

Media Release

For immediate release

April, 2010

Artificial Intelligence Brings a New Era in Perimeter Protection Security

Technology incorporating artificial intelligence is revolutionizing the way perimeter security systems work, preventing theft and removing the threat of sabotage, without nuisance alarms!

The new perimeter intrusion detection systems which incorporate Artificial Intelligence use advanced signal recognition software to clearly identify what is an environmental event and what is an attempted intrusion, thus avoiding the nuisance alarms which have plagued traditional perimeter intrusion detection systems for years.

According to Alec Owen, International Client Manager at Future Fibre Technologies, the use of Artificial Intelligence in intrusion detection systems is a quantum or generational leap forward in perimeter security.

Mr Owen, who authored the widely acclaimed Boundaries of Security resource book, is an expert in perimeter security and was speaking to delegates at the Counter Terror Expo in the UK about the Artificial Intelligence breakthrough in perimeter protection technology.

“This technology can differentiate between intruders and lightning; terrorists and wind and rain; and teenage vandals and wildlife,” Mr Owen says.

Mr Owen cited the example of one of this company’s recent installations on the perimeter of a major gas turbine power station in one of the most lightning prone regions in the world.

“The coastal site is subject to extreme weather conditions, including cyclonic winds, year-round temperatures in the mid to high 30’s, and very high levels of tropical rainfall – in excess of 4 inches or 100mm per hour at times,” he said. “It also has one of the world’s highest incidents of lightning, recording more than 30,000 lightning strikes every year yet nuisance alarms are not a problem.”

This is in stark contrast to older systems, in which alarms have been triggered by environmental conditions such as wind, rain, passing traffic and lightning. Frequent nuisance alarms are both inconvenient and expensive and ultimately erode the confidence of security staff in the system’s effectiveness.

Mr Owen said the key to a superior perimeter security system is one which delivers increased Probability of Detection (POD) and decreased Nuisance Alarm Rates (NAR) and False Alarm Rates (FAR).

The POD is determined by the sensitivity and design of the detection sensor and also the quality of the installation. The experience, knowledge and skills of the intruder also play a role, with a teenage vandal being much easier to detect than an SAS specialist.

Nuisance alarm rates and the probability of detection are different for each installation and definitely site specific. While it is possible to use manufacturer quoted figures as a rough guide, the final figures can only be determined on site as part of a formal test regime.

False Alarms on the other hand are alarms generated by the intrusion detection system itself and not by the field sensor.

In the past, the most basic perimeter intrusion detections systems have used a simple threshold method in which an alarm sounds when the signal detected on the sensor crosses a pre-determined threshold line. Different systems have used “noise” levels or the frequency of events over time to establish the threshold line.

It has been very difficult to reduce nuisance alarms whilst simultaneously maintaining a sensitivity level high enough to detect legitimate intrusion events. Now, the technology is available to achieve this.

Techniques such Artificial Intelligence, Neural Networks and advanced multi-parameter signal processing are employed to dramatically improve the recognition and detection of real intrusion events against a background of nuisance events. This allows intrusion detection systems to minimise nuisance alarms without trading off the sensitivity or probability of detection to a genuine intrusion event.

Consider a fairly dramatic example of an intrusion attempt occurring during a nuisance event – in this case torrential rain.

A system incorporating Artificial Intelligence can recognise a signature buried within a ‘rain’ signal and can ignore the continuous background signal it causes. At the same time, it maintains its capability of picking out a single true intrusion signal occurring simultaneously during this heavy rain without any loss of sensitivity, and processes this signal to alarm and locate the intrusion.

The nuisance mitigation algorithm adjusts to varying levels of rain (or other sources of nuisance alarms) but, importantly, never reduces the intrusion event sensitivity. Once the rain stops, the system recognises this and dynamically returns to its normal mode of operation. Using this technique, rain-induced nuisance alarms as in this example can be minimised or even eliminated.

Using Artificial Intelligence to Analyse Signals

Traditionally, intrusion detection systems have flagged an alarm to the Security staff, who then look at the alarm information, gauge the environmental conditions, “listen in” to the signal on the fence, look at the CCTV, and use their experience and gut feel to decide if the alarm is real or not.

This process is notoriously inconsistent, relatively slow, highly subjective, and relies heavily on the experience and motivation of the operator.

Artificial Intelligence however, can not only perform this task automatically, but in a far more detailed manner by analysing all of the available raw alarm data – in fractions of a second, far more consistently and reliably than could a human brain. Not only do security staff get a simple consistent and reliable YES/NO answer, but the system can identify and notify staff of the type of intrusion that’s happening – such as cutting the fence, climbing the fence, propping a ladder on the fence etc.

How Does it Work?

Artificial intelligence and cognitive modelling try to simulate some of the properties of neural networks, but instead of solving particular tasks like the human brain does, artificial intelligence builds mathematical models that simulate these biological neural or thought systems. In simple terms, Artificial Intelligence tries to replicate in software how your brain makes a decision

Unique features or “signatures” are extracted from the event signals of interest and used to define different event classes such as fence climbing, fence cutting, rain, stone throwing, adjacent traffic, stick dragging etc. These are then fed into the Neural Network which essentially teaches it how to recognise these different events. This now gives the Neural Network the ability to classify any incoming event signal in real-time and an algorithm is used to make a decision as to what the event is and whether it is a nuisance or intrusion event. An effective neural network requires a large enough library of classes to cover as many possible intrusion and nuisance events that will be present in the intrusion detection system over its lifetime.

The Neural Network classifies these events in real-time, providing a definitive “Yes” or “No” alarm signal, as well as an instant explanation of what has caused the alarm. It’s exactly what security staff need to protect the perimeters of their critical sites.

Only a few years ago, this technology was confined primarily to the military and aerospace industries, used in biometric identification systems, biomedical signal analysis, speech recognition, imaging and telecommunications to name just a few.

Now it’s become mainstream in the latest generation of intrusion detection systems.

www.fftsecurity.com

-ends-

Prepared by Connecting Images Integrated Marketing
on behalf of

Future Fibre Technologies

For further media information, photography or interviews please contact:

Email: info@fftsecurity.com, or

Michele Eckersley on +61 3 9819 2566, Mobile +61 422 726 344,

Email: michele.eckersley@connectingimages.com.au