Technical Article

Infrastructure & Cities Sector
Building Technologies Division

Zug (Switzerland), February 5, 2013

Security for Retail Banks

In the retail banking sector, requirements for intrusion detection and related security measures are necessarily more stringent and more specialized than in most other areas of business and commerce. Modern security systems address these special requirements.

By Alistair Enser, Security Products, Siemens Building Technologies

In the banking world, the threat of unwanted intrusions into premises leading to loss of property and even risk to life is always present. Small wonder then that banking institutions take so much care over their security systems and also over their choice of suppliers for those products. Let's consider the suppliers first.

The banks clearly need to work with suppliers whose integrity is beyond question, but that alone is not enough. They should be looking for organizations that can offer expert advice, gained through their knowledge of design and manufacturing security products and systems that have specialist installer partners in order to provide a seamless solution.

These supplier organizations must also fully understand the special requirements of the banking sector and, ideally, should be able to demonstrate proven experience in that sector. They must also be willing and able to work with the bank as a partner, to find better ways of addressing old threats and to develop effective measures to counter new ones.

It is fair to say that security providers that meet all of these requirements are thin on the ground but there are a few companies, including Siemens Building Technologies Division, which can offer all of the relevant expertise, competencies and experience.

Challenges in intrusion detection

Let's consider some of the challenges that the chosen supplier will face, particularly in relation to the provision of intrusion detection. Like other businesses, intrusion detection systems for banks need to monitor doors and accessible windows, and to provide movement detection for vulnerable areas within the premises. With banks, however, there are also more specialized requirements, such as the need to introduce time delays when accessing sensitive areas, as well as providing the earliest possible warning if someone is trying to gain access through a wall, or is attempting the wholesale removal of an ATM.

To cater for these situations, seismic detectors that are sensitive to vibration are often used. The latest versions are sensitive yet dependable, and can protect up to 80m^2 of wall per detector, making them an economical and effective option.

Intrusion detection for banks has other special requirements. In an ordinary business, there is usually one keypad or similar device to arm or disarm the system throughout the premises. In a bank, a single keypad may still be used to arm the whole system, but disarming is usually controlled on an area-by-area basis and more often than not these areas are linked together and dependant on calendar schedules (public holidays, country specific holidays or business closures). Conventional keypad displays are limiting in how much information they can display at any given time, a cluttered rolling display is not helpful or engaging. Rather the user is now looking for a more sophisticated approach where multiple events taking place simultaneously can be displayed in a clear & intuitive manner.

Intruders may, of course, enter the bank in the guise of ordinary customers, and the intrusion detection system must be able to deal with this eventuality. Typically this requirement is met by providing staff with foot-operated alarm triggers, under-desk alarm buttons and the like. These triggers are operational irrespective of whether or not the rest of the intrusion detection system is armed.

In many cases, the trigger devices and even some of the detectors used by the system are wireless, since this allows them to be relocated easily and quickly, matching the needs of the modern banking sector for frequent rearrangement of its premises. In spite of their extra flexibility, however, wireless devices are usually used in combination with conventional wired devices, as wired connections are inherently more reliable.

While banks demand and require the best possible performance from their intrusion detection installations, this must not be achieved at the expense of generating high levels of false alarms, as these are not only costly and disruptive, but may also divert attention from genuine intruder events.

Omitting false alarms

In the past, a large proportion of false alarms were associated with cleaners working in the premises outside normal banking hours. Rather than reducing the coverage of the PIR (passive infrared) detectors that generated these alarms, in many cases the detectors have instead been reconfigured to operate a traffic-light system that the bank manager interrogates before entering the premises. If this shows an amber or red condition, indicating that a PIR detector has been triggered, the manager calls for additional support before entering.

Another technique of eliminating false alarms is to route automatically generated alarm signals via an alarm filtering center operated by the bank itself. The staff at the center is trained to evaluate each alarm signal and determine whether it is a false alarm or not. They then have 90 seconds to cancel the alarm before the police are alerted.

These and other methods of tackling false alarms in banks have been very successful – today, less than 1% of alarm signals passed to the police ultimately prove to be spurious.

While the selection of security systems for banks is most certainly not governed by cost banks are, like all businesses, always happy to find ways of keeping down expenditure. This has led to a growing interest in using security systems to perform functions outside their main role. For example, why not let the security system automatically turn off unnecessary lights and reduce the level of heating in the building when it determines that there is no staff present? This simple action alone can save banks large sums in energy bills as well as helping them to reduce their carbon footprint. State-of-the-art security installations thus offer the possibility to integrate a part of the functionality of a traditional building management system (BMS).

The **Siemens Infrastructure & Cities Sector** (Munich, Germany), with approximately 90,000 employees, focuses on sustainable technologies for metropolitan areas and their infrastructures. Its offering includes products, systems and solutions for intelligent traffic management, rail-bound transportation, smart grids, energy efficient buildings, and safety and security. The Sector comprises the divisions Building Technologies, Low and Medium Voltage, Mobility and Logistics, Rail Systems and Smart Grid. For more information, visit http://www.siemens.com/infrastructure-cities

The **Siemens Building Technologies Division** (Zug, Switzerland) is the world leader in the market for safe and secure, energy-efficient and environment-friendly buildings and infrastructures. As technology partner, service provider, system integrator and product vendor, Building Technologies has offerings for safety and security as well as building automation, heating, ventilation and air conditioning (HVAC) and energy management. With around 29,000 employees worldwide, Building Technologies generated revenue of 5.8 billion Euro. For more information, visit www.siemens.com/buildingtechnologies