SIEMENS

Technical Article

Infrastructure & Cities Sector
Building Technologies Division

Zug (Switzerland), September 7, 2012

Access control: integration not isolation

In the current economic climate, the focus on value for money is greater than ever. Businesses are considering their processes and systems and looking at how to leverage added value from them. Security is part of that focus, including access control and time attendance systems, a central component in the move towards a more integrated approach which recognises the significant benefits to be derived. Such benefits include enhanced protection from intrusion and the prevention of industrial espionage, thereby safeguarding assets, intellectual property and people. By drawing data from a number of different sources and systems, including building management systems, it is possible to better understand the needs of a building and to control and optimize it accordingly.

By Philippe Huysman, Global Portfolio Manager Access Control, Siemens Building Technologies

For the bigger system manufacturers and integrators, customers are primarily corporate enterprises. This means that a green field strategy is not generally possible, with the majority of the business in the access control market therefore being in updating, modernizing or migrating systems, often including the need to take into consideration existing service contracts. Even though many of the multi-national companies employ access control and time and attendance as part of their processes, the market is still characterized by its regional focus, largely due to differences in legislative requirements, particularly in terms of privacy and work time regulations which differ from country to country.
This means that there are real benefits in employing system manufacturers and integrators with the capacity to provide global solutions, both for multi-site and for multi-tenant applications, but that also have local expertise and knowledge. The systems need to be flexible, with the capability to operate locally for a single branch or for numerous networked branches across the world and therefore across different time zones.

Siemens Schweiz AG
Infrastructure & Cities Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

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

Reference number: TA ICBT201209e Access control.doc

Managing costs

One of the main reasons for companies reviewing their access control provision and looking to potential alternative vendors is cost. The economic downturn has brought this into particularly sharp focus as businesses seek to maximize value for money from their systems and processes – security and safety are no exception. ID cards remain the most widely employed means for authentication. At 3 to 5 euros a card, production of the cards is not where the main cost lies but rather in the management of them over the entire lifecycle. The physical cost of replacing the card is small but what is involved in administrative terms is often not: configuring the card, renewing the certificates required for authentication, running a Local Registration Authority (LRA) office to provide that service being typical examples. Having a single multi-application card rather than multiple cards can therefore reduce such costs. Complex administration is common, with the need for frequent ID data updates and re-defining of access rights, particularly in dynamic large-scale, multi-site applications with potentially thousands of IDs.

Optimization can be achieved by segregation and delegation of specific duties to local administrators, but still keeping a central administration and auditing to ensure that global corporate policies are enforced. It is therefore important that systems are easy to manage, with a simple interface for those responsible for access security to edit staff data, access profiles, validity period etc. Implementing automated workflows will further reduce costs and increase overall security. It is important that access control management systems are able to handle organizational changes or relocations of departments efficiently. With more efficient management comes lower cost.

Another area of potential cost saving is through energy efficiency. Security, and particularly access control, has a vital role to play in this process as the security systems provide the information relating to the occupancy of a building. Why do we automate a building? Why do we make a building comfortable? Why do we supply energy into a building? It is for the people within that building so ultimately it is occupancy that drives everything. With the increasing integration of security, fire and building management systems, the potential is there to make significant energy savings, and therefore cost savings. At its simplest, if the access control system knows that nobody is present in a given room, the HVAC (heating, ventilating and air conditioning) systems can be automatically adjusted to reflect that. But, extending this demand controlled approach beyond using just occupancy detectors, in a laboratory, for example, it is even possible to set the conditions based on the person that has entered. An access control reader identifying cleaning personnel entering will know it is for a relatively short period of time. The temperature comfort set point could therefore be lower but with an increased constant air exchange rate than say, for a chemist or a technician entering for their daily work.

Siemens Schweiz AG
Infrastructure & Cities Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

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

A holistic approach to security

For the larger systems, which can leverage on existing IT network infrastructures, integration is an important factor. Companies, certainly the bigger enterprise operations, have moved away from a single discipline purchase mentality to one which sees security in much more of a holistic way, both in terms of integrating different security functions but also in relation to how security and safety can be integrated into general business processes. The market has moved significantly in connectivity terms, particularly with the development of open architecture. For example, until relatively recently connectivity of video surveillance with an access control system would be either at a very low level via hard wired signals or at a very high level through expensive, bespoke software developed by system integrators. Now, with the industry's drive towards open interfaces, customers are expecting integration as standard functionality.

Originally driven by the network video sector, the focus for the security industry has switched to the adoption and development of new physical access control standards with a push to build compliant devices. Many of the leading manufacturers have announced their intentions to bring such devices to market and they are now gradually being introduced. Open architecture continues to develop around the BACnet protocol, with a further drive towards standard protocols led by industry forums such as ONVIF (Open Network Video Interface Forum) and PSIA (Physical Security Interoperability Alliance). Supporting customers to move away from proprietary communication protocols and providing software through cross-domain management and command and control solutions, will become an increasing focus as the trend towards integration accelerates.

Additional challenges

Any access control solution needs to recognize that although there are common issues across different applications, the requirements can also vary significantly depending on the needs of the business and the premises in which it operates. Returning to the pharmaceutical industry as an example, data from the access control system can be invaluable in retrospectively identifying which employee had been working on production of a particular medication if an issue arises.

Harmonization of corporate security can also be important, particularly in enterprise businesses where consolidation of different access control systems may be required in the event of a company acquisition, for example, with any country-specific issues needing to be addressed.

Another consideration in access control is the migration path. To protect an investment, it is vital that the majority of the hardware can remain in place, including the cabling, with any updates achievable primarily through software. It is common for the field level components, i.e. the card readers, locks and cards, to be reusable but for the automation level modules, i.e. the door controllers, to require replacing. It is also vital to recognize the central role that data plays in an access control system and significant costs can be incurred if the new system cannot accommodate the use of data from an existing database. A complete migration plan can be

Siemens Schweiz AG
Infrastructure & Cities Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

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

developed which removes the need to rip out the existing infrastructure and start again, instead using the software to maintain and work with older style field devices and hardware and complement those with newer equipment.

Integration with business software

There are a number of current trends in access control which provide useful indicators as to where the market is heading. One is the demand for enhanced functionality. There is a very definite move towards smartcards. The cards that had previously carried data just to allow access to the building are now being used for multiple applications. This can range from parking to electronic cashless purchase of food, with the additional potential to enhance workplace security through the inclusion of strong authentication for accessing IT network and applications, digital signature and email encryption, biometric data, and printer access management.

Increasingly standardized and certified interfaces are being established with ERP (Enterprise Resource Planning) software systems such as SAP and HR (Human Resources) systems, as well as facilities management. Interfacing with HR or other identity data sources enables an automated process for identity provisioning and de-provisioning, including automatic assignment of access entitlements based on the individual's attributes. The operational cost savings, increased data consistency and security that can be achieved is obvious. However, these capabilities are often not yet exploited.

Sophisticated visitor management

To achieve tighter security visitors and contractors also need to be tracked to know who is on site at any time. The check-in and check-out process and announcement to the host of the visitor's arrival should be handled very professionally and efficiently at the lobby. Web pre-registration, announcement and approval of the visitors by the host prior to arrival greatly improves the speed of this process. A tight integration with the access control increases the security by ensuring that the visitor does not have access unless accompanied by his host.

Electronic door cylinders and fittings are being employed more often, mainly because of the reduced installation costs. The use of a smartcards' memory to store the individual's authorizations and his valid access requests, makes such solutions very attractive for doors requiring basic access control functionality, but not where full online supervision is required. A perfect use case is access to closed meetings that can be restricted to authorized participants by replacing conventional door knobs with card reading devices. This can tie in with Microsoft Office, for example, whereby the booking of a meeting and a room to host it will only allow access to those invited to attend through the data on their card or badge. By offering a combination of electronic door fittings together with fully online supervised solutions an optimal balance between cost-

Siemens Schweiz AG
Infrastructure & Cities Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

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

efficiency and security can be achieved. But in order to fully exploit those benefits it is important that the administration and reporting can be done within one management application.

Strong smartcard encryption

As the potential for smartcards evolves with the opportunity to control an increasing number of applications, so has the need to ensure security is maintained through stronger encryption of the data that they carry. In industries where high security access control is required, such as pharmaceutical and chemical production, this is particularly key to the ongoing adoption of smartcard technology. Moving beyond smartcards, smartphones equipped with NFC (Near-Field-Communication) will find its way to the access control industry. Smartphones, with their capability of being always connected and being location-aware will offer new possibilities that smartcards can't offer today. Although there is a lot of ongoing research into this and early pilot schemes are being developed, it is not yet widely adopted, and further shaping of the complete NFC eco system is required.

Bringing information together

As companies look to get more from their business systems and processes, so adding value from all of the contributory elements, including access control, will be increasingly important. With the focus very much on integration, the role of IT is now fundamental in safety and security provision. The value migration from physical assets to information-based assets, along with the shift to online data storage, has further focused attention on IT, creating new demands for enhanced information security. But in security terms, it is not all about IT. Information is one of the most valuable assets that a company possesses and, as such, one of the highest areas of risk.

An estimated one million people are victims of cyber crime every day. There are diverse methods of attack, both external and internal, with some 80 percent of security breaches generated by insiders, most often employees. Firewalls can help prevent attacks but can certainly not provide comprehensive protection, particularly from insider threats, and should never therefore be treated in isolation. Corporate security provision needs to adopt an "outside-in and inside-out" approach, combining IT based measures with a layer of physical security to provide more robust protection of data. Access control systems provide the means to physically restrict access to sensitive data storage areas and to provide identity management through access control technologies.

For access control, IT has always been more integral than for many other areas of security, with its reliance on databases and transaction logs and its use of the IP infrastructure over many years. However, the IT-based demands from the market will only intensify as the drive to monitor and manage buildings in an integrated way provides the means to create more sustainable and more energy efficient buildings which are also more safe and secure.

Siemens Schweiz AG
Infrastructure & Cities Sector - Building Technologies Division
Gubelstrasse 22, 6301 Zug, Switzerland

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

The need to discover ways of bringing information together is a considerable driver. Now that security is operating very clearly in the IT arena, nearly all protocols are open so the ease with which information can be fed into the security process is improving. The data is often there, under-utilized in terms of how it can enhance security measures. It is a case of tapping into that resource and recognizing what information can help to improve security levels and, in doing so, help to add value to the whole business process.

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, 6301 Zug, Switzerland

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