How to protect critical infrastructure, mitigate fraud and guarantee privacy

New threats in the **energy sector**

Confidence in a connected world. Symantec™

Contents

Introduction

Energy utilities are in transition. Increased competition, globalisation, unbundling, market liberalisation and the pressure for renewable energies have all forced radical change within the industry.

Smart Grids are digitising the traditionally isolated energy network control systems and connecting operational technology (OT) with standard IT networks via bi-directional communication paths. As a result, power generation, transmission, distribution and active control for the end consumer are significantly altering. In fact, the transformation to Smart Grids is the most radical industry change in 100 years.

Utilities are already investing heavily in this transformation, as indicated by the increasing number of smart meter deployments in the US and Europe. IDC estimates the number of smart meters will reach about 71 million devices in EMEA alone, by the end of 2012[1]. This means that one in every four electricity meters will be smart.

Each region has its own transition programme priorities. Back in 2009, the US government announced stimulus funding for the modernisation of the US electric grid towards a Smart Grid. Large portions of this funding were assigned to the deployment of smart meters and the infrastructure that supports smart meters, as well as modernisation of transmission lines. Europe has taken a leadership role with its '20-20-20 by 2020' economic goal to reduce carbon emissions by 20%, increase energy efficiency by 20% and increase the energy mix with 20% more renewable green energy sources. As achieving this will require a huge technological transformation, EU strategy is to foster the development of Smart Grids to support energy efficiency, demand response and facilitate the decentralisation of power production. Some countries have started ambitious programmes to reduce the labour costs of manual metering and respond to the increasing demands of end consumers.

In the Asia Pacific market, particularly in China, demand for energy is rising very quickly as these countries invest in increasing capacity, reliability, efficiency and integrating renewable energy sources to reduce greenhouse emissions.

However, with new benefits come new challenges. The impact of digitising systems has been felt across other industries including gas and oil, transportation and process manufacturing. This report considers the implications of the Smart Grid transition and how differing global priorities will result in the need to manage varying sets of risks, standards and controls.

Managing the transition to Smart Grids

The Smart Grid brings two different technologies and cultures together using open IT protocols: the world of operational technology (OT) with supervisory control and data acquisition (SCADA) and the world of enterprise IT. At the same time, hundreds of thousands, or even millions, of smart meters will be connected via advanced metering infrastructures (AMIs) in order to constantly process real time information from consumers. Inherent threats from open standard based IP networks increase the vulnerability of the Smart Grid to cyber attacks. But it is not just the interconnection between SCADA and IT environments that is a cause for concern: the Stuxnet worm, which attacked the Iranian nuclear programme, has demonstrated that even isolated industrial control systems (ICS) are vulnerable against targeted threats[2].

The electrical grid is critical to modern life, so there is a lot of pressure on security officers to focus primarily on critical infrastructure protection. However, there are other issues that also need to be addressed thoroughly.

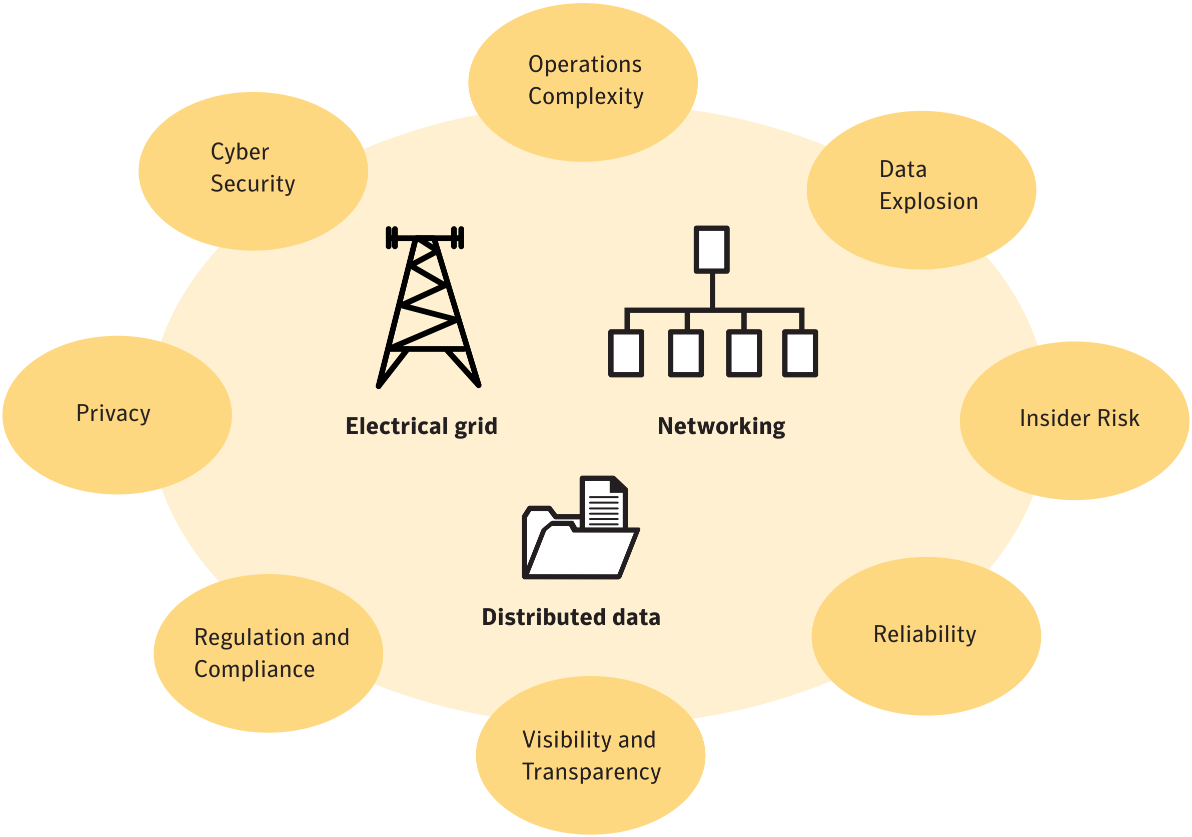


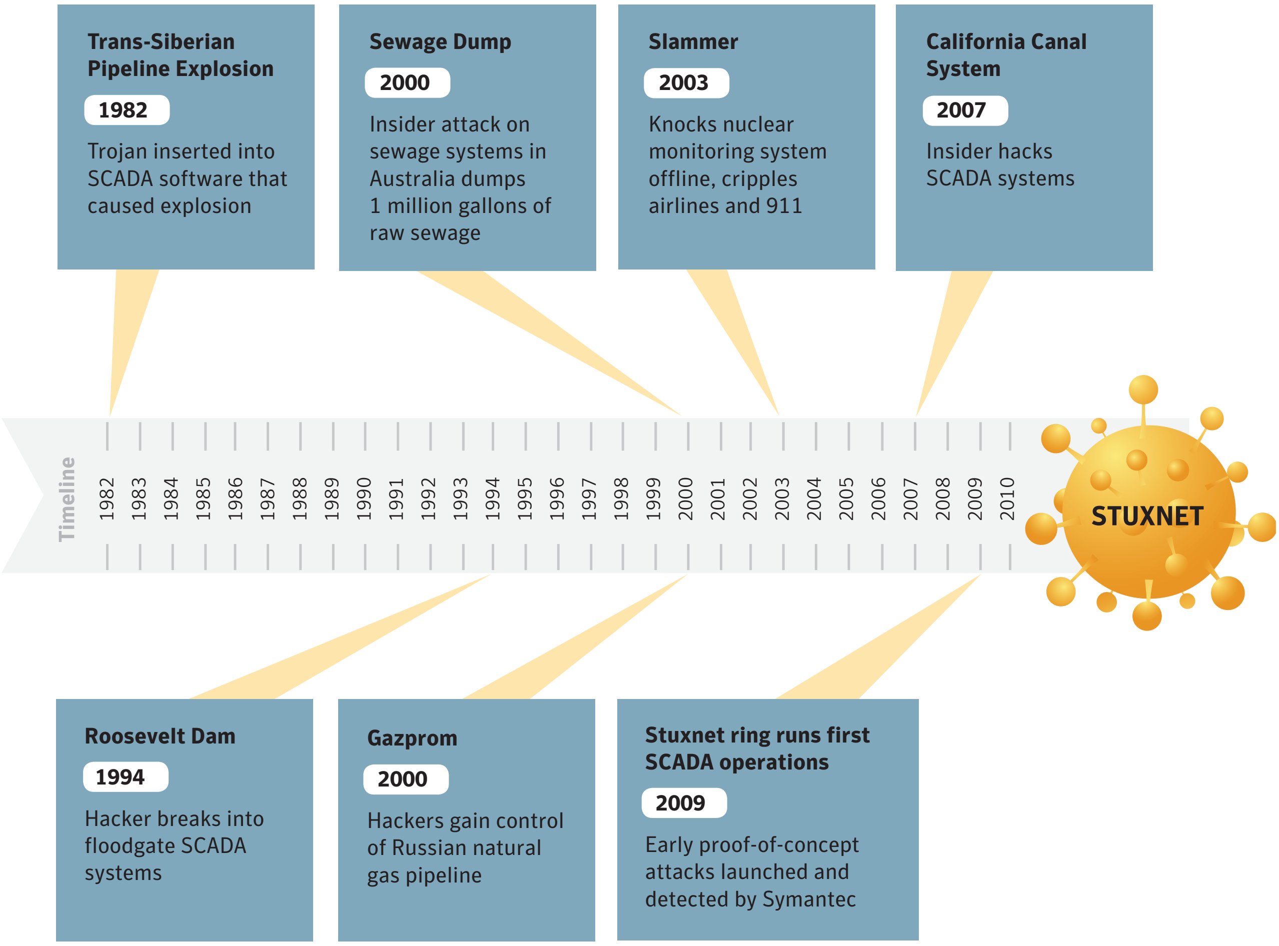
Figure 1: Overview on information protection and security challenges in the deployment of Smart Grids

Critical infrastructures are under attack

Although Stuxnet made the headlines, it is just the tip of the iceberg and prior to this attack, hackers and malicious insiders had broken into SCADA and ICS on multiple occasions in order to manipulate or take control.

The energy utilities are not alone in having to protect critical infrastructures. Many other industries, including transportation and process manufacturing, that have migrated from proprietary platforms to open systems with IP addresses have been subject to both inadvertent and malicious attacks.

SCADA attacks



Trans-Siberian Pipeline Explosion
1982
Trojan inserted into SCADA software that caused explosion

Sewage Dump
2000
Insider attack on sewage systems in Australia dumps 1 million gallons of raw sewage

Slammer
2003
Knocks nuclear monitoring system offline, cripples airlines and 911

California Canal System
2007
Insider hacks SCADA systems

Roosevelt Dam
1994
Hacker breaks into floodgate SCADA systems

Gazprom
2000
Hackers gain control of Russian natural gas pipeline

Stuxnet ring runs first SCADA operations
2009
Early proof-of-concept attacks launched and detected by Symantec

Figure 2: SCADA attacks prior to the Stuxnet outbreak

Targeted attacks are rising

The Symantec Internet Security Threat Report 2011 saw a dramatic increase in the number of publicly reported SCADA vulnerabilities from 15 in 2010 to 129 in 2011. The report also discovered that the number of targeted attacks increased dramatically during 2011, from an average of 77 per day in 2010 to 82 per day in 2011[3]. These targeted attacks use customised malware to gain unauthorised access to sensitive information. This is the next evolution of social engineering, where victims are researched in advance and specifically targeted; typically to steal valuable information such as customer data for financial gain, or to attack critical infrastructures. Advanced persistent threats such as Stuxnet, Duqu[4] and Flame[5] use targeted attacks as part of a longer-term campaign of espionage and sabotage, typically targeting high value information in government, finance and ICS. In October 2011, Duqu came to light, followed by Flame in the Spring of 2012. Neither caused any cyber-sabotage but both were used for extensive espionage and data exfiltration.

Targeted attacks can be extremely stealthy and hard to detect. To combat these threats, security vendors and governments have started joint programmes to improve how industry control systems like SCADA, and also AMI environments, are monitored in depth. Their objectives are to detect intrusions, analyse successful attacks and improve the security of systems. As part of the seventh EU framework programme, the project CRISALIS[6] (CRitical Infrastructure Security AnaLysIS), coordinated by Symantec, was launched in June 2012 with the goal to improve the security of critical infrastructures.

Cyber security for the critical energy infrastructure is a national, if not a multi-national, security issue exacerbated by potential insider risks and a magnified attack surface. Security officers within utilities will see increased pressure from authorities to implement security standards and comply with new regulations and directives.

Targeted attacks trend showing average number of attacks identified each month, 2011

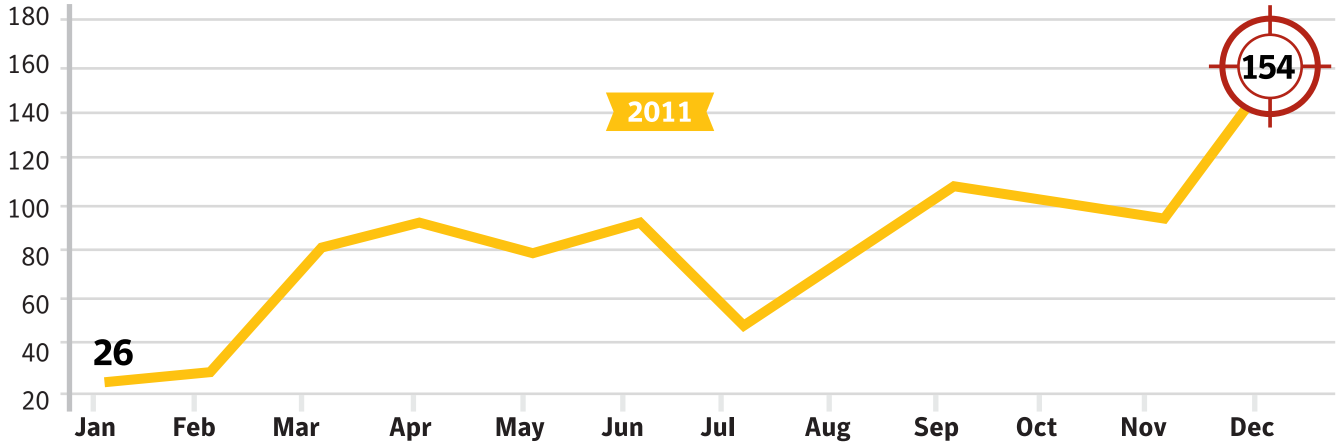


Figure 3: Symantec Internet Security Threat Report 17 Data – April 2012 (Source: Symantec.cloud)

Politically motivated attacks are on the increase

The 2010 Symantec Critical Infrastructure Protection study confirmed that not only are attacks on the increase, but that the threat of attacks with a specific political goal in mind is real and these are becoming increasingly frequent and costly.

During the survey, an IT director from a mid-sized energy company remarked, "We've had people attempt to break in and retrieve documentation, especially the shared material between the oil companies in our library. We had to take some dramatic actions to be able to cut them off."[7]

Furthermore, the attacks are serious, with respondents estimating that three in five (59 to 61 percent) of attacks ranged from somewhat to extremely effective. In North America, 74 to 77 percent of the companies surveyed reported that attacks were effective.

The survey also found that only one-third of respondents felt "extremely prepared" for attacks while 31 percent felt less than somewhat prepared across all types of attack. It should be noted here that energy providers rated themselves as best prepared, while the communications industry came out worst. As the Smart Grid relies on a reliable and secure communications' infrastructure provided by Communication Service Providers, it is clear that potential vulnerabilities in other Smart Grid ecosystem players also need to be taken into account.

Attack frequency

"In general, how is the frequency of each of the following types of attacks changing?"
(Only asked of those who at least suspect each type of attack)

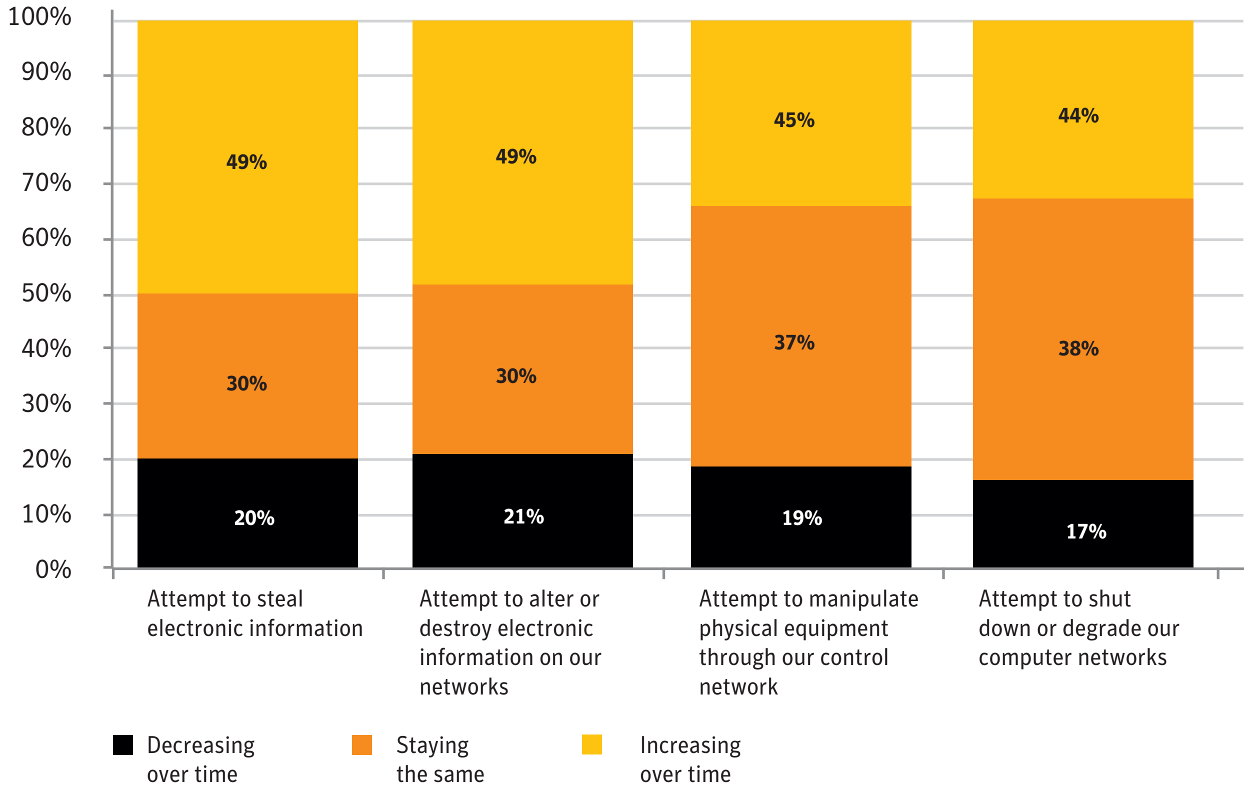


Figure 4: Symantec Critical Infrastructure Protection Study Data, November 2010

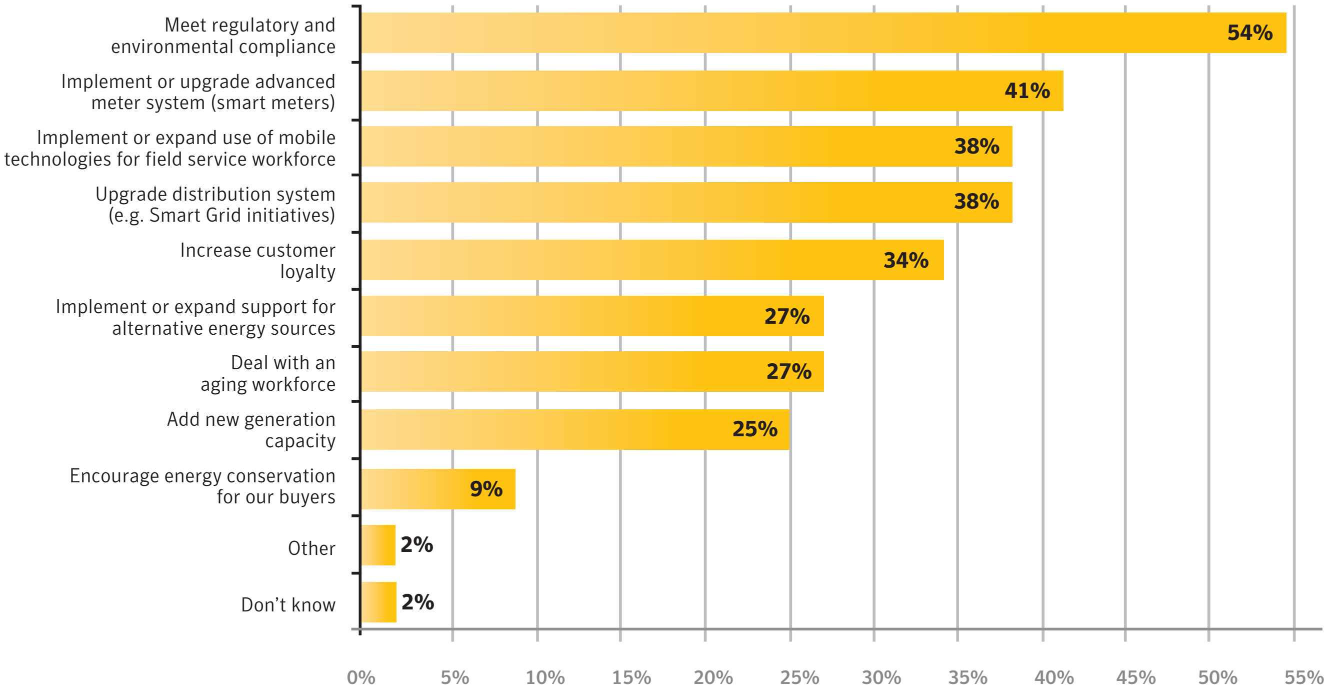
Energy industry challenges

Meeting regulation and compliance

Standards and regulations are globally fragmented and vary by region, making it almost impossible for security officers to gain an overview. Not surprisingly, the most frequent response to the question: “What are your company’s most important energy industry priorities?” in a 2011 Forrester study was “Meet regulatory and environmental compliance”, followed by “Implement or upgrade Advanced Smart Meter system” [8].

Regulatory bodies such as the North American Electric Reliability Corporation, the Federal Energy Regulatory Commission and the National Institute of Standards and Technologies in the US, equivalent agencies in Asia and Smart Grid task forces in the European Union and its member states, do provide standards and guidelines as the Smart Grid evolves, with stricter penalties for non-compliance. However, interoperability between regulation and control is still missing.

“What are your company’s three most important energy industry priorities?”



Base: 56 North American and European IT budget decision-makers in the energy industry (multiple responses accepted)

Figure 5: Forrester Research, Forrsights Budgets and Priorities Tracker Survey Data, Q4 2011

Global security standards for the AMI are still in their infancy and, as a result, some countries have started their own initiatives. Germany has taken a lead with the definition of mandatory security profiles for smart meter gateways[9]. Embedded security modules in these gateways will restrict the electronic metering and transmission of personally identifiable information (PII) to authorised internal and external service providers within the Smart Grid ecosystem. It is expected that the German initiative, driven by the Federal Office for Information Security (BSI) will have an impact on other countries in the EU, whose regulatory bodies are carefully watching its progress.

Demonstration of the successful implementation of compliance based on the different regulations can be a very time consuming and costly process if it is not supported by automated governance, risk and compliance tools.

Addressing privacy concerns

Smart meters collect information about electrical devices used as well as lifestyle and behaviours in general. Most countries have strong directives in place relating to PII collection, processing and storage. Although leakage of this type of information provides no immediate risk for electricity provisioning to the public or to industry, strong information protection needs to be guaranteed for a trusted and smooth adoption of smart meter programmes. Security concerns in the Netherlands caused the government to postpone the introduction of these technologies. Even in the US, privacy concerns have increased and consumer initiatives have been created to reject smart meter installations.

Managing insider risk and fraud

Energy theft through the manipulation of meters is becoming a profitable business for fraudsters. Automated remote metering can create opportunities for malicious insiders. According to an FBI cyber bulletin, an electricity utility company in Puerto Rico was the target of a wide-ranging smart meter fraud[10]. Former employees of the meter manufacturer and the utility used their knowledge to reprogramme meters in exchange for cash, so that the associated buildings appeared to be consuming less power than was actually used. Consumers who exploited these fraud techniques were able to save 50-75percent of electricity costs, adding up to an estimated $400 million annual loss for the energy provider.

In another case of fraud, criminals in the UK hacked a new key card system used to activate prepaid energy meters. Dressed as power company workers, the criminals then simply went door-to-door selling illegal credit at very attractive prices.

Experts predict that the occurrence of similar fraud attacks will rise as smart meter technology is more widely adopted. A Gartner security analyst confirmed to Symantec that the analyst house ranks the fraud risk for utilities as extremely high if no countermeasures are in place.

Protecting and storing increased amounts of data

Power and energy companies are struggling to keep pace with ever-growing data stores and to protect data cost-effectively. New technologies for billing, alongside more granular monitoring of power usage generated by smart meters, have put additional pressure on efficient storage management and information protection. Five million smart meters read every 15 minutes will generate 14 petabytes of PII, if regulatory requirements demand that this data is kept for at least seven years.

In addition, utilities, service providers and end users may need access to this information. Therefore, security architects need to implement a secure storage infrastructure to avoid data leakage and illegal access, but also to provide timely access to information and audit trails whenever requested.

Preparing for organisational and cultural change

Internally, as the traditionally isolated OT with proprietary SCADA systems hits IP-based IT office processing, it will cause generations of technologies to merge, leading in turn to substantial organisational and cultural changes. Traditionally, security risk in OT is managed completely separately from Enterprise IT risk. With Smart Grid, OT and IT will increasingly merge and the fragmented ownership risk across the internal organisation will need unification.

Deregulation and liberalisation will lead to a new ecosystem of external stakeholders, including third party service providers and other market players trading electricity. Communications Service Providers will play a dominant role as they connect the Smart Grid networks and provide the machine to machine (M2M) communication infrastructure between all entities.

However, the number of internal and external players further increases the complexity and the need for end-to-end security architecture. Continual monitoring of SCADA and AMI systems to maintain system integrity and manage risk is a necessity, given the number of complex technologies in place. Only end-to-end visibility and real time analysis of available information in the Smart Grid will help to quickly identity and mitigate security risk and potential outages.

The Forrester survey also shows the introduction of mobile technologies for the field service workforce is another huge investment priority within the utility industry.[8] Due to the rise in mobile malware, project leaders need to take security into account, otherwise new attack vectors will be opened.

Security and information protection for the Smart Grid

Achieving a secure grid is not an easy task. Robust and provable security does not start with deploying point products to fill holes. To begin with, vulnerabilities must be identified and analysed using a risk management process supported by a framework that directly relates to business risk. Meeting regulatory requirements, which include standards and guidelines for mitigating security related business risk, also involves implementing controls for the Smart Grid.

The European Network and Information Security Agency (ENISA) confirmed that 'processes' are seen as the most important pillar to secure the Smart Grid – more important than technology and people[11].

Governance, risk management, and compliance (GRC) provides the necessary framework within which to implement security in Smart Grid segments. GRC helps security leaders in utilities to communicate IT risk in business-related terms, prioritise remediation efforts based on a composite view of risk, and automate assessment processes to improve overall security and compliance posture. Based on best practices and guidelines for protecting ICS, the framework should support various steps: from identifying critical assets, analysing threats and risk, and identifying, selecting and implementing countermeasures, to continuously performing audit processes.

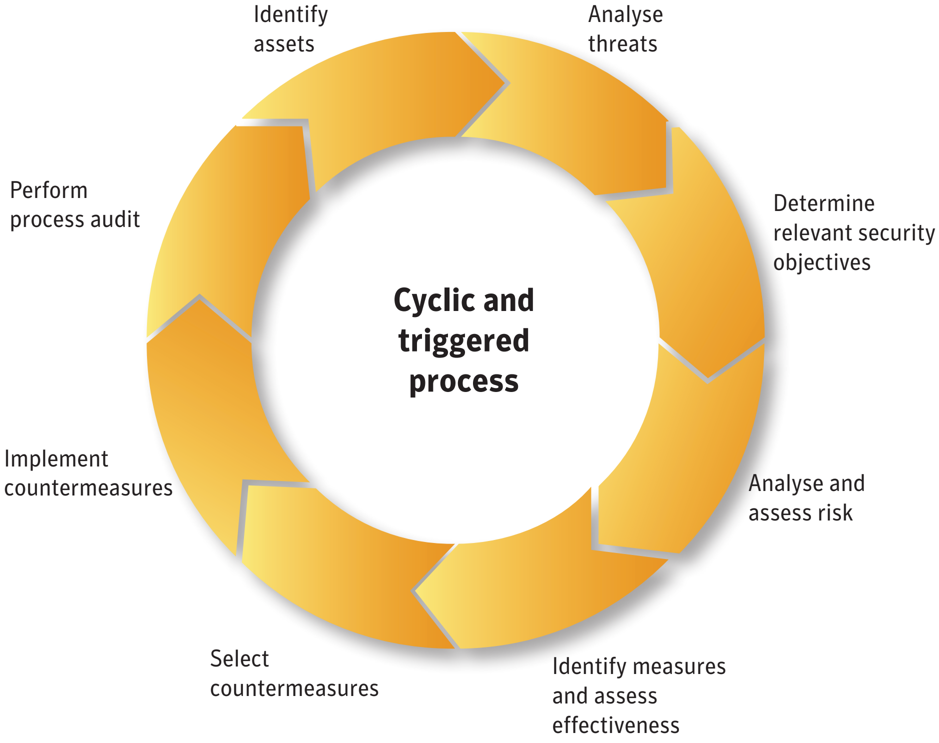

Identify assets
Analyse threats
Determine relevant security objectives
Analyse and assess risk
Identify measures and assess effectiveness
Select countermeasures
Implement countermeasures
Perform process audit
Cyclic and triggered process

Figure 6: A cyclic GRC process as the foundation for ICS (Source: VDI, VDE 2182)

Smart Grid security will also change the priority of critical characteristics. Until now, availability in ICS was the main criterion: more important than confidentiality and integrity, which are the top priorities for IT. Stuxnet has opened the eyes of OT managers and the integrity of the ICS processes and related information has now become at least as important as availability of control systems.

Focusing solely on IT data centers and operation control centres is not enough to tackle the risk challenges of the Smart Grid. As the organisational ecosystem and the technical segments are complex, a comprehensive end-to-end approach is necessary. Each of the Smart Grid segments need to be analysed, assessed and secured, but not in an isolated way. Security officers should consider the following four disciplines as part of their GRC framework and security strategy:

- Securing SCADA systems
- Embedding security within data
- Managing smart endpoints and smart meters
- Controlling the data explosion

Securing SCADA systems

Operation control centres are at the heart of managing and controlling the grid. Recent attacks on SCADA-based critical infrastructure demonstrate the need to make security a top priority.

The 10 most significant SCADA vulnerabilities were analysed by the US Department of Energy's Idaho National Laboratory (INL) between 2003 and 2011. SCADA vendors and energy utilities should use the table below to assess their control systems for these common vulnerabilities and mitigate with appropriate countermeasures[12].

Unsurprisingly, 'unpatched published vulnerabilities' was identified during the analysis as the most likely access vector. Software that is not using the newest patch version and is therefore vulnerable is often spread over many SCADA systems. In some instances, SCADA owners are not allowed to patch their control systems, as they would risk losing the certification and integrity of their control systems. Availability and operational effectiveness must therefore be preserved and a different security approach is required for energy delivery control systems that will not impede operations.

Top 10 most critical SCADA vulnerabilities

Vulnerability	SCADA Impact
Unpatched Published Vulnerabilities	Most Likely Access Vector
Web Human-machine Interface (HMI) Vulnerabilities	Supervisory Control Access
Use of Vulnerable Remote Display Protocols	Supervisory Control Access
Improper Access Control (Authorisation)	Access to SCADA Functionality
Improper Authentication	Access to SCADA Applications
Buffer Overflows in SCADA Services	SCADA Host Access
SCADA Data and Command Message Manipulation and Injection	Supervisory Control Access
SQL Injection	Data Historian Access
Use of Standard IT Protocols with Clear-text Authentication	SCADA Credentials Gathering
Unprotected Transport of SCADA Application Credentials	SCADA Credentials Gathering

Figure 7: Top 10 most critical SCADA vulnerabilities (Source: Idaho National Laboratory)

Unpatched software integrated into SCADA

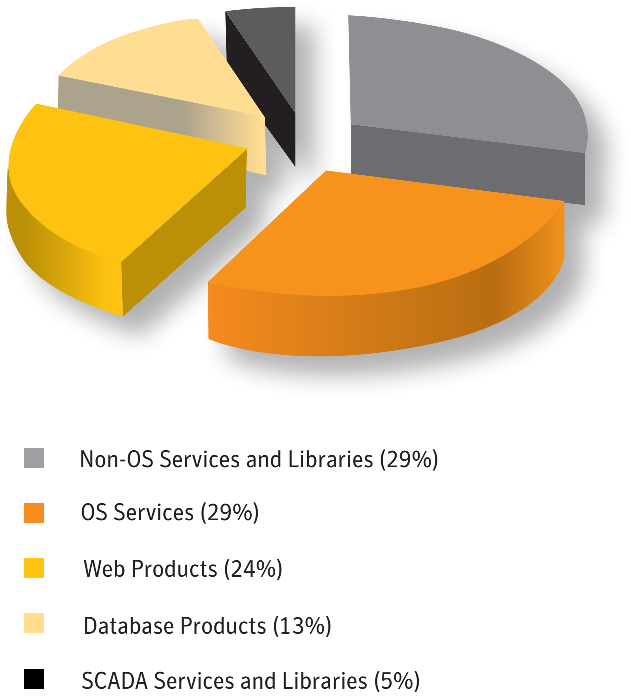


Figure 8: Unpatched Software Integration Statistics (Source: Idaho National Laboratory)

SCADA systems can profit greatly from the deployment of advanced security solutions that harden the environment, detect anomalies and respond to threats, while continuously monitoring the interaction with field devices and the Internet. The use of sophisticated heuristic and whitelisting techniques provides protection against zero-day attacks. In the example of the Stuxnet worm, many of the zero-day vulnerabilities could have been protected by the setting of policies to allow only certain system applications to run.

Among the top SCADA vulnerabilities identified by INL were improper authorisation and authentication, standard protocols with clear text authentication and unprotected transport of SCADA credentials. Identity and access management solutions must have higher priority, especially in consideration of the accelerating interconnection with enterprise IT systems, and the adoption of cloud, mobile and remote management functionalities.

Embedding security within data

Security has changed radically from protecting the perimeter to protecting the information, so the most obvious approach is to embed security within the data itself. Multiple technologies exist and can be combined to achieve confidentiality, integrity and authentication: for example, to prevent fraud using metering data or guarantee privacy of PII.

Transferring critical control information or PII over unsecure lines to service providers or cloud storage locations requires data encryption. User authentication leveraging strong two-factor authentication and one time password entry, allows only trusted personnel to gain access to critical data and control systems. Digital certificates can also be used for authentication, signing and encryption.

Utilities should only select third-party providers who are committed to fulfilling these requirements. Where cloud deployments are part of the Smart Grid, cloud service providers must commit to support the security guidelines developed by the Cloud Security Alliance (CSA)[13].

Furthermore, it is important to automate the controls on critical information and only allow transfer using predefined policies based on the structure and type of data content. Technologies such as data loss prevention can automate the generation of policies controlling the flow, storage and access and of critical information.

Managing and securing smart devices and smart meters

Energy providers need to manage the increasing number of smart devices that play a dominant role in the Smart Grid ecosystem. Scalability and automation will become important functions due to the sheer number of intelligent endpoints, mobile devices and smart meters. Only well-managed systems are secure systems, and utilities should not allow AMI to become a new entrance point for attackers.

In particular, the deployment of smart meters creates new management challenges for energy providers. Experiences in the US market have shown that the complexity of the AMI network required more staffing than originally expected. The lack of in-house expertise with these new technologies can open doors for dedicated service providers offering AMI management and security solutions[14].

Currently, very little regulatory pressure exists to implement security for smart meters. Therefore, most of the devices deployed worldwide have little or no security embedded, which potentially poses major risks for cyber attacks, loss of privacy and fraud. To mitigate these risks, as deployment of smart meters increases, some countries, including the UK through its Department of Energy and Climate Change, have started to define stronger smart meter protection standards.

The German BSI is currently working on a mandatory security profile, protecting AMI with the focus on the smart meter gateway. The smart meter gateway is vital as it facilitates communication between the components in the consumer home area network (HAN) and the outside world. It can be seen as a special kind of firewall dedicated to smart metering functionality, which collects, processes and stores the records from meters and ensures that only authorised parties have access to them. All relevant information is signed and encrypted before sending. The gateway utilises an embedded security module as a cryptographic service provider for generating and verifying digital signatures and negotiating keys.

Due to scalability requirements, the public key infrastructure (PKI) is the key security technology and best practice for large-scale key management. By implementing PKI into the gateways or meters themselves, the Smart Grid can be secured at the communication layer, creating a system that identifies connected meters as authentic, verifies configuration and integrity, then validates the meters for network access. PKIs are ideal for large-scale security deployments that require a high level of security with minimal impact on performance. In a PKI environment, it is essential that private keys and certificates are guarded by a reliable management solution that protects against ever-evolving data threats. As few utilities or Communication Service Providers can afford to build and run such a highly scalable certificate authority (CA) for device authentication, managed PKI service providers with a strong focus on this business provide a good alternative to internal management.

Controlling the data explosion

The digitisation of the electric grid, together with the deployment of millions of smart meters, generates a huge amount of control, status, billing and other information. The greater the sensitivity of the data generated, the higher the risk of not managing it in terms of security and availability. Processing data while protecting customer privacy and controlling critical information is high on the list of concerns for energy providers and their operational and IT staff. Cost-efficient and secure information management requires several layers of solutions. Data must be categorised,

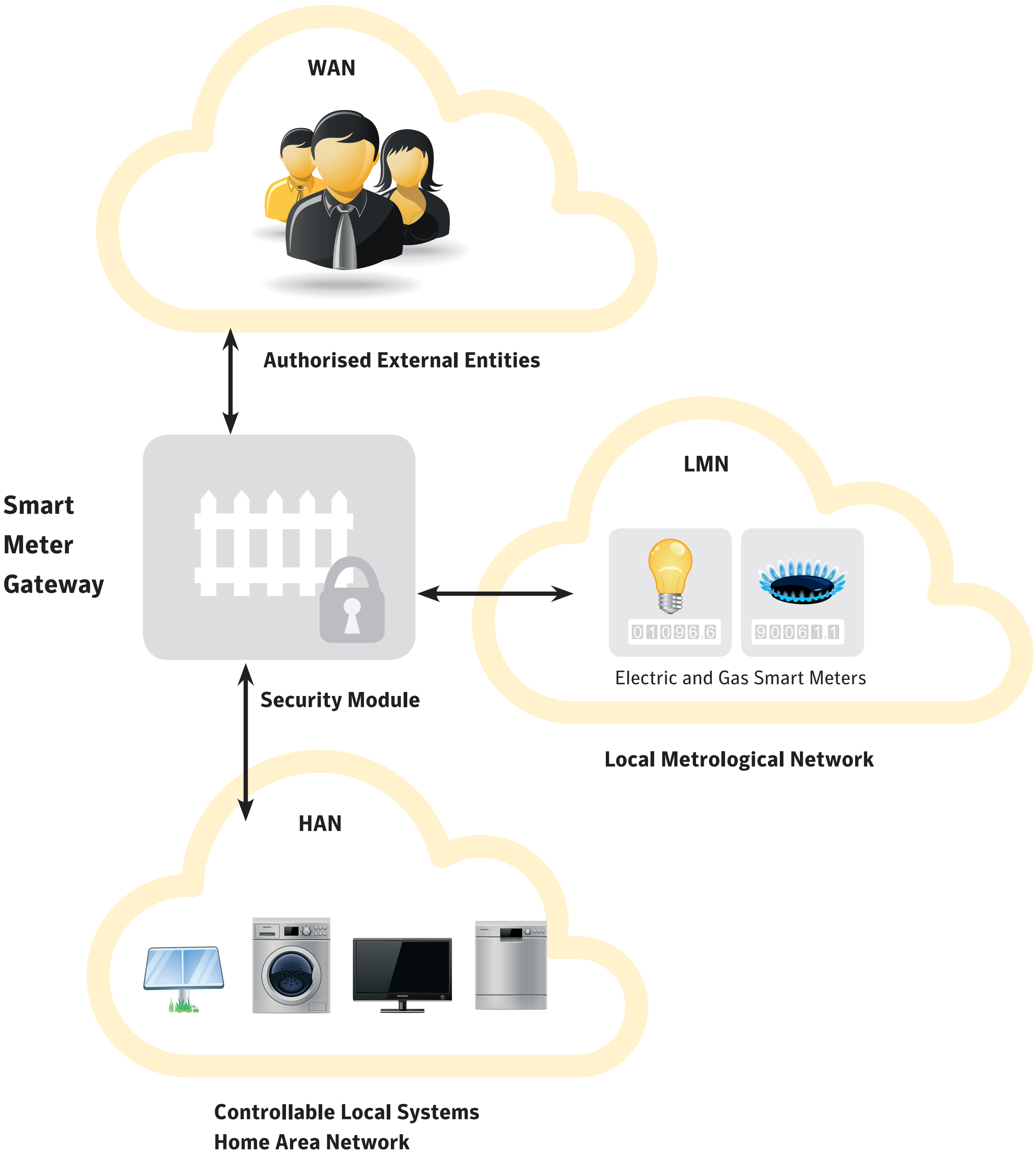

WAN
Authorised External Entities
Smart
Meter
Gateway
Security Module
LMN
01096.6
90061.1
Electric and Gas Smart Meters
Local Metrological Network
HAN
Controllable Local Systems
Home Area Network

Figure 9: Security Profiles for Smart Meter Gateways (Source: German Federal Office for Information Security)

archived and processed in a manner that enables organisations to demonstrate regulatory compliance, provide evidence of accurate customer billing, and respond to potential legal actions. Data loss protection to control data is critical to customers and energy providers, while storage lifecycle management is crucial to ensure that only critical data is stored on fast storage, and less critical data is automatically moved to less expensive disk arrays and even tape. As data must be preserved, there is also a need for efficient backup with all the latest deduplication technology.

Achieving business priorities

There are four key areas to consider when aligning a secure Smart Grid implementation with the needs of the business:

Protect critical infrastructure

Cyber attacks against critical infrastructures and ICS have made headlines. Governments have put a lot of pressure on utilities to implement appropriate security to avoid regional or even nationwide blackouts with catastrophic impact on the population and economy. By starting with GRC as the security foundation, utilities can identify and mitigate potential risks more easily.

Comply within a highly regulated industry

Regulatory bodies provide standards and guidelines that are evolving with stricter penalties for non-compliance. Again, GRC helps to define policies in order to achieve compliance with external regulations and best practice frameworks. These policies map to controls for multiple mandates to avoid redundant efforts and drive costs down through automation.

Gain customer confidence

Experiences of various countries around the world have shown that privacy of PII is vital to gain buy-in from energy consumers. A lack of confidence can cause massive delays in Smart Grid transition. So, device authentication and data encryption for the millions of smart meters permanently generating and sending PII data to the utilities or service providers is a must.

Prevent smart meter fraud and ‘energy theft’

Cyber criminals are always looking for ways to make money. Massive deployments of smart meters will motivate criminals to develop and monetise tools to manipulate the metering of electricity consumption, putting utilities at risk of losing significant amounts of revenue due to large-scale fraud. AMIs protected by state-of-the-art PKI or managed PKI architectures make it impossible to break in and manipulate metering data, therefore guaranteeing fair revenue streams for utilities.

Recommended solutions for a secure Smart Grid transition

To optimise the benefits of this new ecosystem it is important to implement the right processes and best practices.

Start with a risk management process to enforce IT policies and automate compliance. Use GRC for prioritising risks and defining policies that span all segments of the Smart Grid including SCADA and AMI. Utilities can enforce policies through built-in automation and workflow to not only identify threats, but also remediate incidents as they occur or anticipate them before they happen.

Align the two separate worlds of OT and IT as the transition towards the Smart Grid will merge both areas. The risk management process to achieve the necessary end-to-end security must encompass both worlds.

Protect information proactively by taking an information-centric approach. Embedding security within data and taking a content-aware approach to protecting information is vital for identifying who owns it, where sensitive details reside and who has access to it. Classify data and utilise encryption to secure sensitive information and prohibit access by unauthorised individuals.

Authenticate user and smart meter identities by leveraging solutions that allow businesses to ensure that only authorised personnel have access to systems. Strong authentication also enables organisations to protect public-facing assets by ensuring the true identity of a smart device, system, or application. This prevents individuals from accidentally disclosing credentials to an attack site and from attaching unauthorised devices to the infrastructure.

Manage systems by implementing secure operating environments, distributing and enforcing patch levels, automating processes to streamline efficiency, and monitoring and reporting on system status.

Protect the infrastructure by securing endpoints, messaging and web environments. In addition, defending critical internal servers and implementing the backup and recovery of data should be priorities. Organisations also need visibility and security intelligence to respond to threats rapidly.

Ensure 24x7 availability of the critical infrastructure by implementing non-disruptive testing methods and reduce complexity by automating failover. Virtual environments should be treated identically to physical environments, with organisations adopting more cross-platform and cross-environment tools, or standardising on fewer platforms.

Develop an information management strategy that includes an information retention plan and policies. Organisations need to stop using backup for archiving and legal retention, implement deduplication everywhere to free up resources, use a full-featured archive and eDiscovery system and deploy data loss prevention technologies.

Don’t focus solely on cyber security and critical infrastructure protection but also consider privacy issues regarding customer PII, fraud risks and other challenges in your security framework.

Cooperate with a security and information protection partner with worldwide visibility of attack trends to address the complete range of security challenges the energy industry is facing.

Conclusion

To maximise the opportunities offered by the transition to the Smart Grid, energy utilities must embrace the challenges this new ecosystem will bring. Developing an end-to-end architecture designed to manage critical infrastructures, promote compliance, mitigate fraud and protect privacy will be key to successfully navigating this transformed world.

The right partner for infrastructure and information protection

Symantec protects the world's information, and is the global leader in security, backup and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our industry-leading expertise in protecting data, identities and interactions gives our customers confidence in a connected world.

The company supports energy providers and their suppliers in addressing Smart Grid challenges with an end-to-end security and information management approach. Symantec works closely with governments and is coordinating the EU research project CRISALIS on detection and remediation of vulnerabilities and attacks in critical infrastructures.

Symantec operates the largest and most comprehensive PKI solutions for enterprises and service providers available on the market today, and has been doing so since 1995. More than 200 million device certificates have been issued to date.

References

1. IDC Energy Insights Predictions 2012: EMEA Utilities
2. Symantec Security Response: W32.Stuxnet Dossier, February 2011 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
3. Symantec Internet Security Threat Report ISTR 17, April 2012
4. Symantec Security Response: W32.Duqu – the processor to Stuxnet, November 2011
5. Symantec Security Response: http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east
6. CRISALIS - CRitical Infrastructure Security AnaLysIS, an EU funded project for Critical Infrastructure Protection http://www.crisalis-project.eu/
7. Symantec Critical Infrastructure Protection Study, November 2010
8. Forrester, The IT-driven Energy Revolution incl. the Forrsights Budget and Industry Priority Tracker Survey, Q4 2011
9. BSI Germany, Protection Profile of a Gateway for a Smart Meter System, Summer 2012
10. FBI Bulletin, FBI Concerned About Smart Meter Hacking, April 9, 2012
11. ENISA Smart Grid Security Recommendations; Annex III – Survey and Interview Analysis www.enisa.europa.eu
12. Idaho National Laboratory, Vulnerability Analysis of Energy Delivery Control Systems, September 2011
13. Security Guidance for Critical Areas of Cloud Computing www.cloudsecurityalliance.org
14. IDC Energy Insights: Smart Metering in North America: Market Update, October 2011

Additional source material:

Symantec White Paper 'Smart Grid – A view from Symantec'

Glossary

AMI	Advanced Metering Infrastructure
BSI	German Federal Office for Information Security
CA	Certificate Authority
GRC	Governance, Risk and Compliance
HAN	Home Area Network
ICS	Industrial Control Systems
OT	Operational Technology
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
SCADA	Supervisory Control and Data Acquisition

Author

Frank Bunn, Symantec Corporation

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec is a global leader in providing security, storage and systems management solutions to help customers secure and manage their information and identities.