective, flexible communications solutions that can scale to meet not only short-term user requirements, but also longer term organisational goals.

Facilities management organisations are comprised of numerous lone worker functions, including cleaning crews, maintenance workers, etc. Knowing where these workers are and being able to instantly connect with them helps keep them safe and increase efficiencies. While two-way radios have traditionally been the communications technology of choice for these workers, integrated devices with Near-Field Communications (NFC) capabilities, voice and data provide a more robust and lower cost replacement. The primary benefit? Proof of attendance.

With embedded NFC, lone worker devices can track onsite attendance, as well key activities performed. NFC systems consist of a reader and a tag. When activated, the reader emits a short-range radio signal that activates a chip on a nearby tag. This tag communicates data to the reader. Embedded in a mobile device, this technology makes it possible for managers to collect business operations intelligence from front line workers, confirm tasks and ensure quality control.

A proof of attendance function provides real-time data that, for instance, a maintenance person or security guard has checked in at a specific station. These updates can be sent via email, SMS text message, web-service transactions, or some combination of these communications. This system can also verify a specific person has been at a specific location; if they do not indicate their presence through the NFC system within a specified period of time, an alert is automatically triggered. This message can be analyzed to determine where the person might be located so that immediate assistance can be sent.

Shared Requirements

The need for rugged, connected team intelligent communications solutions in this market segment is clear:

- Existing wired infrastructure systems may not be scalable to support existing communications requirements and fluctuating user levels.

- Wireless communications options are vast. The right solution can drive out costs and inefficiencies while improving in-building communications, user tracking and worker collaboration. The wrong solution will cost you time, money and resources.
- Shared equipment that is used during worker shifts and then returned to the device pool, must be ultra rugged and robust given the additional wear and tear on these devices.
- Instant, reliable communications in a rugged form factor is critical for employees on the move who need to immediately assess information or a situation and respond.

Increasingly, security and facilities management organisations are investing in ruggedized GSM phones to meet their communications needs. This sector requires fully integrated solutions that are as rugged as two-way radio devices have become. Several manufacturers have answered the call, providing options that adhere to strict rugged performance standards and offer both passive and active safety features.

In Their Own Words: What Users Want

Long battery life, ruggedness, reliability. These are just a few of what security and facilities management personnel want in a communications device.

CRITICAL NEEDS

- **“We have to work for extended periods, so we need lasting power.”** Whether managing facilities or providing security coverage, workers sometimes need to work long hours. Throughout these extended work periods, communication and continuous GPS-based applications must remain up and operational.
- **“We work in noisy environments and have to be heard above the din.”** Many functions related to facilities management and security operations take place outdoors, where the rumble of equipment, overhead aircraft and related sounds can impair communications and, consequently, the management and safety of the facility.

IDEAL SOLUTION FEATURES

- **Extra-long battery life** enables extended work periods without the need to return to base to recharge or change batteries. Devices need to support two, back-to-back shifts (16 hours), provide continuous GPS tracking every 5 minutes and several hours of talk time.
- **Extra-loud speakers** overcome the challenge of working in a noisy environment. In addition, loud, clear audio may permit hands-free operation, which could be very useful in emergency situations where workers can't use their hands to operate controls.

- **“Dust is constantly fouling our equipment.”** Dust and other micro-particles are the enemy of electronic devices, gumming up operation and impairing communications.

- **Dust protection** can be achieved by sealing the device against natural or industrial micro-particles, minimizing downtime and the expense of repairs while maximizing response time.

- **“Water destroys our gear.”** Like dust, water gets into electronic devices and can cause failure. In facilities management and security operations, it's impossible to avoid water in some form; the best that can be done is to make sure it doesn't disrupt communications. Weather, floods, and burst pipes are realities.

- **Water submersible** devices can be dropped in fresh and salt water to a depth of 1 to 2 meters for 30 minutes. Usually, when a worker drops a wireless device, even into a very deep puddle, it will be pulled out relatively quickly; devices certified as water submersible provide an added margin of safety and up to 3 years of extreme reliability with daily hard use.

- **“Our equipment has to keep working even after it hits the ground hard.”** Wherever work is done, there's the possibility that the mobile device will be dropped, damaging it and interrupting communications vital to an efficient and secure facility.

- **Drop/impact protection** is critical. It's not enough to simply resist damage from being dropped to a hard surface. A mobile device must be able to withstand being slammed against concrete or dropped more than 2 meters onto concrete from any angle. When communications are vital, there is no such thing as too rugged.

- **“The communications equipment we use has to take some shocks and vibrations.”** In rough environments, devices have to be able to hold up to sudden and sometimes violent shocks and vibrations that result from riding in vehicles or working in busy industrial environments.

- **Shock/vibration resistance** is achieved when internal components are designed to withstand up to 4G forces. Even if the casing provides drop/impact protection, that means little if the internal components are shaken loose or damaged.

- **“We work in extremes: really hot and really cold.”** Wireless devices must be able to perform in extreme environments, and accommodate thermal shock – caused by continually going indoors and out.

- **Temperature resistance** requires that devices be built and tested in the most extreme climates across the globe, from minus 20°C to 55+°C.

- **“Our radios get run over all the time. They have to survive major abuse.”** Devices in a work environment will be subject to pressures of all sorts, including being smashed or crushed.
- **Pressure resistance** ensures that devices can withstand being stepped on or run over by a truck.
- **“We don’t expect our communications equipment to stop a bullet, but it has to survive punctures.”** When devices are punctured, they stop operating and communications grind to a halt.
- **Puncture resistance** means you don’t have to worry if the exterior case becomes compromised; it will keep working even when punctured.
- **“Oils and harsh chemicals can destroy equipment.”** Corrosive substances can eat through the casing of a device and destroy it. Solvents can penetrate the seals. Rubber seals get compromised and water penetrates the device
- **Oil and chemical resistance** ensures the device will withstand exposure to hundreds of different chemicals, will not corrode, and can be easily cleaned with the right solvents. Seals stay intact.
- **“Usability for mission critical functions.”** The ability to bring mission critical connections to hosted services.
- **Mission critical usability** means function keys can be used with gloves, devices are designed for use with one hand, critical emergency functions have dedicated keys and NFC tags can be scanned without accessing the menu.

Intelligent Features Defined

1. Lone Worker

Lone worker functionality may include a dedicated panic button that when activated, triggers an immediate speakerphone call to an emergency response centre with GPS information provided. It also will feature a man-down sensor that automatically signals an alarm if security or facilities personnel fall down. This sensitivity can be achieved by a 3-axis accelerometer with g-force and duration thresholds that indicate the precise kind and severity of fall a worker may have experienced.

The precision of this technology helps avoid false alarms, which have a direct impact on operations center responsiveness, resource costs and efficiencies.

Why Connected Team Intelligence Matters

The ruggedness of a device is important in both the facilities management and security space. But without connected team intelligence, even the most rugged and durable communications gear is of limited value. The applications and features a rugged device supports defines its intelligence – and provides the primary differentiators between available solutions.

Key intelligence features to look for when evaluating potential solutions include those specifically designed to meet the needs of lone workers, as well as NFC, Push-to-Talk (PTT) interoperability, Mobile Resource Management (MRM) and Group Over-the-air Phonebook Management, to name a few. Before investing in any solution, it's important to identify both the near-term and long-term needs of your organisation. Based on your specific requirements, not all these features may be weighted equally, but should certainly be considered.

In conjunction with a GPS device, Lone Worker functionality tracks the movements of personnel working alone anywhere within a defined geographic or campus area. Battery life is critical to effective GPS tracking and should be evaluated closely when comparing solutions.

2. NFC Proof of Attendance

NFC is a system for two-way wireless connectivity that uses a very short-range radio frequency to enable a wireless mobile device to read small amounts of data from other devices or tags in the immediate area. NFC technology is based on Radio Frequency Identification, a contactless identification technology that makes it possible for wireless devices like mobile phones to collect and share information.

NFC functionality enables service quality assurance for security and facilities management organisations like cleaning, maintenance and for access control systems.

Consider the impact of enabling access to an area via NFC door locks for a specific time period without

having to go to a central location to source keys and then return to that area once a task is complete. By provisioning the mobile device using NFC, managers can greatly improve quality control and lone workers can ask and be granted access to areas they need to service or investigate during their normal rounds, greatly improving efficiencies and productivity levels. This capability also allows workers to take pictures to capture and report back instantly regarding an incident scene, damaged equipment or simply to prove they were in the area at a specific point in time.

3. Push-to-Talk Communication

PTT technology enables users to connect with another person or a group of people almost instantly. There are no numbers to dial; just one button to push to communicate. However, interference can often be an issue with PTT use inside buildings, often requiring the use of another device for back-up communications. Additionally, the use of PTT devices requires significant ongoing investments in network infrastructure to overcome coverage challenges. GSM devices that offer PTT functionality provide a cost-effective way to provide reliable primary and secondary voice communications in an integrated form factor.

4. Mobile Resource Management

Tracking resources is a basic function of MRM, which can help organisations monitor the movements of vehicles, assets or individuals. This is a critical function for IT managers who need to monitor, track and maintain large fleets of devices in the field.

In both the security and facilities management arena, high turnover rates and large numbers of temporary workers are common. As a result, managing communications devices and assigned talk groups can prove quite challenging. However, dynamic

Group OTA Phonebook capabilities allow administrators to manage these workers effectively, instantly updating workgroups, project assignments and critical phone contact numbers and data necessary for them to immediately be connected and productive.

A Look at Alternative Devices: Rugged and Intelligent Enough?

With the explosive growth of Smart phones in the enterprise arena, IT and Operations managers have a variety of options to meet the needs of its mobile or lone workers. Here's a closer look at the pros and cons of private mobile radios, Smart phones and ultra rugged GSM devices for security and facilities management operations.

Features / Device Type	PMR	Smart Phone	Ultra Rugged GSM Phone
Rugged Exterior	Yes	No	Yes
Reliable Network Coverage	Limited	Yes	Yes
GPS Battery Life	Limited	3-5 Hrs	up to 26 Hrs
Parts Availability	Limited	Limited	Yes
Support Services	Yes	Limited	Yes
NFC	No	Limited	Yes
Mobile Resource MGMT	Limited	Yes	Yes
Native Software	Limited	No	Yes
PTT	Yes	Limited	Yes*
Workgroup Collaboration	Yes	Limited	Yes

*With third-party solution

Meeting a Tougher Standard

The Sonim XP3 Sentinel complies with British Standard (BS) 8484 Code of Practice, which was developed in response to government and industry demands that best practices be established for the health and safety for lone workers.

Ultra Rugged, Safe and Intelligent: The Sonim Solution

For the last five years, Sonim has designed and built radically reliable, ultra rugged phones for workers and enterprises in demanding mission critical industries. Shaped by insights from half a million workers in the toughest jobs on earth, Sonim offers a complete portfolio of ultra rugged, connected team intelligent devices with both passive and active embedded safety features that can perform a myriad of vital tasks to maximize enterprise efficiencies: from informing workers of schedules and tracking their locations, movements and hours to instantly and reliably connecting critical work groups and immediately notifying the proper personnel if an incident occurs.

Built from a ruggedized rubber and a revolutionary fiberglass and resin composite, every Sonim device is built to an exacting performance benchmark:

the Sonim Rugged Performance Standard. For more information about the specifics of this rigorous testing process, [click here](http://www.sonimtech.com/products/rps.php)

Sonim stands behind its products with a comprehensive three-year warranty. With reliable software and multiple layers of safety features for lone worker protection built in, Sonim devices provide a cost-effective, advanced communications solution for those who choose to work in the most demanding jobs in the world.

For more information on solutions designed specifically to meet the needs of lone workers, visit www.sonimloneworker.com.

Rugged Intelligence Required: Ensuring the Safety of Your Workers and Enterprise

The safety of your workers and enterprise operations is paramount. The implications and costs associated with cutting corners could threaten not only your competitive strength, but criminal liability and ultimately, your bottom line.

Investing in reliable, rugged and connected team intelligent communications solutions is not only the right thing to do; it may be the only responsible approach to how you run your business.

And with compliance standards only getting tougher, putting the right solution in place the first time simply makes good financial sense.

Communications solutions are not created equal. Lone workers in security or facilities management roles have very specific requirements. Coverage and extreme reliability cannot be compromised.

Ultra rugged, connected team intelligence is the only safe, responsible option. Let us show you what real communications ROI can look like.

Find out more at www.sonimtech.com.