Technology Trends in Access Control

This year's ISC West conference gives an indication of some of the broader trends taking place in the industry.
Manufacturers appear to be focussing on a variety of different technologies to help make the user's experience with the access system more seamless than ever.

Trends

Use of access control across the enterprise

In the past, access control was often restricted to the perimeter of the building. We are now seeing the deployment of access control systems across the Enterprise. In some cases levels of access are used to restrict access to some and to better protect their entire business.

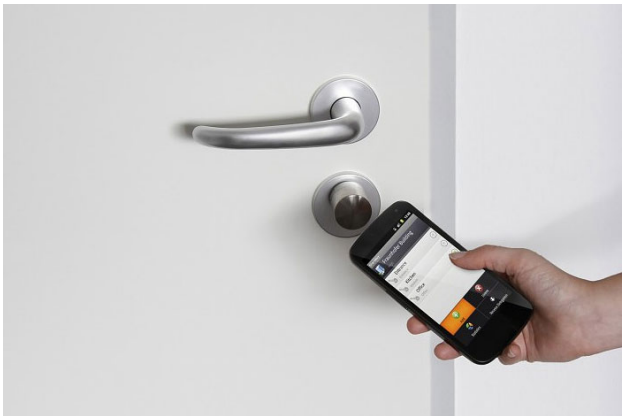
Offline locks with more aesthetic designs and form factors

The Industry is seeing a significant change in the form factor and design of the locks. This has become necessary with the use of such locks across the Enterprise. The lock has to look smart and yet be effective

Evolution from plastic credential to mobile credentials

Use of mobile phone or some sort of active device is gaining in popularity.

Growing interest in wireless and IP-based solutions.

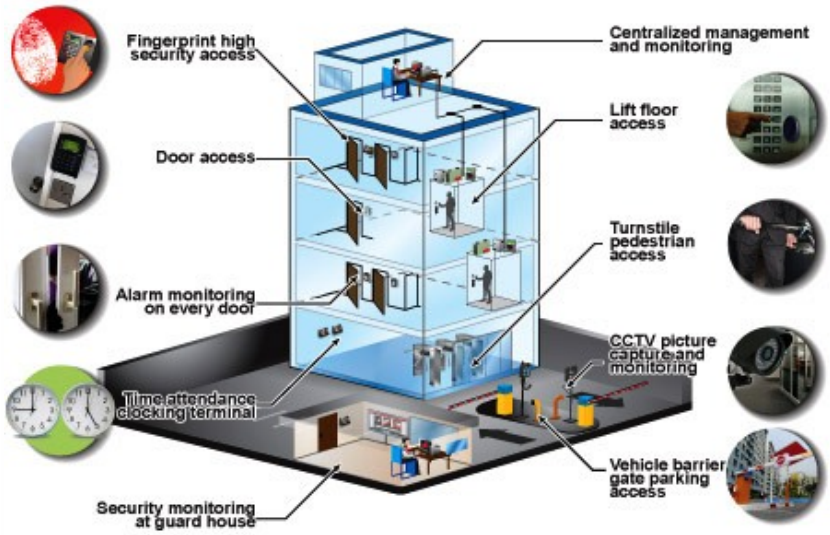


Organizations are seeing greater value in wireless technologies and also the use of IP.
The future is IP.

Access control is now considered in the project design stages

It is being considered right at the beginning when it is still in the design stages. The approach has shifted from what used to be 'let's build the building and then let's think about adding access control later.'

Integration between access control and the NVR system and other building systems is becoming more and more common.



Integration between access control and the NVR system and other building systems is becoming more and more common. It enhances security reaction times – for instance if a door is forced the combined system will sound an alarm, lock-down key areas and direct the security team to the location of the potential incursion.
Organizations have recognised the ability of integrated systems to intelligently provide access. Integrated security makes workforce management much more efficient. It makes it possible to manage working hours, to activate building services only when they are needed (and thus saving energy and resources). **Integration is providing intelligent solutions that will save money.**

Distributed functionality remains a necessity for larger system deployments to be effective.

Distributed system architecture having regional control with properly distributed functionality continues to be a necessity for larger system deployments to be effective.

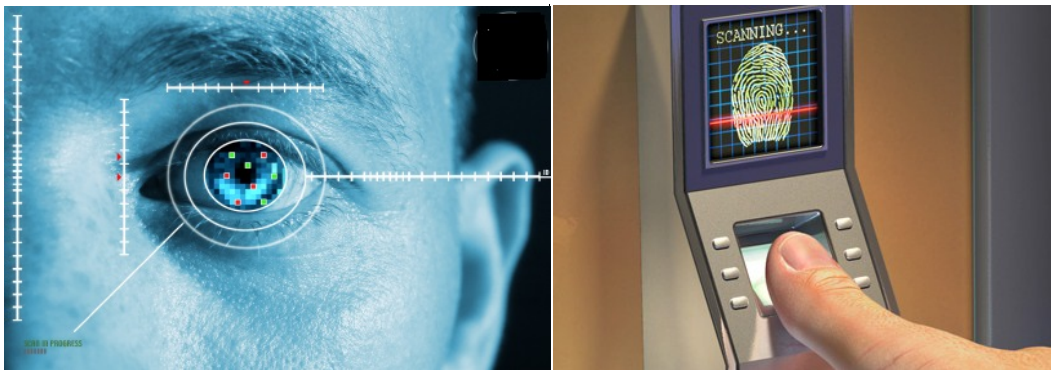
Private labelling of credentials

Enterprises are increasingly using own label credentials i.e. access cards with private labels, logos etc. Some Organizations put a URL or a website on a credential, sometimes their corporate name or maybe even a symbol indicating what level card it is versus another card.

Blurring of boundaries between physical and logical access control

Organisations are moving towards providing physical access control system (PACS) and IT identities on a single card that can be used to open doors and log on to computers. This creates a seamless user experience. Individuals can easily create, use and manage identities across many different applications on both smart cards and smart-phones. Users will soon be able to carry many types of access control credentials as well as one-time password (OTP) tokens on a single microprocessor-based smart card or smart-phone. Such integration will improve efficiency through centralisation of credential management for multiple logical and physical access control identities across IT resources and facilities.

More organizations are seeking biometric authentication



More and more, organizations want to have biometric authentication. Biometrics is finding greater acceptance as the quality and accuracy of biometrics has rapidly improved in recent years. Fingerprint readers and facial recognition systems are now widely accepted. Advances in biometrics will result in the deployment of more complicated systems such as palm vein and heartbeat recognition readers.

Move to Interoperable Platforms Based on Open Standards.

Organizations are increasingly demanding more open and secure architectures. They want to ensure that the organisation's access control solution can adapt to future threats and take advantage of opportunities and applications beyond mere access control. The goal is to deploy a fully interoperable, multilayered security solution across company systems and facilities. By using solutions that are based on industry standards such as OSDP (**O**pen **S**upervised **D**evice **P**rotocol) bidirectional communications, and incorporating dynamic rather than static technologies, security becomes independent of hardware and media and the infrastructure can more easily evolve beyond current abilities and also have the adaptability to combat continuously changing threats.

Conclusion

As new and evolving access control technologies continue to deliver improvements in performance, efficiency and cost-effectiveness, the potential applications for these systems are expanding far beyond their traditional deployments.

In particular, networked and software-based solutions have had a significant impact on the growing role of access control systems in security, as well as other areas.

Further, enhanced features and functionality make it possible for dealers and integrators to provide end users with highly advanced systems that improve security and contribute to operational goals.
