interphone
maintaining your security

How to make the right choices for smart building integration

WHITE PAPER
November 2016

How to make the right choices for smart building integration

Internet of Things (IoT) thinking, where devices are connected over the internet and communicate with one another, is already becoming mainstream. Global IT research company Gartner has estimated that nearly 5 billion connected 'things' – including building security systems, domestic white goods and office equipment – were in use by the end of 2015, up 30 per cent from 2014, and that the total is expected to reach 25 billion by 2020.

From the concept of the 'smart home' (or 'home automation'), already the subject of numerous newspaper and magazine features – via the emerging 'smart office' to the utopia of the 'smart city' – 'things' present in buildings are increasingly being designed and manufactured to work together with each other and with their users.

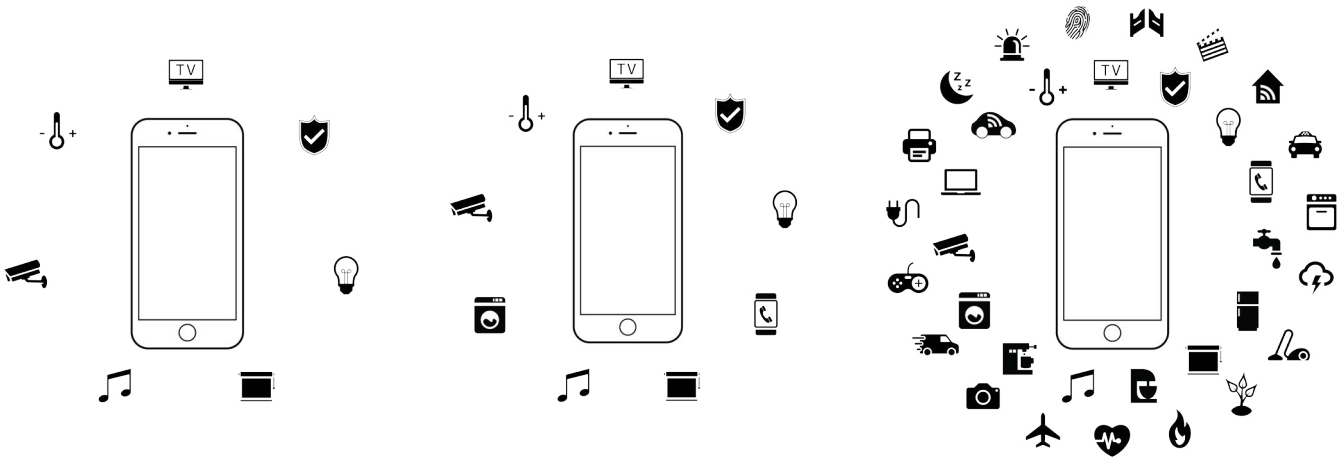
The gains on offer from such complex smart building arrays include increased efficiency, cost savings, comfort, convenience and security. But the essential requirements for securing the optimum benefits from this connected technology are careful advance planning, accurate specification and meticulous installation. This will ensure the effective integration from the outset of individual components equipped with the necessary interconnectivity.

The whole technical feasibility of smart buildings has arisen from the integration basic technology solutions introduced for early access control requirements, with intercom systems using audio and video communications between building or internal entrances and internal spaces. Since these systems typically came with links to telephones and TV sets for the monitoring of entry cameras, the principle of the communication links necessary for full-scale home automation and smart offices was already established. This has opened the way for further technologies to be integrated.

"Nearly 5 billion connected 'things' were in use by the end of 2015"

Growth of 'connected things'

Global IT research company Gartner has estimated that nearly 5 billion connected 'things' – including building security systems, domestic white goods and office equipment – were in use by the end of 2015, up 30 per cent from 2014, and that the total is expected to reach 25 billion by 2020.



3.8 billion
2014

5 billion
2015

25 billion
2020

The full implementation scenario can involve the strategic planning and installation of sensors and communication links for applications including:

- The detection of and reaction to suspected intrusion or gas or water leaks
- Monitoring the internal movement of people (or its absence)
- Automatically controlling and modifying temperature and ighting levels, to suit living and working patterns
- The management of domestic electrical appliances such as fridges and washing machines - with smart meters to track energy usage
- The operation of home entertainment and cinema; and
- The management of office security and equipment

Delivering these successfully is a multi-tiered process involving the operation of:

- The individual components
- Their integration and interconnection; and
- The overall security array

The input of an experienced and accredited system integrator offers invaluable technical support and project management, not least in assessing the capability of the equipment supply industry.

Industry Implications

Widescale home automation and smart office deployment has wide-ranging industry implications. Manufacturers of domestic and commercial electrical products that are now being considered as candidates for integration into IoT networks have not, until recently, needed to devote much time or thought to considering the scope for interconnectivity.

As a result, many companies are still on steep learning curves. This makes it imperative for them to be able to demonstrate convincingly their awareness of the technical, operational and security issues, and risks, as well as the commitment of their research and development departments to deal effectively with these. Manufacturers need to address the issues, not just of the security of products themselves, but also of the connected pathways that link them.

At the other end of the supply chain, manufacturers of connected products will be able, for their marketing purposes, to gather valuable data on how people are making use of their equipment. This can include how often, at what times of day (or night), in what conditions and with what preferences for individual features and available options.

However, taking advantage of this data is, of course, subject to common sense privacy constraints on the wider use of such information. Manufacturers must be able to demonstrate their awareness of the need for compliance with strict EU regulations covering the sharing of personally identifiable data.

Again, the same connections that make it possible to deliver these benefits of home automation and smart offices can also introduce security risks at sensitive points of a complex system. Without effective measures including robust encryption and passwords in place from the outset, the data that is traversing the public internet will be vulnerable to hackers – commercial rivals, fraudsters and thieves.

“Manufacturers must be able to demonstrate their awareness of the need for compliance with strict EU regulations”

"Harmonisation of system architectures and standards in the IoT is critical"

Occupier Priorities

For commercial buildings, where overall control of all access and other data is a key consideration for running a business, occupiers' IT departments need to be involved from the start in contributing to the specification and integration processes of technology consultants and system integrators. These will benefit immensely from critical in-house experience of a company's corporate culture and security risks.

Again, its own technical personnel need to be confident that they are familiar with and capable of managing long-term, the interfaces between the external and internal systems and their own in-company IT systems.

Ideally, the HR department should also be in involved, especially with companies within the creative and high-technology sectors, where staff tend to move freely around rather than being located at specific desks for much of their time. Too restrictive a security regime, for example, risks being abused or even ignored - not necessarily out of malice but often for purely human behavioural reasons. Appropriate defences need to be integrated.

Input from experienced consultants with a range of successful installations to their credit can be invaluable in identifying potential problem areas early enough to avoid their rectification proving expensive later on.

Standards

As with any new technology, robust standards are critical to ensure interoperability between:

- Existing products, which have to be shown to be able to work compatibly; and
- Updates and future alternatives, to enable enhanced operation and avoid the risk of lock-in to any individual manufacture as more competitive models reach the market

In Europe, key activity in this area includes the EU's Horizon 2020 research and innovation programme, its largest initiative ever. This is committed to reinforcing the competitiveness of European industry in "developing, mastering and shaping the next generation Internet that will gradually replace and surpass the current web".

Horizon 2020s scope covers the roles of fixed and mobile networks and service infrastructures, in enabling "the interconnection of trillions of devices across multiple operators and domains that will change the way we communicate, access and use knowledge". Standardisation has a critical role to play.

In the US, the Industrial Internet Consortium and the Institute of Electrical and Electronics Engineers (IEEE) announced in 2015 that they are working together to develop a system 'architecture', This will provide the means of structuring and interconnecting components for an interoperable industrial Internet of Things (IoT). Given the global nature of modern technology, the two initiatives will mutually support and inform each other. An experienced system integrator will be aware of their implications.

Harmonisation of system architectures and standards in the IoT is critical both for growing the market, and for giving confidence to building owners and managers, their professional consultants and the occupiers, in the home automation and smart office sector.

About Us

Interphone is a security systems and building technology integrator providing design, installation and maintenance services for the commercial residential property marketplace. With more the 50 years of experience, Interphone is ideally-placed to overcome the unique challenges faced by managing agents, house builders, property developers, construction contractors, facilities managers and residents, delivering upgrades and completeinstallations for retrofit and new build developments.

Interphone has established longstanding relationships within the property management, development and specifier communities, resulting in its solutions being fitted in many large and prestigious buildings across the UK. In addition, the company services a portfolio of more than 3,100 rental and standalone maintenance contracts covering 2,800 sites and 65,000 individual units.

Interphone is also providing advanced home automation and entertainment systems through its dedicated division Ingeny, providing complete control of virtually any technology in the property at the tap of a touchscreen, smartphone or tablet. These integrated and smart building solutions, suitable for projects of all sizes, are designed to make everyday life easier by combining familiar systems that work seamlessly together for added simplicity, convenience and enjoyment.







CEDIA CUSTOM ELECTRONIC DESIGN & INSTALLATION ASSOCIATION

ACS REGISTRARS Quality Assurance ISO 9001

cai Trade Association for Content Delivery

SafeContractor APPROVED

NICEIC APPROVED CONTRACTOR

GATE SAFE

Constructionline

TRUST MARK Government Endorsed Standards www.trustmark.org.uk