

Performance Characteristics of

Perimeter Security

A typical perimeter security solutions will consist of a number of layered elements. What makes up these layers is going to be highly dependent on the customer expectation, the perceived threats and the potential intruders. It is important that a holistic approach to site security is taken, so that 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 (Rapid Incident Management System or RIMS) to respond to a situation in a timely manner.

In order to provide an appropriate level of protection that meets customer expectations and budget, a clearly defined set of criteria for customer and system acceptance is required. Too many times 'scope creep' on a project or a misunderstanding

between the customer and installer of what is expected from the security solution occurs, for example, a chain-link fence and fence-mounted sensor around an electricity substation being expected to comply to prison test standards. It is always best to have these issues clarified and accepted by both parties up front, before any work commences.

Firstly, you need to have a physical barrier or a fence. Not only does the fence define the boundary of the property or site, it will also deter an

intruder (especially if it has razor or barbed wire on top). Importantly, it will also delay them as they attempt to climb over or cut through it. Selecting the appropriate fence is critical – you need to match the fence to the individual site needs as well as the perceived threat level. For low- to medium-risk sites, such as an airport perimeter, you may be looking at a chain-mesh or weldmesh style of fence; for higher security needs such as a prison or pharmaceutical factory, you may be looking at an anti-climb fence. There is no value in cutting costs by installing a chainlink fence in a high-security environment, and conversely, it is poor value to install an expensive anti-climb fence at a low-risk site. Any security system is only as strong as its weakest link and the type of fence should suit the site.

When evaluating any perimeter intrusion detection sensor, there are at least three key performance characteristics to be considered: the probability of detection (POD), the nuisance alarm rate (NAR), and vulnerability to defeat (i.e. typical measures used to defeat or bypass detection by the sensor).

In the ideal world, the perfect perimeter intrusion detection system (PIDS) would simultaneously exhibit a zero NAR and a 100% POD, and be undefeatable.

The probability of detection (POD) provides an indication of a systems ability to detect an intrusion within the protected area. The POD depends not on only the characteristics of the

particular sensor, but also the environment, the method of installation and adjustment, and the assumed behaviour of an intruder. Any POD figure quoted will be conditional and unique to a site, despite the claims made by some sensor manufacturers. For example, a sensor may have quite a high POD for a low-level threat such as a teenage vandal who has little knowledge of the system versus a more sophisticated threat from a professional thief or special operations person for whom the POD will almost certainly be substantially lower. It is doubtful that there is any single technology on the market that could not be defeated by experienced people, hence the need for a layered multiple technology solution where risks are high.

Almost any sensor manufacturer can quote and offer a 99.99% POD under ideal conditions, that is, a large target and sensor sensitivity set to maximum. Of course, at maximum sensitivity both the confidence level and the NAR may be totally unacceptable. If a manufacturer were to cite a 99% POD figure, they would need to furnish very extensive test data to verify their claims!

The nuisance alarm rate (NAR) indicates the expected rate of alarms not attributable to legitimate intrusion activity. Generally, nuisance alarms are caused by known or suspected environmental events such as animals, rain, wind and storms, and not by an actual intruder. The newer intrusion detection systems categorise the intrusion in order to distinguish

false positives from actual intrusions. A false alarm, however, is an alarm where the cause is unknown, so an intrusion is always a possibility, but analysis after the fact indicates that no intrusion actually occurred. The intrusion detection system has produced an alarm when no event has taken place. Generally, false alarms are generated by the hardware or software supporting the detectors. Today, with the advances in electronics, false alarms are becoming increasingly rare.

Vulnerability to defeat is another measure of the effectiveness of sensors and system design. Since there is no single sensor which can reliably detect all types of intrusions yet still have an acceptably low NAR, the potential for defeat can be reduced by designing overlapping sensor coverage using multiple units of complementary technologies.

Each of these three performance characteristics will vary according to the technology selected and the unique site conditions. Remember, no two sites are ever the same. Also, when comparing POD and NAR rates quoted by manufacturers, the two must be considered together as both are interrelated and to some extent can be traded off against each other. Anyone can quote a high POD by increasing the sensor sensitivity, and conversely, a low NAR by decreasing the sensitivity.

It is important to understand what the simultaneous POD and NAR figures will be, in other words, what can

PRODUCT APPLICATION

really be expected in the field with a real-world installation (this will almost always be site dependent) and how it matches the customer expectation. For example, a customer may be willing to tolerate a greater NAR to increase the sensitivity or POD of the system.

Signal discrimination and the way sensor information is analysed have undergone major developments and advances in recent years. This is only possible because of the large amount of multi-parameter sensing information that can be collected by the newer and much smarter technologies, such as interferometric fibre optic sensors, and the processing power available from multiple CPUs in centrally installed controllers which can run signal fingerprint and pattern recognition type software. This level of processing is typically not available from distributed processing architectures, that is, multiple microprocessor-based sensor controllers installed in the field. The computing required is far more intensive than the capability of these distributed microprocessors.

These advances in technology were originally designed for military applications but have made their way into the security arena where they are capable of clearly discriminating between 'real' events and background clutter. This capability allows the detection system to be made extremely sensitive to intrusions (high probability of detection) without the penalty of creating nuisance alarms (low nuisance alarm rate). It minimises the



effects of wind, rain, storms, aircraft, traffic and lightning while maintaining the required high levels of sensitivity and intrusion detection.

You also need to look at what and how much hardware you are installing in the field. While each component of the hardware may have an individual reliability or Mean Time Between Failure (MTBF) figure of say 10,000 hours, when you combine many pieces of hardware in a 'system', the 'system' MTBF will be significantly less due to the high component count and the many points of failure.

Conversely, if you select a system with a 'head end unit' or with all of the electronics in a single location for improved reliability, then you need to ensure that there is sufficient redundancy built in to minimise the chance of a system failure.

Estimated World Market for Perimeter Security Systems by Region in 2011

IMS Research estimates the global perimeter security equipment market at approximately \$402 million in 2011. Europe, the Middle East and Africa (EMEA) dominates the global perimeter security equipment market, accounting for 42% of the entire market. The Americas and Asia account for the remaining expenditure (58% combined). In EMEA, the Middle East and Africa were estimated to be the largest markets for perimeter security, mainly due to instability in the region, airport expansion, construction, oil and gas – all drivers for market growth. Eastern Europe is seeing an increase in the number of nuclear power generation sites as well as increases in crime, terrorism and other security threats which will drive growth in perimeter security.

PRODUCT APPLICATION

In the Americas, the market drivers for the USA include regulation and legislation, protection of borders, and protection of critical infrastructure. Continued economic growth in South and Central America also contributes to the growth in the Americas market. Asia is the smallest market for perimeter security and is dominated by low margin local suppliers in the Chinese, Japanese and Korean markets. The Indian and Pakistan markets will begin to improve due to increased labour costs and political instability in the region.

World Market for Electronic Perimeter Security by End-User Industry in 2011.

Airports: Until mandated or legislated by government, or becoming a victim of a security breach themselves, many commercial airports will continue to limit their perimeter security to patrolling security guards and a fence line. Hence the relatively low spend on perimeter intrusion detection.

Government and Military Sites: This segment comprises critical government infrastructure, such as prisons, borders, embassies, communications facilities, and military facilities, such as foreign and domestic army bases, training facilities, military air fields, etc. One reason for the size of this market is the large amount of radar technology installed, which is one of the most expensive types of perimeter security available.

Industrial Sites: There are two main drivers for this market – the value of

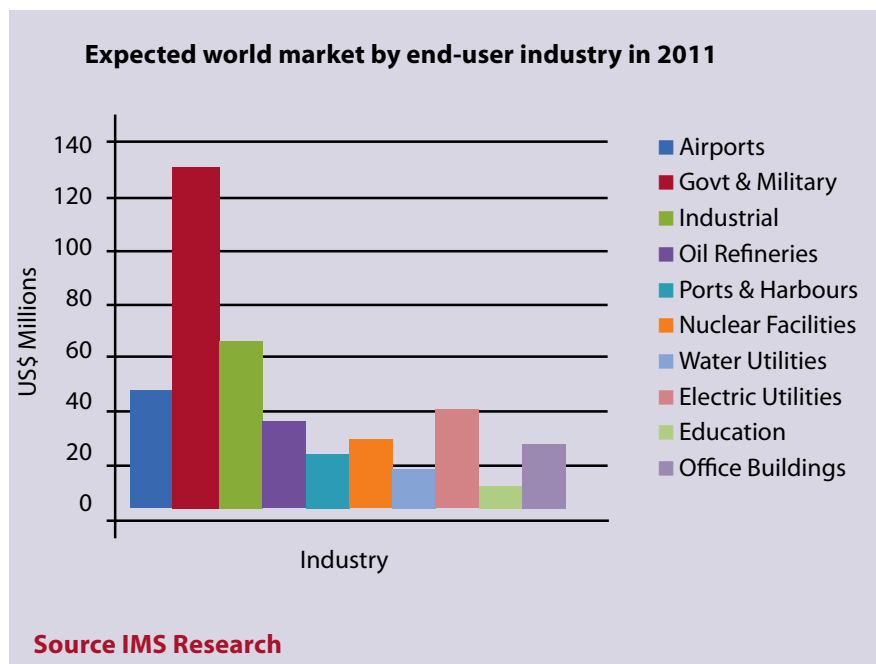
the assets within the site to be protected, and the strong requirement to protect sites that manufacture or store chemicals that could be potentially used as explosives or in the manufacture of illicit drugs.

Oil Refineries: Oil refineries are seen as critical infrastructure, especially for those countries highly dependent on oil revenue, and those countries importing large amounts of oil. For example, in smaller countries relying on oil as their major source of revenue, a terrorist attack on an oil refinery could severely restrict income and potentially create political instability.

Ports and Harbours: Ports and harbours are critical parts of national security. If a major sea port was immobilised, the commercial impact could be millions of dollars per day. While much of the

funding has been channelled into container screening, perimeter security has received some funding. Increased perimeter security is employed to combat people smuggling, and protect container terminals and maintenance facilities from theft.

Electric Utilities: This market segment comprises both power generation (other than nuclear, which is covered above) and distribution infrastructure such as substations, switching yards, etc. The levels of perimeter security required will be highly dependent on the anticipated threat – theft of metal, sabotage, political activists, etc. Where there is little backup in case of an outage, and replacement parts such as transformers may take months, or in the case of solar energy farms expensive solar panels are stolen,





then perimeter intrusion detection is highly recommended.

Education: This is the smallest market, as schools and universities are generally seen as low risk, low value targets. Intrusion detection is usually taken care of by CCTV and DVRs.

Office Buildings: These types of buildings are generally unfenced, as are the realm of security cameras and video analytics, or other free-standing technologies such as microwave and photoelectric beams.

Key Drivers Fuelling Investment in the Perimeter Security Market

Global social and political instability with the ongoing threat of terrorism will continue to drive the need to both fund and enforce regulation and legislation regarding perimeter security at critical national infrastructure sites including nuclear power stations, water reservoirs, data cen-

tres, transportation hubs and historic landmarks. An increase in organised protest movements (environmental, climate, economic and the like) are also heightening the need for advanced perimeter security.

Legislation will continue to play a major role in the growth of perimeter security equipment along with stimulus monies and other regulation. 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. While the potential growth for perimeter security is large, typical government bureaucracy and delays in rolling out any project means that the actual market growth will be more moderate and steady.

There will be increased demand for newer perimeter intrusion detection systems that require limited

or no power in the field, especially for those remote locations and long distance applications where power is not readily available, making these installations more viable than in the past.

Growth in vertical markets is also due to the following:

- Government and military is seeing growth in number of prisons, increased border protection (as countries enter the EU), and in the number of military bases and camps.
- Recent well-publicised security breaches of airport perimeters around the world, as well as the building of new airports and airport expansion programmes.
- Legislation and regulation of the security of petrochemical sites.
- Increased sea port security post 9/11 for illegal people movements and to address the International Ship and Port Facility Code (ISPS Code), although a large portion of the spending will continue to be on container screening.
- As industry demand for power increases, so does the drive to build more nuclear power plants. Each of these has to be protected from potential terrorist activity.

This article is an excerpt from the document “The Boundaries of Security 2011” written by Alec Owen, International Client Manager, Future Fibre Technologies Pty Ltd. All copyrights are reserved to the author and FFT Pty Ltd.