The Institution of Engineering and Technology

http://www.theiet.org/cpd

Engineering the future of communications - 2010

Key communications issues for tomorrow

www.theiet.org

The Institution of Engineering & Technology

The Institution of Engineering and Technology (IET) is a global organisation, with over 150,000 members representing a vast range of engineering and technology fields. Our primary aims are to provide a global knowledge network promoting the exchange of ideas and enhance the positive role of science, engineering and technology between business, academia, governments and professional bodies; and to address challenges that face society in the future.

The IET is registered as a Charity in England & Wales (no 211014) and Scotland (no SC038698).

For more information please visit
http://www.theiet.org

The IET Communications Policy Panel

The IET Communications Policy Panel is tasked by the Institution of Engineering and Technology with proactively identifying policy issues applicable to the communications sector and providing guidance to the IET Board of Trustees, members, Government and the public. It's members are Chief Technologists and their equivalents from across industry, academia and public sector organisations.

The panel conducts most of its business electronically but meets with selected guests a few times a year at the IET in Savoy Place to review key topics. The outcome of each of these meetings is a short summary paper on a key topic - and these form the basis for the annual meeting.

For more information please visit
http://www.theiet.org/policy/panels/index.cfm

Contents

Engineering the future of communication

The ways in which we communicate are changing more rapidly than they have at any other time in history, in fact you may well have learned about this meeting using a method that did not exist ten years ago. The rate of change is relentless and is likely to continue for the next ten or twenty years bringing with it new capabilities and efficiencies that will force changes in almost everything that we do.

The purpose of this dinner is not only to provide an occasion for stimulating conversation over a pleasant dinner but to let you hear from top experts in the engineering profession about recent and likely future developments in communications and have the opportunity to participate in a discussion of the likely consequences of these developments.

Pervasive digital communications infrastructure has become vital not only to us directly but for the maintenance and effectiveness of all of our critical national infrastructure as noted, for example, in the recent *Infrastructure UK report*. It is our responsibility to keep ourselves informed about these developments and I hope that you will get as much as possible from tonight's occasion. This is the second of what I hope will become a series of annual meetings at which progress in communications will be monitored. This year we have aimed to provide more time for discussion.

Lord Broers

Chairman's introduction

As we have heard communications is at the heart of the developing digital economy, and of our vital national infrastructure that supports our future wealth, as discussed in the recently-announced National Infrastructure Plan.

Last year at the first of these events we presented brief outlines of the key topics and our vision for the way forward in four selected areas. Below we briefly summarize these and what has been happening in them in the past year. All continue to be of growing importance, though we have another set of equally important topics for this year.

- **Convergence and Divergence - Access from any place, anytime, anywhere.**
  Here we argued that the rising dominance of digital communication technology and the convergence of broadcasting and internet delivery would revolutionise the media industry, and that this would need management but would create major opportunities for our creative industries. This process proceeds apace and has already had a major impact - but there is much further to go.
- **Communicating sensors in every object - rise of digital low-data-rate devices.**
  Here we pointed to the rapid rise in the number of comparatively low-connected-rate but ubiquitous, mostly wireless, systems that may play a vital role in our digital future. We were particularly concerned with (global) standards and with security considerations, but saw the developments as a major opportunity. In the past year there has been much discussion on one major example - smart meters and smart grids, in which the IET's concerns over security and communications have been noted and partly responded to. There are clearly many other examples.
- **Green Communications - energy issues in communication systems.**
  Here we noted the energy profile of communications systems, which tends to grow with data rate, but also the potential contribution of communications systems to smart energy usage. We were particularly concerned to heighten awareness of energy usage in communications systems. Here there has been some progress and the contribution to overall energy efficiency has been recognised in the national infrastructure plan. More remains to be done (how many of you still have fax machines for example?) but awareness is rising.
- **Where next for Digital Broadband?**
  Here we argued for the importance of continuous, universal, mobile, personal connectivity and, of the need to demonstrate a viable business approach to achieving this if the country is to benefit to the maximal extent. Here the importance has been widely recognised and we particularly welcome the government's embracing of universal and particularly 'super-fast' optical broadband. A wireless-fibre future does look more than a year closer than it did a year ago - but there are still many years to go.

The need for continued attention in the rapidly-developing communications area (and ICT generally) is nevertheless as great as ever. We are living though a revolution - which is exciting but also demanding. The UK has an opportunity to lead, particularly in the vital task of bringing the technology and its applications together; in doing this well lies the real opportunity. To lead here we need to focus on the following.

Visionary and Integrated Approach

There is a real need for leadership to ensure that we do not fragment our approach technology platform development in the UK. It is of course vital that our future telecommunications and smart grid infrastructures are optimised for performance and that duplication and waste are minimised. There is a great danger of technology islands occuring that do not communicate with each other restricting the ability of the infrastructure to really deliver the capabilities we need as a country to be a leading economy. The IEC will develop a technology vision and point out the levels of communication and interoperability required, identifying important standards whilst working with government regulatory bodies and industry to ensure that the UK's future platform investments deliver world leading capabilities to support the functionality required for the future.

Efficiency and Sustainability

It is vital that our technology platforms of the future take into account both efficiency and sustainability. To a great extent both are linked together. As a country we cannot afford in the future to have duplication of technology infrastructure platforms, such as separate mobile infrastructures for each individual operator or individual smart grids for each supplier of electricity. There needs to be sharing at the infrastructure level and separation at the service level going forward. The sustainability for future infrastructures depends on a deal of considerations around issues such as, climate change, network resiliency to equipment failure and power outages etc. Duplication of effort here to mitigate for major loss of services, in disaster situations on multiple infrastructures is costly and complex. It would certainly be easier and provide greater cost efficiency to implement consistent measures on a common infrastructure.

Identity and Security

In the new digital world of the future, where all information and systems are connected to networks, then the control and access becomes a critical issue. In the future we would want to make access in many cases dependent on the individual's or system's digital identity. There are many advantages rising from a ubiquitous method to identify and control who or what has rights to a given piece of digital information. For example, on a smart grid controlling power distribution, security and the identity of the systems which control the grid are critical. In a consumer service like the BBC iPlayer today then licence payers are restricted from accessing programs when they are not in the UK, however this is not ideal it would be best from a user experience point of view for licence payers to have access to programs wherever they are and not on a geographic basis using identity as the controlling criteria. The current watershed on UK television set at 9pm for more adult content transmission cannot be applied to video on demand internet content which has no time boundaries. In some ways the PVR make the watershed ineffective as children can simply set up recordings for program transmitted at any time. Clearly the digital identity of the individual would allow greater control access rights to all forms of content and services. There is a great need for standards here and to ensure that a fair and open system is set up where no one power broker of identity can monopolise the market.

Smart Metering - communications issues

How to avoid being dumb about smart metering

Background

There is great interest worldwide in the use of modern ICT to manage energy usage at home, saving both money and Carbon emissions. The hard-to-supply peaks in consumption could be significantly reduced by the remote control of heavy loads that are not time-critical like water heaters, clothes dryers and air conditioners. On the input side, ICT could ease the integration of the grid supply with consumer-generated power from wind turbines and solar cells.

More speculatively 'live' in-the-kitchen (or on-the-smartphone) displays showing the cost of energy as it is being used might influence behaviour and reduce domestic consumption by as much as 2.5%.

Key to any of these aspirations for smarter and greener living is a smart domestic energy management system, consisting of an interconnected array of smart modules spread throughout the home. This would provide traditional infrastructure services such as electricity, gas and water more in the style of newer infrastructure ones like telephony and internet access[1]. Everyone involved could know what was being used and spent in real time, and by whom (or what), and they could then optimise their systems and usage in real time, just as communications providers and consumers do already.

Key Concerns

These ideas are seductive and in some form inevitable. There is however a danger of implementing a system that will rapidly become obsolete and which will not interface with other universal infrastructures or with developing commercial global standards for in-home networks and equipment, such as the emergent requirements for electric vehicle charging[2]. A well-designed system will consist not of a single 'smart meter' but of a set of networked smart modules performing different functions that can work together. These can be separately (& potentially internationally) sourced and can be added to, upgraded or replaced as necessary. A poorly-chosen solution could fail to allow enough competition in the supply of consumer equipment, impede desirable innovations and lose the chance for UK suppliers to address export markets, 'locking' the UK into a less effective system. This could be far more expensive, even in the short-to-medium term. Sensible 'open-source' choices must be made early on, meaning more-or-less immediately.

This project involves the blending of two technology-based industries (energy-based and information-and-communications-based, 'ICT') with very different cultures and backgrounds, and the best experience of both will be needed if a good outcome is to be obtained.

---

1 Now widely regarded as a 'right' -see http://news.bbc.co.uk/1/hi/technology/8548190.stm

2 The supporting of electric vehicles certainly requires 'smartness' in the infrastructure and probably and extended supply system. See Royal Academy of Engineering report - http://www.raeng.org.uk/news/publications/list/reports/Electric_Vehicles.pdf

Specific areas we have identified as needing urgent attention are:

Engineering the The Smart Living Space. The smart home is not a single device but a network of devices within the home that monitors and manages energy consumption. It also manages many other things, such as internet access, automated 'health & safety' monitoring for the growing numbers of elderly, and security. There are existing products and standards for many parts of this (including energy management) but there is still an opportunity for the smart metering initiative to play a key role. But it will be necessary for the smart meter, like all other modern electronic devices, to 'fit in' as part of an adaptable modular smart system. The crucial advantage of this networked arrangement of independent devices is that each component can be upgraded independently in response to innovations in technology and changing user needs. It also helps consumer choice and competition between suppliers to occur for specific devices or functions without disrupting the fundamental system.

Smart home management needs energy consumption and supply quality data - this can be obtained from either a smart meter, existing 'clip-on' sensors, or by recovering meter data over the web, assuming the meter has its own links[3].

We note that the meter data needs to be fed 'upwards' to enable a full smart grid, and whilst the meter could have its own communications if this were judged cost-effective it could (probably with greater integrity and security) use dedicated secure channels on whatever part of the rapidly-evolving communications infrastructure might be available at the time. The specification of the core smart living system needs to be correct early on to ensure security, and to allow innovation.

Planned non-obsolescence. Typical lifetimes for consumer-based ICT equipment range from 2-4 years for a PC to 1-2 years for a mobile phone, whereas current home meters are expected to last 20 years or so. Hardware to support 20-year-old ICT equipment will mostly have long since become unobtainable. On the other hand widely-adopted ICT interface standards (such as Ethernet and WiFi) may work long-term because new equipment is still designed to support legacy hardware. This shows how the ICT industry has managed rapid technological and market change - systems are 'modularized' (as suggested for the home network structure above) so that hardware & software units supporting key functions can be changed as appropriate. A smart meter needs likewise to be seen as part of a system for smart living and needs similarly to have non-proprietary[4] and widely-supported interfaces so that it can continue to perform satisfactorily in a rapidly-changing world. And it makes sense to keep only the slowly-evolving basic meter functions 'in the box' but put most of the smartness into a higher 'application' layer where it can be upgraded to take advantage of changing technology and to meet new priorities.

3 Thus the smart meter could be in two parts - a smart management (upgradable) section and a secure meter-reading section.

4 Note that the cost of developing dedicated chipsets, for example to support WiFi, GPRS, Bluetooth and the like, is **very** high. Even quite widespread ICT systems therefore prefer to use common standards.

International standards. This is a related point but is so crucial that it merits special attention. The ICT industry is self-driven (much more than government-driven) to standardise its equipment interfaces worldwide, which dramatically reduce the cost of equipment. This is for all the reasons above, but also because 'smart customers' are very reluctant to buy non-standard-interfacing equipment, even if it seems better, because this would tie them to a single supplier for future purchases. The energy industry and its customers (in effect including the regulator) should be similarly cautious, and of course adherence to global standards also gives UK manufacturers access to global markets.

Adaptable communications. As an important feature of the adaptable networking approach suggested above we note that building a parallel communications infrastructure that reaches all users would be a massive undertaking - bigger than the creation of the existing mobile phone infrastructure. A single system would also leave the system vulnerable to disruption (and no more secure) than a diverse communications system that used whatever was available; notably the 'Universal' broadband network envisaged in the government's Digital Britain initiative, but also any other available system at the time, such as improved 3-4-5+G mobile networks.

Human Interfaces. We note that it is increasingly common for designers to see the human user as an integral part of any ICT system. This looks a particularly valuable approach to take to smart energy management, where so much of the gain may depend upon user persuasion. So 'fitting in' to evolving popular interfaces is important (like the iPhone today for example, but very different devices and systems are expected 10-20 years from now). This is another argument for an adaptive, networked, approach.

Holistic Approach. Smart meters will only realise their full potential for energy saving and carbon emissions reduction when they form part of a future smart electricity transmission and distribution grid. Successful deployment of a smart electricity grid underpins the delivery of UK energy policy and carbon goals. The final system will comprise a complex mix of technologies and changed business processes, but the most important properties of the smart electricity grid are system-level properties that can only be assured by system-level design and analysis from the outset. Thus for a smart electricity grid enabled by smart metering to be successful, a holistic approach to both system design and architecture with rigorous testing and modelling overseen by a single competent body with responsibility for the end to end solution will be required.

Links

Relevant discussions can be accessed at many places; good examples are:-
IET submission on smart metering - http://www.theiet.org/publicaffairs/submissions/s871a.cfm
IET submission on smart metering - http://www.theiet.org/publicaffairs/submissions/s871b.cfm

Availability of communications

Background - Availability of Communications

We are all used to the idea that we get dial tone when we pick up the phone and almost always get through first time - even when our local mains electricity has failed. Sadly, the public Internet is not so reliable, despite the well-publicised 'survivability' that is built into parts of the Internet.

Words like availability, reliability, resilience etc get used, sometimes interchangeably, which can cloud issues. If Ofcom is to have a new duty to monitor 'resilience' of the UK communications infrastructure, what should it be measuring? Initially it seemed that Ofcom would be looking purely at architectural issues of resilience[5]. But BIS's secondary information has included clarification about risk assessments and emergency planning, which is welcome, since 'resilience' is not just about choice of architectures.

The overall goal is that services should have high availability, which means long Mean Time Between Failures and short Mean Time To Repair. Experience also suggests that resilience should include the concept that in the face of failures, service should degrade gracefully, not totally.

Another key point is that availability requirements will be different as between:

1. Services which form part of the Critical National Infrastructure (CNI)
2. Mission critical services for other businesses
3. Public communications in general

In general, public networks are designed to support (3) and bespoke design will often be needed to support (1) and (2). It is not reasonable to expect the general performance of the public networks to meet all the needs of (1) and (2), though the central importance of the PSTN to society has led to EU regulations relating to the integrity and security of the public telephony service.

What is Resilience?

Telecoms resilience has been defined as

> "Equipment and architecture used are inherently reliable, secured against obvious external threats and capable of withstanding some degree of damage"

---

5 Based on RFP sent to consultants.

More generally, from the business and Critical National Infrastructure point of view, Business Resilience has been defined as

> "Resilience is the ability of an organisation, resource or structure to sustain the impact of a business interruption and recover and resume its operations to continue to provide minimum services"

These definitions embrace 3 themes:

1. That networks should be inherently reliable, so will withstand some internal failures
2. They can withstand, to a degree, external threats
3. Restoration and repair will be rapid.

High reliability is achieved by using the best 'carrier-grade' components and employing appropriate levels of redundancy, for example, internally using dual plane architectures, and externally by using ring-based transmission architectures, so as to minimise or eliminate 'single points of failure'.

Resilience to external threats depends critically on identifying the threats and using risk analysis to decide whether to mitigate or carry the risk.

Restoration and repair will depend on having appropriate plans and carrying out exercises to ensure they are practical.

What are the risks?

Risks can be grouped under 5 headings:

- Physical
- Loss of key inputs
- System/Logical
- Software
- Electronic 'interference'

Physical

This includes:

- Natural phenomena:
  - Extreme weather (including hurricanes and tornadoes), earthquake, volcanic activity, flood (including tsunamis), lightning and if we are really unlucky: meteor strikes.
- Fire, gas leaks
- Damage caused by:
  - Accidents
  - Vandalism
  - Targeted theft
  - Internal sabotage
  - Terrorism

Loss of Key Inputs

This includes:

- Power (Electricity and Telecoms have a high degree of inter-dependency)
- Fuel (impact of strikes and long term shortages)
- Human access (e.g. exclusions and cordons during emergencies, but might also include more general transport problems)
- Materials and equipment (including logistics of supply)

System/Logical Failures

These are the basic failures of the components and systems which comprise the network.
Issues include:

- Resilience
    - "Telco grade" equipment i.e. high reliability telecoms equipment
    - Back-up power supplies
- Redundancy
    - Duplicated processors
    - Diverse, separated routings (no Single Points of Failure)
- Restoration
    - Good visibility of network
    - Network Management
- Repair
    - Time to unattended sites

Software

- All software has faults
- Systems should never stop, but may need to rollback or restart
- Big danger is systemic or 'common mode' failures, especially those that propagate throughout the network
- Dual sourcing can sometimes address this

Electronic Interference

- Over-voltage, over-frequency inputs
- Signalling corruption
- Traffic overloads
- Denial of Service
- Hacking
- Billing fraud
- Malware (viruses, Trojans, worms etc)

Key issues for availability

From the foregoing, it should be appreciated that choosing a 'resilient' network architecture is not sufficient on its own to deliver sustained availability. Indeed, in terms of the well-known 'self-healing' networks it can be noted that:-

- The Internet can take several minutes for new routings to 'converge' after a major failure; during this time service is unavailable
- Synchronous Digital Hierarchy (SDH) has excellent properties in terms of speed of switchover to redundant paths, but the world seems to be moving away from SDH on grounds of cost.

In the last decade, major risks to networks have shown the danger of preparing for the 'last war'. The Millennium Bug, Foot & Mouth, the Fuel Crisis, 9/11 etc all raised completely new and largely unforeseen vulnerabilities and issues. Being prepared to face the unknown is therefore important. How many airlines were prepared for the consequences of volcano ash? Few - but all had to react to these unforeseen circumstances.

The world is becoming far more dependent on mobile communications, but the planned resilience of the commercial mobile networks is far less than traditionally provided by the large fixed networks. For example, a mobile base station may only have backup batteries designed for a one hour power outage, with no generator backup.

As telephony migrates to broadband path delivery, service becomes dependent on the domestic mains supply. In many cases, the widespread sole use of DECT phones has caused potential difficulties in this area already. However, providing back-up power may not alone be sufficient. Many broadband networks have much lower levels of resilience in the backhaul than traditional voice networks. There has been some reluctance by governments and regulators to impose rules on network integrity and availability to Voice over IP (VOIP) networks.

Global warming is unlikely to create unknown vulnerabilities, but may increase the likelihood of certain types of risk, e.g. high temperatures, floods, wind, ice-loading on masts etc. Therefore, more risks may warrant mitigating investment where today the risk may be small and therefore carried. The IET intends to study this question and it will be interesting to see if any completely new failure modes and threats are identified.

Television Broadcasting and IPTV, Evolution and Revolution

Television as we know it is about to be radically changed by the Internet. This change goes beyond an evolution (i.e. an improvement in the service) to a revolutionary redefinition of the whole service concept from root and branch

Assertions:

1. Consumers of "Television" care little about the method of transmission; to them it is all about user experience.
2. We are moving from a world where "Television" was locked in the living room on one screen to a multi-screen world, where the service is truly mobile.
3. IP connected TVs also mean that content available on the TV is no longer restricted to that provided by traditional broadcasters.
4. TV is no longer a linear, scheduled experience.
5. The global nature of the internet will enable the creation of world-wide "Television" channels. These channels may be both linear and nonlinear and they will have the advantage of economies of scale, lower cost internet c.f. traditional transmission infrastructure and will have a greater attraction to advertisers as they have much larger audiences.

"Television":

We need a new definition of the television service.

- A multi-screen linear and non linear video service
- Using multiple transmission methods, Broadcast, mobile (streamed and download), Internet
- With encompassing subscription/funding model across all screens

Longer term revolution:

Looking longer term video will be embedded in almost everything. (Magazines, Newspapers etc) What we know as television today is a very limited part of the longer term service revolution to come of video ubiquity and convergence of media on a grand scale.

Considerations:

1. We should consider both traditional and internet broadcasting in the round rather than separately, i.e. if we have superfast broadband AND multicast capabilities then why can this not carry broadcast channels both audio and video as well as non linear Video on Demand (VOD)?
2. We need to think about the mobile Internet and how this can be linked into the broadcast revolution.
3. We should think how we can enable broadcasters to get global reach , how we can identify the individual and not restrict services to a geography but make them person centric.
4. Content protection - how do you prevent consumers from being presented with legitimate and

pirated material all on one interface? (Or at least ensure that they are aware of the content's origins.)

5. Net neutrality… can the internet cope with this explosion of video or should we regulate?
6. Broadcasting regulation plans for the future need to take account of this paradigm shift - what's in and out of scope?

Glossary of Terms

Backhaul	High capacity link to core network.
Carrier grade	High quality and reliable transmission equipment utilised by the voice and data transmissions companies.
Denial of Service (DoS)	System failure due to overloading data requests (often malicious).
IEC	International Electrotechnical Commission.
IPTV	Television broadcast using internet protocol.
Multicast	A term used to transmit IP traffic to many computers concurrently.
PSTN	Public Switched Telephone Network.
SDH	Synchronous Digital Hierarchy, or sometimes refered to as SONET. A type of optical transmission system.
Telco grade equipment	High reliability transmission equipment used by voice and data carriers.
VOIP	Voice over Internet Protocols - the method used to carrier voice data over an IP network.

The Institution of Engineering & Technology
Michael Faraday House
Six Hills Way
Stevenage
SG1 2AY

01438 765690 - Policy Department
email: policy@theiet.org
http://www.theiet.org/policy
http://www.theiet.org/factfiles

This content can contribute towards your Continuing Professional Development (CPD) as part of the IET's CPD Monitoring Scheme.
http://www.**theiet.org**/cpd