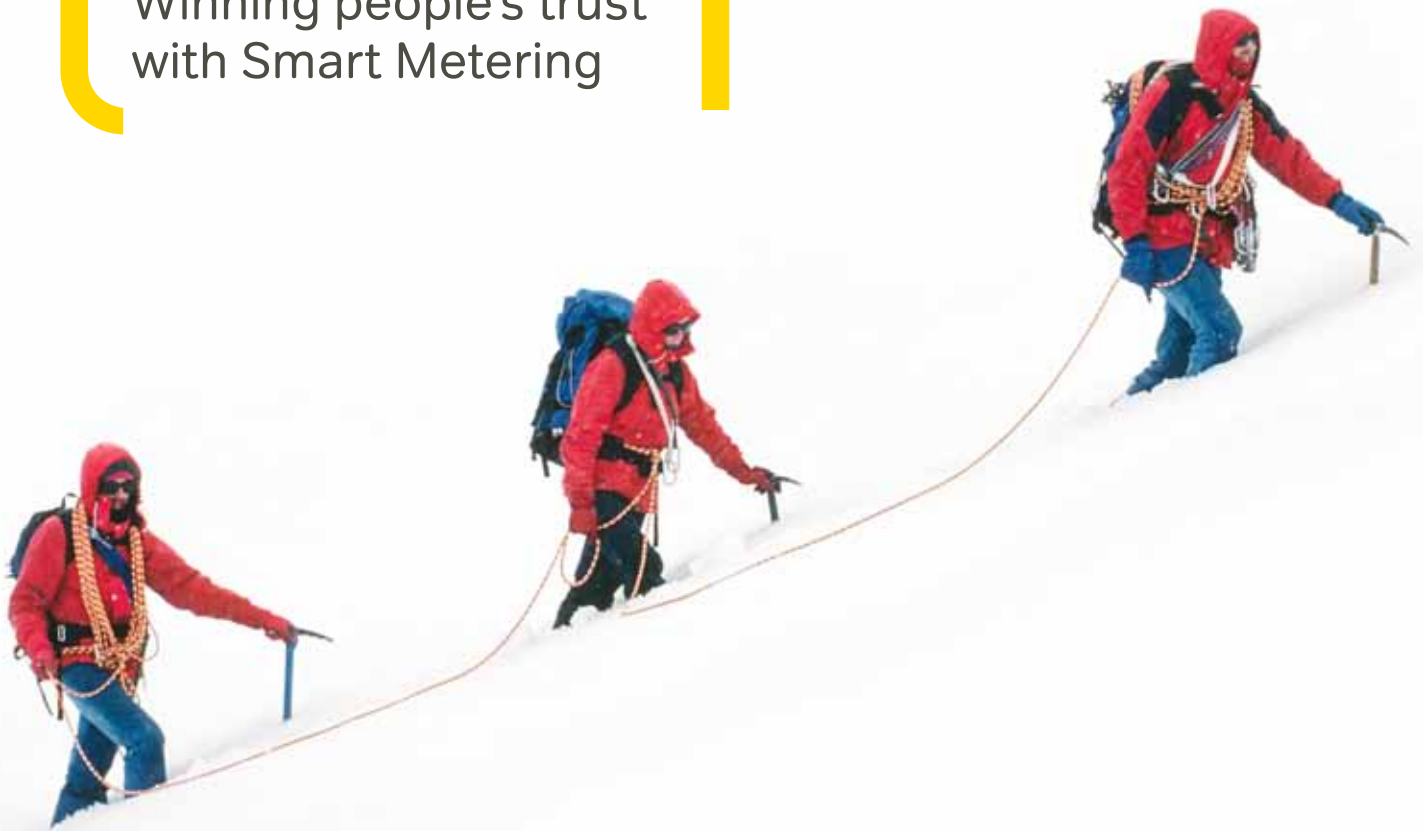


Winning people's trust
with Smart Metering



CONTENTS

[Back to Contents Page](#)

[Previous Page](#)

[Next Page](#)

[Last Page](#)

Logica is delivering the security architecture, design and accreditation for the UK's Defence Information Infrastructure programme – Europe's largest, most complex infrastructure project.

INTRODUCTION

This paper is one of a series looking at the issues that will need to be addressed as Britain introduces smart metering.

As the security of smart metering around the world attracts growing attention, our aim is to look objectively at the key security questions and put them into context.

There is no doubt that smart metering will provide the essential information and communication infrastructure to enable the country's shift to a low carbon economy and underpin its medium- and long-term energy security. If people truly understand and accept the broader, fundamental importance of smart metering, security becomes just one more key consideration in the design of the technology.





TRUST - THE CRUCIAL FACTOR

Energy supply affects almost every part of our lives almost all of the time but it's not something most of us think about until there's a power cut and we have no electricity or gas. Few outside the energy sector are overly interested in the infrastructure – from power station and gas storage facilities to transmission and distribution systems to meters – that supplies our homes and businesses, or the range of risks that have to be managed to ensure that our supplies of energy aren't interrupted.

But Britain's objectives of reducing the impact of climate change and ensuring energy security in the mid-term create different issues from the ones faced today. Risk is not only about disruptions to or denial of supply. It's about consumer confidence in the security of the personal information they give to utility companies and the impact that concerns over the security of this data may have on the public's acceptance of smart metering and billing.

People allow electricity and gas companies to have access to their personal data in return for services related chiefly to energy supply, billing and payment. The security of this personal data is already taken seriously by utilities because of the impact that potential breaches could have on the trust of their customers and on their reputation in the market. To operate in today's conventionally metered market they already have robust processes in place to address the security of customer data and those processes are reviewed regularly to ensure they remain appropriate for the level of risk. The perceived degree of risk and scale of potential damage caused by a security breach increases as the amount of data increases.

The biggest risk arising from these concerns is to the public's acceptance of smart metering and billing. While the benefits are no longer in doubt, the perception of a security risk could undermine public confidence and increase the potential for active resistance to the implementation of smart systems.

It is vital that people are able to understand the risks objectively and in the context of the wider picture of climate change and secure energy supplies. Failing to establish an infrastructure capable of enabling the change to a low carbon economy would lead, in the long term, to continued climate change. In the medium term, it could also lead to power cuts and higher prices for the energy supply we enjoy today.

We know from the retail sector that people are prepared to give personal information and allow it to be used if they see advantages in terms of cost, convenience or to receive offers that meet their needs and wants. Where people value the services, they accept that data is held on their day-to-day activities through loyalty cards, ATM and credit card transactions, telephone records, internet browsing records and social networking.

We developed an innovative solution for the Dutch police providing two-way communication with community volunteers using text, voice, instant messaging and e-mail.

They accept all this on a basis of trust. They are confident that their information is secure and is being used in their interests. Energy companies need to give consumers the same assurances about why they need to hold their personal data and what they are doing to keep it secure. Smart grids and an advanced metering infrastructure undeniably create new security challenges, but these are addressable – indeed, similar matters have already been faced and successfully managed in other sectors.

Media stories about security breaches tend to focus on the scale of the impact rather than the likelihood of it happening. This lack of objectivity and context has the potential to create fear and does the public a disservice by failing to promote an understanding of the real issues.

Several presenters at the 2009 Black Hat USA technical security conference focused on the potential vulnerabilities created by smart grids. Covering the development of security standards for smart grids¹, the lack of inherent security in older devices and the successful penetration of newer devices in lab tests², their focus was on promoting the importance of security within the design, installation and lifetime operation of advanced metering infrastructure (AMI) and smart grids.

The UK has the opportunity to learn from these breaches and to draw on best practice from other sectors, such as telecommunications and finance. Smart metering will create inter-connectivity and introduce control devices (such as electrical contactors and gas isolation valves) into the energy supply infrastructure where they do not exist today. The goal must be to design an infrastructure that can withstand penetration or attack, isolate any breach and minimise its impact.

¹ Hacking the Smart Grid, Tony Flick, FYRM Associates, Black Hat USA 2009

² Recoverable Advanced Metering Infrastructure, Mike Davis, IOActive, Black Hat USA 2009



SECURING THE SMART INFRASTRUCTURE

Most homes and businesses are connected to the gas and electricity distribution networks but in today's conventionally metered world there's no communication network enabling interconnectivity between premises. Information on consumption is gathered manually. It's worth noting that, while the focus of attention on security for smart metering has been about cyber security issues, there's been little appreciation of some of its security benefits. Remote communication with the meter means you don't need to allow meter readers into your home to record how much you've consumed. This cuts the risk of criminals impersonating meter readers.

Today, the causes of interruptions to energy supply in the UK are largely physical: for example, floods during the summer of 2007 endangered the power supply to thousands of homes and businesses in various regions of the UK. Parts of the distribution network are already inter-connected to provide monitoring and active control. But it's not easy to access the SCADA (supervisory control and data acquisition) systems, which help to provide the country with a reliable and resilient energy supply. The protocols are not commonly understood, the systems are not easily accessible and few are aware of the potential scale of the impact, should they be breached. This gives the networks a degree of security through obscurity.

So, for now, there are other, more easily accessible and attractive targets that hackers might see as providing greater rewards, through high profile disruption and damage to corporate reputations.

Establishing a smart metering infrastructure across Britain will, in effect, extend the SCADA system by a further 28.5 million communication and control points – more if you count individual smart appliances. The introduction into the home of inter-connectivity to the meter and beyond will present new tests for the utilities sector in protecting supplies from cyber attack, which might arise from the greater accessibility of the communication technology and the expected drive towards greater use of standard protocols, such as IP.

As corporate networks become more secure and the extended smart SCADA system becomes more easily accessible, the potential rewards for a hacker will grow. Security has to be integral to the design of the Britain's smart infrastructure.

We built a secure mobile solution used by more than 1,000 European police officers to remotely access and send information, files and pictures using smartcards and laptops booted from a secure USB.

SECURING THE HOME AREA NETWORK

NATURE OF THE RISK

One of the great benefits of smart metering to the consumer is the type and timeliness of the information it makes available. The expectation is that a consumer's increased awareness of how much and when they use energy will change their consumption behaviour, giving them control over their total energy expenditure.

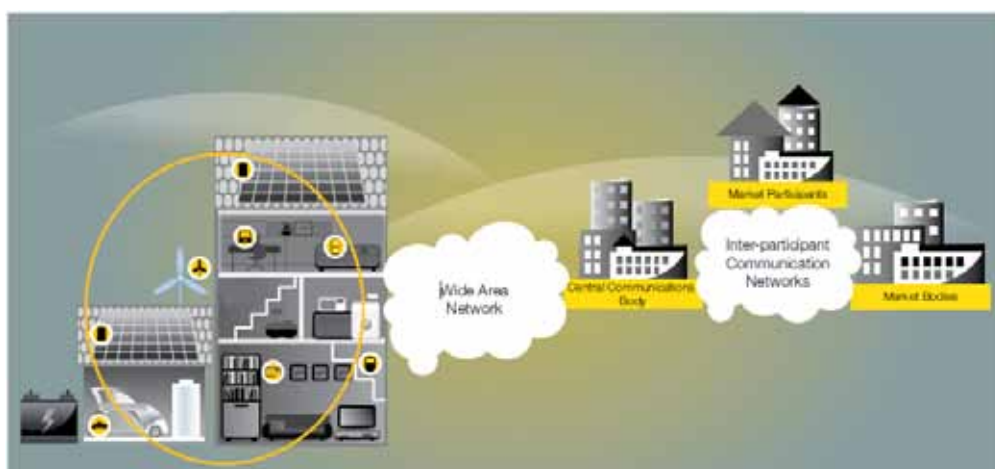


Figure 1 – Home area network

Consumers receive information via a visual display unit paired with the meter over a home area network (HAN). In the mid-term, multiple smart devices are likely to be connected to a communications hub via the HAN. These devices, ranging from electric vehicle charging units to micro generators (such as wind turbines) and smart appliances, could all be controlled automatically to optimise energy expenditure or to help balance and improve use of the local distribution network. If people are to see the full benefits of a smart home, being able to connect intelligent devices securely to the correct HAN will be an important step. This is an issue that every home using a wireless router already faces. Simplifying this process to make the technology accessible to all, yet without compromising security, will be the real test for designers.

While the usability of smart technologies is important, devices must be intrinsically secure. From the design of the device to the selection of the components down to chip level, security is a vital consideration. Vulnerability arises from a hacker's ability to access unencrypted or poorly encrypted software and then to design worms or viruses that can spread across either the HAN or the wide area network (WAN) for the purpose of anything from the acquisition of personal data to cutting off supply. The origin of components within smart devices is also important. Organised and well-resourced criminals – and even some governments – have been accused of embedding trojans in components and products. Once these are connected to the network, they are able to spread to other connected devices and lie dormant until activated for criminal or otherwise malicious purposes.

REDUCING THE RISKS

Intrinsic security throughout the design process calls for a systematic approach to identifying potential vulnerabilities and attack scenarios, quantifying the scale of the risk exposure and developing plans to reduce the risk and counter any attacks as they happen. Reducing the threat of identified risks is likely to rest on the connection standards and codes to which equipment manufacturers can design their products. Design will include the correct sourcing and rigorous testing of components from trusted suppliers in order to avoid the risk of inadvertently introducing trojans into any system.

ACCESSING THE WIDE AREA NETWORK - PREMISES

NATURE OF THE RISK

The introduction of a communications hub for smart metering into every home and small business in the UK brings a variety of security challenges



Figure 2 – Access to the wide area network, premise side

The benefits of smart metering come from two-way communication across the wide area communications network. The threat arises from the risk of a security breach in the HAN leading to a breach in the WAN and its spread to other communication hubs connected to the network.

REDUCING THE RISKS

It is crucial to segregate the networks to prevent the spread of malware from an infected HAN to the WAN and then onto other networks. To ensure the long-term security of the automated information management the communication hub must provide segregation between the networks and create a firewall, with remote updating of its firmware and anti-virus software.



ACCESSING THE WIDE AREA NETWORK - ENTERPRISE SYSTEMS SIDE

NATURE OF THE RISKS

The central communications body is the control centre for communications between the WAN and energy companies' networks. It has a critical role in enabling legitimate access to the WAN by the various market participants – suppliers, distributors and service providers – who have a legitimate right to access the smart metering infrastructure – and preventing access by unauthorised parties. Identity and access management (IAM) procedures are key to the security of the wide area network



Figure 3 – Access to the wide area network, enterprise systems side

REDUCING THE RISKS

Authenticating signals received from the smart metering infrastructure and routing them to the correct market participants is a vital function of the central communications body. Connection codes that include security standards are essential for the validation of field devices attempting to access the WAN. Equally important is the authentication of market participants and individuals who attempt to access the WAN from the enterprise systems.

Encryption, multi-factor authentication and intrusion detection are all important ways in which to protect the WAN. Anti-virus protection needs to be held at a network level. The protection should be readily and pro-actively updatable in response to evolving and changing risks.

Network monitoring for unauthorised or unwanted traffic is key to the early identification of potential risks (such as the propagation of malware), allowing remedial action to be taken before damage is done.

The security of the interface between the smart metering infrastructure and corporate IT networks of the market participants also needs to be studied. Any breach to the security of the smart metering infrastructure should be isolated from the corporate networks, and vice versa.

When looking at infrastructure security, the focus is generally on the design and specification of the technologies – but we mustn't forget the human factor. There's little point in designing a secure infrastructure if security can be breached through inadequate access controls. Staff selection and recruitment procedures and network access permissions need to be part of a robust security strategy. The overall design of the end-to-end smart metering infrastructure must not only look at factors such as points of entry and remote access authentication, it must also ensure that only people who have a legitimate reason for requiring access get it. Finally, it is vital that the system design provides the ability to isolate breaches, minimise their impact and enable effective recovery, with improved counter-measures.

ACCESSING THE SMART METER INFRASTRUCTURE - MARKET PARTICIPANTS

NATURE OF THE RISKS

Like all businesses, the utility sector already has to ensure that its systems and processes are secure and that their customers' personal data and business information are protected.

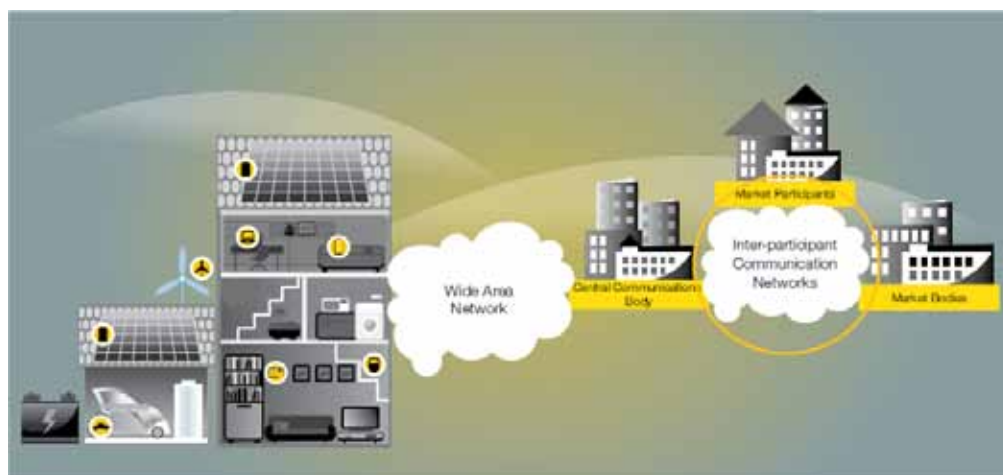


Figure 4: Accessing the smart meter infrastructure – market participants

Smart metering will not only encourage a more intelligent use of energy in homes and businesses, it will also massively increase the volume of data transmitted and handled by utility companies. This wealth of detailed information will allow companies to develop sales proposals that address consumers' real needs and wants, giving suppliers the opportunity to enter new markets.

Taking advantage of these opportunities could entail reassessing existing data security protocols or creating a need for new regulations. Companies will have to evaluate and improve their security continuously to make sure that their customers' data remains secure and that their brands and corporate reputations are not adversely affected by security lapses.

The smart programme has a broader security implication. If high profile breaches and consequent negative publicity justify public concern about the protection of personal data, that concern could turn into active resistance to the deployment of smart meters, with the consequential implications for our energy security and economy.

REDUCING THE RISKS

Corporate IT networks safeguard the personal data they hold through a combination of software and process. On the technology side, corporate networks have become harder to crack and software vendors have become more adept at building security into their applications.

An essential tool in mitigating threats is the operational processes that allow risks to be proactively identified and dealt with, and so contribute to secure design.

Equally critical in preventing data loss are the business processes around managing access to personal data. From recruitment processes through to delegations of authority, effective corporate governance is vital.

Beyond this, once employees or approved third parties have permission to access different levels of data, the authentication processes that prove an individual is who they claim to be become critical. Management of individual logons, passwords and remote network access are key to controlling access to the corporate network and applications.

GLOSSARY

Malware: Malicious software that infiltrates a computer or network without the informed consent of the owner or administrator. Malware includes viruses, worms, trojans, spyware and many rootkits.

Rootkits: Programmes designed to hide the fact that a computer or network has been compromised by the installation of malware.

Trojans: Malware that apparently performs legitimate and valuable functions, but which allows unauthorised access to the device or network, enabling a hacker to take control for activities ranging from identity theft to denial-of-service attacks through the creation of robot networks (BotNets).

Virus: Malware that replicates across a network, destroying or corrupting data and code.

Worms: Self-replicating malware – a worm spreads across a network to other smart devices. At its least damaging, it disrupts a network through the consumption of bandwidth.

Logica is a business and technology service company, employing 39,000 people. It provides business consulting, systems integration and outsourcing to clients around the world, including many of Europe's largest businesses.

Logica creates value for clients by successfully integrating people, business and technology. It is committed to long term collaboration, applying insight to create innovative answers to clients' business needs.

Logica is listed on both the London Stock Exchange and Euronext (Amsterdam) (LSE: LOG; Euronext: LOG).

More information is available at www.logica.com

This document is for general information purposes only and is subject to change without notice.

Copyright © 2010 Logica

All rights reserved. This document is protected by international copyright law and may not be reprinted, reproduced, copied or utilised in whole or in part by any means including electronic, mechanical, or other means without the prior written consent of Logica.

Whilst reasonable care has been taken by Logica to ensure the information contained herein is reasonably accurate, Logica shall not, under any circumstances be liable for any loss or damage (direct or consequential) suffered by any party as a result of the contents of this publication or the reliance of any party thereon or any inaccuracy or omission therein. The information in this document is therefore provided on an "as is" basis without warranty and is subject to change without further notice and cannot be construed as a commitment by Logica.

Logica
Tel: +44 (0) 207 637 9111
smart.metering@logica.com

www.logica.co.uk

CODE 018 0310

.....
AUSTRALIA / BELGIUM / BRAZIL / CANADA / CZECH REPUBLIC / DENMARK / EGYPT / ESTONIA / FINLAND / FRANCE
GERMANY / HONG KONG / HUNGARY / INDIA / INDONESIA / KUWAIT / LUXEMBOURG / MALAYSIA / MOROCCO
NETHERLANDS / NORWAY / PHILIPPINES / POLAND / PORTUGAL / RUSSIA / SAUDI ARABIA / SINGAPORE / SLOVAKIA
SPAIN / SWEDEN / SWITZERLAND / TAIWAN / UKRAINE / UNITED ARAB EMIRATES / UK / USA