

# **Today's Wireless Technologies For Ports**

**Converging Technologies With Strategies**



## Table of Contents

1. Business Conditions And Market Forces.....	3
1.1. The Port As Part Of The Global Supply Chain.....	3
1.2. Value-added Services.....	3
1.3. The Vision For The Future .....	3
1.4. Core Requirements and Strategies for Competitive Operations .....	4
2. The Wireless Ecosystem.....	6
2.1. Wireless Technologies: The Basics .....	6
2.1.1. What Is RF? .....	6
2.1.2. Do You Need RF?.....	6
2.1.3. The Evolution Of RF Technology .....	7
2.1.4. Why Has LXE's 2.4 GHz Replaced 900 MHz And Narrow Band?.....	7
2.1.5. Key Reasons To Choose LXE's 2.4 GHz In Ports .....	9
2.1.6. What Characteristics Do You Need In Your RF Equipment? .....	9
2.1.7. Who Should You Buy From? .....	10
2.1.8. How Do You Implement An RF System? .....	10
2.1.9. How Do You Manage An RF Project? .....	11
2.2. The IEEE 802.11b and 802.11g Standards .....	12
2.2.1. Wireless Bridging .....	12
2.2.2. What About 5 GHz?.....	13
2.3. Different Wireless Options .....	13
3. Technologies For Real-Time Management Of Intermodal/Ports Operations.....	20
3.1. Mobile Computers .....	20
3.2. RFID .....	20
3.3. Global Positioning System.....	22
3.4. Voice Applications.....	23
3.4.1. Voice-Over-IP For Telephony Applications.....	23
3.4.2. Voice Recognition For Data Capture Applications .....	24
3.5. The Value Of Video.....	24
3.5.1. Video-Enabled Network Systems .....	25
3.5.2. The Need For Video Management.....	25
3.6. Applications Trends .....	26
3.6.1. Graphical Applications .....	26
3.6.2. Hosted Applications.....	26
3.6.3. Integration Into ERP .....	26
3.6.4. Other Applications .....	27
4. LXE's Value Proposition.....	28

# **1. Business Conditions And Market Forces**

## ***1.1. The Port As Part Of The Global Supply Chain***

Ports are no longer simple cross roads or drop points for goods; they are an integral part of complex, global supply chains. This is putting the intermodal industry under great pressure. New container terminals are opening to challenge established operations and improve logistics. Shipping companies are demanding that cargo is moved as quickly as possible to maximize their operational efficiency. At the same time, increasing security and tightening customs procedures mean that the speed with which cargo can be moved is inevitably compromised. In addition, port operators need to find ways to increase their revenues by offering additional, value-added services to their customers.

## ***1.2. Value-added Services***

Given these requirements, it is vital that the information flowing around a port, between a wide range of employees and clients, at dock side, in the head office and at sea, is in real time, and available over a flexible, adaptable and secure network. Networking technologies based on Internet Protocol (IP) allow convergence between all the functions of a port, such as:

- Crane scheduling systems and communication
- Ship-to-shore communication
- Container operations and management
- RoRo facilities
- Customs office
- Harbor Masters office
- Emergency services
- Wireless network
- IT infrastructure
- Security and access control
- Gate management
- Corporate, financial, human resources
- Services for tenants.

## ***1.3. The Vision For The Future***

The vision for the future is to create an efficient and integrated fixed and wireless communications system encompassing all these elements. The single system does not have to be created and implemented at once; a port can steadily integrate various elements piece by piece, or application by application. However, any port considering an investment into a new IT infrastructure should seriously consider how efficiently these

elements could be integrated together. In other words, a port should make the right investment that allows growth into an integrated system like this in the future, which clearly depends on a company's investment strategy and budget.

The platform for this vision is an intelligent information network, that incorporates data, video and voice, and which offers integration of the various functionalities:

- Fixed/wireless connectivity
- 3<sup>rd</sup> party connectivity
- Broadband WAN
- Enhanced telephony services
- Crane/cargo efficiency
- Digital video surveillance
- Video conferencing
- Interactive yard services
- Ship-to-shore communication
- Distributed applications

The benefits of the vision include:

- Improved productivity thanks to improved cargo flow. A ship waiting to be unloaded is a lost cost opportunity for the port
- Improved security and safety thanks to CCTV, access controls, emergency notification, biometrics.
- Increased revenue opportunities as the port can offer tenants enhanced services like IP telephony and information access
- Technology cost reductions due to the ability to leverage the existing network and a common investment for support and upgrades
- Reduced response time due to remote monitoring and control of critical equipment and systems on a 24-hour basis

#### ***1.4. Core Requirements and Strategies for Competitive Operations***

Both business and non-business drivers exist for technology investments in ports, to enable operations to be conducted competitively.

##### **Business Driven**

Ports around the world are in a fierce competitive battle to improve the quality of service while improving their bottom line. New ports are emerging to compete with the older, established ports, and can frequently offer yard optimization thanks to space to expand. Customers are demanding online container traceability. Furthermore, FOFO (Faster Operations – Faultless Operations) is fast becoming a core strategy.

An additional challenge for some port operators will be the job of handling the Ultra Large Container Ships (ULCS). This new class of container ship, scheduled for service by 2010, will increase shipload capacities from 5,000 TEU to over 8,000 TEU. The arrival of these large ships will further complicate and stress already busy port facilities.

### **Non-business Driven**

Security is a key issue as ports have a major role to play in national security. The introduction of the International Ship and Port Security code (ISPS) and Maritime Transportation Security Act (MTSA) in November 2002 meant that shipping companies were required to meet detailed security criteria on all vessels and facilities. The ISPS Code requires that a port provides efficient planning and management of the security of all vessels. Security assessments, security plans, training, exercises, and the documentation of a port's security regime all require careful consideration.

Data management in ports is becoming increasingly important, with port and harbor Electronic Data Interchange (EDI) procedures being involved in harbor entry and departure. This entails simplifying application items and standardizing the forms required for the authorized use of berthing facilities. EDI also encourages port management bodies and port masters to exchange data related to applications, reports and other administrative procedures electronically, and allows port and harbor employees to submit applications and reports online.

## 2. The Wireless Ecosystem

### 2.1. *Wireless Technologies: The Basics*

#### 2.1.1. What Is RF?

RF is the abbreviation for Radio Frequency Data Communications. This refers to the wireless transmission of data by means of digital radio signals at a particular frequency. RF maintains a bilateral, on-line radio connection between a mobile terminal at the workstation and the host computer. Use is made of particular frequency band, which, depending on the frequency, can be freely chosen if a license has been granted.

The mobile computer is used for collecting and displaying the data. Such a mobile computer can either be portable (i.e. handheld) or be mounted on a gantry crane, straddle carrier or RTG. The host computer can either be located on the facility or at a remote location, like a central data centre, and be connected over the Internet.

#### 2.1.2. Do You Need RF?

A more pertinent question is “Can you do without RF?” because RF offers considerable advantages to port operators. The most important advantage of RF is that the transmission of data is not tied to a specific location. RF allows for direct transmission of data from the point of collection to the host computer and vice versa. Data is processed in a 100th of a second and files updated.

The use of bilateral communication means that mobile users (e.g. cranes, RTGs, straddle carriers) do not have to cover large distances to collect instructions or to report. They can thus do their work much more efficiently, without wasting time. In other words, more work can be carried out with the same quantity of people and less material.

The results of the advantages of RF communication can be summarized as follows:

- Availability of up-to-date information
- Faster vessel turn-around times
- Prompt response times
- Improved use of people and material resources
- Higher productivity
- Increased accuracy and service levels
- Replacement of time-consuming batch processing by rapid real-time data processing
- Reduced paperwork
- Elimination of lost containers
- Faster and more efficient yard operations

- Faster and more efficient gate operations
- Flexibility to reschedule resources and tasks
- Mobile office for supervisors.

Given these advantages, it is clear that most ports – and most certainly container ports over 100,000 TEUs – need RF, to achieve their objectives in terms of quality of service, speed, competitiveness, productivity and utilization of resources.

### **2.1.3. The Evolution Of RF Technology**

To best understand the advances in Wireless Local Area Networks (WLANs), a short historical perspective is useful.

In the 1980s, the only solutions for wireless data networks were in the licensed narrow bands of 450-470 MHz. By definition, these bands have relatively little bandwidth and therefore support low data rates of about 4.8 or 9.6 kbps.

In the 1990s, 900 MHz Spread Spectrum radio technology became available, allowing greater throughput of up to 64 kbps. Government licensing was not necessary – a distinct advantage – although their use was limited to certain countries. The coverage distance or range of these Narrow Band and 900 MHz radios is very good. A typical 1-Watt 450 or 900 MHz transmitter has a clear line of sight range of well over 1000 meters and a high power transmitter of 5 Watts has a range of more than 3000 meters. The high signal strength and low data rate mean that the coverage inside a port area is quite good. A Narrow Band or 900 MHz system enables terminal emulation applications such as container tracking at quay cranes, truck lanes or even inside the reefer areas.

However, the data rate of these systems is so low that they do not support client/server systems. Furthermore, these products work only with character-based applications and not the graphics-based applications that are increasingly being demanded by customers used to the look and feel of Windows. Also, as the number of users grows with the software applications, the overall capacity of these systems quickly approaches maximum loading.

The next step was therefore the 2.4 GHz bandwidth. The minimum speed is 1 Mbps and the maximum is 54 Mbps; the power output varies between 35-100 mW depending on the manufacturer; and the range is 100-400 meters depending on the technology used. The range for point-to-point connections can go up to 5 km.

Since 1998 LXE has installed 2.4 GHz RF networks in over 100 ports around the world and has proved that this technology works in the real world.

### **2.1.4. Why Has 2.4 GHz Replaced 900 MHz And Narrow Band?**

(a) 2.4 GHz is open

2.4 GHz technology is based on open standards defined by international standards bodies. Narrow Band and 900 MHz technologies are by definition proprietary to one vendor. Using open system 2.4 GHz technology, you will be able to choose “best of breed” products from more than one vendor. With Narrow Band or 900 MHz, you can only buy products, good or bad, from one company. If that company goes out of business then your RF system could be unsupportable.

(b) 2.4 GHz provides unlimited functionality

The architecture of 2.4 GHz is that of a Local Area Network, just like the LAN that you use in your office. The terminals are “personal computers”. The only difference is that they are connected to the network by a radio rather than a wire. This architecture gives maximum flexibility for adding new functionality and products while minimizing support costs. In short, it is the proper technical foundation for the future. For instance, you could use the 2.4 GHz network to utilize “Voice-over-IP” for verbal communication with workers in the yard. Office PCs could be attached to the wireless network. For RORO operations deep inside ships, the wireless devices can connect information in a batch mode and perform file transfers to update the system. Narrow Band is only suited for dumb terminal emulation and can not perform these other functions.

(c) 2.4 GHz allows easier management and lower cost of ownership

A 2.4 GHz network is a wireless LAN that can be managed and supported like a wired LAN. Standards such as Simple Network Management Protocol (SNMP) are used. This means you can largely use the same tools to manage your wireless network that you use for your wired network. Your IT personnel can reuse their wired LAN management and support skills on the wireless LAN. Since Narrow Band and 900 MHz are proprietary they require specialized tools and training from the vendor – which all add to the lifetime cost of the system.

(d) 2.4 GHz will support future applications

Video-based imaging applications, such as the imaging of container numbers and the image processing of CCTV cameras, are becoming increasingly useful in intermodal environments. However, these applications, as well as voice-based applications, require considerable data throughput. Narrow Band systems simply cannot handle this data throughput, whereas 2.4 GHz can.

(e) 2.4 GHz supports Windows

Finally, an important consideration is the software platform for which the container management package is being developed. Narrow Band and 900 MHz do not support graphics-based operating systems such as Windows, whereas 2.4 GHz technology does.

In summary, 2.4 GHz offers a true wireless foundation for the future. If you are going to purchase a new RF system or upgrade your existing system you should select the system that will provide maximum benefit. 2.4 GHz provides the most flexibility, best performance and lowest long-term cost of operation.

### **2.1.5. Key Reasons To Choose 2.4 GHz In Ports**

The reasons given below are valid for a new implementation but should also be taken into account for existing Narrow Band or 900 MHz installations for which upgrading to an LXE 2.4 GHz solution could represent valid opportunities and economic benefits.

A 2.4 GHz wireless LAN offers:

- An architecture identical to wired LAN open architecture, that is based on international standards, and can be used worldwide
- High speed
- High bandwidth
- Improved coverage with LXE's 'port designed' SPIRE® Antenna solution
- Reduced specialized knowledge (compared to proprietary systems requiring specific competence and training)
- Reduced operating costs
- Investment protection
- A migration path to future technologies and applications.
- Enterprise class management and security
- Easy user training due the use of graphical applications (language independent!)

### **2.1.6. What Characteristics Do You Need In Your RF Equipment?**

Ports are among the harshest environments for RDC (Radio Data Computers) and wireless networking devices, due to the conditions caused by salt spray, rain, snow, ice, dust, and extremes of temperature and humidity, to say nothing of rough treatment by workers!

To function optimally under all these conditions, your RF equipment should be truly ruggedized and thus suitable for port applications. Key features of specific importance for port applications include:

- Large keys
- Backlit keyboard
- Backlit display

- Full range of accessories allowing for tailor made ergonomics
- Extended temperature range operation (-30oC to + 50oC)
- Strong power supply able to withstand voltage peaks and drops common in industrial vehicles
- Single board construction
- Highest IP ratings for mobile computers
- High resistance to shock, vibrations, humidity.

### **2.1.7. Who Should You Buy From?**

When selecting a vendor for your RF equipment, criteria that must be met include the following:

- Financial stability
- Sound current and future RF strategy (an RF system is installed for 5 to 10 years)
- RF is its core business
- Ports and intermodal applications are core sectors
- Experience in 2.4 GHz WLAN
- Integration capabilities of any WLAN system (e.g. Cisco, Vivato)
- Product development focused specifically on ports
- Good working relationships with major software vendors
- Global organization and best-in class service portfolio.
- No conflicting technologies offering (e.g. 2.4GHz + narrow band)

### **2.1.8. How Do You Implement An RF System?**

There is no single method to implement an RF system. Each application is different, because each port is different. For example, no two ports will ever provide the same interference patterns. Mounting locations will differ considerably. And every customer has unique objectives to be met from an RF system. That's why it is important to choose an RF vendor with experience, because the more projects a vendor has successfully implemented, the more chance that vendor has of dealing with new problems that are thrown up by a new installation.

However, there are certain steps that are common to each application. Below is a checklist of technical points that LXE works through to design an initial RF installation:

- Analysis of existing situation
- Description of desired situation
- On-the-spot investigation of the radio-technical situation (facility analysis): Are there sources of disruption? If so, which ones? How large should the transmission coverage area be when the container yard is full and empty?
- Connection possibilities of the system to the host (host-connectivity)
- Calculation of expected response times

- Map with locations of Access Points, antennas and connection cables
- Analysis of the hardware and communication infrastructure required (number of base stations, mobile terminals, antennas, cables, availability of power, etc.).

### **2.1.9. How Do You Manage An RF Project?**

Project management is a key element of the successful implementation of an RF system in a port or container terminal. It requires precise planning, co-ordination and management of every aspect of a project from concept to production. At every level of your RF project, LXE can perform the following tasks for you:

#### (a) Design

- Analyze your specific requirements
- Understand your procedures and objectives
- Provide you with the appropriate system
- Evaluate your integration requirements (host, network, voice, video, peripherals and software)

#### (b) Planning

- Set up a project team between LXE and the customer
- Define tasks and activities
- Publish calendar with detailed milestones
- Decide on geographic extent of work

#### (c) Implementation

- On-site testing
- Installation and integration of software and hardware
- Global roll-out after acceptance of pilot site (for multi-site and/or international projects)

#### (d) System acceptance and operation

- System acceptance following pre-defined checklist
- Training of users and system administrators
- Full operation

#### (e) Reporting

- Set up meetings to closely follow the evolution of the project
- Publish reports to track progress and check accordance with time scales and plans

- Address issues arising after the project is fully operational regarding changing business/operations requirements

## **2.2. The IEEE 802.11b and 802.11g Standards**

2.4 GHz wireless LANs being installed today are, in most cases, fully integrated with their wired Ethernet counterparts. Wireless LANs conforming to the Institute of Electrical and Electronics Engineers (IEEE) 802.11 specification connect to an Ethernet TCP/IP (Transmission Control Protocol/Internet Protocol) backbone with a simple bridge called an access point, making the wireless network appear as just another network segment.

Mobile devices associated with an IEEE 802.11 access point can communicate with nodes on the wired network just like any stationary workstation. This lets manufacturers and systems integrators bring to their wireless customers the benefits of technology bought and paid for by the much larger wired network market.

The IEEE 802.11b and 802.11g standards provide an over-the-air interface between a wireless client and a base station (also called an access point) as well as between wireless clients. The older 802.11b standard supports an 11 Mbps data rate while the new 802.11g standard boosts that to 54 Mbps.

### **2.2.1. Wireless Bridging**

Wireless bridging allows container ports and bulk cargo ports to wirelessly connect networks in various buildings/light poles or to provide online connection to vehicles on a container yard.

The main driving forces behind such a solution are:

- The difficulty of installing wired cable in some locations (light poles)
- The high running costs for leased lines
- The long waiting time for obtaining a leased line connection from a local operator
- The cost and time involved when temporary networks have to be installed and then removed.

The Wireless Bridging Solution operates at 11 - 54 Mbps and provides a wireless connection range of up to 6.4 km depending on local government regulations as well as configuration. The solution encompasses both point-to-point and point-to-multipoint configurations.

This solution provides many advantages:

- It is much quicker, easier and less expensive to set up than a cabled network
- Telephone poles are not necessary
- Digging ditches for cables belongs to the past

- Greater flexibility when adding or changing a network as it only require antennas to be added or moved

### 2.2.2. What About 5 GHz?

The 802.11 standard also has applications in the 5 GHz band. 5 GHz products are capturing some market share in office and home applications, but are not as well suited to the port environment as 2.4 GHz products. Because of the physics of radio propagation, 5 GHz covers only about half the area that a comparable 2.4 GHz signal will cover. In addition, 5 GHz client radios consume more power than their 2.4 GHz counterparts, which would cause a substantial reduction in battery life in handheld devices.

Nevertheless, 5 GHz might become useful for ports in the future. We can expect dual radio access points where the 2.4 GHz radio will be used to provide client access, and the 5 GHz radio will be used for wireless backhaul. In the port, these units would mount on light poles and “shine down” a 2.4 GHz signal to provide client access on the ground using LXE SPIRE® antennas, and at the same time use high gain omni or directional antennas to provide an “umbrella” of 5 GHz backhaul. These may even be mesh networking nodes.

### 2.3. Different Wireless Options

(a) In a wireless controller based system, all wireless traffic is routed to a central controller unit before being forwarded to its destination address. In the central office, one controller is connected to the network. In the container yard, radios – attached to light poles – communicate with the controller.

(b) In a distributed wireless system (e.g. Cisco's solution), the access points attached to the light poles are each individually connected to the wireless network. Each access point incorporates an antenna and controller, so are independent, intelligent devices. Wireless traffic is routed directly to its destination address, without the need to pass through an intervening controller.

(c) At the heart of a Vivato system is a single powerful base station with a phased array antenna that can provide wireless connectivity over a vast area, complemented by Bridge/Routers for hard to reach or adjacent areas. In the base station, a powerful phased-array radio antenna creates narrow beams of transmissions that are directed to clients on a packet-by-packet basis.

The first two technologies are available worldwide. To implement Vivato technology, the local authority needs to give approval as the high transmission power can affect neighboring RF devices. It is approved in US, Canada, Japan, China and Malaysia, but not as yet in any other country.

(d) GPRS/CDMA. Some smaller ports do not want to make the necessary investments in the three technologies described above as they have limited data exchange requirements. In such applications, an alternative is GPRS, which uses the public telephone network. The disadvantage is that data costs are high, so is only cost-effective if a facility has fewer than 15 mobiles users.

### *The Right Technology for The Right Application*

It is clearly important to choose the right technology for your specific application, as indicated by the technologies comparison below:

#### (a) Network security

**Narrow Band:** Reasonable security. Narrow band solutions rely on 'security by obscurity'. There are no explicit security mechanisms in these systems, but the proprietary nature of the protocols and their limited adoption reduce their vulnerability to wireless attacks.

These products are all proprietary. The protocols are all trade secrets of their respective vendors. This creates a weak security mechanism, since an attacker has to discover the protocol itself. However, no specific security features are typically built into the protocols. These systems have never undergone an extensive security review. On the positive side, the protocols are not widely deployed. This decreases the incentive to hack them. The bottom line is that it is not likely a narrowband system would withstand a determined attack, but they are quite secure from casual intrusion or unsophisticated attackers who rely on readily available hacking tools.

**802.11 Controller Based Systems:** Good security. These systems can be very secure if they implement WPA or 802.11i protocols. Many controller based systems include rogue access point detection, intrusion detection and prevention, and other advanced security features.

Systems that implement WPA or 802.11i provide a high level of security. These systems are not vulnerable to any of the attacks that have been demonstrated against static WEP. In addition to stronger encryption requirements, WPA and 802.11i systems provide for mutual authentication of both the network and the client device or user. Controller based systems from all major vendors support WPA; many support 802.11i. Controller based systems from Cisco support both WPA and 802.11i. They also include rogue access point detection and suppression, intrusion detection and intrusion prevention, and attack signature files that can be updated.

**802.11 Distributed Systems:** Good security. These systems can be very secure if they implement WPA or 802.11i protocols. Solutions are available for rogue access point detection, intrusion detection and prevention, and other advanced security features.

Systems that implement WPA or 802.11i provide a high level of security. These systems are not vulnerable to any of the attacks that have been demonstrated against static WEP. In addition to stronger encryption requirements, WPA and 802.11i systems provide for mutual authentication of both the network and the client device or user. All enterprise quality distributed wireless networks support WPA, and many support 802.11i. Distributed systems from Cisco support both WPA and 802.11i.

Rogue access point detection and IDS/IPS solutions are available from third party vendors. In some cases, such as with the Cisco 1200 series access points, these solutions are available as vendor-branded solutions.

**Vivato:** Reasonable security. Vivato products generally support WPA. Vivato currently has not implemented 802.11i. Rogue access point detection and intrusion detection and prevention solutions are available from third party providers. In most cases, third party IDS products will require a 'sensor access point' overlay to the Vivato network.

**GPRS:** Reasonable security. GPRS provides good security for the RF connection, with both data stream encryption and mutual authentication. There are several potential points of attack within the service provider's network. Network providers generally do a good job of securing their networks, but GPRS does force the enterprise to rely on the security of the network provider.

GPRS provides both user authentication and data encryption. Note that user authentication credentials are contained on the SIM chip. There is no interaction from the user required to become authenticated, so this is really device authentication. It is important to protect the devices and SIM chips to maintain the integrity of the security.

The biggest vulnerability in a GPRS network is in the service provider's network. A GPRS packet travels through several network nodes between the handset and the enterprise firewall. At each of these nodes, security is outside the control of the enterprise IT management. Special attention must be given to security in service agreements with the network providers.

#### (b) Network Management

**Narrow Band:** Reasonable network management. Narrowband networks use a centralized controller based architecture which provides a single management point for the wireless network. However, management of narrowband networks is limited to system configuration.

Controller based architectures provide a convenient platform for implementing centralized management. There is a single location or console that provides for management of all the RF devices. In narrowband networks, management systems are not

very sophisticated. They provide only configuration capabilities, and even this is a manual process. They do not enforce configuration policies, detect RF interference or provide any alarms. They do not detect or compensate for RF failures.

**802.11 Controller Based Systems:** Excellent network management. The controller provides a convenient point to implement centralized network management. Since it is a non-optional network component, all controller based systems include centralized management. Enterprise quality controller based systems provide a wide range of management capabilities, far beyond simple configuration, and their sophistication is continually evolving.

Controller based architectures provide a convenient platform for implementing centralized management. There is a single location or console that provides for management of all the RF devices. Enterprise class 802.11 controller based products all provide network management, policy enforcement, interference reporting and standards-based alarms for a variety of conditions. They also provide intrusion detection and prevention, rogue access point detection and rogue access point suppression functions. They provide RF maps that can aid in site surveys, and they can adjust RF power levels to compensate for failed access points.

**802.11 Distributed Systems:** Excellent network management. All of the management capabilities available to a controller based system are also available to a distributed wireless network. In a distributed network, the centralized management components are optional items.

A distributed access point architecture requires one or more add-on tools to provide centralized management. More sophisticated intrusion detection and prevention capabilities are available as third party add-ons.

**Vivato:** Reasonable network management. Vivato products are essentially a distributed access point solution. The management capabilities are less sophisticated than those provided for more mature product lines. Third party support for Vivato is limited, and centralized management solutions provide only very basic management capabilities.

Vivato does not provide a centralized product for managing multiple access points or base stations. Vivato provides an embedded configuration tool included with each device, but this tool is limited to configuration functions only, and only on the one specific device.

**GPRS:** Poor network management or good network management, depending on the enterprise's point of view. The GPRS network is largely out of the control of the enterprise. The enterprise must rely on service contracts with the network provider. Some enterprises may find this an advantage, as it relieves them of the network management responsibility. Other enterprises may find the lack of control to be a disadvantage.

---

(c) Interoperability/Standard/Enterprise system integration

**Narrow Band:** Poor interoperability, good integration. Narrowband systems are proprietary to each vendor. Products from one vendor do not interoperate with products from a different vendor. However, the function of the network controller is to bridge the proprietary wireless protocols to standard Ethernet protocols, making integration with the wired enterprise network easy.

**802.11 Controller Based Systems:** Reasonable interoperability, excellent integration. 802.11 controller based systems interoperate with all standard 802.11 client products. However, access points from one vendor will not interoperate with another vendor's infrastructure. Controller based systems provide standard Ethernet interfaces to the enterprise network. Better products in this category provide a variety of physical interface options, from 10 Mbps Category 5 cabling to multiple Gigabit interfaces.

**802.11 Distributed Systems:** Good interoperability, excellent integration. Distributed access point systems interoperate with all standard 802.11 client products. Access points provide standard Ethernet interfaces to the enterprise network. Enterprise access points provide advanced features such as VLAN trunking and protocol filtering.

With distributed systems, mixed vendor installations must still be approached with care. There is no standard inter-access point protocol, so AP to AP roaming must be thoroughly tested. Also, access points from different vendors typically use different management tools. Third party tools such as Wavelink's Mobile Manager can alleviate this issue somewhat. Mixed vendor environments are typically not recommended.

**Vivato:** Good interoperability, excellent integration. Vivato systems interoperate with all standard 802.11 client products. Access points provide standard Ethernet interfaces to the enterprise network. Enterprise access points provide advanced features such as VLAN trunking and protocol filtering.

With Vivato, mixed vendor installations must still be approached with care. There is no standard inter-access point protocol, so AP to AP roaming must be thoroughly tested. Also, access points from different vendors typically use different management tools. Third party tools such as Wavelink's Mobile Manager can alleviate this issue somewhat. Mixed vendor environments are typically not recommended.

**GPRS:** Good interoperability, reasonable integration. Thanks to inter-carrier roaming agreements, GPRS clients have nearly ubiquitous connectivity. Integration with the enterprise network is reasonable. Due to the limited bandwidth of GPRS, special accommodations must often be made for mobile applications. Since the GPRS network is operated by a third party, a firewall must be maintained at the interface between the enterprise network and the GPRS network.

GPRS coverage is nearly ubiquitous in Europe. In other parts of the world, GPRS coverage may be sparse or non-existent, although GPRS provides the best coverage pattern of any of the terrestrial wireless networks. However, GPRS bandwidth is limited. GPRS can support data collection activities, but is generally not capable of supporting advanced applications such as video monitoring or conferencing. Browser based and other applications may require an application gateway to limit bandwidth to the client device.

#### (d) Performance/speed/throughput

**Narrow Band:** Poor performance. Narrowband networks deliver only about 9600 bps connection speeds. This is adequate for traditional data collection applications, but will not support any audio or video applications. Even small file transfers are slow using a narrowband system.

**802.11 Controller Based Systems:** Excellent performance. 802.11 systems support signaling rates up to 54 Mbps. This is adequate to support any of the applications envisioned today or for the near future. Adding access points to a coverage area can increase throughput.

**802.11 Distributed Systems:** Excellent performance. 802.11 systems support signaling rates up to 54 Mbps. This is adequate to support any of the applications envisioned today or for the near future. Adding access points to a coverage area can increase throughput.

**Vivato:** Excellent performance. Vivato systems support signaling rates up to 54 Mbps. This is adequate to support any of the applications envisioned today or for the near future.

**GPRS:** Poor performance. The maximum data rate for GPRS is about 50 kbps. This is more than adequate for data collection, but is not practical for video or other advanced applications.

#### (e) Integration of new technologies (RFID, voice recognition, VoIP)

**Narrow Band:** Very poor technology integration. No new technology or integration developments are taking place for narrowband systems.

**802.11 Controller Based Systems:** Excellent technology integration. There is a rapid rate of new technology innovation taking place for controller based systems. Examples of new technologies now entering the market, or coming soon, are mesh networking, location tracking, intrusion detection and prevention, and RF performance maps. The new technology is either integrated into the controller functions, or provided by add-on appliances or applications.

**802.11 Distributed Systems:** Excellent technology integration. There is a rapid rate of new technology innovation taking place for distributed access point systems. Examples of

new technologies now entering the market, or coming soon, are mesh networking, location tracking, intrusion detection and prevention, and RF performance maps. Most of the new technology is provided by add-on appliances or applications.

**Vivato:** Good technology integration. New technologies are available through integration into the Vivato base stations, or by add-on appliances or applications from third parties. Vivato lags somewhat in new technology integration. Most third party products that rely on standard 802.11 functionality are compatible with the Vivato system.

**GPRS:** Reasonable technology integration. Technology integration is somewhat limited by the abilities of the network providers. GPRS networks are very large and very expensive. Integrating new technologies into the GPRS network is expensive and time consuming. Clients in the form of handsets have limited computing resources, making new application development difficult.

(f) ROI/TCO/investment protection

**Narrow Band:** Reasonable ROI. Generally, narrowband products are no longer offered for sale. Where they are available, they are relatively expensive. The ROI of narrowband is therefore limited.

**802.11 Controller Based Systems:** Excellent ROI. Customers should typically look for payback in one year to 18 months for new wireless systems (replacing paper based data collection). Price competition among standards based systems is still driving product prices down, and innovations in management are reducing TCO of these systems.

**802.11 Distributed Systems:** Excellent ROI. Customers should typically look for payback in one year to 18 months for new wireless systems (replacing paper based data collection). Price competition among standards based systems is still driving product prices down, and innovations in management are reducing TCO of these systems.

**Vivato:** Excellent ROI. Customers should typically look for payback in one year to 18 months for new wireless systems (replacing paper based data collection). Price competition among standards based systems is still driving product prices down, and innovations in management are reducing TCO of these systems.

**GPRS:** Good ROI. GPRS systems tend to be more expensive than 802.11 systems since they are owned and managed by a third party. GPRS requires less initial capital expense since the network infrastructure is not being purchased. However, this is offset by the recurring subscription costs. Still, ROI can be very good, and for certain applications, 802.11 is not an option due to the small size of the area that needs wireless coverage.

## **3. Technologies For Real-Time Management Of Intermodal/Ports Operations**

### **3.1. Mobile Computers**

Vehicle-mount computers are now available with full-screens and Pentium processors, allowing you to make the most of Windows technologies. Models are available to fit various applications and environments. They can be used in the straddle carrier, RTG, gantry crane and forklift truck, whereas handheld computers are most likely used at the security gate or by personnel in the field.

Vehicle-mount computers can be used in two ways. First you put the screen in a crane where it provides remote access to your office environment through two-way messaging. Second, you integrate the vehicle-mount computers in the environment using local processing capacity, to provide and give much more information – which can be used for purposes such as remote monitoring. Whether you want a “dumb” display or more sophisticated capabilities depends on the needs of the customer.

Handheld computers are available with large displays and easy-to-use keys. Ruggedized handheld computers are essential to cope with the dust, temperature fluctuations, salt spray, rain and other adverse conditions commonly experienced in ports.

These days, mobile computers are specifically designed to meet specific requirements, such as low temperature operation, in freezers or cold countries, or in hazardous environments. Pen Tablets with Windows Operating Systems are useful for management tasks in the head office.

### **3.2. RFID**

RFID (Radio Frequency Identification) tags can contain unique information that identifies whatever they are attached to, and can share that information wirelessly with computer databases and networks so items can be tracked efficiently.

RFID is a means of identifying an object through a wireless radio link. The identification is accomplished by an interrogator, also called a “master”, and a tag, also called a transponder or “slave”, that has a unique identification code. Data is exchanged between tags and readers using radio waves between the tag and interrogator, and no direct line of sight is required for the transaction. The interrogator asks the tag for the code, or processes the signal being broadcast by the tag, decodes the transmission and transfers the data to a computer. The computer, in turn, may simply record the reading, or look up the tag ID in a database to direct further action, and may also direct the interrogator to write additional information to the tag.

The advantages of RFID are many:

- Greater control over inventory
- Increased security
- Greater visibility of your facility
- Better time management of mobile personnel and resources
- Reduction in time spent on maintenance and record-keeping
- Better organization of assets and resources
- Reduction in paperwork
- Delivers accurate and precise information.

Many RFID applications are converging around a single, robust, flexible and globally acceptable standard – the Electronic Product Code (EPC). In the past, there were many different standards and many of them were proprietary. Having that many standards meant that nothing was really 'standard'. Today there is convergence around EPC across many supply chains.

Developing a global RFID standard has posed more challenges than those faced by bar codes. Bar codes are read by light, and that's uniform around the world and is not highly regulated. Radio frequencies, however, are tightly regulated.

Despite this, global RFID regulations are beginning to fall into place within the 860-950 MHz band. Even with regional differences in frequencies between Asia-Pacific, the Americas and Europe, it is possible to produce RFID tags that work across the entire range of RF frequency allocations. These tags can be applied anywhere in the world and then be read by readers designed to comply with local frequency and power restrictions. The requirement for globally acceptable standards is critical in the light of the increasingly multi-national nature of business.

### **RFID For Security**

From the port and customs' perspectives, containers are inspected and bonded by the customs' agents in the port. When the container is sealed, an active RFID tag (or multiple tags) is placed on the container. Each RFID tag can be connected to "sensor" devices that monitor particular parameters – motion, air pressure, door movement etc.

If a sensor indicates a problem, the RFID tags emit an emergency signal to a fixed reader on the terminal which forwards the signal to a "command and control" center established to monitor security in the container yard. This software can be provided to the border agents, enabling each border point to track those vehicles destined for that crossing point.

At the border, if the vehicle has not gone "off course" or made unauthorized stops (as tracked by the software), and the RFID tag has not emitted an emergency signal, then the container and vehicle would be considered "secure" and allowed to cross the border without inspection. This clearly has the potential to save considerable time and removes the necessity to make multiple inspections of the same cargo at different points along its journey.

## **RFID For Location Application (RTLS)**

Trying to find the exact location of one of thousands of containers in a large area where all of the containers essentially look alike is a huge challenge. While traditional technologies can help record when a container was received and where it was delivered, the implementation of RFID in Real Time Locating Systems (RTLS) provides accurate real time location information to the managers of complex operations.

Real Time Locating Systems are fully automated systems that continually monitor the locations of assets and personnel. An RTLS solution typically utilizes battery-operated radio tags and a cellular locating system to detect the presence and location of the tags. The locating system is usually deployed as a matrix of locating devices that are installed at a spacing of anywhere from 50 to 1000 feet (16 to 330 meters). These locating devices determine the locations of the radio tags.

The systems continually update the database with current tag locations as frequently as every several seconds or as infrequently as every few hours for items that seldom move. The frequency of tag location updates may have implications for the number of tags that can be deployed and the battery life of the tag. In typical applications, systems can track thousands of tags simultaneously and the average tag battery life can be five or more years.

For this application, the main advantage of RFID over bar codes is that RFID does not rely on line-of-sight technology. A bar code has to "see" the bar code to read it, which means people usually have to orient the bar code towards a scanner for it to be read. RFID by contrast, doesn't require line-of-sight. RFID tags can be read as long as they are within range of a reader. Bar codes have other shortcomings as well. If a label is ripped, soiled or falls off, there is no way to scan the item. And standard bar codes identify only the manufacturer and product, not the unique item.

802.11 based active RFID tags are now emerging for location based applications. These systems take advantage of the existing 802.11 wireless network to determine the location of the tag. No overlay networks are required if 802.11 is used for data collection.

### **3.3. Global Positioning System**

The Global Positioning System (GPS) provides a 2-dimensional, 24-hour, all-weather location system that can be used for mapping and surveying. In ports, GPS is being increasingly used to position and track containers. For example, if you put a GPS on a crane or a straddle carrier, you can easily, accurately and automatically identify their position and consequently position and track containers.

Some container port operators have also been investigating using GPS for controlling Automated Guided Vehicles (AGVs). Whatever the application being considered, certain

technical issues are inhibiting the widespread use of GPS in ports; most noticeably satellite visibility and multipathing.

The GPS works on the triangulation principle. The satellite system is designed to provide good location when at least three satellites are in view. In general, high accuracy systems rely on at least six satellites in view and sometimes more. This is typically not a problem for finding operations that are in large open areas and which have a good view of the sky.

However, in the typical container port there can be significant ground level blockage produced by stacked containers, making satellite visibility less than optimal. As the number of satellites decreases, positioning errors increase. This problem can be solved for quay cranes and rubber tire gantry cranes by placing the GPS receive antenna high above the stacked containers. The receive antenna could then have a clear view of all satellites and would provide optimal performance. However, operations at ground level may have higher location errors because of reduced satellite visibility.

Multipathing can lead to accuracy problems for any GPS and can cause significant errors in location because of the increased time delay. This is the most significant problem for operations down on ground level because of the high level of reflections that can occur in a port.

Once the location of a crane or AGV is determined, the coordinate must be relayed back to the operations center. This would typically be done by using a wireless LAN. Until recently wireless LANs were also significantly affected by blockage and multipathing. However, significant technology improvements at 2.4 GHz have now made these systems possible. In other words, while the GPS has improved significantly over the last few years, the effects of multipathing in a port will prohibit millimeter location accuracy at ground level, although 2.4 GHz LANs can now provide excellent coverage and throughput in the entire port area.

### **3.4. Voice Applications**

#### **3.4.1. Voice-Over-IP For Telephony Applications**

New opportunities are presenting themselves at both extremes of wireless technology development, as increasing wireless bandwidth and tighter integration between wired and wireless LANs open up applications that would not work on less robust backbones.

Voice transmission is one such frontier, where great progress is being made both in traditional Voice-over-IP (Internet Protocol) "phone calls" carried over wireless backbones and in voice transmission to speech recognition servers. At the other end of the bandwidth spectrum, an exploding new technology is putting rudimentary, but reliable, web browsers into millions of cell phones and other hypermobile, low-power devices.

Voice-over-IP (VoIP) is one application receiving a lot of attention lately. The economics can be compelling. In many intermodal environments, data manipulation projects carry the burden of justifying wireless backbone installations. With the backbone in place (or merely cost-justified), it can be easy to justify the incremental cost of linking the network to a telephone system and purchasing handsets that operate over the IEEE 802.11 backbone.

Voice-over-IP is a technique for sending real-time voice over data networks including the Internet or an internal IP network. Normal data traffic is carried between PCs, servers, printers, and other networked devices through a company's TCP/IP network. Each device on the network has an IP address, which is attached to every packet for routing. Voice-over-IP packets are no different. To place a call from one device to another, users may enter the IP address of the called party using one of several voice conferencing software packages available today.

### **3.4.2. Voice Recognition For Data Capture Applications**

Voice controlled operation allows operatives to collect and transmit information without using their eyes or hands. They can fully concentrate on the physical execution of their tasks, while reducing the time of operation and limiting errors.

Industrial voice recognition devices must work in rugged, often noisy environments; they must be accurate to avoid early operator frustration; and they must be easy to use, since the voice operator is always busy doing something else, such as driving a forklift, or working a shipping/receiving line.

Portable voice recognition devices use two different approaches. In one design, the headset is connected via radio to a base station. The portable package can be light and small, but the radio transmissions are susceptible to noise and cross talk if multiple operators are involved. The second design approach puts the speech recognition engine inside the portable unit. These devices provide a more secure, higher reliability and higher recognition rate.

### **3.5. The Value Of Video**

Port and harbors occupy vast areas where cargo of considerable value is in transit and in which relatively few security operatives are in situ. Increasingly, these operatives are tasked with a number of different functions and so have a range of other tasks to perform. We are seeing and will continue to see manpower giving way to technology in large area and high value security applications. Closed-circuit TV video images have proven themselves to be invaluable in augmenting existing security provision at ports and harbors.

With the use of appropriate video/camera technology used over an IP network, intelligence can be added to systems such as infra-red night view images, heat sensing, facial recognition, vehicle recognition, movement and color change to name but a few.

Furthermore, the output of a CCTV can be sent directly to a Windows-based computer. This allows a security guard to walk around the site and see CCTV images, instead of having to return to his control room.

### **3.5.1. Video-Enabled Network Systems**

Many seaport operators use fixed analogue video systems with copper cables for transmission of images to a central monitoring point. Though they are of proven benefit in ensuring that more areas of the yard can be covered than with patrols or other means of surveillance, they remain limited in their use, as they operate along a fixed system. As more cameras are required to provide greater coverage, each one has to be installed to the present system, which is both expensive and ultimately limited by the capacity of the analogue system. Digital cameras attached to an IP network create an infinitely more flexible and scaleable surveillance solution. Both fixed and portable cameras can be added to an IP network with ease and with minimal additional cost.

### **3.5.2. The Need For Video Management**

With many images being viewed, stored and retrieved, the effectiveness and thus the value of a video system is directly related to its ease of operation. In the systems created by Cisco and Petards, command and control of the video systems are performed from a customized graphical user interface using icons and maps. This allows quick and efficient operation by operators who do not have to be familiar with electronic technology, and provides them with both manual and automatic responses to alarms and events.

Furthermore, the use of IP-networks to carry video means that information and images can be passed to operatives outside the confines of the port control room and even to external agencies such as the security and emergency services or customs.

Typically, video management systems will control all disparate elements of security electronics, access control, and perimeter and barrier alarms, including fire detection and plant management systems, thus adding the all important intelligence to a system.

The solutions provided include:

- Video command and control
- Monitoring and alarm management
- Simulation and training
- Disaster recovery
- Crisis management: prevention, preparation, response and recovery
- Threat analysis.

Many business benefits can be achieved thanks to increased security. Not only are customers assured that their cargo is more likely to arrive intact, but gains can be made in efficiency and administrative simplicity. Among the direct business benefits from investment in better security systems are:

- Increased operator and management efficiency
- Simplified methods of operation
- Corporate governance and accountability
- Risk avoidance
- Insurance cost reduction
- Lowering of operational and procurement costs
- Consistent structured response to incidents
- High level policing and control.

### **3.6. Applications Trends**

#### **3.6.1. Graphical Applications**

As applications move into more remote areas, flexibility and ease of use are key factors to maximize efficiency, so the focus is on graphical applications rather than character based applications. The benefits are numerous: operator training can be performed quicker and easier; the screens are clearer and easier to read and use; temporary workers can quickly become acquainted with them; the operator faces less distraction; and they are language independent.

#### **3.6.2. Hosted Applications**

With customers increasingly moving into inland container terminals and remote ports, they are looking at hosting applications on a central application and giving remote access to that location. This makes it easier for a company to deploy their systems remotely, and avoids having to set up a local IT infrastructure, as engineering and diagnostics can be performed from a remote IT center, maybe even on another continent.

#### **3.6.3. Integration Into ERP**

Ports and container terminals running an ERP system in their back office need their operations systems to interface into these applications. They therefore require that when the data is captured, it is not only used for operations, but also for statistics, financial management, accounting etc.

This ERP system must interface with all other systems in place (e.g. TOS) and must also be 'fed' with information, preferably in real-time, for maximum efficiency and rapid decision-making.

### **3.6.4. Other Applications**

- Crane diagnostics – using vehicle-mount computers to provide information that is useful for remote monitoring and preventive maintenance.
- In-lane checking – handheld terminals can be used to pre-check trucks that are in a queue to enter a facility. The operator types in the license plate and the information on that truck is immediately in the system.
- Integrated gate security – security cameras can register the license plate of incoming traffic.
- Biometrics – recognition of a person's eye imprint, fingerprint or face, to make gate security more watertight.

## **4. LXE's Value Proposition**

LXE has been a global player in this industry for over 30 years and its rugged mobile products are specifically designed to fit in the port environment – and offer a lower total cost of ownership too.

We offer comprehensive data collection equipment incorporating RF Identification (RFID), imaging and voice communications. Our standard solutions are all based on open systems, and are fully compliant with a customer's standard IT infrastructure and office networking systems.

LXE is a leader in global service, even in remote areas. We can also access these systems on a worldwide basis because they are IT based and are interconnected to each other. This opens up the possibility of performing remote diagnostics of any of the components in the wireless network from a central location without physically being on site.

### **Mobile Computers**

LXE is the market share leader in rugged wireless vehicle-mount computers and our handheld computers range offers an unmatched combination of ruggedness, ergonomics and processing power.

LXE mobile computers are built to withstand the toughest environments; are simple to operate (high visibility screens, ruggedized keyboards with large, backlit keys); and are supported by LXE's award-winning customer support team.

They are engineered for operations in the tough environments of ports and are designed with the port operator in mind. All are powerful enough to run today's and future applications.

### **Integration Of Secure Wireless Systems**

LXE provides a host of industry standard, secure RF networking products including access points from Cisco and Vivato, numerous RF antenna options including our patented SPIRE® Antenna, and additional network management software and hardware that simplifies network management, improves network security and system reliability, and increases the ROI of your data collection network.

On top of all this, LXE has specific experience in installing wireless components in port environments.

### **Optimization Of Secure Wireless Systems**

LXE's SPIRE® Antenna provides increased coverage and superior performance. Based on technology originally designed for space applications, this omni-directional antenna

increases coverage, performance, and reliability of 2.4 GHz wireless LANs. The patented design provides improved horizontal and vertical coverage patterns, resulting in a larger footprint, improved throughput, and superior performance in multipath environments.

It is also extremely cost-effective. SPIRE® installations require fewer access points. Fewer access points reduce power and data cabling requirements as well as maintenance and management resources. With coverage increases of 25-50%, compared to other omni antennas of similar gain, the SPIRE® Antenna makes 2.4 GHz technology a viable option for ports.

### **Lower TCO (Total Cost of Ownership)**

An LXE solution ensures a lower Total Cost of Ownership thanks to the ruggedness and durability of our equipment combined with the high level of enterprise integration capabilities of our standard-based and scalable systems.

Our innovative service package, ServicePASS, allow customers to integrate maintenance value into the purchasing price of an LXE solution also helping planning and controlling the Total Cost of Ownership.

### **Global Service**

LXE's RF experts are knowledgeable, skilled and trained to facilitate the definition, implementation and support of RF solutions that enable customers to attain, and even exceed, their Supply Chain objectives.

LXE's full range of turnkey services include radio integration, project and installation management, network design, technical support, and repair services. Its emphasis on industry standard solutions rather than proprietary solutions gives customers the opportunity to connect LXE's mobile computers to an existing wireless network infrastructure, which saves money and increases system flexibility.

Our experience in implementing systems in ports and intermodal operations is unmatched and truly global.

### **Partnership For Turnkey Solutions**

Working in conjunction with key software providers and material handling suppliers in the port industry, LXE provides turnkey solutions on a global scale for improved customer service as part of a port's information system.

Major software vendors around the world integrate LXE hardware. They would not do so unless they were 100 percent satisfied that LXE systems comply with industry standards.

## 5. Conclusion

The vision outlined in this white paper leads port operators in the direction of more collaborative working methods and systems. At the same time, it will help them achieve their business goals without adding to their operating costs that would erode their profitability. In other words, they will be able to do more with less.

This approach also addresses port operators' increasing concerns about security. It enables them to secure the physical environment in which cargo and people are handled, as well as ensuring that information and systems are equally secure against attacks and intruders.

Maximizing revenues of port operators can also be achieved. By using a secure and adaptable IP network, operators can allow third parties to have access to services and information.

This visionary solution for ports combines a secure, unified, open standards-based communications infrastructure with wired and wireless, end-to-end IP networking technologies that maximize flexibility and productivity. With an underlying infrastructure in place, core processes can be consolidated across port operations, whether on the dock or in the office. It also positions a port to capitalize on emerging security, operational, and cost-cutting opportunities.

In short, it enables operators to move more goods (TEUs) in less time with less manpower, yet with maximum accuracy and security, and with real time visibility from anywhere in the world.