SIEMENS

Technical Article

Infastructure & Cities Sector
Building Technologies Division

Zug (Switzerland), November 15, 2012

Access Control or Intrusion Detection?

With modern technology and the growing trend toward integration in security installations, the line between intrusion detection and access control systems is becoming increasingly blurred. So what are the essential differences, and is a single system that combines both functions a good option? Siemens has the answers.

By Alistair Enser, Security Products, Siemens Building Technologies

Superficially, at least, intrusion detection and access control systems have a lot in common. After all, the basic objective of both systems is to keep people out of places where they shouldn't be. There are, however, fundamental differences. Intrusion detection is, in the main, outward facing – it protects the building against any unauthorized access from the outside. Access control, however, is much more inward facing – its principal function is to control the movement of people within a building, i.e. who can access certain areas at certain times.

The distinction is not absolutely clear-cut. Most access control systems monitor the entry of people into a building from the outside via authorized routes, and many also provide monitoring for forced entry via doors – though not necessarily via other routes – as well as warning if doors are held open for longer than a predetermined time.

Nevertheless, the conclusion has to be that despite their apparent similarities, intrusion detection and access control systems have different functions, although there are areas of overlap. So how do facilities managers and other specifiers decide which system, or combination of systems, will best meet their requirements?

The first thing to note is that the choice may not be entirely in the hands of the specifier. Depending on the type of premises and the location, insurers may insist on the installation of an approved

Siemens Schweiz AG
Infrastructure & Cities Sector - Building Technologies Division
Gubelstrasse 22, 6300 Zug, Switzerland
TA ICBT 201211e Access control or intrusion detection

Public and Press Relations: Catharina Bujnoch
Telephone: +41 41 724-5677
E-mail: catharina.bujnoch@siemens.com

intrusion detection system, or alternatively may substantially increase the premium if such a system is not fitted.
Assuming the decision is not forced by the insurers, however, the next thing to consider is whether intrusion detection is needed. This decision is likely to be based on the type and value of the contents of the premises, and whether the location means that there is a significant risk of attempts at unauthorized entry.

For the majority of businesses, the conclusion is very likely to be that intrusion detection is either essential or at the very least, highly desirable. The system needs, of course, to be designed to suit the application, but will typically include sensors on all external doors and accessible windows, together with PIR movement detectors to cover critical areas and, in high risk applications, possibly other devices such as seismic detectors to monitor for undue vibration and shock.

So much for intrusion detection, but what about access control? The key questions to ask here are whether there is a need to restrict access of certain groups of people - be they staff or visitors - to the building or areas within the building via normal routes, and whether there is a need to keep detailed records of persons entering and leaving the building or areas within it. If the answer to any of these questions is yes, then an access control system is needed.

Access control as the lynch pin

Before making a final decision, it is worth considering the additional features that an access control system offers a business that allows it to become integrated into the fabric of an organization to provide added value. This can include using the records generated by an access control system for additional uses over and above their security applications. Many organizations, for example, use data from their access control system about the number of hours staff have worked as the basis for payroll calculations. The access control can also be the lynch pin of a building's technology infrastructure by providing links into its CCTV, building management, company databases and of course the Intrusion system, with all sub systems being sometimes viewed or controlled from a common front end.

For applications where it has been decided that only an access control system or only an intrusion detection system is needed, the next steps are relatively straight forward – assess your needs now, and potentially for the future, and match those needs to available products on the market. And then find an installer.

Siemens Schweiz AG
Infrastructure & Cities Sector - Building Technologies Division
Gubelstrasse 22, 6300 Zug, Switzerland
TA ICBT 201211e Access control or intrusion detection

Public and Press Relations: Catharina Bujnoch
Telephone: +41 41 724-5677
E-mail: catharina.bujnoch@siemens.com

There are some points worth noting, however.

The first is that it always pays to specify proven products from a reliable source. This will help in a number of ways, as the product or manufacturer specified should have a proven market pedigree and support infrastructure. An unreliable installation is, in some ways, worse than no installation at all, as it gives a false sense that the building is well protected when, in reality, this could be far from the truth.

The second point to note is that installers of intrusion detection systems are regulated by law, whereas those of access control systems are not. For this reason, access control installers called upon to provide intrusion detection systems sometimes sub-contract the work. If intrusion detection is what's needed, therefore, it may well be a better option to go direct to a company that's approved for this type of work and can offer a complete solution.

No universal answers

Now let's move on to the situation where both intrusion detection and access control are needed. Is it better to find one system that will do both, or would two separate systems be a better option? And, if two separate systems are used, to what extent should they be integrated, if at all? There are no universal answers to these questions that apply to every case – every application must be considered individually. It is possible, however, to provide guidance on some of the key factors that will influence the decision.

The first is that, once again, the choice may be out of the hands of the specifier. Over 90% of security systems are installed in premises where an existing system is already in place and, in most cases, the new system must work alongside the old. This is likely to force the decision in favor of separate systems for intrusion detection and access control.

Where the decision is not forced, functionality is a key issue. Systems that combine intrusion detection with access control are essentially intrusion detection systems with added access control functionality. This functionality is typically adequate for normal applications, but where additional software features that an access control system offers are required, then this route may not be sufficient.

It is worth noting, however, that manufacturers are rapidly enhancing their integrated capabilities of their combined systems, so it is always a good to idea to check on the latest developments.

Siemens Schweiz AG
Infrastructure & Cities Sector - Building Technologies Division
Gubelstrasse 22, 6300 Zug, Switzerland
TA ICBT 201211e Access control or intrusion detection

Public and Press Relations: Catharina Bujnoch
Telephone: +41 41 724-5677
E-mail: catharina.bujnoch@siemens.com

There’s no doubt that, if they provide all of the functions needed, combined systems have important benefits to offer. These include enhanced usability and greater convenience, as users need only a single card or token to control the intrusion functions and also to gain access through doors. There is also the potential for benefits during the installation phase. A combined system invariably needs less wiring than would be required if separate intrusion and access systems were installed, and this leads to significant cost savings.

Integration of intrusion and access control can also bring operational benefits. For example, a user who normally has access to the building when the intrusion system is unset can readily be denied access when the system is set – provided, of course, that they do not have set/unset rights for the intrusion system. Not only does this provide additional security, it also helps to eliminate a potential source of false alarms.

Finally, combined systems offer administrative benefits. Provided they are well designed, they will support the concept of a single user profile, which means that the intrusion and access privileges for a user are contained in the same profile. This makes it faster and easier to set up the system, and eliminates the need to enter user data in two separate locations.

Despite the undoubted benefits of combined systems, however, it is important to be aware that they also have a downside. Combined systems can be more complicated to set up than separate systems, and finding an installer with the appropriate experience in both fields may not be easy. So what about installing separate systems and tying them together in some way?

This may seem an attractive option, especially where an existing system must be retained, but it too has its problems. For instance, the level of integration that can be achieved between the two systems is often varied, but flexible, and will take careful planning to achieve the desired functionality. Considerations regarding how an alarm is reported and dealt with, along with the divided responsibilities of different manufacturers for the support of each separate system, will also need to be made.

In short, linking independent systems can be useful as you can utilise the advantages of both disciplines in a system that works for you, but options should be examined very carefully before a decision is reached.

Siemens Schweiz AG
Infrastructure & Cities Sector - Building Technologies Division
Gubelstrasse 22, 6300 Zug, Switzerland
TA ICBT 201211e Access control or intrusion detection

Public and Press Relations: Catharina Bujnoch
Telephone: +41 41 724-5677
E-mail: catharina.bujnoch@siemens.com

Conclusion

As we have seen, intrusion detection and access control systems have slightly different roles. Where both systems are needed, a combined solution is often a good choice, provided that the necessary functionality can be achieved. Separate systems may be more versatile and easier to implement, however, but the possibilities for interconnecting them will require some consideration. Clearly, making the right decision may not be a simple issue, so support from an experienced and expert supplier should be sought. Ultimately whatever the required solution is, the products need to fit the building and application so choosing an established supplier like Siemens Building Technologies Division, Security Products business segment, which offers a full range of options and is in a position to offer impartial advice, will be invaluable in making the right decision.

The **Siemens Infrastructure & Cities Sector** (Munich, Germany), with approximately 87,000 employees, offers sustainable technologies for metropolitan areas and their infrastructures. Its offerings include integrated mobility solutions, building and security technology, power distribution, smart grid applications, and low- and medium-voltage products. The Sector comprises the Divisions Rail Systems, Mobility and Logistics, Low and Medium Voltage, Smart Grid, and Building Technologies. For more information, visit www.siemens.com/infrastructure-cities

The **Siemens Building Technologies Division** (Zug, Switzerland) is the world leader in the market for safe and energy-efficient buildings (“green buildings”) and infrastructures. As a service provider, system integrator, and product vendor, Building Technologies has offerings for building automation, heating, ventilation and air conditioning (HVAC), fire protection and security. For more information, visit www.siemens.com/buildingtechnologies

Siemens Schweiz AG
Infrastructure & Cities Sector - Building Technologies Division
Gubelstrasse 22, 6300 Zug, Switzerland
TA ICBT 201211e Access control or intrusion detection

Public and Press Relations: Catharina Bujnoch
Telephone: +41 41 724-5677
E-mail: catharina.bujnoch@siemens.com