

Risk Management Framework for the Smart Grid

Riadh W. Y. Habash^{1,2*}, Voicu Groza¹, Daniel Krewski^{2,3}, and Greg Paoli³

¹ School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, Ontario, Canada.

² McLaughlin Centre for Population Health Risk Assessment, University of Ottawa, Ottawa, Ontario, Canada.

³ Risk Science International, Ottawa, Ontario, Canada.

Authors' contributions: Please write this section

Authors may use the following wordings for this section: This work was carried out in collaboration between all authors. " 'Author Riadh. W. Y. Habash, Voicu Groza, Daniel Krewski, and Greg Paoli' designed the study, performed the statistical analysis, wrote the protocol, and wrote the first draft of the manuscript. 'Author Riadh. W. Y. Habash' managed the literature searches..... All authors read and approved the final manuscript."

Research Article

Received 1st March 2013
Accepted xxxxxxxxxxxx 2013
Published xxxxxxxxxxxx 2013

ABSTRACT

Aims: This paper addresses critical issues of the smart grid primarily in terms of information and communication technologies (ICTs), standards, security threats, and possible health effects.

Study Design: A risk-based approach has been presented, which could be implemented to address the security aspects and health impact of the smart grid.

Place and Duration: This study was carried out in Ottawa, Ontario, Canada during the period of January 2012 to January 2013.

Methodology: The paper evaluates the security threats to the smart grid as well as the health risks of smart meters and wind turbines currently under implementation in the context of radio frequency (RF) radiation, vibration, and noise. A combined framework for risk management in major technological and health domains has been proposed.

Conclusion: The proposed framework calls for a coordinated assessment of cyber and power grid risks keeping the whole grid security and human safety goals in mind. Integrated risk management approaches are significantly needed to efficiently guide resource allocations and optimize practices at all levels of the smart grid platform to identify the risk, measure it, minimize it, and finally engineer out the risks by the use of available resources, to an acceptable and approved standard.

Keywords: Smart grid, standards, security risk, health risk, risk management.

*Corresponding author: E-mail: rhabash@site.uottawa.ca;

1. INTRODUCTION

Electric power systems are very complex interconnected networks which include a series of independently operating regional grids that would greatly benefit from the optimization that comes with interconnection provided by the smart grid. The smart grid has been described by IEEE [1] as “a next-generation electrical power system that is typified by the increased use of information and communication technology (ICT) in the generation, delivery and consumption of electrical energy”. The smart grid [2], which is in general referred to as the next generation power electric system, integrates varieties of digital computing and communication technologies to provide efficient, secure, and reliable electricity and information delivery between power generators, suppliers and customers.

The objective of transforming the current electric power grid into a smart grid is to provide reliable, high-quality electric power to digital societies in an environmentally friendly and sustainable way [3]. Deployment of smart grid technologies will happen over a long period of time, adding succeeding layers of functionality and capability onto existing equipment and systems. ICT is the key, but it is only a means to an end. What is not explicitly stated here, but is equally important, is that a fully developed smart grid concept includes in addition to smart meters, technologies at both the transmission and distribution level and extends to both hardware and software, such as monitoring and control systems, as well as primary equipment like transformers and relays. Under this model, the smart grid should be adaptive, with less reliance on operators, especially in responding rapidly to load changing conditions; efficient, by reducing the cost to produce, deliver, and consume electricity; predictive, in terms of identifying potential outages before they occur; integrated, in terms of real-time communications and control functions; interactive between customers, suppliers, and markets; reliable, by reducing the cost of interruptions and power quality disturbances; secure, by reducing the probability and effects of attacks; and safe, in terms of possible health effects, injuries and loss of life from grid-related events.

The smart grid will introduce millions of intelligent computing components that communicate in two-way communication [4]. As such, how to address networking security risk, reliability challenges, and possible health impact are critically important in the design of communication networks for the smart grid. Potential networking intrusion caused by intentional attackers may lead to a variety of consequences [5], from customers' information leakage to a cascade of failures, such as massive power outage and destruction of infrastructures.

This paper is designed to inform utilities, policymakers, researchers, and consumers on concerns and sets forth recommended best practices to reduce the risks of adverse consequences from the adoption of various technologies in the pursuit of the real objectives of smart grid. Various applications of ICTs have been identified in Section 2. Section 3 presents several standards that guideline the implementation of the smart grid. Section 4 discusses a risk-based approach that has been used to protect physical assets but can be modified to help protect the components of the smart grid. Smart grid security threats have been presented in sections 5. Section 6 discusses possible health risk of smart meters and wind turbines in the context of radio Frequency (RF) radiation, vibration and noise, respectively. Section 7 proposes a risk management strategy to mitigate the anticipated risks. Finally, Section 8 provides conclusion.

2. SMART GRID TECHNOLOGIES

Innovation of the electric grid was driven by technology in the past, the current power industry is being modernized and tends to deal with the challenges more proactively by

using state-of-the-art technological advances in the areas of ICTs, sensing, and control [6]–[8]. While the smart grid system is made up of a number of energy subsystems including generation, transmission, distribution, operation, and utilization, many of the communications and security components, are common between these energy subsystems. Fig. 1 shows the typical components of smart grid and the ICT paths that will connect the components.

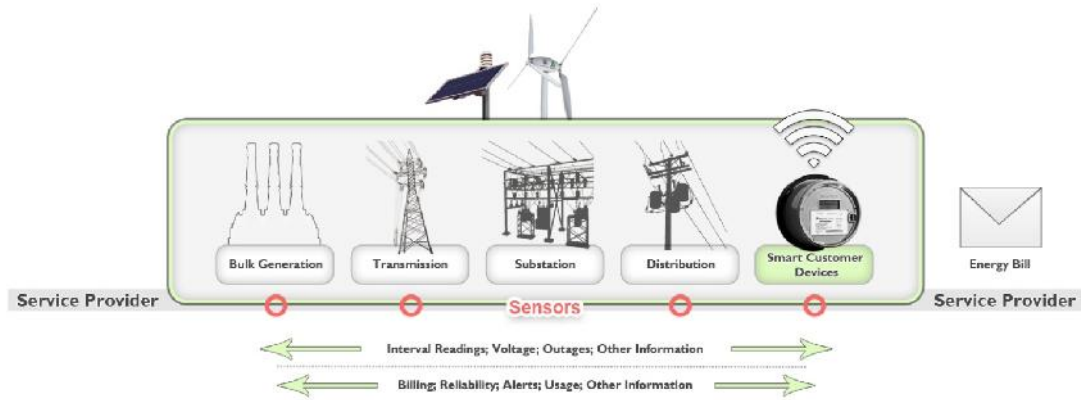


Fig. 1. Typical components of an electric smart grid.

2.1 Communication Technologies

A communications system is the key component of the smart grid infrastructure [9]. With the integration of advanced technologies and applications for achieving a smarter electricity grid infrastructure, a huge amount of data from different applications will be generated for further analysis, control and real-time pricing methods. Hence, it is very critical for electric utilities to define the communication infrastructure requirements to handle the output data and deliver a reliable, secure and cost-effective service throughout the total system [10]. Fig. 2 provides an overview of the smart grid communication landscape.

Various ICTs supported by two main communications media, wired and wireless, can be used for data transmission within the smart grid. Wireless networks are commonly used in the current smart grid deployments. The wireless communications solutions can be either licensed or unlicensed, again depending on the needs of the utility. For the highest reliability, licensed should be the choice. Each of the above options has their advantages and disadvantages, but what is consistently true of any and all of the solutions is the need to have a scalable security solution [11].

Two types of information infrastructure are needed for information flow in a smart grid: first flow is from electrical appliances to smart meters and second from smart meters to utility's data centers. As suggested in [12], the first data flow can be accomplished through power line communication or wireless communications, while cellular technologies or the Internet can be used for the second flow. Table I shows the main communications technologies and their specifications.

There are also many data exchange protocols used between entities such as transmission control protocol (TCP)/Internet protocol (IP), hypertext transfer protocol (HTTP), and file transfer protocol (FTP) are also widely used in the global information technology domain.

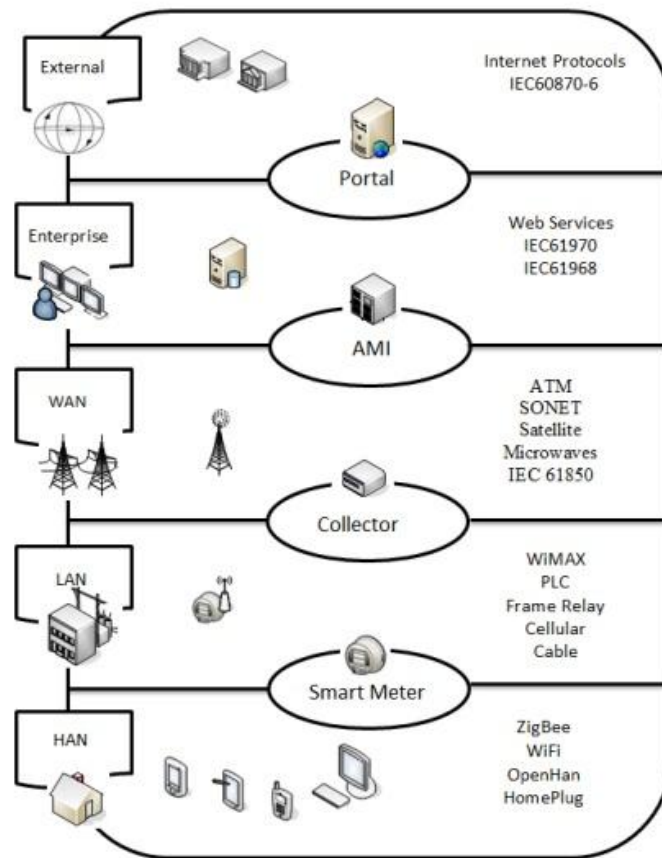


Fig. 2. Smart grid communication infrastructure and examples of technologies.

2.2 Advanced Metering

Advanced metering infrastructure (AMI) is viewed as a foundational-enabling technology for the smart grid. The implementation of AMI solutions in the power distribution system has the potential to benefit both energy suppliers and consumers. Advanced meters will be in constant communication with the electric utility, retrieving real-time prices and transmitting real-time demand upstream. The energy suppliers may benefit by more efficient meter reading, less maintenance cost, and outage location identification. Consumers will also have new opportunities to reduce their energy costs by taking advantage of real-time energy pricing, off-peak rates, and other programs that are possible with the two-way communication networks. AMI solutions can be meshed or point-to point, with local coverage or long range communications. Options for backhaul solutions are fiber, wireless broadband, or broadband over power line. In general, AMI communication solutions are built around five technologies: wireless star, wireless mesh, power line carrier (PLC), broadband over power line (BPL), and fiber optics. Wireless star technologies are available in both licensed (200 MHz, 900 MHz) and unlicensed spectra (900 MHz, 2.4 GHz). Mesh networks are considered very reliable because they provide redundant communication paths that compensate for failures from natural causes.

Table 1. Main communication technologies for the smart grid

Technology	Specifications	Suitability for Smart Grid
GSM	900-1800 MHz; 14.4 Kbps; 10 km.	Suitable for AMI; demand response (DR), and home area network (HAN)
3G	1.92-1.98 GHz, 2.11-2.17 GHz; 10 km.	Licensed; suitable for AMI; DR, and HAN; costly fee!
WiMax	2.5 GHz, 3.5 GHz, 5.8 GHz; 5 km (NLOS), 50 km (LOS).	DR; Wireless automatic meter reading (WMAR) as part of utility AMI.
ZigBee	868-915 MHz, 2.5 GHz; 250 Kbps; 50 m; 1 mW.	Unlicensed; most suitable communication standards for smart grid low- power residential network domain: HAN [12].
GPRS	900-1800 MHz; 170 Mbps; 10 km.	AMI; HAN; DR.
PLC	1-30 MHz; 3 Mbps.	AMI and HAN; promising technology for smart grid applications due to the fact that the existing infrastructure decreases the installation cost of the communications infrastructure; implemented in China and France [13].

GSM: Global system for mobile communication; 3G: Third generation; WiMax: Worldwide inter-operability for microwave access; GPRS: General packet radio service.

2.3 Sensing and Measurement

The integration of phasor measurement units and sensing devices into comprehensive wide-area monitoring networks will enhance the situational awareness of the grid and enable system operators to react to system disturbances and anomalies more accurately. The data collected by these systems can be used to develop advanced operating procedures and finally allow some level of automatic advanced control of the grid. The data from these systems could also be utilized to make the grid self-healing by avoiding or mitigating power outages, power quality problems, and service disruptions.

2.4 Islanding

Islands or microgrids may emerge to take over from electric utilities should conventional generation and distribution experience a fault. An island should be able to physically disconnect and reconnect itself from the larger grid and perform all the functions that central utilities currently perform, including voltage and frequency control.

3. SMART GRID STANDARDS

There are a variety of technological solutions for smart grid system that have been developed or are still in the development process. However, the key challenge is that the overall smart grid system is lacking widely accepted standards and this fact limits the

integration of advanced applications, smart meters, smart devices, and renewable energy sources and constrains the interoperability between them. The adoption of interoperability standards for the overall system is a critical prerequisite for making the smart grid system a reality. Seamless interoperability, robust information security, increased safety of new products and systems, compact set of protocols and communication exchange are some of the objectives that can be achieved with smart grid standardization efforts [14]. There are many regional, national, and international attempts towards achieving this goal. An overview of currently implemented smart grid standards is given in Table 2.

Table 2. Smart grid standards

Standards	Application	Details
IEEE P2030	Customer applications	A guide for smart-grid interoperability of energy technology with end-use applications and load.
IEEE P1901	Utility and smart grid applications	High speed power line communications.
IEEE 929-2000	Distributed generation (DG)	Utility interface of photovoltaic (PV) systems.
IEEE Std. 1547-2003	DG	Interconnecting distributed energy resources and storage information.
IEC61970	Energy management systems	Transmission domain and enterprise application integration.
IEC 61969	Energy management system	Distribution domain.
IEC 61968	Electrical distribution system	Inter-application integration of a utility enterprise.
IEC 61850	Substation automation	Communications between devices in transmission, distribution, and substation systems.
IEC 60870-6/TASE.2	Inter-control center communications	Data exchange between utility control centers.
ITU-T G.9955 and G.9956	Distribution automation; AMI	Physical layer specifications and data link layer specification.
IEC 62351	Power system management	Security for IEC 61850.
ISO/IEC 15408	Security functions of IT products and systems.	A resource for the evaluation of the security of IT products and systems. It can be implemented in any sector including the smart grid.
HomePlug	HAN	Power line technology to connect smart appliances with in HAN.
ISA100.11a	Industrial automation	Wireless systems.
SAE J2293	Electric vehicle (EV) supply equipment	Energy transfer from utility to EVs.
ANSI C12.22	AMI	Data network communications.
ANSI 12.18	AMI	Data transportation via infrared optical port.
ANSI C12.19	AMI	Meter data communications.

Z-Wave	HAN	Alternative solution to ZigBee
ZigBee	Wireless communications	Based on IEEE 802.15.
M-Bus	AMI	European standard for reading all kinds of utility meters.
PRIME	AMI	Multi-vender interoperability.
G3-PLC	AMI	Interoperability and cyber security.
SAE J2836	EVs	Plug-in EV communications.
SAE J2847	EVs	Communication between EVs and grid components.
OpenADR	DR	Communications using Web Services to send demand response signals to end-use customer systems.

4. THE CONCEPT OF RISK

Risk in the context of smart grid may be defined as the probability of a threat agent exploiting vulnerability to cause harm to a computer, network, system, or **grid** utility, and result in operational and business consequences. The numerate definition of risk may be expressed as:

$$\text{Risk} = \text{Uncertainty of a variable} \times \text{Consequences}$$

The following equation attempts to correlate different elements of risk in the smart grid domain [15, 16].

$$R = P_A \times (1 - P_E) \times C \quad (1)$$

R represents the level of risk assumed, or the level of risk that still remains after accounting for threat, consequence and protection mechanism. It is a value between 0 and 1 representing the combined probability that the system will be attacked, the effectiveness of the system and the consequence of a successful attack. P_A is the likelihood of attack, with a maximum of 1 if the probability of attack is set at 100%. **With the level of threat against the grid is high**, it is safe to say that the probability of an attack on grid infrastructure is large. P_E is the probable effectiveness of the **security in place to protect the system** and $(1 - P_E)$ measures lack of security mitigation. C is a value between 0 and 1 that rates the consequence of a successful attack. P_E may be expanded to

$$P_E = P_I \times P_N \quad (2)$$

Where, P_I is the probability of interception and P_N is the probability of neutralization of a given threat. P_I determines how likely an attack is to be discovered and a response initiated. Once a response has been initiated P_N helps determine how effective that response will be in stopping the attack. Like the rest of the variables in Eq. (1), C is a value between 0 and 1 indicating the impact a successful attack would have on the organization. It is important to understand what assets would have the largest impact if lost, damaged or destroyed and then protect them accordingly. Various stakeholders tend to view assets differently.

In general, three parameters attributes to help determine consequences: geographical size of the impact C_A (international, national, regional, local); time to recover C_T (permanent,

years, months, days, hours); and cost to recover C_C (very high, high, medium, low, very low). Understanding the asset and knowing the impact values for each attribute makes it possible to calculate C using Eq. (3).

$$C = 1 - (1 - C_A) \times (1 - C_T) \times (1 - C_C) \quad (3)$$

5. SECURITY RISK

Cyber security risk is difficult to measure even in a static environment because it is a complex function of threat, vulnerabilities and consequences. The ISO/IEC Standard 15408 (see Table 2) (Common Criteria—Fig. 3) includes a fact model showing the value relationship of owners to their assets. The utility needs to analyze the potential threats in order to verify which apply to its environment. Such analysis may help in the selection of the suitable countermeasures needed to reduce the relevant risks to acceptable levels. The countermeasures are implemented for the purpose of reducing vulnerabilities and meeting security policy requirements. Same approach can be applied for home users based. This application allows home users to access information about threats which affect home user environments and thereby select the security objectives based on this environment. The challenge is to introduce countermeasures that restrict a threat agent from successfully exploiting a known threat against vulnerabilities.

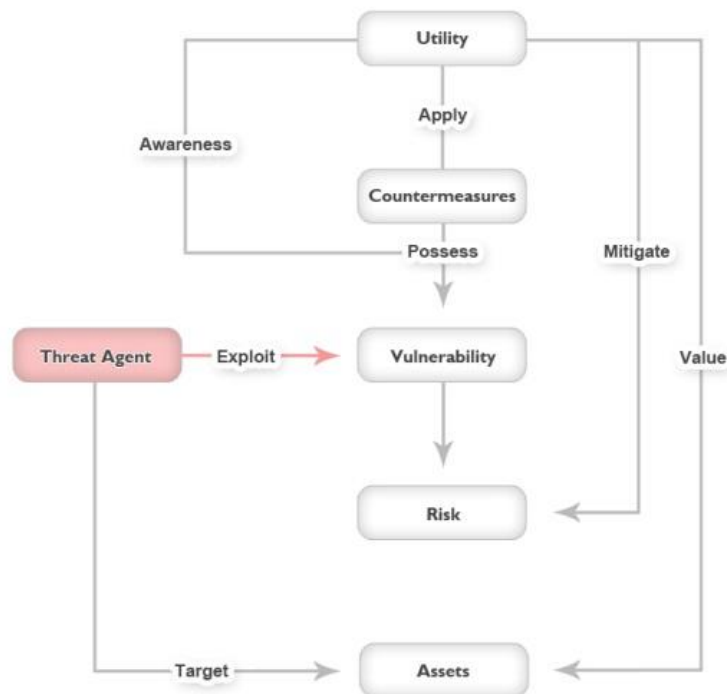


Fig. 3. Fact model showing the value relationship of owners to their assets based on ISO/IEC Standard 15408.

5.1 SCADA Security

One subsystem which is at the core of smart grid systems is the supervisory control and data acquisition (SCADA) solution. SCADA systems have undergone cyber security assessments as part of the National SCADA Test Bed (NSTB) program. Multiple vendors offer SCADA solutions with varying capabilities and security mechanisms. SCADA systems are currently isolated, preventing external access. While some standards exist around SCADA, such as distributed network protocol 3 (DNP3), there is still a need to make more consistent the security solutions applied to SCADA deployments. Future SCADA systems may need to deal with orders of magnitude more information than current SCADA approaches handle.

5.2 Substation Security

In any national grid, there are thousands of transmission and distribution substations which have various levels of automation. The level of automation in substations is increasing, however, level of automation is indirectly related to security because increased automation implies increased computer-controlled electronics and software, which tends to increase the potential for cyber security weaknesses, although increased automation does not necessarily involve reduced security. Potential consequences of successful substation cyber attacks include the destruction of generators, power outages, and grid instability.

5.3 Network Security and Availability

Malicious attacks targeting network availability can be considered as denial-of-service (DoS) attacks, which attempt to delay, block or corrupt information transmission in order to make network resources unavailable to nodes that need information exchange in the smart grid. Since it is widely expected that at least part, if not all, of the smart grid will use IP-based protocols (for example, IEC 61580 [17] has already adopted TCP/IP as a part of its protocol stacks) and TCP/IP is vulnerable to DoS attacks, sophisticated and efficient countermeasures to DoS attacks are essential to the smart grid. DoS attacks against TCP/IP have been well studied in the literature regarding attacking types, prevention and response [18, 19]. Since intruders only need to connect to communication channels rather than authenticated networks in the smart grid, it is very easy for them to launch DoS attacks against the smart grid, especially for the wireless-based power networks that are susceptible to jamming attacks [20]–[22].

5.4 AMI Security

The wireless devices used in AMI exist in the smart meters located on the customers' premises. Since these devices are outside the utility's physical security perimeter, they are at high risk of compromise. Attackers can extract data from the memory of these devices including keys used for network authentication and device memory can be modified by an attacker to insert malicious software. Once the device is compromised it can be used to attack other parts of the smart grid by communicating through the network. Attacks that originate with an AMI wireless network device can lead to direct control systems compromise. Many compromised smart meters or data collector nodes could be programmed by the attacker to simultaneously send messages that cause power demand to be reduced dramatically and then to be increased dramatically. These phony messages could cause grid instability and power outages.

5.5 Data Integrity

Integrity of data is clearly important in general, but since so many different types of interactions are taking place in the smart grid, the integrity requirements will need to be specific to the particular application. Differing from attacks targeting network availability, attacks targeting data integrity can be regarded as more sophisticated attacks. The target of the attacks is either customer's information or network operation information. The final security objective is confidentiality. The loss of data confidentiality in the smart grid has a lower risk than loss of availability or integrity. There are specific areas in the smart grid where confidentiality is more important such as the smart meters. The privacy of customer information, corporation data, and electric market information are some examples.

6. EVALUATION OF HEALTH IMPACT

In this mini-review, we provide a brief primer that serves as an entry point into the evaluation of potential health risks from two emerging technologies within the development of the smart grid, namely smart meters and wind turbines. These risks clearly warrant further investigation and assessment in the future.

6.1 Smart meters

The advent of smart meters as an integral component of AMI implementation within homes has raised questions from the public as to RF exposures from smart meters and potential health and safety risks that may be related to these exposures.

The official line on the health implications of wireless networks is that exposure to low-level RF radiation is well below the international recommended levels and that there is no evidence of risk. But despite this assurance, the concern is mounting, with some people blaming everything from headaches to cancer on exposure to RF fields [23]-[25].

There exist two major specific absorption rate (SAR) limits defined as: 1) a whole-body average SAR; and 2) a local (spatial) SAR when the power absorption takes place in a confined body region. Safe local SAR limits are generally based on estimates from the whole-body average SAR and incorporate substantial "safety factors" for users [24]. How much RF energy is safe? This is a complex problem, comprising public health, life sciences, engineering, and social (including economic and legal) considerations. During the past few years, many countries and international organizations developed safety standards for RF radiation. It is evident that two major safety limits for local SAR in the head exist, 1.6 W/kg averaged over 1 g (SAR_{1g}) in North America, and 2 W/kg averaged over 10 g (SAR_{10g}) developed by the International Commission on Non-Ionizing Radiation Protection (ICNIRP) of the European Union. The ICNIRP limit is accepted for use in Australia, Japan, and other parts of the world [26].

A common concern about wireless technologies is related to the possible long-term health effects of the radiated RF signals. However, the only health effect from RF fields identified so far in the majority of scientific reviews has been related to an increase in body temperature (>1°C) from exposure at high field intensity found only in certain industrial facilities, such as RF heaters or being very close to RF transmitters. A few individuals have reported that RF signals from wireless networks and other low-level sources of RF fields can trigger allergy-like reactions—a phenomenon called **electromagnetic hypersensitivity**. This is a complex issue that scientists have studied with respect to low-level RF fields from various sources for a number of years. While the distress of hypersensitive individuals is very real,

controlled studies have failed to connect their symptoms to RF exposure. The World Health Organization (WHO) fact sheet [27] states that “RF fields have not been shown to cause such symptoms. Nonetheless, it is important to recognize the plight of people suffering from these symptoms.”

With this perspective in hand, comparative levels of RF emissions from commonly used sources are shown in Table III. In regard to smart meters under implementation in the smart grid, the table indicates levels for distances of 3 and 10 feet, with meters operating at 1 W and at a quarter watt (or 250 mW) with duty cycles of 1% and 5% for each power level. The entries in the table indicate that smart meter emissions, even at the maximum point, are at the same order of magnitude as emissions from such sources as WiFi routers and far lower than the fields emitted by cell phones or microwave ovens.

Table 3. RF Levels from three commonly known sources

Source	Frequency	Exposure level (mW/cm ²)
Mobile Phone	900, 1800 MHz	1-5 at ear
Cellular Station	900, 1800 MHz	0.000005—0.002 (10—1000 m)
Smart Meter	900, 2400 MHz	0.0001 (250 mW, 1% duty cycle) (1 meter) 0.02 W, 5% duty cycle)

A measurement investigation [28] indicates that exposure level from the smart meters are a small fraction of the RF exposure limit for the general public, and diminishes, as expected, with increasing distance from the smart meter. However, when the smart grid is fully functional the smart meters would be expected to transmit much more RF energy than the existing ones, due to higher duty cycle.

A recent study found that the level of RF energy in homes from a smart meter transmitting at 2450 MHz was below the background level from operation of a laptop computer, a microwave oven, and a Wi-Fi controlled power outlet and home thermostat [29].

An extensive survey of time-averaged exposures in homes in European cities found that the highest time-average RF exposure was from the use of mobile phones by individuals in the home (the survey did not measure the far higher exposures to the user of the phone itself) [30].

The IEEE EMBS Committee on Man and Radiation (COMAR) [31] has recently approved a technical information statement on smart meters basing on various opinions, and considering the small RF exposure relative to national and international safety limits. COMAR concludes that RF emissions from smart meters should be considered to be safe. Health agencies and standards setting bodies will continue to follow closely the developing scientific literature in this area.

6.2 Wind Turbines

Wind turbines emit a low-frequency vibration and noise, generating sound through mechanical and aerodynamic rotation of the turbine blades through air, which human beings might be sensitive to and the vibrations may disrupt the inner ear's vestibular system. The sound level depends on various factors including wind turbine design and wind speed. The normal human ear perceives sounds at frequencies ranging from 20 Hz to 20 kHz. Frequencies below 200 Hz are commonly referred to as low frequency sound and those below 20 Hz as infrasound. Although generally considered inaudible, infrasound at high-enough sound pressure levels can be audible to some people [32]. Noise is defined as an

unwanted sound [33, 34]. The aerodynamic noise is present at all frequencies, from infrasound to low frequency to the normal audible range, producing the characteristic “swishing” sound [35]-[37].

The impact of sound on health is directly related to its pressure level. High sound pressure levels (> 75dB) could result in hearing impairment depending on the duration of exposure and sensitivity of the individual. In Ontario, Canada, Under the Ontario renewable energy approval (REA) regulation [36], the limit noise at the nearest residence is 40 dBA. This is a sound level comparable to indoor background sound. This noise limit is consistent with the night-time noise guideline of 40 dB that the WHO recommends for the protection of public health from community noise. According to the WHO, this guideline is below the level at which effects on sleep and health occurs. However, it is above the level at which complaints may occur [37].

Available scientific data indicate that sound levels associated with wind turbines at common residential setbacks are not sufficient to damage hearing or to cause other direct adverse health effects, but some people may still find the sound annoying. Studies in Sweden and the Netherlands [38]-[42] have found direct relationships between modelled sound pressure level and self-reported perception of sound and annoyance. The association between sound pressure level and sound perception was stronger than that with annoyance. The sound was annoying only to a small percentage of the exposed people; approximately 4 to 10% were very annoyed at sound levels between 35 and 45 dBA. Annoyance was strongly correlated with individual perceptions of wind turbines.

A small increase in sound level at low frequency can result in a large increase in perceived loudness. This may be difficult to ignore, even at relatively low sound pressures, increasing the potential for annoyance [43]. A Portuguese research group [44] has proposed that excessive long-term exposure to vibration from high levels of low-frequency sound and infrasound can cause whole body system pathology (vibro-acoustic disease), however, an evidence to support this claim was not provided. Keith et al. [45] proposed that in a quiet rural setting, the predicted sound level from wind turbines should not exceed 45 dBA at a sensitive receptor location (residences, hospitals, schools), a value below the WHO guideline for sleep and speech disturbance, moderate annoyance and hearing impairment. The authors suggest this level of noise could be expected to result in a 6.5% increase in the percentage of highly annoyed people.

A report from the Chief Medical Office of Health, Ontario, Canada [32] concludes that “the sound level from wind turbines at common residential setbacks is not sufficient to cause hearing impairment or other direct adverse health effects. However, some people might find it annoying. There is no scientific evidence to date that vibration from low frequency wind turbine noise causes adverse health effects.”

Knopper and Ollson [46] states in a review that: “Conclusions of the peer reviewed literature differ in some ways from the conclusions of the studies published in the popular literature. What both types of studies have in common is that wind turbines can be a source of annoyance for some people. In the peer reviewed studies, some reported health effects have been statistically associated with wind turbine noise at sound pressure levels greater than 40 dBA, but found to be more strongly related to subjective factors like visual impact, attitude to wind turbines in general and sensitivity to noise.”

Further, a comprehensive report from Massachusetts Department of Environmental Protection and Massachusetts Department of Public Health [47] evaluates and discusses information from peer-reviewed scientific studies, reports, popular media, and public comments on the nature and type of health complaints commonly reported by individuals who reside near existing wind farms.

7. COMBINED RISK MANAGEMENT FRAMEWORK

Risk management is about discovering critical assets and realizing their weaknesses, loss expectation, and the suitable risk mitigation approaches for ensuring their sustained value. Consequently, risk management involves choosing among alternatives to reduce the effects of risks. Specifically, to measure the consequences, likelihoods of occurrences, and severity of risks as well as the efficacy of risk management is the ultimate objective of utilities.

For the utility, security and safety start with defining a risk management framework that will be used to identify threats and vulnerabilities; assess the effectiveness of existing controls in mitigating the risks; recommend new controls to mitigate the risks to a level acceptable to the utility and public; periodically repeat this process to account for changes in the threat situation; and set up policies that address human behaviour, which is the basis for all risks whether technical or health.

Inspired by CAN/CSA Q-634-91 [48], Fig. 4 presents a unified framework for risk management in all technological domains. This combined framework demands interactive, step-wise actions to reduce the overall risks. Such a framework calls for a coordinated assessment of cyber and power grid risks keeping the whole grid security and safety goals in mind. The process comprises of several steps including: risk identification and threat characterization; risk analysis; risk planning including level of risk acceptance; risk prioritization based on objectives; periodical risk tracking; risk monitoring including countermeasures; and risk communication to the management, stakeholders, and organization. The risk management process must enable sound decision making. Since threats cannot be totally eliminated, the process must focus on vulnerabilities and risk actions.

When a risk is identified, a risk strategy can be applied whether to avoid it, accept it, or reduce its impact. More than one risk strategy may be applied in a given situation. While best strategies are applicable to all environments, utilities may discover that some are less relevant to a particular situation. The specific implementation details differ according to the purpose, technology road map, available resources, and other factors.

8. CONCLUSION

The emerging smart grid, while benefiting consumers and utility companies, also provides powerful tools for adversaries. For most utilities operating in a regulated business environment, the implementation of an integrated smart grid capability poses many challenges. In fact, the tight coupling between ICTs and physical systems introduces new security risks and safety concerns.

The most important elements in the risk management process in relation to improve security and safety are risk identification and assessment of control effectiveness. Adopting an approach to risk management which concentrates on hazard identification and control effectiveness while relegating subjective risk estimation is consistent with the overall objectives of regulations.

Research should be conducted to accelerate the development of standards that fill existing gaps including those for security, smart grid network and device management, information privacy management, and field area network interoperability. Further research should be carried out by interdisciplinary teams to investigate health impacts of RF fields from wireless networks and low-frequency noise from wind turbines.

Integrated risk management approaches are significantly needed to efficiently guide resource allocations and optimize practices at all levels of the smart grid platform to identify

the risk, measure it, minimize it, and finally engineer out the risks by the use of available resources, to an acceptable and approved standard.



Fig. 4. Risk management framework for the smart grid.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. IEEE 2030-2011, IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads, STD97148, STDPD97148, September, 2011.
2. Office of the National Coordinator for Smart Grid Interoperability. NIST framework and roadmap for smart grid interoperability standards, release 1.0. NIST Special Publication 1108, 2009.
3. Santacana E, Rachliffe G, Tang Le, Feng X. Getting smart. IEEE Power and Energy Magazine. 2010;March/April:41-8.
4. The Smart Grid Interoperability Panel-Cyber Security Working Group. Smart grid cyber security strategy and requirements. NIST IR-7628;Feb 2010.
5. Metke AR, Ekl RL. Smart grid security technology, Proc. of Innovative Smart Grid Technologies (ISGT);Jan. 2010.

6. Hoffman M, Daim TU, Building energy efficiency technology roadmaps: A case of Bonneville Power Administration (BPA). *Proc Technol Manag. Global Future*. 2006: 1503–27.
7. King RL., Information services for smart grids. *Proc. IEEE PES Gen. Meet.* 2008;1–6.
8. Li F, Qiao W, Sun H, Wan H, Wang J, Xia Y, Xu Z, Zhang P. Smart transmission grid: vision and framework. *IEEE Trans Smart Grid*. 2010;1(2):168-77.
9. Gungor VC, Lu B, Hancke GP. Opportunities and challenges of wireless sensor networks in smart grid. *IEEE Trans Ind Electron*. 2010;57(10):3557–64.
10. Güngör VC, Sahin D, Kocak T, Ergüt S, Buccella C, Cecati C, Hancke GP. Smart grid technologies: communication technologies and standards. *IEEE Trans Ind Inform.* 2011;7(4):529-39.
11. Gunther EW, Snyder A, Gilchrist G, Highfill DR. Smart grid standards assessment and recommendations for adoption and development. 2009; EnerNex Corporation, Draft 0.83 03/1/2009.
12. Peizhong Y, Iwayemi A, Zhou C. Developing ZigBee deployment guideline under WiFi interference for smart grid applications. *IEEE Trans Smart Grid*. 2011;2(1):110–20.
13. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson DA, Rabkin A, Stoica I, Zaharia M. Above the clouds: A berkeley view of cloud computing. 2009; University of California at Berkeley, Research Report.
14. Gungor VC, Sahin D, Kocak T, Ergüt S. Smart grid communications and networking. *Türk Telekom Tech. Rep.* 2011;11316-01.
15. Clements SL, Kirkham H, Elizonda M, Lu S. Protecting the smart grid: a risk-based approach. *IEEE Power and Energy Society General Meeting*. 2009;1-7, San Diego, 24-29 July, 2011.
16. Ray PD, Harnoor R, Hentea M. Smart power grid security: a unified risk management approach. *IEEE Int. Carnahan Conf. Security Tech. (ICCST)*, San Jose, CA, pp. 276-285, 5-8 Oct. 2010.
17. Sidhu TS, Yin Y. Modelling and simulation for performance evaluation of IEC61850-based substation communication systems. *IEEE Trans Power Delivery*. 2007;22(3):1482–89.
18. Yaar A, Perrig A, Song D. Pi: A path identification mechanism to defend against DDoS attacks. *Proc IEEE Symposium on Security and Privacy*. 2003.
19. Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. *SIGCOMM Comput Commun Rev*. 2004;34(2):39–53.
20. Strasser M, Capkun S, Popper C, Cagalj M. Jamming-resistant key establishment using uncoordinated frequency hopping. *Proc. IEEE Symp. Security and Privacy (S&P 2008)*. 2008:64–78.
21. Popper C, Strasser M, Capkun S. Jamming-resistant broadcast communication without shared keys. *Proc of the 18th USENIX Security Symposium (Security '09)*. Aug. 2009.
22. Liu Y, Ning P, Dai H, Liu A. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. *Proc. 29th IEEE Conference on Comp Comm (INFOCOM '10)*. March 2010.
23. Habash RWY. Environmental and human impact of electromagnetic energy: views toward technology and risk. *J. Energy Environ.* 2010;21(2):107-14.
24. The Committee on Man and Radiation (COMAR Collaborators). COMAR technical information statement: expert reviews on potential health effects of radiofrequency electromagnetic fields and comments on the Bioinitiative report. *Health Physics*. 2009;97(4):348-56.
25. Habash RWY, Krewski D, Byus GV, Glickman BW, McNamee J, McBride ML, Prato FS. Recent advances in research on radiofrequency fields and health: 2004-2007. J

- Tox Environ Health, Part B. 2009;12(4):250-88.
26. Habash R W Y. Bioeffects and Medical Applications of Electromagnetic Energy, CRC Press, Boca Raton, FL, 2007.
27. WHO Fact Sheet. Electromagnetic fields and public health. 2006.
28. Supplemental Report on An Analysis of Radiofrequency Fields Associated with Operation of PG&E Smart Meter Program Upgrade System, Richard A. Tell, Richard Tell Associates, Inc., October 27, 2008.
29. Foster KR, Tell RA, Radiofrequency energy exposure from the Trilliant smart meter. Health Phys. in press.
30. Viel JF, Clerc S, Barrera C, Rymzhanova R, Moissonnier M, Hours M, Cardis E. Residential exposure to radiofrequency fields from mobile phone base stations, and broadcast transmitters: a population-based survey with personal meter. Occup Environ Med. 2009;66(8):550-56.
31. IEEE EMBS Committee on Man and Radiation (COMAR). Radiofrequency Safety and Utility Smart Meters-Technical Information Statement, 2013.
32. The Potential Health Impacts of Wind Turbines. Chief Medical Officer of Health. Ontario. 2010.
33. Rogers AL, Manwell JF, Wright S. Wind turbine acoustic noise: a white paper. Amherst, MA: University of Massachusetts at Amherst. Department of Mechanical and Industrial Engineering, Renewable Energy Research Laboratory; 2006. Available from: http://www.ceere.org/rerl/publications/whitepapers/Wind_Turbine_Acoustic_Noise_Rev2006.pdf. Retrieved 26 April 2013.
34. Leventhall G, Pelmear P, Benton S. A review of published research on low frequency noise and its effects. London, England: Department for Environment, Food and Rural Affairs. 2003. Contract No.: EPG 1/2/50. Available from: <http://www.defra.gov.uk/environment/quality/noise/research/lowfrequency/document/s/lowfreqnoise.pdf>.
35. Leventhall G. Infrasound from wind turbines: fact, fiction or deception. Can Acoust. 2006;34(2):29-36.
36. Colby WD, Dobie R, Leventhall G, Lipscomb LD, McCunney RJ, Seilo MT, Søndergaard Bo. Wind turbine sound and health effects. An expert panel review: American Wind Energy Association and Canadian Wind Energy Association; 2009. Available from: http://www.canwea.ca/pdf/talkwind/Wind_Turbine_Sound_and_Health_Effects.pdf.
37. World Health Organization, Regional Office for Europe. Night noise guidelines for Europe. Geneva, Switzerland: World Health Organization, 2009.
38. Pedersen E, Hallberg LRM, Waye KP. Living in the vicinity of wind turbines: a grounded theory study," Qual Res Psychol. 2007;4(1-2):49-63.
39. Pedersen E, Larsman P. The impact of visual factors on noise annoyance among people living in the vicinity of wind turbines. J. Environ. Psychol. 2008;28(2):379-89.
40. Pedersen E, Waye KP. Wind turbine noise, annoyance and self-reported health and well-being in different living environments. Occup. Environ. Med. 2007;64(7):480-6.
41. Pedersen E, van den Berg F, Bakker R, Bouma J. Response to noise from modern wind farms in The Netherlands. J. Acoust. Soc. Am. 2009;126(2):634-43.
42. Pedersen E, Waye KP. Perception and annoyance due to wind turbine noise – a dose-response relationship. J Acoust Soc Am. 2004;116(6):3460-70.
43. Jakobsen J. Infrasound emission from wind turbines. J. Low Freq Noise Vib. Active Contr. 2005;24(3):145-55.

44. Alves-Pereira M, Castelo Branco NAA. The scientific arguments against vibroacoustic disease. Proc. Inter-Noise Congress. 2007; Istanbul, Turkey, August 28-31.
45. Keith SE, Michaud DS, Bly SHP. A proposal for evaluating the potential health effects of wind turbine noise for projects under the Canadian Environmental Assessment Act. J. Low Freq. Noise. 2008;27:253-63.
46. Knopper LD, Ollson CA. Health effects and wind turbines: a review of the literature. Environ Health, 2011;10(78).
47. Massachusetts Department of Environmental Protection (MassDEP) and Massachusetts Department of Public Health (MDPH). Wind Turbine Health Impact Study: Report of Independent Expert Panel, 2012. Available from: http://www.mass.gov/dep/energy/wind/turbine_impact_study.pdf. Retrieved 26 April 2013.
48. CAN/CSA Q-634-91, Risk Analysis Requirements and Guidelines, Quality Management, A National Standard of Canada, November, 1991.