Meeting of the Parliamentary and Scientific Committee on Tuesday 22nd October

SMART BUILDINGS RESEARCH – FOCUS FOR THE FUTURE

Dr Deborah Pullen
Group Research Director,
Building Research Establishment

The last 20 years have seen the expansion in innovative systems to create smart buildings, with the primary criteria being:

- a system which integrates the smart operational systems with the building fabric
- the system responds to internal and external changes, and finally
- there is a communication to the occupier to allow them to adjust the operation to meet their own needs.

This has led to many developments where the building fabric has incorporated smart products which improve performance and create a stable envelope to which management systems are applied. This needs to be able to be modified without an adverse effect on the performance.

They often include energy generation systems and controls for heating, lighting and power. Monitoring and metering are key features so that building controls can be adjusted and support billing and external support services such as maintenance. This could also support security and also assisted living which will be increasingly relevant to the ageing population.

In recent years the importance of considering the occupant when creating a system which is smart has become apparent, with wellbeing critical to a successful outcome. There are many examples where the room is either too hot or too cold and the controls too complicated.

BRE Smart Home, opened 2013

The work undertaken by BRE over the last 15 years has focused on evaluating the effectiveness of the whole system. The Innovation Park at BRE in Watford includes test bed buildings where the evaluation and dissemination have been developed. Two examples provide insight into the growing science-base in this field and the outcomes of experimental programmes.

THE SMART HOME

The first is the Smart Home, developed from 1998 and featured in a BBC programme called Dreamhouse. The focus was on highlighting technologies and products which might be found in a future home. Over the next 10 years thousands visited the house. It has stood the test of time.

It had one of the first green roofs, an early photovoltaic array, a greywater recycling system, and a ground source heat pump and prototype intelligent

BRE Innovation Park, Watford

electronics – commonplace today. Devices to control temperature and water level in the bath to a pre-determined set-point, a clever feature then, but now adopted to improve safety for less able people.

The house has undergone an extensive retrofit. It tackles some of our key challenges: particularly the need for our homes to be more energy efficient, to adapt to the effects of climate change and to address the needs of the ageing population. Using design and building techniques, the retrofit has made the house 50% more energy efficient and halved its carbon emissions, upgrading it from an E to an A/B EPC rating.

One of the major differences in the retrofit project was that the house was designed as a whole system. Products were selected not only on individual performance but on the potential for them to work alongside other products.

Some specific innovative products used include:

Phase Change Materials have been on the market for a few years. They work on the principle that when the temperature rises above 22°C, the polymer/wax compound in the wall melts to absorb the heat, slowing temperature rise by up to 7°C. The wax solidifies when the room temperature falls to 18°C and the stored heat is released back into the room. This works well in areas where solar gain could be prevalent, and a few degrees can make a difference to comfort.

Phase Change Materials

Building Integrated Photovoltaics have also been installed on the roof and conservatory glazing panels that can produce electricity from light coming from either side, making them a flexible option.

The building control system includes sensors which allow responses to movements from occupants and more accurate monitoring of specific performance properties. There is also the opportunity for devices to communicate with each other.

The next stage is to carry out more detailed assessment of the system under experimental conditions, and with occupants. There is also the need to consider the economics around the installation of these systems both for the original builders and as retrofit solutions. Aspects of payback and skill needs in ensuring these systems are fitted correctly, and can easily be repaired, are a key element to achieving optimum performance and resilience.

THE NATURAL HOUSE

The development of the Prince's Foundation Natural House was to demonstrate that efficiency and sustainability could be delivered for a classically designed dwelling using many natural and renewable materials. The smart systems in this house are passive. They respond automatically to external changes without the need for external power. The driver is to create an environment which enhances the wellbeing of the occupants.

The building contains wool insulation, clay blocks, recycled wood internal flooring and partitioning. Its construction can be built using conventional skills. One of the major innovations is the passive air flow stack, a design which was first used in Victorian buildings. It uses no mechanical air flow or air conditioning.

TEST METHODS

Test methods used to assess performance of the internal environment include:

- temperature probes in the walls and in a range of locations around the building,
- the use of thermal imaging to consider gaps and
- various monitors which measure gases such as CO_2 and other volatiles.

The Prince's Foundation Natural House

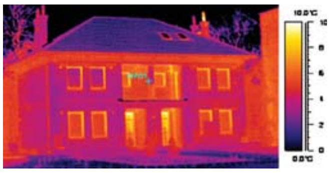
These are considered as a collective assessment of the performance. Changing the levels of heating, lighting or air flow can be assessed.

Once the baseline and a check that all systems were working properly, an occupancy assessment was carried out. A couple moved into the house for 12 months. During this time similar indoor environment tests were carried out to track the change based on their activities. In addition, feedback from the occupants and overall experience of living in the house were obtained via a questionnaire. The house has performed very well, with new systems demonstrating enhanced performance for the people who live in it. Further work will look at resilience

REALLY SMART BUILDINGS

The attributes needed to achieve really smart buildings:

- They have to work as a whole system.
- They have to respond to changes, both in terms of daily operation but also seasonal and climatic changes over time.
- The importance of the occupant. The building has to work for them.



Thermal Image of The Natural House

- The systems have to be resilient to wear and tear and easy to upgrade.
- They have to form the building blocks of efficient operational cities of the future.

Finally, there is a need for multidisciplinary teams to work together with industry in applying their own speciality in developing effective complex systems.

SMART BUILDINGS AND PEOPLE

Doug King FREng FInstP FCIBSE FEI HonFRIBA
Building Performance Consultant, Doug King Consulting
Visiting Professor of Building Physics, University of Bath

INFORMATION

The term 'smart' is applied to a host of enabling technologies in modern buildings, the 'smart meter' being probably the most familiar. Examination of smart meter technology allows us to begin to understand interactions between people and technology applicable to both dwellings and commercial buildings.

The equivalent of domestic smart meters, meters that signal half hourly consumption data to the utility company, have existed for many years in commercial buildings. If equipped with an in-home display (IHD) or commercial equivalent, the building occupiers can also access the data. However, in both cases the term 'smart meter' is a misnomer, as the meter merely conveys information. It is up to the occupier to do something smart with that information.

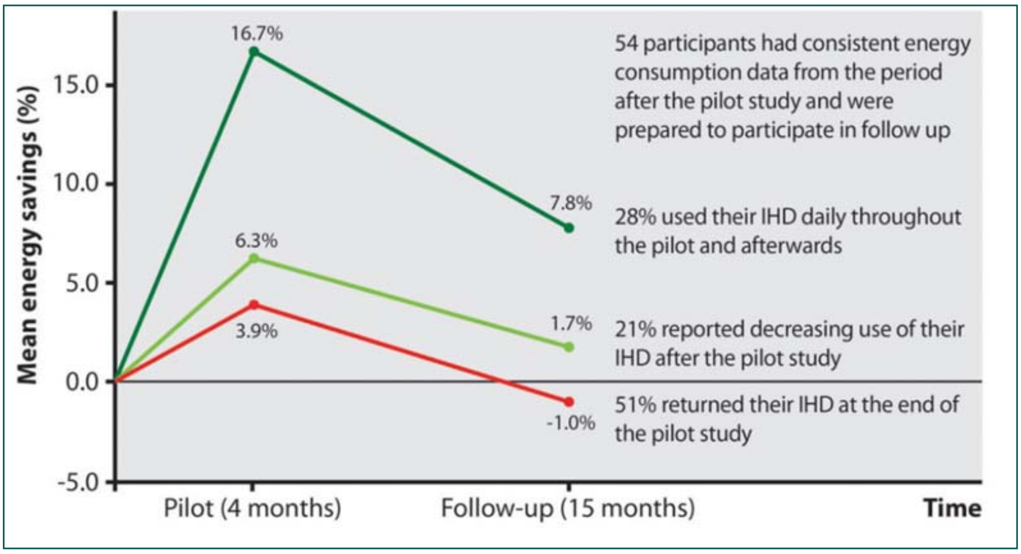
The presentation of data alone is of little value without context. Stevenson and Leaman (2010) said: "It is not enough to presume that the information from 'smart metering' will encourage people to reduce their energy consumption any more than a car speedometer will reduce speeding." A car speedometer provides information, but the driver must have knowledge of the speed limit in order to correctly interpret that information. Without significantly improved energy numeracy amongst the populace it is unlikely that the smart meter will deliver its full energy savings potential.

In-home displays (IHDs) need to present information in context in order to be useful. A PV generation monitor (right) can be easily calibrated against the size of array to present contextualised information. It is impossibly complex to calibrate an in-home display (left) against all the variety in UK households.

ENGAGEMENT

Van Dam, Bakker & Van Hal (2010) found that novelty appears to play a significant role in savings in short term trials of in-home displays. Revisiting households that had previously participated in a pilot study they found that the initial savings had generally not been maintained. Moreover, the lapse rate was more or less consistent regardless of how well the participants had engaged with their in-home display during and after the pilot study.

The study shows a lapse towards prior behaviour over time, but was unable to corroborate the hypothesis that the magnitude of energy savings achieved correlates to level of interaction with the in-home display. It is clear that, if we are to make the most of the opportunity of smart metering,



54 participants had consistent energy consumption data from the period after the pilot study and were prepared to participate in follow up

28% used their IHD daily throughout the pilot and afterwards

21% reported decreasing use of their IHD after the pilot study

51% returned their IHD at the end of the pilot study

Results of a study by Van Dam et al (2010) suggest that energy savings achieved in pilot studies of in-home displays may be transitory regardless of the level of engagement by homeowners.

we need to understand better people's interpretation of, and response to, energy information and tailor it to their needs in both domestic and commercial situations.

CONTROL

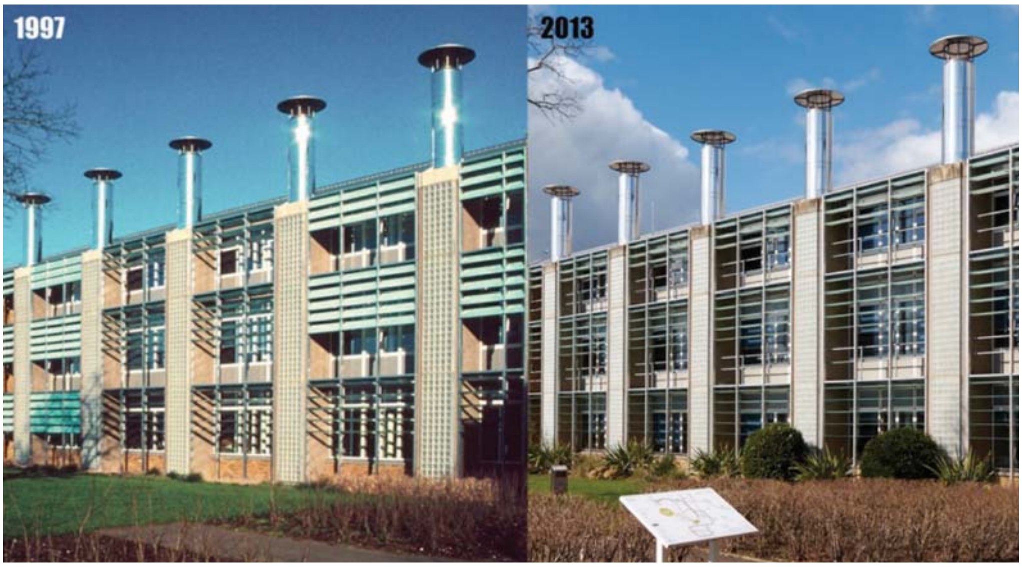
It is not only in-home displays that need to be designed with attention to the human interface. The control systems in commercial buildings are complex, yet the design effort put into the user interfaces is poor. Bordass, Leaman & Bunn (2007) found that: "If user controls are ambiguous in intent, poorly labelled, or fail to show whether anything has changed when they are operated, then the systems that lie behind them are unlikely to operate effectively."

SWITCHOFF
Switching off the lights overnight in an empty meeting room throughout the year can save 440kg CO₂

Ambiguous controls create confusion and can lead to users distrusting the system or simply ignoring subsequent useful information or control signals.

User interfaces need to be engaging, where possible intuitive, and make it easy for individuals to do the right thing, particularly given the increasing tendency to install complex controls in domestic situations, where the understanding of control functions is poor.

Further, if control systems do not provide building occupants with the functionality and convenience that they expect, they will take actions to override the control systems in order to achieve what they consider to be more favourable outcomes.



Completed in 1997 as an exemplar of energy efficiency, The BRE Environmental Building featured external shades which were designed to respond automatically to changing daylight and over-heating conditions. However, over time the state of the art control system became obsolete and the actuators progressively failed and were not replaced. Instead, simple manual blinds were installed to control glare and overheating. Today, the louvres remain static and the building's occupants rarely adjust the blinds, even when daylight levels fall, as the lighting controls compensate by bringing the lights on even in the middle of the day.

Thus, it is common in commercial buildings to find thermostatic controls being used as on/off switches and for daylight sensors to be covered with sticky tape to ensure that the electric lights remain on.

MANAGEMENT

Building structures are designed for long lifespans, whilst smart building technologies will fail or become obsolete several times during that span. As with any information technology system, it is essential that a clear upgrade path is available and is followed throughout the life of the building. All too often, building controls become obsolete, making subsequent repair prohibitively expensive and leading to the controls being abandoned.

Cohen, Ruyssevelt, Standeven, Bordass & Leaman (1998) wrote: "The myth of [building] intelligence is that it is 'fit and forget': buy it, and the electronics will do the rest. The actuality is that it is very much 'fit and manage'. Complex engineering and control systems tend to work best in an environment in which the occupier can resource a high level of facilities and engineering management. Problems start to occur where sophisticated technology is applied in a management-poor environment."

DESIGN

To deliver smart buildings that sustain their smartness requires more thorough design than is presently the norm. Greater interaction is needed between the building's users and designers, both at project inception, to articulate requirements clearly, and after handover, to tune the systems and gather feedback. There also needs to be a much more robust system for communicating design and performance goals throughout the chain from design through delivery to operation.

Waide, Ure, Karagianni, Birling & Bordass (2013) wrote: "Building Automation Technology often fails to deliver its potential because those specifying the system have limited understanding of how it will be operated." They go on to assert: "The best design can only come from a thorough understanding of operation." In order to be truly smart a building must be

People will use buildings in ways that can never be anticipated by the designers. A smart building must be flexible enough to accommodate the needs and desires of the users without forcing them into compromises, which will result in them ultimately overriding the systems.

designed to be 'user centric'. It needs to accommodate the habits, needs, desires and capabilities of those who will use and operate it.

PROCUREMENT

Mapping the typical, mass market construction process onto a systems engineering diagram indicates that there are gaps in the key areas for the design of smart buildings.

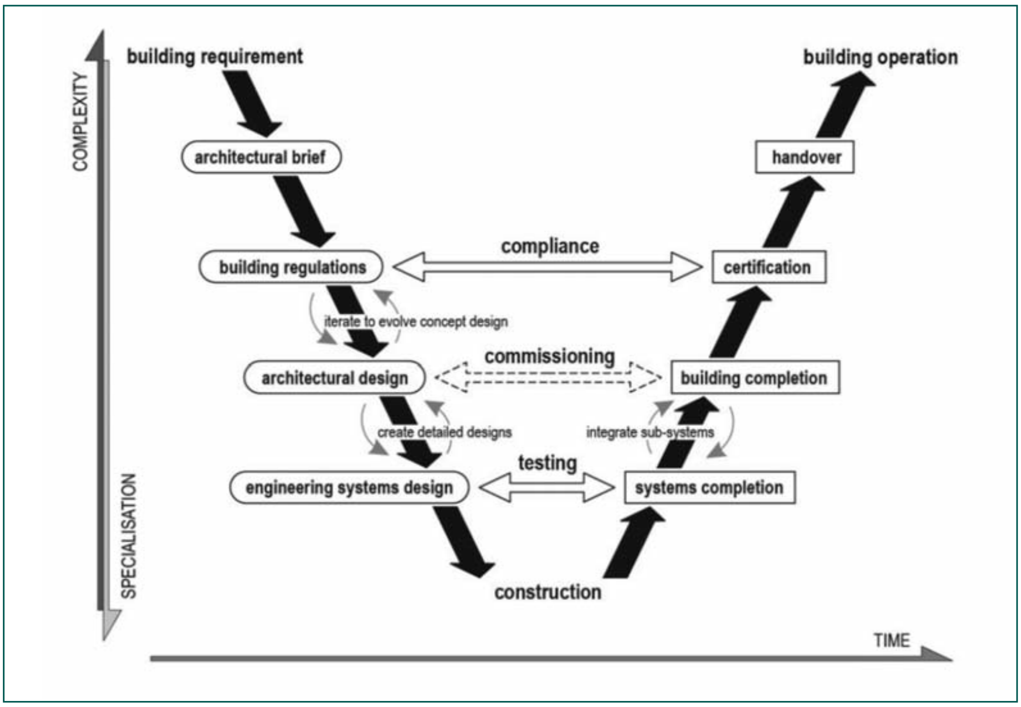
As an alternative one could propose a construction diagram, including confirmation of outcomes and feedback into subsequent designs, that may be capable of delivering genuinely smart and sustainable buildings.

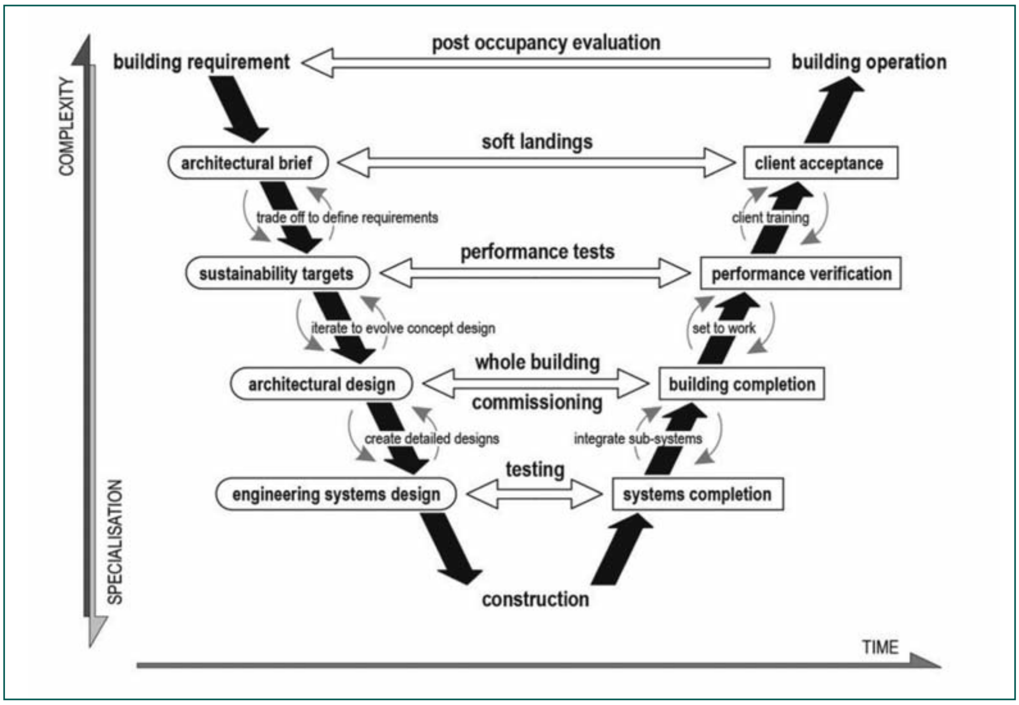
However, we need to acknowledge that the present methods of procurement in both the public and private sector do not allow the requisite interaction between users and system designers before and after the construction period. If we are to deliver smart and sustainable buildings we first need to address the shortcomings in the procurement process.

CONCLUSION

For a building to be smart, it must get the best from both its automated systems and from the intelligence and understanding of its occupants. It needs to be robust, cost-effective and not too complicated. Smart building design must account for the desires and capabilities of those who will use them.

This creates major challenges. Although there are exemplars, in typical UK construction scant attention is paid to human factors, to the design of the product, and to the creation of integrated systems. Shortcuts are taken in the installation, commissioning and handover. Provision of complete operating information and user training is rare. Systems designers do not learn from performance in use.





These challenges are not insuperable. However, they will need to be addressed if the benefits of smart buildings are to be realised. We need to improve skills and education amongst the designers, constructors and operators. We must put the users at the heart of smart building design and operation.

"A 'smart building' is one that doesn't make its occupants look stupid" *Adrian Leaman - The Useable Buildings Trust*

References

Bordass, W., Leaman, A., and Bunn R. (2007) 'Controls for end users: A guide for good design and implementation' British Controls Industry Association report 1/2007, BSRIA

Cohen, R., Ruyssevelt, P., Standeven, M., Bordass, B. and Leaman, A. (1998) 'Building intelligence in use: lessons from the Probe project' Conference 'Intelligent buildings: realising the benefits', BRE Garston, 6-8th October 1998

Stevenson, F. and Leaman, A. (2010) 'Evaluating housing performance in relation to human behaviour: new challenges', Building Research & Information, 38: 5

van Dam, S., Bakker, C. and van Hal, J. (2010) 'Home energy monitors: impact over the medium-term', Building Research & Information, 38: 5

Waide, P., Ure, J., Karagianni, N., Birling, G. and Bordass, B. (2013) 'The scope for energy and CO_2 savings in the EU through the use of building automation technology', Report for the European Copper Institute. Waide Strategic Efficiency Limited

All images and diagrams copyright Doug King

SMART BUILDING SECURITY

Martyn Thomas CBE FREng
Vice-President, Royal Academy of Engineering

SMARTER AND BETTER

There are many definitions of a Smart Building: for example, it is "smart" to use rainwater harvesting to flush the toilets or to use self-cleaning glass for windows. Security only becomes an issue with another and rapidly growing "smartness" – the use of sensors, algorithms and control systems to make a building more responsive to its occupants and easier to manage.

Automation can bring many benefits. If the building management system knows that a room is unoccupied it can turn off the lights and turn down the heating. A chip in your entry pass can tell the security systems to open the door as you approach with your arms full of files. Wireless communication avoids expensive and unsightly cables, and allows CCTV, room status, heating, ventilation and air-conditioning to be monitored and controlled from wherever is most convenient, or even remotely.

Integration of systems multiplies the benefits. If the Building Management System (BMS) is integrated with office IT and phones, then putting a meeting in your calendar can book a room and ensure that it is open, lit and heated when you arrive, that your phone calls are redirected and your latest printing available on the nearest printer. In an emergency such as a fire, the AV systems can show the safest and quickest route to an exit and the BMS can make sure the relevant doors are unlocked, the windows set to clear smoke or avoid draughts that would spread the fire and tell the Fire Service which rooms and lifts are still occupied.

Architects are already planning greater integration between systems and between buildings. As Smart Buildings grow into Smart Neighbourhoods and Smart Cities, their BMSs could co-operate to manage demand on the electricity networks, exchange environmental data and co-ordinate with smart transport systems.

SMARTER AND MORE COMPLEX

Greater automation and greater integration increase the system complexity. A typical commercial building's heating, ventilation and air-conditioning installation could require the integration of 20-50 local control systems from 12-15 different manufacturers with an overall building control system that has to interface with the lighting control, fire and security and access control. The customisation will be done quickly and often by contractors who have won the job on a lowest cost tender. The building will be accepted from the developers, not by the final occupants (who may not have been involved at any point in the design and construction) but by the customer – perhaps an overseas investor or hedge fund. By the time it is fully occupied, some of the knowledge needed to manage the building optimally will have been lost; after a few years of maintenance and changing occupancy, the BMS and its connected subsystems may be very different from the original design and managed in ways not foreseen by the architect.

... a building more responsive to its occupants ...

MORE COMPLEX AND LESS SECURE?

As buildings become smarter, they will contain more automated systems, with increasingly complex interconnections. Such "systems of systems" create unexpected behaviour, new vulnerabilities and new management challenges. To quote an example given by Hugh Boyes of the IET at a Round Table organised by the RAEng , if building management systems operated by the facilities team are connected to systems operated by the corporate IT team, there needs to be clarity about who takes responsibility for protecting the security of the BMS, which has the characteristics of a control system rather than a typical enterprise computer system. The BMS may not be able to run a commercial virus checker or software firewall and there may be good reasons why it should not be connected to the internet to download updates and new virus signatures. Protecting the BMS from malicious software will need specific attention every time that a connected system is changed or upgraded.

Unplanned "emergent" behaviour of complex systems is well known in other application domains. For example, as vehicle electronic systems have become more complex, there have been reports of uncommanded acceleration, of novel ways to break into the car (kick the front bumper to simulate an accident; the airbags fire and the doors unlock), and of drivers and passengers trapped inside. In one car model, the design of the electronics created a "sneak circuit" such that if the radio was on and a rear-seat passenger was opening their electric window at the same time as the brake pedal was pressed, the airbags fired. Other undesirable interactions have occurred in electronic healthcare systems and in air-traffic control; they are a known risk in all complex systems and may be latent in a system for years and then cause complex failures any time the system is reconfigured or updated.

Building management systems need to be secure not just against error but also against attack. There are many reasons why a building needs to be protected from becoming a target for organised criminals or some other malicious group. Buildings contain valuable property, both physical and intellectual. They house people responsible for major financial services, policing and government. They house hundreds or even thousands of people whose safety could be at risk. As building systems become more complex, cybersecurity becomes increasingly important. The National Security Strategy has identified "hostile attacks upon UK cyberspace by other states and large scale cyber crime" as a Tier One risk alongside international terrorism or an influenza pandemic. Unfortunately there is currently no way for a prospective occupant of a building to know what level of security it provides, as there are no effective security standards or certification regimes for Smart Buildings.

SMART BUILDINGS: THE RISKS

Many risks could arise from insecure "smart" building systems. If the BMS can be controlled by an unauthorised person, the physical security and safety of the building and its occupants is compromised and the organisations that occupy the building could suffer reputational and financial damage including loss of intellectual property, disruption to critical functions, and breaches of legal and fiduciary duties. Even a limited demonstration that a hacker could trigger the sprinkler system or control the lifts may be enough for successful extortion.

A 2007 report from the US Government GAO gives examples of cyber attacks that have already occurred against control systems. *"In the spring of 2000, a former employee of an Australian software manufacturing organisation applied for a job with the local government, but was rejected. Over a 2-month period, this individual reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewerage pumping stations and caused malfunctions in their operations, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks."*

It is not widely understood that it is not possible to provide assurance that a system is secure by testing it (even though this has been well known by computer scientists for more than 40 years). Even a small software-based system can exist in hundreds of thousands of different "states", any of which might lead to a security breach. For any practical system, testing every state is impossible, so the best you can discover by testing is that the system ran these specific tests successfully but this tells you nothing about what might happen if the tests were run again, or in a different order, or with different inputs.

... Protecting the BMS from malicious software ...

The consequence is that no-one can discover what vulnerabilities have been introduced (accidentally or deliberately) into the systems that control smart buildings, or who knows about them There is a strong international market for "zero-day" vulnerabilities (barely diminished by the recent dismantling of the *Silk Road* criminal website selling malware alongside drugs and weapons) so it would be surprising if developers were not creating vulnerabilities and selling them, with or without the active encouragement of those who might wish to exploit them at some time in the future.

This situation need not continue. Software engineers who work on regulated, safety-critical applications (such as aircraft control systems, nuclear power or railway signalling) increasingly use mathematically based "formal methods" that provide the ability to analyse the software they develop and to prove that it behaves as required for all possible inputs. The proofs can then be provided and demonstrated to a customer or regulator as required. Formal methods have been shown to be practical and cost-effective but they have not yet come into wide industrial use. It is highly unlikely that a commercial BMS and the control systems to which it is connected will have been developed using these methods, which is one reason why the vendors will not offer effective guarantees for their systems. Customers do not yet demand evidence of security when they specify systems (and if they did, probably no supplier could offer a compliant bid because of the weaknesses in their development methods and in their supply chain). This is a classic market failure where competition will not provide the stimulus to create the improvements that are needed.

CONCLUSIONS

The security of BMSs and related control systems should be seen as a strategic issue. Even if no current buildings are at risk, many more smart buildings will have been constructed by the time the market for secure systems has matured enough to allow architects to specify secure systems, for developers to acquire systems they know to be secure and for building occupants to have effective assurance about the level of protection that their building provides. Strategically, it would be better if UK industry were creating secure building management systems, rather than UK customers purchasing possibly compromised systems developed in countries that may not have the UK's well-being as a high priority.

Smart buildings: people and performance. http://www.raeng.org.uk/news/publications/list/reports/RAEng_Smart_Buildings.pdf

GAO report number GAO-08-119T Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. http://www.gao.gov/assets/120/118147.html

See, for example, http://www.adacore.com/sparkpro/tokeneer