Keys to Implementing Optimal Perimeter and Intrusion Detection Systems

After selecting the right products, a few points should be kept in mind during installation. Detector sensitivity, necessary tampering prevention and price/performance considerations should be thoroughly discussed and understood by system integrators and end users.

BY CAMILLE SHIEH

When installing or upgrading perimeter and intrusion detection systems, the first thing to check are local standards. In the U.S., the Department of Homeland Security outlines new federal security regulations through the Chemical Facility Anti-Terrorism Standards program. Similar efforts are also in place in Canada, as shown by the Canadian Nuclear Safety Commission for nuclear sites. Several countries in the EU also implemented different protection levels — Grade 2 for monitored systems and Grade 3 for public and high risk sites. There is a gradual trend to make EN50131 national security standards mandatory for all intrusion systems that are monitored in Europe.

DON'T BE SO SENSITIVE!

Detection sensitivity is important in an effective perimeter and intrusion detection system. Fine-tuning detector sensitivity is a necessary procedure after installation, as end users do not appreciate a system that is either nonresponsive or overly responsive. Typically speaking, correcting detector sensitivity is to lower nuisance alarm rate (NAR) — alarms caused by an environmental stimulus such as rain, animals or lightning — more so than false-alarm rate (FAR).

"The install site will have predetermined levels of acceptance for detection, FAR and NAR that the system must achieve," said David Curtiss, Director of Engineering at Smarter Security Systems. "Initial calibration is generally performed with a specialty tool or human subject. The performance of the system should then be exercised until the requirements are met. After the system is operational there still may be some fine-tuning to find the optimal settings. Generally, within 30 days of installation the hardware will have proven itself and the users will have become familiar with the system operation. Regular maintenance is recommended to ensure proper operation."

Take fence sensors for instance. Achieving good results is a combination of site preparation and maintenance work, proper installation and the degree of "smarts" built into the sensor, said Stewart Dewar, PM of Senstar.

"Site preparation ensures that the fence fabric is reasonably tight to minimize excessive movement under windy conditions, and also removes or secures any loose objects striking the fence, such as signs or tree branches," Dewar explained. "For a fence sensor, proper instal-

▲ Detection sensitivity is fine-tuned to minimize nuisance alarms caused by weather conditions or wild animals.

lation means that the sensor cable is securely attached to the fence and that an appropriate threshold is set. A modern fence sensor will provide Windows software that allows sensor configuration and testing to be done via interactive screens. Modern fence sensors will also use advanced digital signal processing techniques to optimally discriminate between real intrusions and nuisance alarms."

Sensitivity levels need to be adjusted throughout the day, depending on activities in daytime and nighttime. Also, required sensitivity levels correspond to the threat level of the site protected. This can be configured by setting up different zones, which limits the number of active sensors in the system during daytime — such as acoustic and contacts only — while making all sensors active during nighttime, said Luc Joosens, Detection Product Management Leader for EMEA, UTC Fire & Security. "Another way is to use standard high-sensitivity sensors, such as mirror-optics motion sensors, that are only active during nighttime to ensure maximum sensitivity when required."

David Curtiss, Director of Engineering, Smarter Security Systems

Juergen Grasmehr, Global Portfolio Manager of Intrusion and Perimeter Systems, Siemens Building Technologies

"Typically this will be done via arming/disarming procedures independently for areas or zones," added Juergen Grasmehr, Global Portfolio Manager of Intrusion and Perimeter Systems, Siemens Building Technologies. "These procedures can be triggered by users via a management station, field devices such as lock or access readers, or automatically by schedulers."

Some advanced systems collect information like environmental conditions or special settings — day, night, working time and more — to adjust sensitivity automatically, Grasmehr said.

TAMPER-PROOF

A good perimeter and intrusion detection system should be designed with tampering prevention in mind. Without appropriate tampering detection, the perimeter and intrusion detection system could be at risk for malfunctions. Some basic tampering detection include: mechanical tamper contact, anti-masking and anti-blocking detection, encryption, discrimination detection, sporadic cut alarms, mechanical and electronic adjustment detection.

The first level of protection is a housing tamper, which triggers an alarm when the cover of a sensor or control panel is opened, Joosen said. "A second level of protection, which is required in public and high risk environments, is a pry-off tamper which is triggered when the device — control panel, keypad or sensor — is removed from the wall."

"A micro-switch should be in place to detect removal of the sensor cover and monitor sensor, and communication cables to detect cutting or short-circuiting," Dewar said. In the case of a microwave volumetric sensor, it has a built-in fraud protection; the system will monitor the signal received at the receiver unit and trigger an alarm if the signal level falls below a set threshold or a jamming signal is detected.

Cable sensors are by nature sensitive to detect tampering and the circuitry enclosure is protected by security hardware and trip switches, Curtiss said. "The more sophisticated systems employ digital signal processing to detect network 'spoofing' attempts." Periodic maintenance should also include checking up on the tamper-proof condition for the system to deliver optimal performance.

David Smith, CEO of Optellios

PRICE VERSUS PERFORMANCE

The maxim "You get what you pay for" holds true in perimeter and intrusion detection procurement. Budget offerings typically sacrifice features and functionality, said David Smith, CEO of Optellios. "Features such as intrusion pinpointing, cut immunity and multiple simultaneous intrusion detction are not seen on low-budget offerings."

Security is very much like insurance policy — how one proves the ROI; however, the risk of crime, vandalism and loss of production should be considered, Dewar said. "Once the investment is done, the comparison is between low-cost and high-end solutions. Here, the customer will feel the difference through: integration TCO, documentation level, maintenance by the system integrator, ease of recalibrating the system and more. A well-maintained and calibrated system would last decades."

Leaving cost and technical considerations aside, external site factors such as landscape (flat or hilly) and climate (rainy, dry or harsh) influence the performance of any product. For virtual fencing systems, such as radar or infrared beams, weather and climate conditions do not cause interference. However, devices need to be carefully placed and aligned so that the signals are sent and received accurately, meaning that precise engineering of products is a must.

More importantly, the quality of the installation, setup and maintenance could affect product performance. For instance, a site that includes an open area would be well-served with a buried cable system, which provides a wide detection zone that is immune to most sources of environmental nuisance alarms and is difficult to defeat since it is covert, Dewar explained. "For sites without such a clear-zone, a fence-mounted sensor with a continuous sensor cable can be used to detect fence vibrations and a digital processing system to analyze the vibration patterns to differentiate real intrusion attempts from nuisance alarms. If there is no clear zone or a pre-existing fence, a barrier sensor such as a taut-wire system is an option since it provides the deterrence and delay aspects of a fence, along with integrated sensors to detect an intrusion."

"The No. 1 thing that can be done is to make sure that the end user is getting the right sensor for the application," Dewar suggested. "As of yet, there is no one sensor that works well in all environments. For any given infrastructure site, the optimal physical intrusion detection system will depend on the specific site conditions." a&s