

## PERIMETER PROTECTION

# Government Regulation Changes the Market

## Market Trends and New Technologies for Intrusion Detection

The following information has been taken from the newly released 2011 edition of "The Boundaries of Security", a guide to the intrusion detection industry. Published by Future Fibre Technologies, the report provides security consultants, managers and specialists with clear explanations and up-to-date general background on commonly available perimeter intrusion sensing technologies, as well as valuable research information and data on the global perimeter security market, and market drivers. In addition, it details the emerging intrusion detection technologies, market trends and developments in the intrusion detection industry. The "Boundaries of Security" is available free to qualified individuals from [www.fffsecurity.com](http://www.fffsecurity.com)

### A New Political Environment

Changing political environments and the nature of perceived security threats, new government legislation and rising costs of insurance are all playing a part in shaping the size and defining the segmentation within the perimeter intrusion detection market.

Global, social and political instability along with the ongoing threat of terrorism are increasing the need to both fund and enforce regulation and legislation regarding perimeter security at critical national infrastructure sites. Chemical, petrochemical and liquefied natural gas (LNG) facilities are now being identified as critical national infrastructure and subject to legislation and regulation in many countries and perimeter security is a key component of ensuring the security of these sites.

Critical National Infrastructure sites will also include nuclear power stations, water reservoirs, data centres, transportation hubs etc. An increase in organised protest movements (environmental, climate, economic and the like) is also heightening the need for advanced perimeter security at installations such as coal fired power stations, airports, military and nuclear facilities.

### Growth Predicted for the Market

All of these factors are leading to an increase in the size of the intrusion detection market. This increase is supported by recently released research from IMS Research, which reveals the world market for perimeter security sensors is

expected to grow at a steady rate until at least 2014 with a compound-average annual growth rate (CAGR) in the range of 6 %.

Fueled by this growth, the technology incorporated into global perimeter intrusion detection equipment continues to evolve and security professionals are faced with the ongoing challenge of keeping up with these latest developments. Historically, the most commonly used intrusion detection technologies include fence mounted sensors, buried sensors, open area sensors and video sensors. New systems use innovative, advanced equipment, and new technologies are being developed and introduced into the marketplace regularly. Some examples of these include Ground Based Radar, and the new generations of fibre optic sensors.

### New Technologies

Today, there is a diverse range of sensing technologies available for perimeter security, varying greatly in their effectiveness, affordability and accuracy. Each has unique capabilities and limitations and it's important for security professionals to understand the subtle differences so they can make informed choices about what system will best suit their individual requirements.

As has long been the case, techniques employed to control nuisance alarms are a major focus of the current crop of intrusion detection systems. In the past, this typically required reducing the sensitivity of the entire detection system during times of high environmental noise. For example, anemometers or wind speed measuring devices were used to 'automatically' increase the alarm threshold in times of high winds. Unfortunately, these measures also reduced the sensitivity of the systems to real intrusions.

Currently, advanced techniques such as artificial intelligence (AI), neural networks and

advanced multi-parameter signal processing, are being incorporated into intrusion detection systems to dramatically improve the recognition of real intrusion events against background activity.

Regardless of the intrusion detection system selected, the need for adequate warning and a response mechanism to an unwanted intrusion remains essential. The basic premise of effective perimeter security remains deterrence, detection, assessment and delaying of an intruder for a response to be initiated. Every perimeter security application is unique and dependent on variables such as the type of facility to be protected, operating environment, perimeter fence construction, intrusion and security history, and perception of threats.

### A Key Factor: The Environment

One often-overlooked aspect in the design of security systems is the environment. The unique environmental factors for a site that may need to be considered include climate (such as wind, rain, and salt air), animal activity, man-made environmental factors such as human activity patterns, electrical fields, radio or radar transmissions, and nearby vehicle, truck, rail or air movement. Failure to consider all these factors can result in excessive nuisance alarms.

If your installation is in a coastal or other corrosive environment, as many seaports, refineries

and airports are, then the type of perimeter intrusion sensor you select needs to take this into account. For example, copper sensors or communications cables will rot out quickly in salt air and so should be avoided, and any electronics or controllers installed in the field should be completely sealed to prevent corrosion and subsequent reliability issues. Anything metallic, such as camera housings, electronic enclosures and junction boxes, should be avoided altogether or be constructed of UV stabilised plastic or marine grade stainless steel instead.

The protection of these individual facilities needs to be tailored to suit the unique requirements of the site. Site layouts, sensitive areas, facility buildings, the surrounding environment, activity in and surrounding the site, local weather conditions and topography are all factors to be considered when planning a perimeter intrusion detection system. These influence the detection technologies selected and subsequent overall system performance. Often the final intrusion detection solution will consist of several different but complementary technologies to form 'layers of protection'.

What makes up these layers is going to be highly dependent on the customer expectation, the perceived threats and the potential intruders. Operators must adopt a holistic approach to site security, so that each of the elements of a layered security solution are complementary

and work together in unison to provide a strong security regime which protects against both known and perceived threats.

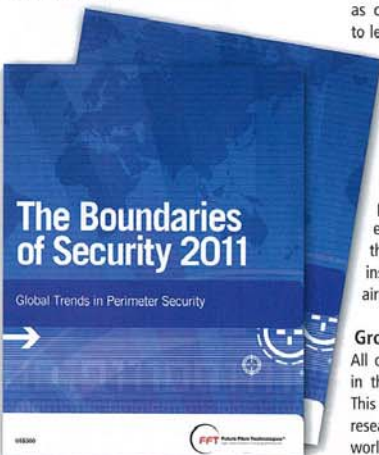
These layers may include a fence, a fence-mounted intruder detection system, some open area or volumetric sensors, some CCTVs, and of course, security staff and appropriate procedures or (Rapid Incident Management System or RIMS) to respond to a situation in a timely manner.

### No System Is Perfect but You Can Get Close to 100 %

Today, barrier, surveillance or alarm systems can never guarantee 100 % security. Outdoor perimeter intrusion detection systems are expected cope with animals, changing environmental conditions such as being coastal or subject to winds, or alongside a motorway or railway line, and often difficult weather conditions such as lightning, temperature extremes, snow and ice yet not generate any spurious or nuisance alarms. While no PIDS system is perfect, the newer generation systems and technologies are gradually getting closer.

### CONTACT

Richard Mayhew  
Future Fibre Technologies Limited,  
Chertsey, United Kingdom  
Tel.: +44 1932 895 317 · Fax: +44 1932 895 318  
[info@fffsecurity.com](http://info@fffsecurity.com) · [www.fffsecurity.com](http://www.fffsecurity.com)



# DIGITAL ABSOLUTE PLUS

## DIGITAL Dual TECHNOLOGY Barrier

range 200 mt.

**SICURIT** ALARMITALIA®  
outdoor protection  
our profession

**IMN200RS series**

State of the art combination of Microwave and IR technologies to assure maximum protection while drastically reducing false alarm rates due to uncontrollable agents.

- Detection Mode: MW + IR
- Range: 200 mt.
- Heights: 2.0 - 2.5 - 3.0 - 4.0 mt.
- Nr. of IR beams: from 2 to 8
- Nr. of microwaves: 1 / 2
- Alarm signal: Contact Relay and/or RS-485
- RS-485 output for remote programming and diagnostic

**SICURIT Headquarter**  
Via Gadames, 91 Milan - Italy  
T: +39.02.380.70.1  
F: +39.02.308.80.67  
I: [www.sicurit.com](http://www.sicurit.com)  
E: [export@sicurit.it](mailto:export@sicurit.it)

**intersec**  
trade fair and conference  
January 16 - 18, 2011  
Dubai, UAE

MADE IN ITALY