



● ● Guaymas Port Mexico. Photo courtesy of InfiNet Wireless

Eliminating the danger spot: The special needs of seaports ● ●

When we think of homeland security, we often focus on the land aspects, and completely overlook the maritime concerns. However, with any countries around the world boasting purely sea borders, it's vital that security be effective and far-reaching. Here, Kamal Mokrani, Global VP at InfiNet Wireless, discusses the special needs of seaports security in securing the homeland.

As a major entry point into countries across the world, seaports are one of the most preferred methods for transporting goods and cargo for international trade. Clothes, technology, cars and food are often brought in by the thousands through these access points, with the UK's major ports alone handling 115.9 million tonnes of freight in the first quarter of 2017 alone, as reported by the Department of Transport. As the main transport method for international trade, ports are a key component for a healthy economy and a critical contributor to the wellbeing of a nation.

That said, seaport security has become an extensive talking point since any attack or breach could potentially have a direct impact on a nation's entire economy and welfare. With stowaways and looting situations commonly reported in these facilities – and just like airlines and airports are under increased pressure to boost security on a daily basis – seaports have become an incredibly tempting entry point for fugitives to make their way in or out of the country.

As well as the obvious security concerns such as cargo theft, attacks and stowaways, growing terrorism fears and high levels of piracy concerns have also made it vital for port operators across the globe to have a reliable and robust security system in place 24/7, monitoring the entirety of their ports and their immediate vicinities. Any lapses in their security could have a domino effect and if a single connection to a video camera cuts out, whether deployed in a Line-of-Sight (LOS) or, arguably more

crucial, a Non-Line-Of-Sight (NLOS) locations, the consequences could be dire.

The ability to identify issues and vulnerabilities before they actually turn into crises is imperative, and if a threat does indeed arise, security staff must rely heavily on the feeds from their remote sites to prevent or tackle any type of crime, as well as be able to respond and act whenever required in the shortest time possible. Robust CCTV, fence monitoring and motion detection systems should always be operational in a seaport facility in order for the management and authorities to dynamically learn when a problem has occurred or is about to. This real-time information enables them to quickly establish a fast and appropriate response to either prevent the disruption, or minimise the damage that has already been done.

Thriving by wireless

Some of the greatest communications challenges seaports face in their security platforms are linked with connecting their remote locations to the control rooms, as well as overcoming the obstructions along the way to provide real-time information. Major ports across the world vary in size and complexity, some of them spanning areas of thousands of acres, such as the Port of Rotterdam. Networks deployed in such seaports are often required to withstand harsh and demanding environments, as well as monitoring fixed assets and moving vehicles across the entire facility.

Many seaports across the world have installed cabled networks which have been in place for many years, having reached saturation or just in a tired state. Adding additional wired infrastructure can be not only costly and ineffective, but also very difficult to deploy especially in isolated and difficult to reach areas. Such cables are also vulnerable to damage by extreme weather conditions or rodent's activity. Although these existing networks have most probably provided good-enough connectivity in the past, operational requirements are always evolving, and seaports need flexibility just like in any other outdoor operation. While wired infrastructure cannot provide such flexibility, a wireless platform is ideal for improving

connectivity and delivering the quality service that is now so mission critical for the security of seaports and that of their workers.

Across all continents, wireless broadband networks are becoming a catalyst for generating and growing revenues, whilst at the same time enhancing security and providing high-speed transmission of data, voice and video feeds. Momentum is shifting to wireless for good reason, as triple-play services can be transferred from remote locations and devices in real-time to a central monitoring and control room, as well as to a fleet of first-responders out in the field.

Furthermore, wireless networks can be deployed very quickly, often in a matter of hours as opposed to weeks or months for wired networks, and they can deliver superior performance over long distances and in challenging environments, even in the frequent NLOS conditions we so often find in seaports, all whilst being cost effective and requiring very low maintenance after installation.

Moving targets

In order to ultimately improve seaport security around the world and deliver real-time data to seaports and vessels alike, organisations and executives are hard at work developing advanced wireless technologies that will improve the speed of data transfer while simultaneously ensuring its reliability in all operating conditions.

Moving vessels or vehicles that often change their direction of travel and speed need high-quality and always-on connectivity to meet their data, voice and video requirements. Thanks to such reliable wireless links, fast download and upload speeds can be guaranteed and can be delivered for everyone on the network, whether located in the seaport itself or in its immediate surrounding areas.

InfiNet Wireless, a global leader in fixed broadband wireless connectivity, successfully delivered fast and reliable broadband networks in various seaports across the world. In the South of France, for example, the company deployed an advanced access network to provide seamless connectivity to visiting boats and yachts with all the services they usually enjoy by on-shore customers, such as local TV channels, internet access and voice communication.

Similarly, in the Distrik Navigasi Kelasi I Port in Surabaya, Indonesia, known to be the second busiest shipping port and city in this country with probably the largest number of islands in the world, an InfiNet solution was deployed to ensure that the main commodities traded, such as tobacco, sugar and coffee, were all exported to parts of the world safely and on time.

Long-term benefit

From the largest ports in Singapore to small docks in Scandinavia, it is easy to misjudge how crucial communication networks are in these seaport areas. According to the Transported Asset Protection Association's (TAPA) Incident Information Service (IIS) database, there has been more than a 92 percent increase of recorded cargo crimes in the EMEA region alone year on year.

While a brand-new security system requires very careful planning, the required expenditure is a critical investment when assessing the ensuing savings that robust security provides. The cost to a seaport of losing critical cargo because of an insufficient security infrastructure cannot be underestimated and must always be taken into consideration. Seaport operators need to focus on the long-term benefits of their security system, which leads to an increase in cargo operations and ultimately to increased revenues for the seaport itself and wealth to the local economy.

GMC



● ● Indonesian shipping port. Photo courtesy of InfiNet Wireless