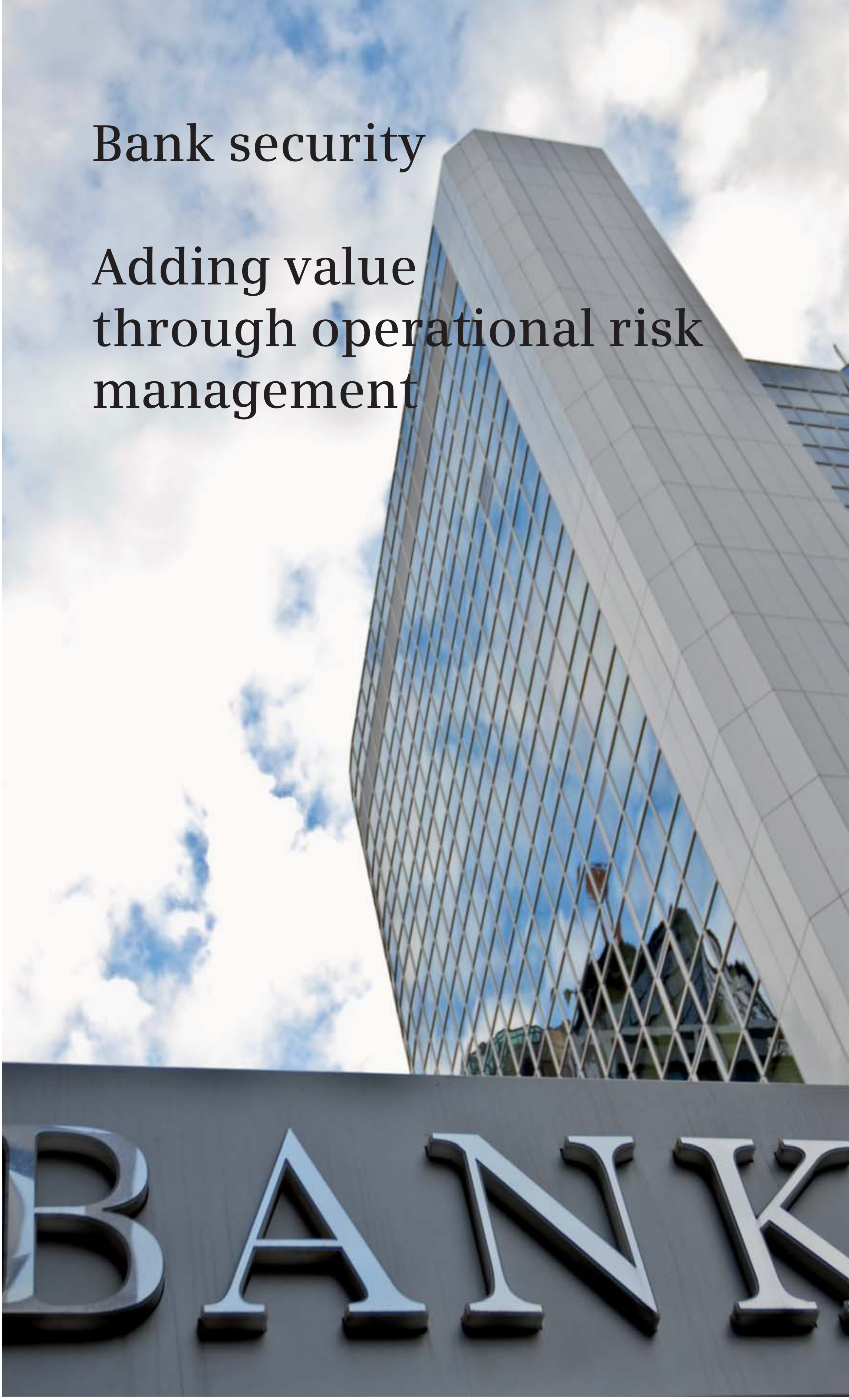


Bank security

Adding value through operational risk management

Answers for infrastructure.

SIEMENS

A new dimension to banking security

Faced with today’s market uncertainty, banks and financial institutions are rethinking the way they do business, with a clear focus on two vital areas: the customer trust – directly linked to their ability to ensure business continuity and secure assets, people and sensitive data; and operational efficiency – targeting improved competitiveness by redirecting payments to lower-cost channels, changing the role of branches to focus on the customer experience and service cross-selling, as well as by streamlining processes and systems.

Combined with stringent operational risk and compliance regulations, this has led to security issues being increasingly viewed and managed as a single, end-to-end concern within a bank’s risk management strategy, looking beyond the physical environment to incorporate IT systems, channel management and identity and access management.

At Siemens, we understand that the level of sophistication and functionality required from security systems is driven by the specific business role of bank premises, from ATM zones, to local branches or data centres. The scalable products and systems we offer can help customers and staff feel safe without interrupting daily business, interoperating seamlessly to support a more “self-service” and customer-friendly banking environment – for maximum operational efficiency and return on investment.

Banking on security with a holistic approach to risk management

Keeping the vital customer trust

To compete successfully in today's tough market place, financial institutions need to keep the trust of their customers – a trust which relies not only on their capacity to deliver good value services, but also on their ability to protect people, assets, premises and the highly sensitive data they hold. Despite the increase in electronic fraud, a worrying trend identified by a recent EBF[1] report is the growing use of violence in physical raids. With any security breach potentially having devastating effects on a bank's reputation, security is understandably a growing priority and banks need to have – and be seen to have – adequate security measures.

Protecting the "new bank"

In addition, banks have diversified the range of services they offer and their delivery channels to improve both customer retention and acquisition: the simpler services are now available through lower-cost, "self-service" channels such as ATMs and online banking, whilst branches are refocused on more complex service sales, with open, customer-friendly spaces. Whilst this shift improves service levels and drives operational costs down, with this new bank business model come new threats, and the need therefore for a more holistic approach to security, where sales channels are no longer seen in isolation: security systems should not only encompass a bank's security as a whole – protecting everything from a single ATM to branches, data centres and entire networks – but also enable the exchange and cross referencing of security and transaction data across all bank channels.

Ensuring business continuity

Losses resulting from security breaches are not just monetary: collateral damages can also include compromised data, lost productivity and reduced turnover – ultimately damaging a bank's credibility. Regulatory requirements such as Basel II[2] and Sarbanes-Oxley (SOX) also emphasise the need for banks to proactively protect business continuity and guard against operational risks[3]: interoperable security systems can help address these requirements, either by preventing attacks and business disruptions, or by speeding up incident recovery through e.g. the provision of tools to investigate – and prosecute – more effectively.

Security with measurable return on investments (ROI)

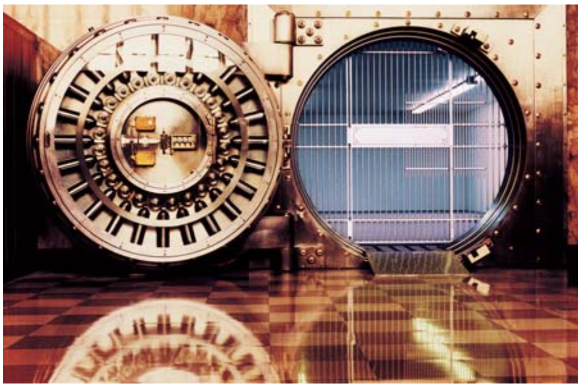
Siemens draws from over 30 years of security know-how to deliver interoperable systems which support a truly holistic approach to banking security: access control, intrusion detection and video surveillance systems work together to deliver the required functionality for given sales channels, enabling security resources to be deployed more cost-effectively. Capable of integrating into existing IT networks, they can help reduce the initial level of investments, yet still make room for system upgrades or expansions. Powerful reporting tools, combined with the bank's transactional data, provide an enterprise view of potential security threats, improving both prevention and response capability: losses due to theft of cash, assets and sensitive data are reduced – as are threats to business continuity – thereby providing measurable return on investment.

Compliance with international standards

International standards – such as VDS and EN – are vital in ensuring that electronic security systems are installed professionally and remain reliable. Siemens embraces this compliance in every way, with also for example, video surveillance systems that are Kalagate and BGV (UVV-Kassen) compliant. These ensure, amongst others, that evidence is admissible in court and that suspicious events can be saved separately and securely exported to various media.

Highlights

- Develop cross-channel security intelligence to more effectively protect people, data, assets and premises
- Reduce losses to fraud, theft and vandalism
- Improve operational efficiency and business continuity with measurable ROI
- Increase compliance with operational risk management regulations
- Protect brand equity and customer trust



[1] European Banking Federation

[2] Within the Basel II accords, operational risk is now treated as a clear focus area, alongside credit and market risks.

[3] "The risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events." (Basel II definition)

In a bid to improve customer convenience and shift payment transactions to lower-cost channels, banks have become increasingly "self-service" organisations, rolling out ATMs accessible 24/7 at branches or in "remote" areas (e.g. in the High Street, at petrol stations, supermarkets, transport terminals etc.). Indeed, not only have ATMs provided banks with a more cost-effective service delivery channel, but they are also a key channel through which banks can conduct powerful one-to-one marketing – this is reflected in the ATM numbers, estimated to go over the 2 million mark worldwide by 2011[1], and with nearly half of them deployed in off-site locations.

The "self-service" bank brings its own security challenges, with a dramatically increased pool of potential – and easier – targets for card frauds, robberies, muggings, forced withdrawals or even ram raids ...

Protecting the "self-service" bank

Bank owned or sponsored stand-alone ATMs, 24-hour zones, ATM operator networks.

The "self-service" security challenge

Banks and financial institutions have a legal duty to prevent cardholders' financial and personal information from being compromised or misused[2]. They need to ensure that ATMs are safe to use and protected for malicious purposes (card skimming, credit/debit card fraud). Electronic security systems can help banks address these challenges, adding a useful layer of protection for the users, as well as at every step of the ATM management process – from replenishment and maintenance to continuously monitored operation. Adequately tailored systems can even help banks optimise ATM cash flows and the level of capital they have tied to their vaults by reducing the security risks associated with keeping higher amounts of cash in ATMs.

Reducing fraud-related costs

A high proportion of ATM-related fraud is estimated to be committed by organised crime and internal staff, and the cost of those incidents is getting higher for the industry. Beyond the cash losses is the effect heightened ATM security concerns have on insurance premiums, which impact directly on cash management costs. Implementing tighter security measures will reduce losses, and as a result insurance claims – and premiums.

Protect stand-alone ATMs

As an increasing number of ATMs are being installed away from branches, speed of intervention is critical, making constant monitoring a key success factor in protecting them from vandalism, theft and electronic or mechanical tampering. This supports cost-effective and speedy event responses whilst also providing reassurance to lone users.

Security systems from Siemens enable the simultaneous monitoring of many ATMs in real time from a single, central location. This gives ATM operators and banks more pro-activity – for example taking an ATM offline immediately if suspicious activity is detected. Seismic detectors, when fitted to ATMs, will provide immediate and reliable detection of attacks on the enclosure without any false alarm being generated by passing traffic or by the vibrations generated by the ATM operation. With faster, more reliable alarms, speed of intervention is improved whilst the risk of damage to ATMs is reduced. An additional layer of security can be added through video surveillance systems – acting both as a visual deterrent and providing useful evidential material – for example with day/night cameras from Siemens linked to a SISTORE MX digital recording system: live or recorded images can be tagged to alarms or ATM events, thereby documenting complete transactions – a useful evidential feature in case of disputes regarding cash withdrawals.

24h services at branches

The 24-hour availability of ATMs and deposit boxes inside branches calls for a minimum level of protection of both the users and the machines against theft and

Access control

Intrusion detection

Central controllers

SiPass Entro

The ATM zone functionality in SiPass Entro includes programming of card details and branch serial codes into the Entro software to enable door opening in 24h zones, as well as alarm control, Alarm Status Feedback (ASF) and SISTORE DVR integration. All event logs are encrypted for data security and can be securely exported for reporting purposes. The system also offers access groups, time schedules and zone definable functionality (anti-pass-back and interlock) and a centrally held database.

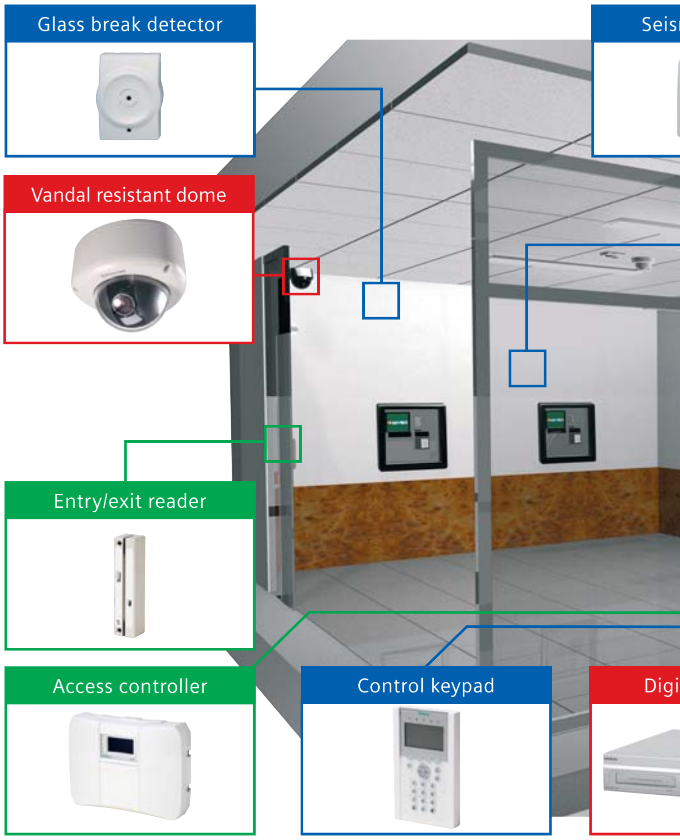
Intrunet SI120 or SI220

The Intrunet SI220 system can act as a l
or encompass multiple ATM zones. Ala
ously trigger video recording and be tr
with live video – to a monitoring centr
video alarm verification prior to interve
offers flexible, reliable alarm transmiss
ISDN with IP and GSM back-up) and ca
set/unset from the SiPass Entro access
scheduler facility.

Interoperability in action – 24-hour ATM zone

06h00 – The cash-in-transit (CIT) team arrives at the 24-hour ATM zone located on a busy high street, to proceed with cash replenishment ahead of the weekend. The ATM zone has its own local electronic security system, linked to an outsourced Alarm Receiving Centre (ARC). The CIT team enter using their personal card swiped at the reader at the entrance. Once inside, they block the door to prevent anyone from entering. All ATMs in the area (a mix of wall recess-mounted and free standing machines) are equipped with Intrunet seismic detectors. The motion detectors are automatically deactivated, at the same time triggering automatic recording via the SISTORE AX digital recorder. Live video images are sent to the ARC to ensure any suspicious event during replenishment is acted upon immediately.

12h30 – The bank's system which monitors all transactions made through the ATM network has flagged up an unusually high number of aborted transactions in the 24-hour zone. The ATM network manager contacts the ARC to access video footage from this location. The images recorded via the SISTORE AX, which interfaces to the ATM machines, enabling a quick access to events and search of the video footage relating to those aborted transactions. The team identifies the same individual using the ATM over the course of 2 hours.



Field devices

Swipe card readers
Connected to a SiPass Entro system to control access to 24-hour zones. The system can be programmed to recognise card data, allowing or refusing entry to the ATM zone.

Cash-in-transit services can be given a personal access card, with specific rights, which can be set to not unset the alarm system automatically. Instead, they would have to deactive the alarm using the alarm keypad, giving them the opportunity to enter a duress code and signal the alarm if forced to enter the ATM zone under duress.

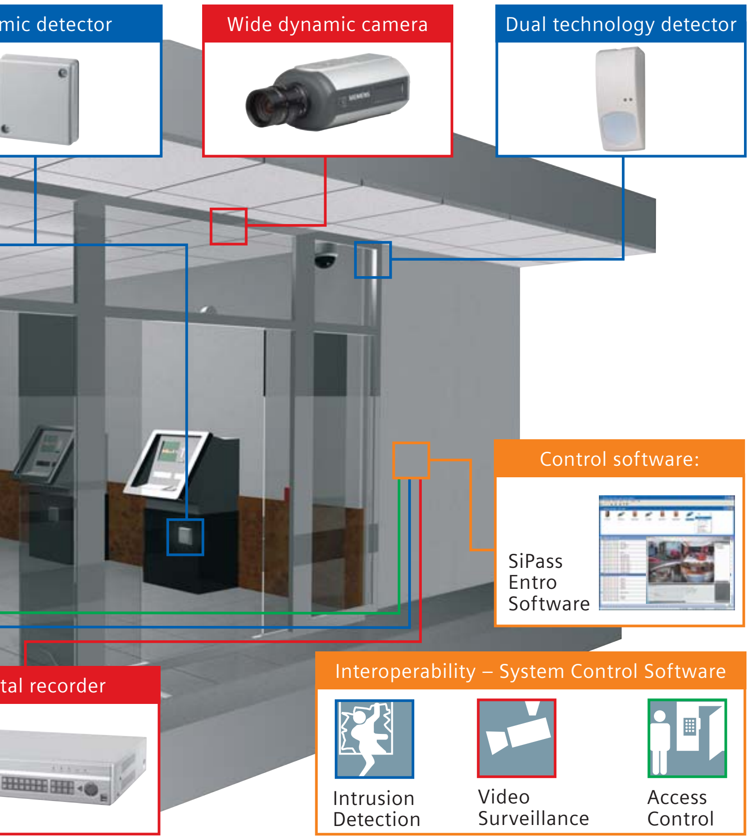
Motion detectors
Used to monitor movement inside the
ATM zone, and to detect any unauthorised entry. With multi-criteria signal
analysis for high immunity to false
alarms, and advanced mirror technologies for superior detection. Easy snap-i
installation concept for ease of installa-
tion and maintenance.

Seismic detectors
Positioned inside free standing ATM ma-
chines, directly in the wall structure nea
the machines or inside bollards positioned outside stand-alone ATMs. Alarm
are triggered as soon as an attack is detected, whilst environmental vibrations
passing traffic, ATM operational vibrations – are reliably ignored.

ocal alarm system,
rms can simultane-
ansmitted – along
e for audio and
ention. The system
ion (e.g. PSTN,
n automatically be
control system's

SISTORE AX

The SISTORE AX digital recording system offers direct connection to ATMs and up to 16 cameras. It can be controlled locally or over the network via the Remote Administration Software (RAS). The call-back functionality enables ARCs to receive alarm messages on event (alarms from Intrunet SI220 or access control events from SiPass Entro). For more advanced functionality, use SISTORE MX (BGV (UVV-Kassen)/Kalagate certified; programmable to read card details and tag video footage with transaction time/date).



The ATM is immediately taken off-line whilst investigation continues but remains under alarm and video surveillance – the police are also informed so personnel can be dispatched to the location if required.

15h00 – After review of the video footage, the police have confirmed that the individual caught on camera is a known repeat offender. A police patrol is dispatched on site to attempt arrest.

22h10 – The ARC receives an alarm originating from an ATM located at an unmanned petrol station. The ATM was sponsored by the same bank and is fitted with seismic detectors, which have now triggered an alarm. The area surrounding the ATM is also under video surveillance: day/night cameras are connected to the petrol station's SISTORE AX digital recording system, which is programmed to record every time ATM transactions take place, or if an alarm is triggered. The ARC operator simultaneously accesses live video images and pre-alarm recorded images via the SISTORE AX network viewing software to check the current situation on the site: There is damage to the wall on which the ATM is installed but by reviewing the pre-alarm recordings, he is able to establish that a car has reversed into the wall by accident and driven off. The ARC contacts the bank's ATM network manager so the ATM service provider can be called on site.

Glass break detector

The acoustic glass break detector is ideal for 24h zones with large glazed areas as they can be positioned up to 8.5 m away from the glass surface to be monitored, offering flexible positioning options.

Door and window contacts

Can be used to signify the opening of the door, simultaneously de-activating the PIR detectors inside the ATM zone, and triggering real-time recording from a SISTORE AX.

Cameras

High-resolution models ensure detailed information is captured.

- Wide dynamic models for bright areas such as facing entrances to ATM zones, for clear images both inside and looking at the outside.
- Day/night models in conjunction with infrared illumination for clear images 24 hours a day.

Vandal resistant domes

Positioned at the entrance of 24-hour zones or above stand-alone ATMs, they will provide the crisp images required to investigate suspicious events. IP66 they can withstand a blow up to 1000 kg.

TFT displays

With various sizes of screen and performance of display – suitable for in a control room or as public display monitors.

ATM replenishments can be made safer through remote monitoring.

tampering – with video surveillance, an alarm system and a means of restricting access to legitimate customers. A SiPass Entro Lite access controller, linked to an access reader on the door, can be used to read the bank card details and authorise – or not – entry to the 24h zone. Motion detectors, linked to an Intrunet SI220 intrusion system, are then deactivated once the entry is authorised, at the same time triggering automatic recording via a SISTORE AX (unless continuous recording is preferred). Through the use of IP-based video surveillance, the images can be transmitted back to a central control facility from where any suspicious activities can be monitored and investigated, either for an appropriate real-time response or for a follow-up in the event of an incident.

■ Extend security to sponsored ATMs

As financial institutions increasingly sponsor ATMs that are placed by independent commercial entities such as retailers or public transport organisations, ensuring adequate ATM security becomes a more complex challenge. However, banks can take best practices and due diligence a step further, by taking a more active role in ensuring that these ATMs benefit from the same level of protection as their own. A basic – yet efficient – system can start with seismic detectors, combined with a local SISTORE AX recording system, set to record continuously.

■ Ensuring safe ATMs replenishment

The increasing reliance on ATMs as a means of reducing operational costs has translated into the addition of more services obtainable through the machines, from cash remittance and deposits to mobile phone top-ups. Replenishment can therefore now take longer, moving from just cash-related operations to checking the ever more complex machine functions – potentially giving more time and opportunity for robbery. Video surveillance systems from Siemens can be set to record on events, for example when the enclosure is open for replenishment or maintenance, with live images streamed over an IP network to a monitoring centre, giving added protection to the replenishment process – and importantly, the staff undertaking this process.

■ Reducing operational costs at ATMs

Cash management is an essential part of managing the profitability of ATMs, and a difficult balancing act between optimal cash levels in ATMs and replenishment frequency – and costs. However, as cash is better protected within ATMs, a more optimal amount of cash can be kept in the ATM itself, therefore reducing the risk of downtime and the number of (costly) replenishments. This can also have a positive impact on insurance costs, as better security translates into reduced claims and premiums. Security systems from Siemens also support remote services, reducing the need for costly on-site visits for upgrades or maintenance purposes.

■ Tackling ATM ram-raids

Ram-raids – where an ATM is forcibly removed from its location to be broken into off-site – are showing an upward trend, and are increasingly conducted by well-organised crime gangs. While basic precautions can be taken to prevent ram-raids – by using concrete bollards, bolting the machines to the floor and keeping ATMs away from doors and windows – an alarm system incorporating seismic detectors will enable fast response and dispatch of intervention services. Coupled with video surveillance for evidence and investigation purposes, electronic security will increase the chance of catching the criminals and recovering the cash.

Highlights

- Optimise ATM operational costs thanks to reduced losses to frauds/attacks, better cash levels management and reduced insurance premiums
- Protect ATM users at all times with video surveillance
- Reduce the risk of ATM fraud with seismic detectors against mechanical tampering
- Identify suspicious patterns across ATM networks with networked video surveillance and seismic detection
- Optimise the chance of successful investigation and prosecution through event-driven video recording with complete transaction audit trail

[1] Source: ATM Industry Association (ATMIA)
[2] Cf. Gramm-Leach-Bliley Act

As a bank's most central channel, the role of the local branch is changing to maximise customer interaction and increase the return on investment. This now tends to involve putting more staff in advisory and selling roles to push cross-selling, redesigning and standardising the physical space across branches (with the risk of making it much simpler for organised criminals to plan and target multiple branches of the same bank), and opening up the working environment. As a result, members of staff are less protected by physical barriers against attacks by abusive customers – or robbers.

Electronic security can help compensate for the reduction in physical barriers in the public areas by making it harder to gain access to sensitive assets or data and making it easier and less risky for staff to raise the alarm.

For a more secure “retail” bank

Post-offices, local branches, currency exchanges.

For a safer “proximity” branch

Achieving the right balance between the security of customers and staff on the one hand, and convenience and competitiveness on the other, is the challenge facing financial institutions today. Banks are generally more at risk of attack during quieter periods – such as opening times – when staff numbers are low and fewer customers are present. Apart from established bank security procedures, adopting other "common sense" practices – such as limiting customer access, controlling staff access and locking interview rooms when not in use – is fundamental to a more secure banking environment. Through training, staff should be encouraged to remain alert at all times and to be on the lookout for suspicious or unusual behaviour. With these types of basic practices in place, electronic systems are the effective "final layer" of security – both during and outside business hours.

Improve risk containment in the branch

Bank branches should be separated into zones with clearly defined risks and control levels (see graphic overleaf): Public (areas that all employees and customers can access), controlled (areas that can and must be locked when unattended) and very controlled (where access is restricted to authorised users). This can be achieved through a combination of physical barriers (such as air locks) and electronic security: an interoperating system of video surveillance, access control and intrusion detection in areas of high risk allows bank managers or security staff to view any area whenever an alarm is triggered or a door opened, therefore enabling them to check the visitor's authority and progress throughout the branch. This can be complemented by automatic video recording for evidential or investigation purposes.

Protect staff at all times

The increasing use of open-plan office design to build relationships with customers also puts staff at greater risk. But the risks are not limited to robbery. Personal finance is potentially an emotive subject which can sometimes escalate to violence against staff. Video cameras from Siemens with wide dynamic technology will ensure crisp images even when facing a brightly-lit entrance, acting as a deterrent in the more public areas whilst providing useful evidential support should a prosecution follow any attack. Silent alarms at individual counters and in interview rooms, linked to a central monitoring centre or security room, will also provide valuable reassurance to staff and ensure immediate response to incidents.

Secure executive homes

The increase in the number of bank robberies where staff and their families are held hostage to gain access to the safe shows that implementing a security program which would encompass executive homes as part of the bank's own security system could also make the difference between early and appropriate intervention or successful robbery. An intrusion detection system incorporating silent alarms and triggering live video streaming to a monitoring station will ensure that no such situation goes unnoticed until it is too late, and will provide valuable support to police forces during the intervention phase.

Access control

Intrusion detection

Central controllers

SiPass integrated

This scalable system provides seamless role-based access control between the defined branch risk zones, e.g.: door interlocking enables the creation of man traps or airlocks between the public and mixed areas; with escort control, 2 valid cards must be presented at the door before it can be unlocked; Records of entries/exits enable visitors to be accounted for at all times; elevator control restricts access to staff-only floors. The system also offers powerful reporting tools.

Intrunet SI220

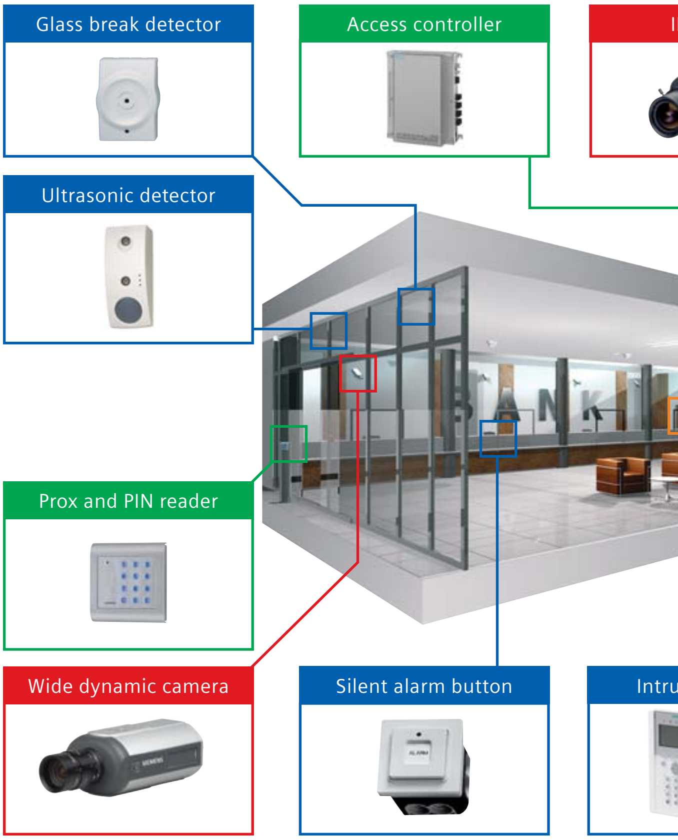
With versatile alarm transmission mod
for local intrusion detection with remo
offers: activation/deactivation on badg
cards (SiPass integrated) with simultan
ing (SISTORE MX); independent alarm
for each branch security zone based or
business requirements; alarm triggered
transmission to the ARC for alarm verif
taneous access rights changes to other

Interoperability in action – town centre branch

07h30, Monday morning – The cash-in-transit van arrives with the internal mail and the amount of foreign currency pre-ordered for the day. Respecting the red/green "traffic light" system which indicates the integrity of the security systems, the security guards open the front door, drop sacks delivered and resecure the front door. Their arrival is recorded through external cameras linked to a SISTORE MX digital recording system; their opening of the front door de-activates the Intrunet SI220 alarm system in the area, simultaneously triggering real-time video recording via internal cameras until the front door is resecured. "Traffic light" system again shows "green" to indicate all is well within branch, and the security system is fully reinstated.

08h00 – The bank manager arrives alone and – seeing green security light – opens front door by badging his access card and entering his own PIN code using a SiPass Prox & PIN access reader. This deactivates the intruder alarm and the "traffic light" system. An audible alarm sounds, indicating that the alarm system in the safe and strong room is still armed.

08h30 – While staff prepare for the day's business, two designated key holders access the safe area using their personal proximity card and PIN number, at the same time deactivating the motion detection system in the area. The safe's integrity is continuously monitored via seismic detectors, which can detect electronic/mechanical tampering.



Field devices

Proximity and PIN reader
Robust design and metal casing design and metal casing for vandal resistance. Ideal for use at staff entrances.

Models for indoor use also include a duress functionality.

Smart card technology
Enables physical access rights to be combined with logical access via digital authentication and single sign on to HR databases and directories, sales reporting, procurement systems, process documentation of loans/mortgages, etc.

Motion detectors
Used to monitor the various zones insid
a branch, from the ATM zone to customer and staff areas or offices, safes, etc. With multi-criteria signal analysis fo
high immunity to false alarms, and clever mirror technologies for superior detection.

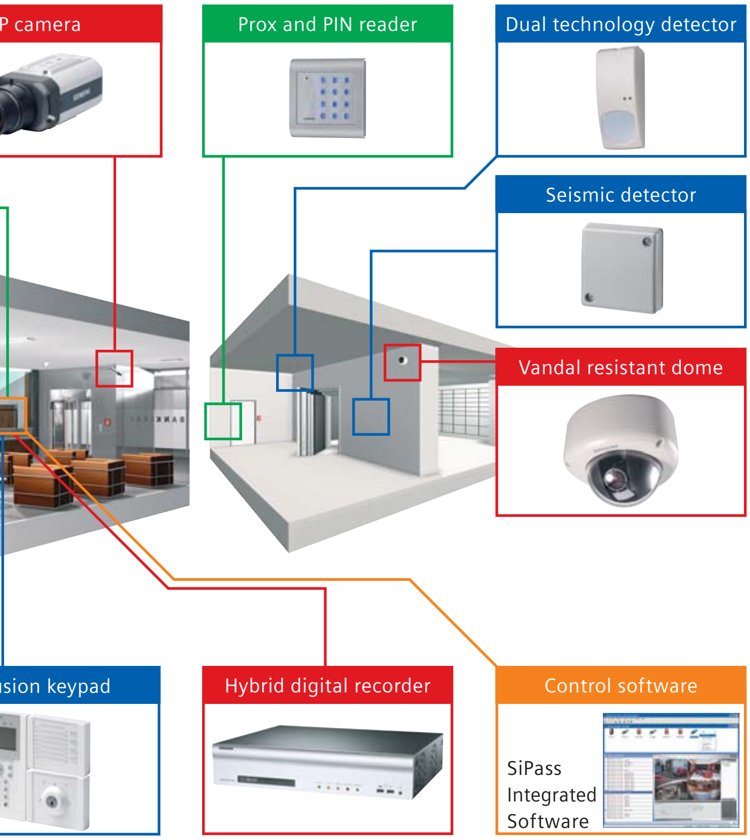
Seismic detectors
Positioned inside ATMs, or directly in the wall structure near the machines or
vaults. Alarms are triggered as soon as an attack on the machine or wall is detected, whilst environmental vibrations – opening of the vault's door, ATM opera
tional vibrations – are reliably ignored.

Video surveillance

es, SI220 is ideal
te monitoring. It
ing of authorised
neous video record-
actuation/settings
n risk scenarios and
d video recording/
ication and simul-
r areas.

SISTORE MX

BGV (UVV Kassen)/Kalagate certified, this hybrid video recorder can adapt to bandwidth restrictions in support to other critical banking systems, and can read details of cards used to access ATM zones: event images are tagged with transaction data/time/date (15 minutes pre-/post-event recording). The event "logbook" is saved in a central, secure database. Enables access/intrusion event driven real-time recording on IP/analogue cameras, and hardware/software based network recording (resp. SISTORE MX NVR/NVS).



09h00 – The bank opens. The video surveillance system records continuously throughout the premises. Staff enter the interview rooms by badging their personal access cards to proximity readers. This simultaneously disables the motion detectors in the room, switches the lights on and triggers live video recording (potential evidence).

13h30 – A customer claims he tried to withdraw cash from the ATM and was issued a receipt but no cash. With the SISTORE MX DVR, the bank manager reviews the video footage tagged with the relevant transaction data, thereby confirming that the cash had not been dispensed. An engineer is called on site to investigate the problem.

15h00 – The assistant manager notices the growing numbers of queuing customers via the video surveillance system. To reduce waiting times and free up counters for complex transactions, he sends staff to redirect customers needing simple transactions to ATMs and guide them through the self-service options.

17h00 – Closing time. CIT staff arrive to transfer the cash accumulated during trading. Video surveillance systems cover all their time on bank premises. The safe is then locked and the alarm activated in the area. The manager locks the front door. All security systems are activated ("traffic light" system shows green).

e

or

a-

Silent alarms
The Intrunet hold-up foot rails and contacts enable a discreet alarm actuation. They can also be used to activate cameras.

Door and window contacts
These will alert staff closing the branch to any window or door left open, and will send an alarm should someone forcably open a door or window to break in.

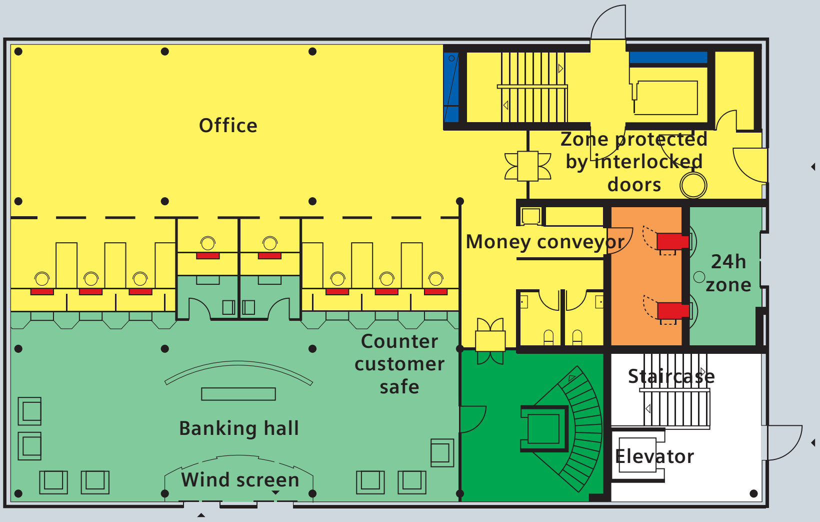
Cameras
High-resolution models, to monitor till lines, queuing systems and reception/enquiries desks, or near entrance areas to monitor customers exiting from the branch.

- Wide dynamic models for bright areas povide clear images both inside and looking at the outside.
- Day/night models in conjunction with infrared illumination for clear images 24 hours a day.
- IP models for true digital transmission of streaming images.

Vandal resistant domes
For the monitoring of all building elevations, external fire exit doors, entrance points to the building and car parks/barriers. IP66 they can withstand a blow up to 1000 kg.

Speed domes
Can be moved with the utmost precision. Up to 36x optical zoom and 400°/sec preset speed.

TFT displays
With various sizes of screen and performance of display – suitable for in a control room or as public display monitors.



Examples of security zones

- □ Publicly accessible zone
- 🟩 Customer zone
- 🟩 Controlled customer zone
- 🟨 General staff areas
- 🟦 Vital technical installations
- 🟧 Sensitive staff area
- 🟥 Highest security area

Protect valuable assets and data

Banks hold not just valuable cash, but also data and data storage devices, which, if removed from the premises will turn into a lucrative business for the criminals. Protecting access to offices and data rooms is therefore critical at branch level. "Prox & PIN" access readers positioned at strategic entrances will prevent unauthorised access to the areas, with attempts at forcible entry automatically triggering an alarm and video recording. Tags fitted to sensitive data storage devices, and linked to the access control system, can trigger an alarm if they are removed from the building without authorisation.

Secure safes and deposit boxes

To protect safes and deposit boxes, access control readers at entrances will stop members of the public accessing controlled areas. The wide range of readers from Siemens includes "Prox & PIN" models with 'duress' code functionality (for instance when a member of staff is coerced to enter an area under threat). Seismic detectors fitted to safes and deposit boxes will trigger an alarm if forcible removal or access is attempted (particularly suitable for unmanned self-service deposit boxes, which make it possible for thieves to rent a box for the sole purpose of gaining easy access to the vault). This can be complemented with video surveillance for enhanced monitoring, with real-time video recording of images throughout the trading period and live recording on alarm after hours.

Reduce cash-in-transit risks

Cash-in-transit services remain a prime target for robbers. Significant investments have been made to make the actual journey much safer, and this has shifted the focus towards the actual cash handover point – in the bank itself. Conducting cash delivery or collection in the public area of banks, building societies and post offices also causes a degree of risk to public and staff safety. It is therefore essential that cash exchanges take place in secure areas (access controlled and fitted with video surveillance and alarms) or at times when no member of the public is present.

Increase compliance through security

More sophisticated security functionality can also contribute to compliance, enhancing transaction trail auditing by providing more advanced access control or alarm event reporting, and backed up with video recordings with time and date. For example, a recording system, linked to the bank's ATM system, can be set to record on certain conditions, e.g. if the card swiped to enter a 24h ATM zone is identified as being blocked or stolen. The video is then tagged and linked to the suspicious transactions, with pre- and post-event images also recorded.

Maximise sales opportunities

Security systems inside the premises should support both intervention and investigative activities, and raising the alarm should be easy and inconspicuous to prevent violent or panic reactions. By implementing interoperable security systems, local branches can strengthen well established bank security processes with a centralised – even remote – overview and control of all the security functionality and areas. This enables routine or incident scenarios to be translated into logical action/reaction between the access control, intrusion detection and video surveillance systems. Tighter security makes the branch less attractive to criminals: the resulting banking environment is safer for staff and customers, and therefore more conducive to fruitful business transactions.

Highlights

- Turn branches into true "sales centres" by lightening the security burden for staff
- Enhance the customer's experience with a safer banking environment
- Reduce the risk of identity fraud at branch with physical data protection and verification tools
- Address higher risk areas with interoperating systems for the control of access, video monitoring and alarming
- Increase compliance with data protection and due diligence requirements

To achieve greater competitiveness on a national or even global level, banks need the flexibility to implement company-wide business models that will optimise their margin levels and turnover. Whilst channel diversification is a key success factor, the challenges this brings for banks are multifold – from consolidating payment channels whilst ensuring compliance across ever more complex networks of ATMs, branches, data centres and headquarters to promoting business intelligence sharing, and streamlining systems and processes.

Interoperable security systems support more efficient enterprise-wide risk management strategies (ERM), by enabling banks to reduce the complexity of their processes and systems, at the same time facilitating an enterprise view of security across entire networks.

Enterprise level security, compliance and global competitiveness

National and global bank networks, data centres, bank headquarters, national gold reserves, central bank hubs.

Enterprise level security

In support to successful bank ERM strategies, security risks ought to be managed as a single end-to-end topic. Interoperable access control, intrusion detection, and video surveillance systems provide the tools to manage, monitor and report security risks and events as required by the legal framework. They can provide the sophisticated security functionality required to reduce losses stemming from the operational risks defined in the Basel II accord, at all levels of the service delivery channels network. They provide a central security platform for both company wide policies and the locally managed specific security issues pertaining to each channel.

Support payment consolidation through improved data security

Continuing competitive pressures are leading financial institutions to work towards consolidating payments to reduce handling costs. But with these payment "hubs" – infrastructures that are capable of processing payment from multiple channels – there is a growing potential for unauthorised access to even larger amounts of sensitive data for the purpose of manipulating, stealing or even destroying it. With increasingly stringent regulatory requirements, such as the Gramm-Leach-Bliley or Sarbane Oxley Acts, data centres should therefore be treated as high security buildings, and can therefore greatly benefit from interoperable systems. Applying a role-based access management to payment and data centres, is best achieved with centrally managed access rights as this ensures up-to-date access authorisation at all times for legitimate staff. Access events can be backed up with live or recorded visual verification of a person's identity on badging through video surveillance systems, whilst interoperation with alarm systems will enable the alert to be given should access to a restricted area be attempted by an unauthorised user.

Role-based access management

Tight access control to information and the systems holding them is a complex matter in a global banking world where the consolidation of the core systems used to manage the varied operational channels has only just started. Access control systems from Siemens can offer a "one card" answer for financial institutions that have locations nationwide or even worldwide. Instead of multiple cards or ID badges that would normally be needed to perform multiple functions (e.g. entry in building or electronic signatures) one card includes all these services.

Access control

Intrusion detection

Interoperable controllers

SiPass integrated

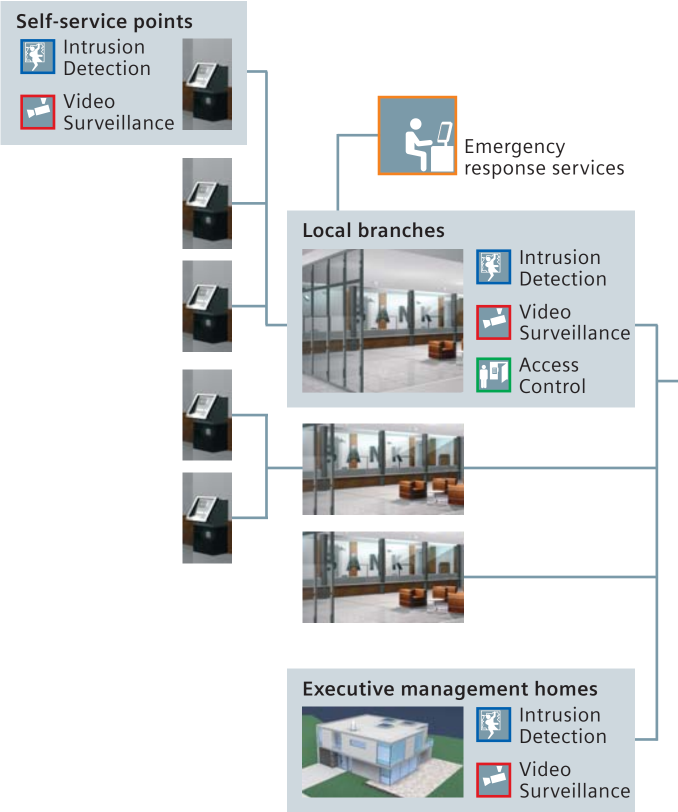
A true backbone for enterprise applications: distributed architecture for central/local event management, cardholder enrollment, data authentication and encryption, reporting and configuration changes; "One card" concept with role-based access to offices, IT networks/applications; anti-passback; visual verification; elevator control; HR system integration (LDAP compliance); overview of all access/alarm events with video footage back-up, accessible from SiPass software; full system archiving/restoration.

Intrunet SI410

This scalable system facilitates centrali ment over standard communication ch back-up for reliable transmission. Indivi can be programmed based on zones/ris port for alarm type specific interventio access control "duress" events). Its Mac remote standardised updates of securit multiple sites provides a cost-effective personnel codes are up to date.

Interoperability in action – national bank network

A large bank has implemented a new nationwide security system to bring all local systems under one uniform and common standard. The objective is to reduce the costs of security systems themselves, but also to close any security gaps, particularly with data access and reporting capability. Central to the system is role-based access management, supported by a SiPass integrated access control system, which integrates into the bank's standard IT environment and HR database applications. The system is configured to work across the bank's corporate domain, ensuring the network integrity is not compromised. The system forms the basis of an enterprise wide interoperable security system – also including Intrunet SI410 intrusion detection system and SISTORE CX video codec recording – from which all security functionality can be managed and controlled. The entire bank network is in turn linked to an MM8000 Danger Management System, which facilitates the management of data from various sub-systems, including fire detection systems.
The SiPass integrated system manages the access rights and cardholder data of over 3000 staff from the bank's central security and safety hub located at it's general headquarters. The one card concept supported by SiPass integrated (combining physical access rights and digital sign-on) has been implemented in all sites: changes to access management policies can now be rolled out automatically, ensuring consistent access restrictions to sensitive areas,

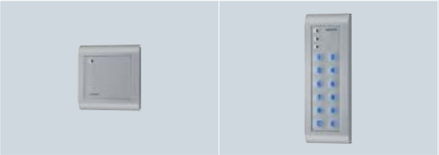


Field devices

Proximity and PIN reader with a robust design and metal casing for vandal resistance.

Proximity readers
Ideal for controlling access to doors in offices.

Smart card technology
Enables physical access rights to be combined with logical access via digital authentication and single sign on to HR databases and directories, sales reporting, procurement systems, process documentation of loans/mortgages, etc.



External motion detectors
Siemens external motion detectors enable an alarm to be triggered as soon a intruders set foot on restricted outdoor areas, allowing for intervention to take place before access to critical areas or assets has been gained.

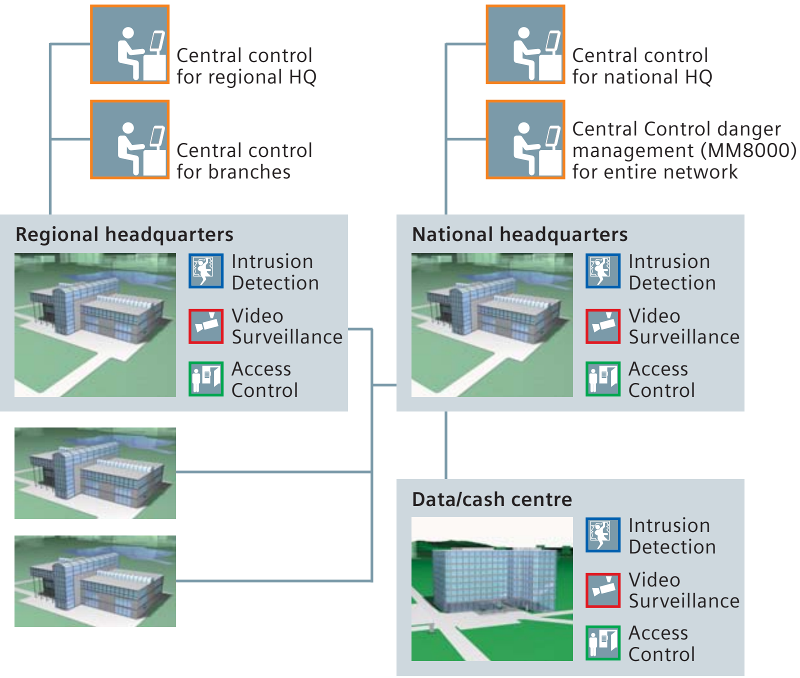
Internal motion detectors
The range of Siemens internal motion detectors caters for all bank environments: from 24-hour zones to retail branches and data centres.

The range covers requirements for all grades of risk areas, and offers the highest detection rate and false alarm immunity.

sed alarm manage-
annels with IP/GSM
dual security settings
sk levels, with sup-
n procedures (e.g.
cro functionality for
ty settings across
way of ensuring all

SISTORE CX

Kalagate certified, this codec recorder supports distributed systems e.g. a unit per branch or building – all connected to a central control room, and provides: fast transmission/streaming of the highest quality video, centralised storage of recordings for secure archiving (NAS); bandwidth management tools; advanced search functionality (addressing legal requirements to report security events with supporting information); back-up of business critical security data; perimeter surveillance capability (SISTORE CX EDS/ODR).



business data or applications across all sites and employees. In line with security breaches reporting requirements, any suspicious event flagged up in local systems can also be accessed, managed and reported both locally and in the central SiPass database.
Similarly, the Intrunet SI410 Macro functionality enables consistent alarm settings across all sites, with for example safes being set in all branches under constant alarm monitoring, with bypass only accessible to authorised holders of special codes. Specific event types can also be defined to trigger video recording or alarm activation/deactivation based on established business scenarios and risk levels that are common to all sites. The SISTORE CX codec recording system enables the centralised management of local video recorders in branches through its virtual matrix functionality. This enables locally recorded critical event footage to be centrally and securely archived away from the branch. All sites are equipped with SISTORE CX EDS for outdoor video motion detection and SISTORE CX ODR to e.g. detect any unauthorised parking in front of bank branches.

The SiPass software provides a central control point for all security functionality, enabling remote access to local intrusion event log or to conduct live viewing, playback and recording of images based on access or intrusion events, overlaid on user-friendly graphical site maps.

ns
r
e

Secure intrusion keypad
The stylish keypad enables quick and simple multi-partition operation. Key switch and annunciation modules offer additional security levels and parallel partition indication and operation, as well as unique tamper detection concepts.

Super high-resolution cameras
Offering the highest detailed images for evidential use, the range of super high-resolution models are ideal for the monitoring of main entrance points to each floor, lifts, lobbies and staircase/fire exits.

Vandal resistant domes
For the monitoring of all elevations of the buildings, external fire exit doors, all entrance points to the building and car parks/barriers. IP66 they can withstand a blow up to 1000 kg.

TFT/LCD displays
Typically used to create "video walls" for use in a control room the range of security TFT displays offers features such as anti-glare security glass.

Control keyboards
Able to control both the digital recording system and speed domes, the CKA range of keyboards offers ease of control and flexibility particularly when using the variable proportional joystick.

In a SOX and Basel II context, this ensures that identity and access rights are up to date and traceable – and that security breaches are reportable at all times.

Replicate security best-practices

Interoperable systems provide the means to access and manage intrusion detection, access control and video surveillance data and processes centrally, thereby facilitating the implementation of streamlined security measures and procedures. This also enables best practices to be identified and shared throughout the network. With all the security data collected centrally and easily retrievable, a bank can keep an ongoing watch on all its activities within – and across – sales channels. This translates into more efficient bank channel integration, ensuring that all channels are communicating with one another and seamlessly sharing security-related information, so tracking of suspicious account activity and cash can occur simultaneously, raising red flags if something goes wrong.

Protect IT and data networks integrity

IT integration sits high on banking institutions' strategic agendas, in the search for more efficient and transparent ways of managing and protecting data and business processes. Compliance requirements have permeated to IT networks used by financial institutions, calling for secured back-up of critical data for example. Interoperable security systems from Siemens can sit on their own network, ensuring they will not compromise the network integrity. In addition, they deliver sophisticated reporting tools, which allow for event logs and recorded video to be exported over secure connection to centralised data centres, away from the branch.

The compliance success factor

Interoperable security systems, by providing banks with an enterprise level view of all security-related matters, can contribute to improve compliance levels, on the one hand by helping to prevent cardholders' financial and personal information from being compromised or misused, and on the other, by providing the tools to implement a successful role-based access management to sensitive data or assets. More specifically, in a context where banks are legally required to fully disclose all events that are material to the business and report all security breaches (Basel II third pillar) being able to back-up transaction data with authenticated video recordings and access and alarm event reporting brings significant advantages from an auditing process perspective.

Security in support to business intelligence

With centralised monitoring of sites, and integration into a bank's operational systems, bank headquarters can achieve better understanding of their "proximity" businesses (be it ATMs or branches), thereby improving the efficiency of their network. On a national scale, the added visibility brought about by interoperable systems also enables a more efficient staff deployment across multiple branches, based, for example, on changing business activity levels in branches, or the need to transfer skilled staff to other sites for cross-training purposes.

Highlights

- Harmonised security concept across entire bank network improves the efficiency of security strategy and reduces the total cost of system ownership
- Certified products and systems contribute to better insurance compliance
- Understand and react to security breaches more readily with holistic approach to security
- Common security user interface facilitates cost-effective staff deployment across multiple branches
- Protect IT network integrity with certified electronic security systems

Siemens has won one of the largest security contracts in Norway – a complete security and services solution agreement with SpareBank1, an alliance of 23 banks and 350 offices that together make one of the largest providers of financial products and services in the Norwegian market with 460 branches.

The bank wanted a fail-safe and sophisticated security solution with a central system operation and maintenance that involves the upgrading of video surveillance, intrusion detection and access control systems – and therefore provides increased security against unauthorised access and criminal activities – in all 460 branches.

Case study: Siemens improves security for SpareBank1 across 460 branches

Highlights

- 333x SISTORE digital video recorders (SISTORE MX with 2 TB hard drives for all branches, and SISTORE AX4 Lite for most of the ATM machines)
- Replacement of 1,385 cameras with Siemens models
- 420x Intrunet SI410/SI220 intrusion panels securing most branches and 2,236 motion detectors from Siemens
- 1,300 doors across all branches secured by SiPass integrated access control systems and readers

The challenge

Each of the 23 member banks – which together constitute one of the most familiar names in the Norwegian financial market – ran their own security systems and services locally. Although the alliance's main goal was to ensure the individual banks' independence and local connections, the objective of the agreement was to create a mutually binding co-operation between the partners within the security operation, focusing on security levels, cost optimisation and the development of predictable security levels and services throughout the alliance.

The answer

All branches within the bank network will have video surveillance and intrusion alarm systems installed, with the majority of the branches also supplementing their security measures with access control. A centralised access control system utilising operational services (with server hosting at Siemens' MARC station for 23 branches), is also being specified.

The alarm management services respond to all types of alarms (both life-threatening and everyday events), thereby contributing to business continuity, crime prevention, staff safety and, ultimately, providing peace of mind. The centre will manage information from all locations, offer support on technical questions, receive service calls and remotely manage the security systems.

The result

Key to the requirements was the implementation of an interoperable security system that is capable of working together to deliver the required security levels. This enables the control of the various security functionalities (access control, intrusion detection, video surveillance, alarm management) from one central point. For example, whenever events trigger access or intrusion alerts, video recording will start and live images will be received to provide verification at the MARC from where, if necessary, intervention forces will be alerted. In rerouting existing alarm transmission to the MARC, several areas for improvement in the customer's existing system were identified, all of which have been addressed by the new system.

Systems overview

	Access control		Intruder detection		Video surveillance		Remote monitoring
Self-service area		**SiPass Entro Lite** Up to 8 doors/1,000 cardholders **SiPass Entro** Up to 512 doors/40,000 cardholders Both systems provide a bank lobby function (white list) that uses the customers' bank cards to provide access to the self-service area.		**Intrunet SI120** 2 partitions/12 rooms **Intrunet SI220** 6 partitions/36 rooms Both systems provide flexible alarm transmission and verification		**SISTORE AX** – Local operation – Generic ATM interface – Event callback	Via Alarm Receiving Centre
Retail bank (local branch)		**SiPass Entro** – Easy integration with video surveillance/intrusion systems – Multi-site concept – Easy software maintenance via terminal server support **SiPass integrated** – For system expansion from SiPass Entro – For larger retail banks		**Intrunet SI220** – SMS event messaging – Supports audio and video alarm verification		**SISTORE MX** – Hybrid recording – Support of main ATM interfaces – Event callback	Own or outsourced control room
Global organisation (headquarter offices)		**SiPass integrated** – Virtually unlimited number of doors/cardholders – Mutiple workstations – Visitor management – Integrates with HR databases – High security bank features: duress codes, dual custody and integration of biometric identification		**Intrunet SI410** – 16 partitions/128 rooms – Easy system customisation for banks – Highly scalable – Fully networkable – Flexible alarm transmission and verification – SMS event messaging		**SISTORE CX** – Hybrid recording – Virtual matrix for centralised operation – Out-/indoor video analytics surveillance – Event callback with alarm picture	Own or out-sourced control room (SiPass integrated, MM8000 DMS or IVM danger/video manage-ment)
Field devices		**Magnetic stripe readers** (with or without keypads)		**External PIR motion detectors** (perimeter surveillance with alarm triggered video recording)		**Indoor "All in one" camera** – BGV-approved	
		Proximity readers (with or without keypads)		**Internal motion detectors** (wired or wireless. For ATM zones, counters, back-offices, safe areas, etc.)	 	**High-resolution analogue and IP cameras** **Vandal resistant domes**	
		Hands-free Cotag readers		**Seismic detectors** (safes, vaults or ATMs protection)		**TFT/LCD displays**	
		Smart card readers (with or without keypads)		**Glass break detectors** (wired or wireless)		**Control keyboards** (control virtual matrix via IVM)	
				Door/window contacts (wired or wireless)			

* The information contained in this table is only meant as a guide. Other combinations are possible.

Answers for infrastructure.

Megatrends driving the future
The megatrends – demographic change, urbanization, climate change and globalization – are shaping the world today. These have an unprecedented impact on our lives and on vital sectors of our economy.

Innovative technologies to answer the associated toughest questions
Throughout a 160-year history of proven research and engineering talent, with more than 50,000 active patents, Siemens has continuously provided its customers with innovations in the areas of healthcare, energy, industry and infrastructure – globally and locally.

Increase productivity and efficiency through complete building life cycle management
Building Technologies offers intelligent integrated solutions for industry, commercial and residential buildings and public infrastructure. Over the entire facility's life cycle, our comprehensive and environmentally conscious portfolio of products, systems, solutions and services in the fields of electrical installation technology, building automation, fire safety and electronic security, ensures the:

- optimum comfort and highest energy efficiency in buildings,
- safety and security for people, processes and assets,
- increased business productivity.

Siemens Switzerland Ltd
Industry Sector
Building Technologies Division
International Headquarters
Gubelstrasse 22
6301 Zug
Switzerland
Tel +41 41 724 24 24

Siemens Ltd
Industry Sector
Building Technologies Division
Units 1006-10
10/F, China Resources Building
26 Harbour Road
Wanchai
Hong Kong
Tel +852 2870 7888

Siemens Pte Ltd
Industry Sector
Building Technologies Division
The Siemens Center
60 MacPherson Road
348615
Singapore
Tel +65 6490 6000

Siemens plc
Industry Sector
Building Technologies Division
Brecon House
Llantarnam Park
Cwmbran
NP44 3AB
United Kingdom
Tel +44 871 386 0800

The information in this document contains general descriptions of technical options available, which do not always have to be present in individual cases. The required features should therefore be specified in each individual case at the time of closing the contract.

www.siemens.com/banksecurity