IT COMPLIANCE IN SMART GRIDS

Martin SCHAEFER
Vattenfall AB – Sweden
Martin.Schaefer@vattenfall.com

Erik ÅBERG
KTH – Sweden
eaberg@kth.se

Jens ZERBST
Vattenfall AB – Sweden
Jens.Zerbst@vattenfall.com

Iiro RINTA-JOUPPI
Vattenfall AB – Sweden
Iiro.Rinta-Jouppi@vattenfall.com

ABSTRACT

The increasing complexity of Smart Grid architecture resulting from interconnectivities and higher levels of information exchange as well as the level of detail of customer data involved creates additional risks. The architectural design and implementation of the technology according to generally accepted standards can reduce risks of technological incompatibility or the violation of customer data requirements, for example.

Accepted standards and certifications that confirm compliance with these are needed, and could become a competitive advantage or requirement for service and technology providers

INTRODUCTION

One challenge in developing a Smart Grid is the introduction and expansion of a communication network underlying the electricity grid in order to support intelligent control and communications between the various participating domains, e.g. bulk generation, markets or customers.

The introduction of new communication and intelligent control systems implies new threats and vulnerabilities for the communication network. This leads to substantial risks to the reliability, ruggedness, safety and security of the electricity network, and to the life cycle of the Smart Grid in general.

The sustainable security of the communication network and information systems is essential for building up trust between the participants and enabling the necessary connectivity in the Smart Grid concept. IT compliance enables the alignment and interconnection of Smart Grid IT technology, and a certification strategy can assure trust between the various Smart Grid actors.

SMART GRID ARCHITECTURE

In 2008, the EU agreed to work towards the 20/20/20 target. Smart Grids are expected to help reach this target by altering consumer behaviour towards increasing energy efficiency as well as enabling greater use of renewable energy in the grid [1]. This includes balancing power utilization peaks and developing high production/low consumption scenarios, e.g. with electric vehicles (EV) [2] or steering the output levels of non-renewable energy sources depending on the output levels of renewable ones such as wind or solar energy [3]. To achieve these targets and implement possible Smart Grid functionalities as described by the Electric Power Research Institute (EPRI) [4], some challenges and constraints have to be considered

Challenges:

- Introduction and expansion of a communication network for the current and future electricity grid
- Introduction of new technology
- Introduction of intelligent control and connectivity between different domains (see Figure 1)

Constraints:

- Long-term use of legacy assets in the domains of operation, bulk generation, transmission and distribution
- In some parts, use of a large-scale homogeneous technical environment, e.g. Smart Meters
- There are currently no common or aligned standards designed to achieve an architecturally compatible technology.

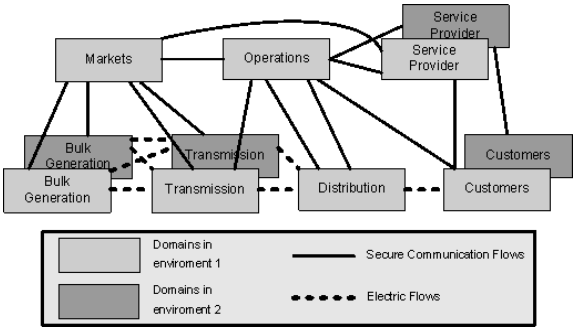

Figure 1. Conceptual Model from NIST [5] extended with domains which are partly subject to different rule sets (e.g. standards, legal, and location)

Interconnectivity between different domains (see Figure 1) will require multiple stakeholders to share information, and a Smart Grid Cyber Security Coordination Task Group (CSCTG) has started the work of identifying Smart Grid logical interfaces requiring standardization and common definitions to coordinate the security efforts of so many diverse actors [5].

As the number of users of Smart Grid increases comparable to the number of user of the internet today and the grid becomes more advanced in passing information back and forth, the security system must not only cover the need to maintain the availability of the power grid and its critical infrastructure services but also ensure the integrity and confidentiality of the customer data that it handles [6].

RISK SCENARIOS

The increasing number of users, new technologies, legacy systems, higher complexity due to greater interconnectivity

(even to non-trusted partners), the huge number of devices with homogeneous technology and partly exposed infrastructures increase the risks faced by the Smart Grid.
Beside the typical IT security threats (see Table 1), new threats and risks have to be managed. The increasing involvement of customers as well as the interconnection of technology over several domains introduces new attack vectors.

Customer Data

The granularity of the customer-use data collected via Smart Meters means that threats to customer integrity must be considered, especially as the interconnectivity of different systems implies sharing and aggregating customer data throughout the grid actors (across national borders and thus across different legal environments) for tracking energy exchanges between many parties in order to permit correct billing [5].
Examples of the misuse of customer data include profiling a customer's daily activity patterns based on energy use, at what times and even where, and live monitoring of customer data permitting unauthorized surveillance. The unauthorized aggregation and selling of customer data to third parties in order to target customers with directed advertising could also jeopardize customer integrity [6].
The incorrect handling of user data or insufficient data protection measures introduce further risks. In an example from the UK, this form of misconduct was found to constitute a breach of the Data Security Act, leading to fines being imposed on the guilty company [7].

Fraud

The problems noted above refer to the confidentiality of customer data, but from the service providers' point of view, its integrity may be even more important. If a customer manages to tamper with his data input to the Smart Grid, e.g. so that the user can recharge his EV without being recorded for billing or can reassign his record to another user, this could enable fraudulent behaviour with financial implications [6].
Even inadvertent breaches of customer data integrity could lead to financial loss if this data is used as a basis for billing. In view of the many actors expected to be involved in the Smart Grid, technical issues such as an actor's failure to comply with the use of standardized data mark-up or protocols for its successful exchange could also jeopardize the integrity of the data used.
The potential impact of such false financial reporting can be seen in various industries such as banking and telecoms, where falsified reporting and manipulated data, for example, can have huge financial repercussions, as seen in the WorldCom or Enron scandals.

Technical Threats

The development of Smart Grid technologies is especially challenging because of the various sectors and diverse stakeholders involved (national/international utility companies, various suppliers of technology and services). The main challenge here is to develop a technology that is mutually compatible across all actors involved. Diverse data formats or protocols can lead to incompatible or inefficiently compatible technologies, and any solutions imposed to overcome this problem would introduce new technological or security risks.
Legacy devices are another technological challenge [8]. The long life cycles of electric grid components, often several decades, increase the demand for integration of legacy systems, with the associated risk of incompatibility. The critical role played by energy in our society also makes its technology an inviting target for espionage, sabotage or terrorist attacks. This requires other IT security risks to be considered as well: they can be any combination of intentional/unintentional and malicious/non-malicious risks, as shown in Table 1[9].

	Intentional	Unintentional
Malicious	E.g. a dedicated attack by criminal individuals, groups, terrorists or nations	E.g. an undirected attack by a 'common' Botnet virus
Non-malicious	E.g. a disgruntled employee/ outsourcing vendor intentionally manipulates sensor data	E.g. malfunction of software or procedures

Table 1. Matrix of possible threat types highlighted by an example

One of the latest examples is the Stuxnet attack [10], where a specific virus was created that used multiple vulnerabilities and targeted a specific type of system to intentionally alter its behaviour and possibly cause damage [11].

COMPARISON WITH OTHER MARKETS

These examples have shown that compliance is required in several areas. The critical role played by energy in our society, its technical complexity, customer involvement and the financial importance of the energy industry require a differentiated approach to compliance. Critical infrastructures serving different markets in various locations require diverse legal aspects to be considered.
A common rule set must also be adopted when a utility handles huge amounts of data from customers in different locations and legal environments involving real-time data exchange with third parties operating in other legal environments. Compliance to a common rule set would promote trust between various participants and domains.
Smart Grids are not the only area where technology is applied in a global context. The financial and telecoms industries have a similar (isomorphic) IT architecture and provide services throughout different domains in diverse legal environments.

The fact that these markets operate in an international context and have already faced similar challenges and risks makes them a valuable reference.

Financial market

The Sarbanes-Oxley Act (SOX) was introduced by the US after major corporate and accounting scandals. It was subsequently adopted by Europe and Japan (EuroSOX, J-SOX) to create a global rule set for activities such as governance, reporting and enterprise risk management.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) was founded by the American Accounting Association. Its frameworks provide guidance on critical aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud and financial reporting [12].

Control Objectives for Information and related Technology (COBIT) is a framework designed for technical compliance. It is fully aligned with other IT standards such as ISO/IEC 27000-series or the NIST 800 series. Compliance with such standards is becoming increasingly important for companies operating on the international market and wishing to maintain their competitiveness.

Compliance for Telecommunications

A need to improve the consistency of the regulatory framework within the telecommunications industry in the EU led to the forming of the Body of European Regulators for Electronic Communications (BEREC) in 2010. Among its goals is to ensure compliance with the EU regulatory framework in a consistent manner even between the regulatory authorities of the different member states and to disseminate best practices across the industry [13].

The telecoms sector also makes use of technical standards such as Signaling System 7 (SS7) that enables interconnectivity between large networks requiring continuity testing for compliance [14]. This standard is also a basis for telecommunication services that are compliant with different legal requirements. The European Telecommunications Standards Institute (ETSI) has also developed standards specifying common baseline models for user data [15].

METHODS

Due to the complexity and interconnectivity of the different parts of the Smart Grid, from bulk production to the transmission and distribution to customers, a number of standards are already in place to guide the various parts of the process, such as the ISA99 series, the NERC Critical Infrastructure Protection (CIP) series and NIST 800-82.

As the need arises for developing additional standards that are specialized for the Smart Grid, the resulting abundance of standards increases the demand for compliance. One way of dealing with this increased complexity is to develop a model that maps the different domains of the Smart Grid on the basis of the standards that govern them.

By using such a model, actors within specific domains can see which standards apply to their part of the process, thereby highlighting where compliance is needed. One such model has been described as a normalized zone model in "Zone Principles as a Cyber Security Architecture Element for Smart Grids" [9].

However, it is not always straightforward to subsequently coordinate such standards, and as the Smart Grid is still being developed and has not yet been implemented on a large scale, it would be useful for the standardization efforts to be coordinated from the start. This would help to avoid developing incompatible standards, i.e. where complying with one standard would imply non-compliance with others.

Many of the current standards applicable to the Smart Grid focus on the technical aspects. Recent publications review and compare such technical standards in different areas [16].

Technical compliance could be tested by comparing implementations with standardized reference architectures and common configurations. However, these architectures are currently descriptive, designed to be used as an aid in developing the Smart Grid, rather than prescriptive, designed to steer its implementation [5].

The need for standardization and harmonization of the electricity grid has also been identified by the European Regulators Group for Electricity and Gas (ERGEG), which is planning work on a pilot framework guideline [17]. However, there are currently no common standards that steer and enable a common Smart Grid rule set while considering the different aspects of customer privacy, technical issues and fraud.

Such common standards or best practices could steer the standardization process and spread the responsibility for developing standards to address various threats to Smart Grids. If one standard addresses customer data issues and another one addresses technical issues, they would fit together into a framework of mutually compliant standards. Once this open, flexible and scalable framework has been established, efforts could be made in the different countries to align their requirements and certification efforts with this framework in order to comply with their various local laws. Such a framework could aid the development of compliant Smart Grid technology on a global market as well as build trust between compliant actors.

There are two sides to compliance, however, and both need to be addressed if it is to carry any weight: this approach could be promoted by the framework suggested here. Firstly, standards or legislation must be established to define the required compliances. Secondly, authorized standards institutes must introduce a certification process to ensure such compliance.

CERTIFICATION

Once certain requirements have been defined, compliance with them can be evaluated. As a rule, independent organizations issue certificates that verify such compliance.

Certification leads to competitive advantages or is stated as a requirement in several areas.
Good examples are certifications to the ISO 9000 series (quality management system), to the ISO/IEC 20000 series (IT service management) or to the ISO/IEC 27000 series (information security management). Many industries, such as cars and railways, require certified subcontractors for their products. In the IT sector too, certifications are often a requirement for being qualified to provide services to other companies or partners.
Special certifications for Smart Grids could ensure technological compatibility, security, reliability, availability and the privacy of customer data, for example. Some first certification initiatives have already become available in special areas [18]. In the current phase of Smart Grid development, such certification could lead to competitive advantages over other service and technology providers.

CONCLUSION

The harmonization and standardization of the relevant technology is a requirement for the interconnected functionalities of Smart Grids. As in comparably evolved markets, Smart Grid actors could benefit from compliance with standards which can be verified by checks and certifications.
Compliance to standards and best practices in Smart Grid technology could allow interconnected functionalities to minimize risks involving customer data, fraud and the technology used.

REFERENCES

[1] European Commission, 2010, *COM (2010) 265 Final Analysis of options to move beyond 20% greenhouse gas emission reductions and assessing the risk of carbon leakage*, European Commission, Brussels, Belgium.

[2] U.S. Department of Energy, *The Smart Grid: An Introduction*, Online: http://www.oe.energy.gov/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf, last visited 2011-01-10 21:46

[3] A. Battaglini, J. Lilliestam, C. Bals & A. Haas, 2008, *The SuperSmart Grid*, European Climate Forum, Potsdam Institute for Climate Impact Research.

[4] EPRI, *Use Case Repository*, Webpage, Online: http://www.smartgrid.epri.com/Repository/Repository.aspx, last visited 2011-01-11 14:16.

[5] NIST, 2010, *NIST SP 1108 NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*.

[6] NIST, 2010, *DRAFT NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements*, The Smart Grid Interoperability Panel – Cyber Security Working Group.

[7] D. Flint & V. Surgenor, 2010, *United Kingdom: How Secure Is Your Customer Data*, Mondaq, Online: http://www.mondaq.com/article.asp?article_id=108670, last visited 2011-01-10 21:58.

[8] Cisco Systems, Inc., 2009, *Securing The Smart Grid*, White Paper, Online: http://www.cisco.com/web/strategy/docs/energy/SmartGridSecurity_wp.pdf, last visited 2011-01-10 22:09

[9] J. Zerbst, M Schaefer, I. Rinta-Jouppi, 2010, "Zone Principles as a Cyber Security Architecture Element for Smart Grids", *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES*.

[10] N. Falliere, L. O. Murchu & E. Chien, 2010, *W32.Stuxnet Dossier*, Symantec Security Response, Online: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, last visited 2011-01-10 22:31.

[11] Y. Katz, 2010, *Stuxnet virus set back Iran's nuclear program by 2 years*, Jerusalem Post, Online: http://www.jpost.com/IranianThreat/News/Article.aspx?id=199475, last visited 2011-01-10 22:37.

[12] The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Official webpage, Online: http://www.coso.org/, last visited 2011-01-10 22:41

[13] J. Buzek & Å. Torstensson, 2009, *Regulation (EC) No. 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office.* Official Journal of the European Union, L337/1.

[14] Cisco Systems Inc., *SS7 Continuity Testing for Network Access Servers*, Webpage, Online: http://www.cisco.com/en/US/docs/ios/11_3/feature/guide/Cot.html, last visited 2011-01-11 01:13

[15] ETSI, 2010, *TS 132 182 V9.0.0*, France.

[16] P. Koponen, M-L. Pykälä, J. Peltonen & P. Ahonen, 2010, *Interfaces of consumption metering infrastructures with the energy consumers. Review of standards.* VTT Technical Research Centre of Finland, Vuorimiehentie, Finland.

[17] European Energy Regulators' News, *Issue: December 2010 – January 2011*, Online: http://www.energy-regulators.eu/portal/page/portal/EER_HOME/EER_PUBLICATIONS/NEWSLETTERS/December%202010%20-%20January%202011, last visited 2011-01-10 23:47.

[18] TÜV Rheinland, *Smart Grid Product Testing*, Webpage, Online: http://www.tuv.com/en/corporate/business_customers/product_testing_3/telecommunication_it/smart_grid_product_testing/smart_grid.jsp?null, last visited 2011-01-11 00:19.