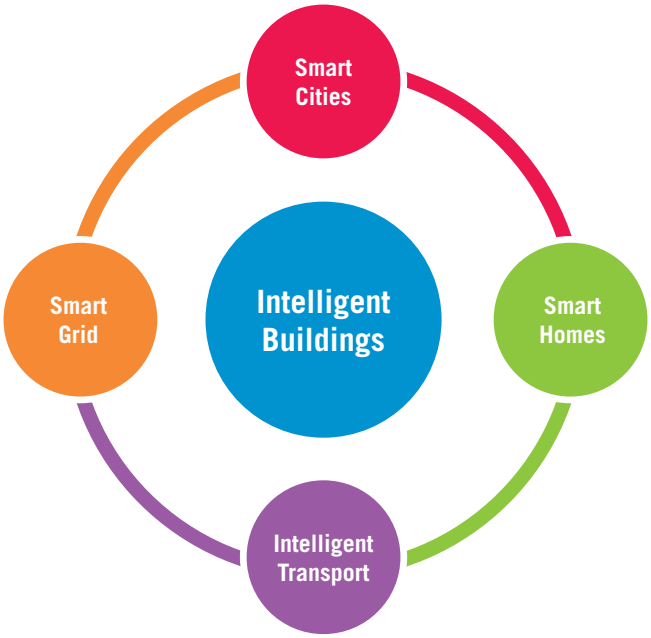
The Institution of Engineering and Technology

Intelligent Buildings: Understanding and managing the security risks

More efficient and cost-effective use of the built environment is increasingly being driven by economic and environmental pressures requiring reduction of the cost of ownership and operation of commercial and public buildings. The emerging solution to these pressures is the creation of innovative IT-enabled solutions, as shown in Figure 1.

> "Security should be an integral part of the design of intelligent buildings and not an afterthought."

Figure 1: Intelligent buildings are part of an increasingly integrated built environment



Information & Communications

Built Environment

www.theiet.org/sectors

The benefits of an intelligent building potentially include energy savings, reducing the cost of changing occupancy and configuration (churn), maintaining a comfortable, safe and secure environment, and improving user productivity.

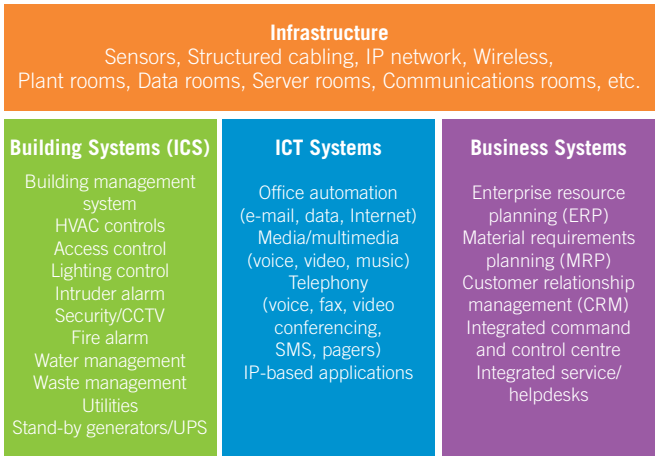
This, in a world where our technology is under threat from a variety of sources and any IT system is potentially at risk, regardless of whether it is stand-alone or part of an integrated system, means the deployment of these innovative solutions is not without risk. We need to recognise that intelligent buildings are complex systems and put in place appropriate practices to ensure the safety and security of the buildings' users.

This document forms the basis of a programme initiated by the Institution of Engineering and Technology (IET). It examines the issues related to the increasing automation and integration of building systems, identifying a number of steps that may be taken to ensure that benefits offered by intelligent buildings are not offset by the risks potentially inherent in their design and operation.

What is an intelligent building?

Whilst the precise definitions vary around the world, a common theme is the integration of technologies. For the purpose of this document we define an intelligent building as one where the combination of technologies and interconnected systems supports the use of the accommodation by the building's users, enables the efficient operation of the building and enables reconfiguration of the space in response to changing use. Intelligent buildings may also be referred to as smart buildings. The systems which may be integrated in an intelligent building are illustrated in Figure 2.

Figure 2: Systems which may be integrated in an intelligent building



What advantages do they offer?

From an IT perspective it is this integrated use of systems and technologies which delivers the commercial advantage. For example, the convergence of the network infrastructure enables the flexible use of accommodation, and operational efficiencies arise from the integration of systems which support or manage the building environment, space, and operational systems.

The infrastructure convergence is typically achieved through the use of a common cabling and/or wireless infrastructure, supporting IP-based networks within the building. Thus the building management systems (BMS) will typically use an open protocol running over an IP-based network for all data acquisition and control

functions; and CCTV systems are increasingly IP-based irrespective of the physical and data transport layers.

The advantages of employing a converged infrastructure include:

- a workplace that can be used more efficiently and effectively, by making the use of space more flexible and reducing the cost of churn;
- the ability to reconfigure access control and security systems to reflect changing use or to enable multiple occupancy;
- self-service access to facilities management tools by the building occupants from their office computers.

The integration of systems may occur on two levels:

- the integration of building systems and ICT systems; or
- the integration of both building systems and ICT systems with business systems.

The advantages that are realised will depend on the level of integration. An example in an office environment is the use of 'smart' building passes to manage access to printer and photocopying services. Similarly, when a user logs on to a desktop computer, it may trigger the automatic association of an adjacent desktop telephone with the user's extension number. This integrated approach can lead to a reduction of workspace reconfiguration costs as the users are no longer tied to specific workstations, i.e. any desk becomes a hot desk. To improve the energy efficiency, systems may be integrated to internal monitoring of the smart building passes to determine when an area is no longer occupied. The BMS may then be configured to allow energy-saving measures to be automatically implemented, e.g. reducing lighting and air conditioning.

What risks are associated with intelligent buildings?

The introduction of a converged infrastructure and integration of building and business systems potentially creates a range of new risks associated with aspects of the personnel, technology and operations.

The human elements of the building operations are potentially the greatest risk. Whether deliberately or accidentally, individuals may seek to bypass security controls or incorrectly operate systems. The integration of systems can magnify the impact of errors or omissions. Systems integration will bring together IT and facilities management teams who may have different priorities, cultures and reporting chains. All of these can inhibit an effective response to incidents or faults.

From a technology perspective, integration may introduce new failure modes, where building systems can interfere with business systems and vice versa.

www.**theiet**.org/sectors

For example, it is normal for office computers to run the latest antivirus software and be regularly patched. This may not be true for the BMS or computers used for safety-critical systems, thus leading to potential vulnerabilities from malware introduced over the network or from infected media.

The use of IP-based technologies creates opportunities for operational savings through the centralising and outsourcing of control and monitoring stations. But this can lead to a loss of local knowledge and control. The problem is exacerbated if the support personnel are only deployed in response to incidents as they may not be familiar with the layout and operation of individual buildings.

Is cyber security an issue?

From a security perspective the key issues are protecting the security and privacy of a building's owners and users, maintaining the integrity of the building and operations within it, and ensuring the continuing availability of the accommodation for its owners and users.

The security and privacy of the building's occupants and owners may be compromised when the convergence of the technical infrastructures and integration of systems creates unplanned or unauthorised pathways, allowing unauthorised access to systems or data loss. For example, unauthorised access to the building access control and room-booking systems may reveal personal data such as when a person is away from home or the presence of a visiting VIP.

The integrity of the building may be compromised if third parties gain access to or control of critical building systems. If a third party were able to disable or take control of building systems it might no longer be safe to continue to occupy the building. This could be due to physical damage (e.g. fire or flooding) or due to threats to the health and lives of occupants. Disabling security and access control could put lives at risk and necessitate personnel being redeployed to implement manual checks in place of the automated systems. For energy-efficient buildings, integrity might be compromised if the operation of the energy management functions were degraded or disrupted by the actions of a third party, whether by direct manual interference or the deployment of malware.

The availability of the building may be seriously affected when building systems are disrupted, thus preventing the building from delivering the required functionality. The nature of the availability risk will depend on the type of building and the criticality of the affected building service. As an example, where a BMS became inoperable and allowed the temperature to stray outside acceptable limits, the building could become inhospitable to the occupants, damage equipment through excessive temperatures, or cause damage to

stored materials. In tall buildings disruption to vertical transport systems (lifts and escalators) could seriously affect the availability of upper areas if occupants are unable or unwilling to use the stairs.

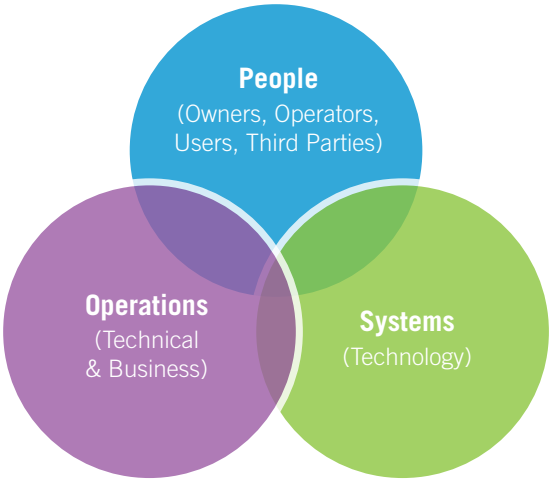
What can we do about the risks?

Intelligent buildings are potentially mission-critical environments. As such the risks associated with people, systems and operations need to be appropriately managed and mitigated (Figure 3).

The people risks will arise from four constituencies:

- the designers – who need to be aware of, and have mitigated the potential consequences of, actions by third parties, whether they are support contractors with legitimate remote access to systems, or unconnected parties with a malicious or hostile intent;
- the building owners – who need to consider what degree of systems integration is required and/or desirable during the specification, design, construction and commissioning of the building;
- the building operators – the daily tasks and responsibilities of the intelligent building facilities manager and technicians need to be clearly defined, and include a clear understanding of the complexity of integrated systems;
- the building occupants and visitors – who may need to be informed about the correct and safe operation of building systems.

Figure 3: The key risks to securing intelligent buildings can be assigned to three broad categories



The system and technology risks have already been discussed. The mitigation of these risks needs to include an assessment of which features of the building and its use are critical and therefore in need of the greatest protection. The design and implementation of a building 'black box' to capture information may be considered important to support the investigation of incidents. It may also be necessary to consider frequent remote back-ups of building occupancy information for use in the event of a building evacuation. The mitigation of system risks must also take account of the appropriate use of technology; for example, Wi-Fi is susceptible to

www.**theiet**.org/sectors

interference and jamming and should be avoided in safety-critical and security systems.

The operational risks need to be assessed and understood from both business and technical perspectives. The training and knowledge of the facilities management team should be commensurate with the sophistication of the systems integration and the impact that system failure will have on building occupants. There should be cross-training of some IT and building support staff to facilitate collaboration during incidents and fault diagnosis. The operations team needs to collect feedback from building users to understand whether the building is supporting or hindering them. This is important as users will often seek to bypass controls if they feel they hinder rather than support the user.

A number of legal issues also arise from these risks, and require an assessment of the legal process and legislation available and applicable when things go wrong. The legal remedies available will depend on who is deemed liable for any failures, whether they were caused by accident or deliberately.

The risks and their mitigation should be addressed in a holistic fashion for all implementations, but are essential for multi-occupancy and multiple-use buildings where the needs and priorities of the users will vary.

Conclusions

The drivers for intelligent buildings and thus systems integration typically arise from the need for new energy-efficient interventions, real-time decision support systems, enhanced building and personnel security and better management information dashboards that offer easy access to key performance indicators. The development of intelligent buildings introduces new and novel risks into the built environment, some arising from the integration of traditionally separate systems, others as a result of the increasing risk of cyber-attacks on any IT-based system.

Intelligent buildings are a relatively new and evolving area, so there is a need for building owners and occupiers to ensure that the novel risks are fully understood and addressed throughout the building lifecycle. With the help and support of the UK Centre for Protection of National Infrastructure (CPNI), the IET has developed a briefing document on 'Resilience and Cyber Security of Technology in the Built Environment'. This document is available for free download from the IET's website.

What do you think?

If we are to ensure the advantages of intelligent buildings are realised, there is a need for better recognition and understanding of the risks and operational issues. Following on from the publication of the briefing document the IET is planning to develop further guidance material. If you would like to contribute to this work please contact: **intelligent-buildings@theiet.org**

Simon Yarwood, Head of Information & Communications Sector, says,

"This Sector Insight on intelligent buildings and its associated risks is the start of a programme of work on cyber security which demonstrates the IET's continued commitment to the IT field."

www.**theiet**.org/sectors