Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure

Göran N. Ericsson, *Senior Member, IEEE*

***Abstract*—The introduction of "smart grid" solutions imposes that cyber security and power system communication systems must be dealt with extensively. These parts together are essential for proper electricity transmission, where the information infrastructure is critical. The development of communication capabilities, moving power control systems from "islands of automation" to totally integrated computer environments, have opened up new possibilities and vulnerabilities. Since several power control systems have been procured with "openness" requirements, cyber security threats become evident. For refurbishment of a SCADA/EMS system, a separation of the operational and administrative computer systems must be obtained. The paper treats cyber security issues, and it highlights access points in a substation. Also, information security domain modeling is treated. Cyber security issues are important for "smart grid" solutions. Broadband communications open up for smart meters, and the increasing use of wind power requires a "smart grid system."**

***Index Terms*—Communication systems, control systems, cyber security, information security, IT security, power system communication, power system control, power systems, SCADA, security, smart grid, wide-area networks.**

I. Introduction

THE concept of "smart grid" [1]–[7] has become a "hype." It has received considerable momentum during the recent years, and this is expected to develop even more. Critical parts here are the cyber security issues and the power system communication (PSC) systems, which are stressed in this paper. The use of electricity is of paramount importance to our society, and the need for power supply is increasing. Here, the concerns on physical security are quite mature and easy to grasp, whereas now the digital threats are increasing. By means of the PSC capabilities, supervisory control and data acquisition (SCADA) systems and substations are now interconnected with other systems. These communications take place both over dedicated line and over the Internet. Also in the earlier projects, information and Information Technology (IT) security issues were not considered to a great extent, or not at all.

Generally, the trends are that vendors are using commercial off the shelf (COTS) products as part of their SCADA/energy management system (EMS) systems, instead of using proprietary solutions. Here, the increasing use of standard products, such as personal computers (PCs), operating systems, and, networking elements, now opens up new possibilities and threats. The knowledge of security can now be more easily known and divided on more people; the "security-by-obscurity" principle does not apply to the same extent as before. Instead, the digital threats arise and must be handled in a structured way. Here, the awareness of the new possibilities and risks is important. All people involved must strive to take active decisions on the choice of adequate technical solutions when deploying a new SCADA system, or protecting an existing one.

A. Purpose

The purpose of the paper is to emphasize the role of cyber security and PSC systems in conjunction with each other, in a smart grid infrastructure, where the information infrastructure is as critical as the physical. Also, a historical development perspective is given, explaining some of the facts of the PSC systems of today, possessing partly vulnerable structure. The work described herein is developed and based on several years of CIGRÉ working group efforts within the field of power systems communications [8]–[18], where the author has been actively involved (part of the work as a convener). The most recent results have been presented in [8] and [12]. Also, the works of [19]–[21] should be considered.

B. Outline

In Section II, the development phases of power system communication systems are described, together with a classification of different communication capabilities and requirements. Thereafter in Section III, the development of power system control systems are given, from "islands of automation" to fully integrated systems. Here also, a discussion on "open systems" is given. In Section IV, the cyber security issues are treated. In Section V, cyber security highlights with respect to "smart grids" are given. The paper ends with concluding remarks in Section VI.

II. Development and Classification of Power System Communication Systems

Communication capabilities have developed from narrowband, low speed communications to high speed broadband "highways" for all sorts of communications. From being a

Manuscript received December 01, 2009. First published April 22, 2010; current version published June 23, 2010. Paper no. TPWRD-00884-2009.

The author is with Svenska Kraftnät (Swedish National Grid), Sundbyberg 17224, Sweden (e-mail: goran.n.ericsson@svk.se).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRD.2010.2046654

very delimiting factor, new possibilities have opened up, which have supported the development of PSC systems described in Section III.

A. Classifications of Communications

Communication requirements should be classified, since this facilitates the handling of requirements and the order of requirements. One way is to classify requirements into three categories, namely:

- real-time operational communication requirements;
- administrative operational communication requirements;
- administrative communication requirements.

These three classes were first introduced in 2001/2002 [22], based on works at the Swedish National Grid. Experiences have now shown that this classification approach is very suitable [23]. It is now widely used both within and outside Swedish National Grid.

1) Real-Time Operational Communication Requirements: Real-time operational communication encompasses communication in real time that is required to maintain operation of the power system. The class is in turn divided into *real-time operational data communication* and *real-time operational speech communication.*

Real-time operational data communication encompasses:

- teleprotection;
- power system control.

The communication is characterized by the fact that interaction must take place in real time, with hard time requirements. The communication requirements define the design of the technical solutions.

For teleprotection purposes, messages should be transmitted within a very short time frame. Maximum allowed time is in the range of 12–20 ms, depending on the type of protection scheme. The requirement has its origin in the fact that fault current disconnection shall function within approximately 100 ms.

Power System Control mainly includes supervisory control of the power process on secondary or higher levels. These systems are of the kind SCADA/EMS. Measured values must not be older than 15 s, when arriving at the control center. Breaker information shall arrive no later than 2 s after the event has occurred.

Real-time operational voice communication encompasses traditional telephony; where voice communication has an operational purpose, e.g., trouble shooting in a disturbed power operational case, power system island operations. The actual possibility of having voice communication is, by the control center staff, considered as one of the most important tools, both in normal and abnormal operation cases. Real-time operational voice communication also includes facsimile for switching sequence orders.

Also, the means of using electronic mail (e-mail) for transfer of switching sequence orders is considered.

2) Administrative Operational Communication Requirements: In addition to real-time operational communication, information is needed that, in more detail and afterwards, support description of what has happened in minor and major power system disturbances. This class is referred to as administrative operational communication. Examples are interactions with local event recorders, disturbance recorders, and power swing recorders.

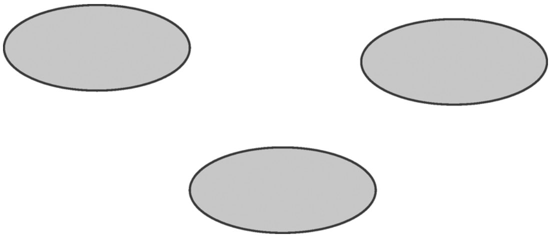

Fig. 1. "Islands of Automation".

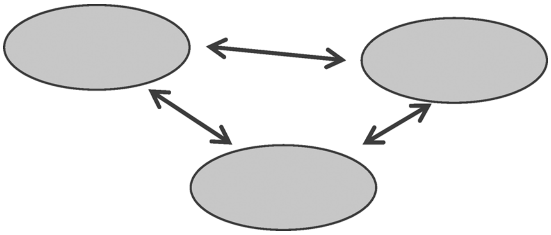

Fig. 2. Interconnected system structure.

The communication is characterized by that interaction does not need to take place in real time. Time requirements are moderate.

Also, the following functions are included in this class.

- Asset management.
- Fault location.
- Metering and transfer of settlement information.
- Security system.
- Substation camera supervision.

3) Administrative Communication Requirements: Administrative communication includes voice communication and facsimile within the company (also between the offices that are at different geographical locations), as well as to/from the company, where the communication has an administrative purpose.

III. Development of Power System Control Systems

The PSC system has been and will increasingly be the life nerve of the power system. It is the necessity and prerequisite for adequate operation and control of a power system. Also with respect to new requirements based on information and IT security, the focus will increase on the communication system.

Data communication systems have been developed from proprietary solutions to standardized off-the-shelf solutions, where the vendors more become system integrators, rather than power control system designers. Therefore, power system control systems that used to be formed as "Islands of Automation" [21], now have developed to interconnected, and even integrated—see Figs. 1–4.

In fact, it is the technical evolution of communications systems and their capabilities that have opened up for this interactivity. Furthermore based on these possibilities, there were major forces in the 1990s striving for "open systems" [24], [25] when procuring power control system. The utilities required the SCADA/EMS to be more open, and the vendors all claimed that their system products were open.

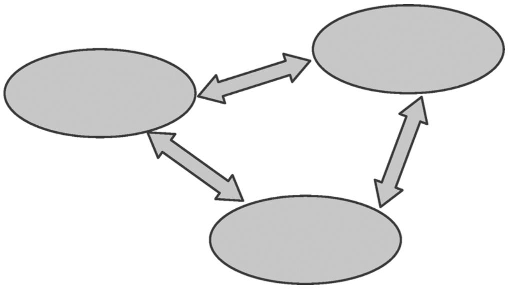

Fig. 3. Partially integrated system structure.

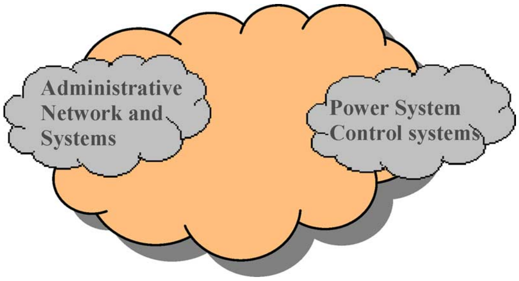

Fig. 4. Today—full integration system structure.

If the projects of procurement of such systems in the 1990s and early 2000s are studied, it can be noticed that several of the systems were procured with the requirement of obtaining openness in the PCS system environment. For data communication systems, the truth is that some PSC systems parts have opened up [26], whereas other parts are still based on proprietary solutions.

Nevertheless, a customer typically gets what he asks for from the vendor. So if one asks for "openness" one may get it. And if one does not ask for "IT security," one does not get that.

Hence, there are several power utilities around the globe that now have installed SCADA/EMS and industrial control systems, which were opened up from the design phase, but had very limited security incorporated in the system solutions. It was of course tempting to require the openness, since new possibilities then arose. But these utilities now have information and IT security problem to tackle. This fact is serious, it is a growing concern, and it must be taken into account for system daily operation and control by each utility.

IV. Cyber Security Issues

Based on the described evolution of PSC systems and limited concern of cyber security in the 1990s, new issues have arisen, which are described here.

A. De-Coupling Between Operational SCADA/EMS and Admin IT, to Secure Operational

When existing SCADA/EMS systems now are being refurbished or replaced, the information and IT security issues must be taken into account.

If an SCADA/EMS system is to be refurbished, the operational SCADA/EMS system part must be shielded from the Administrative part, such that the Operational part is protected from digital threats that are possible over the Internet connection.

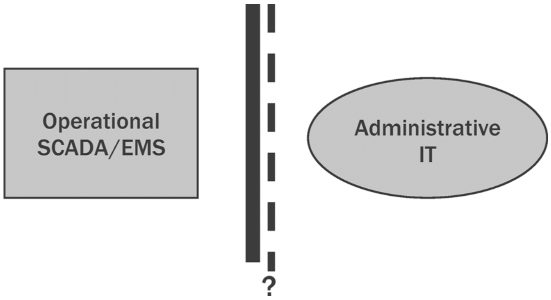

Fig. 5. De-coupling between operational SCADA/EMS and administrative IT environments.

If an SCADA/EMS system is to be replaced, it is then a very good occasion to reconsider an overall system structure, and then incorporate IT security on all SCADA/EMS levels.

A way towards this more secure state is to, if possible, de-couple the Operational SCADA/EMS system and the Administrative IT system. Also, an alternative may be to secure the firewall configuration in between operational and administrative parts—see Fig. 5.

B. Threat and Possibilities

The fact that SCADA/EMS systems now are being interconnected and integrated with external systems creates new possibilities and threats. These new issues have been emphasized in the CIGRÉ working groups JWG D2/B3/C2.01 "Security for Information Systems and Intranets in Electric Power Systems" [11] and D2.22 "Treatment of Information Security for Electric Power Systems" [12], wherein the author has been an active member. As part of the JWG efforts, the various interconnections of a substation were investigated [27]; see Fig. 6. All the numbered "access points" (1–10) elucidates the possible points whereto the substation can be accessed. As the reader may see, there is great number of points. And of course, this number creates an operational environment that implies possible digital entrances and hence digital vulnerabilities.

C. SCADA Systems and SCADA Security

The fact that SCADA systems now are, to a great extent, based on standardized off-the-shelf products, and increasingly being connected over Internet for different purposes (remote access, remote maintenance), implies that SCADA systems are being exposed to the same kind of vulnerabilities as ordinary office PC solutions based on Microsoft products.

This is a delicate question, on what to do and how to handle this new unsecure situation, since SCADA systems are vital for several critical infrastructures, where a power control system is one such system and public transportation is another. The use of SCADA systems is cross-sectional and it has an impact on different parts of a society. Here, the protection of the digital structure of an infrastructure typically refers to "critical information infrastructure protection" (CIIP).

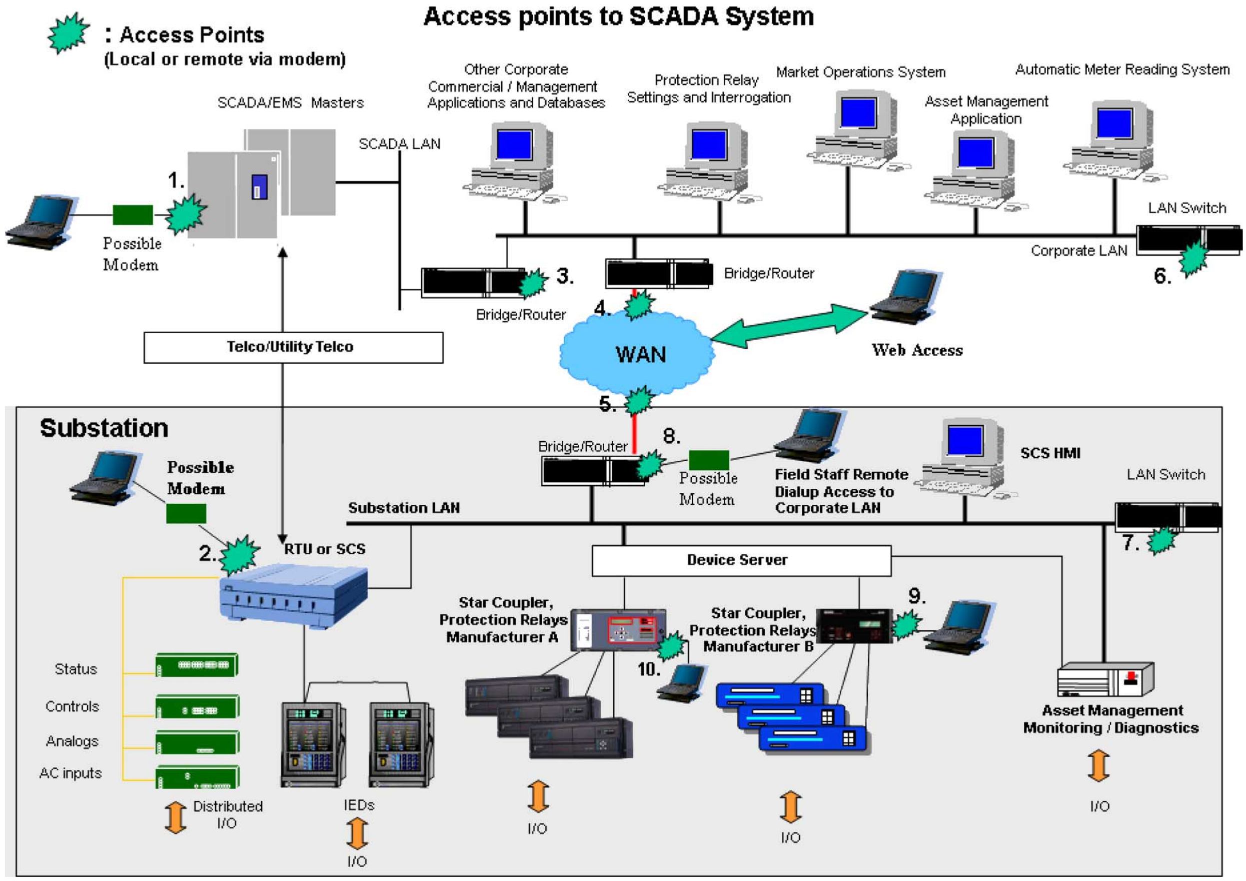

Fig. 6. Access points to SCADA system.

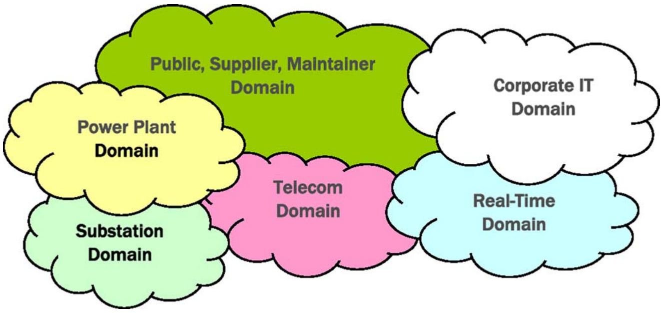

Fig. 7. Information security domains.

D. *Governmental Coordination in Sweden on SCADA Security*

Like in many other countries, the issues of securing CIIP systems have been emphasized in Sweden. A governmental coordination action between different authorities and agencies were started in [28], focusing on SCADA security. The action is based on that existing organizations participate, such as power utilities, water companies, and railway, which have SCADA systems as critical part of operations. Also, the security police are represented. Here, the expertise is gathered and experiences are shared, including both domestic and international knowledge; everything with the purpose of securing the SCADA systems being part of the critical information infrastructures of Sweden. As a natural step, the SCADA Security Guideline has been developed [29]. Also, technical guidelines and administrative recommendations are developed which are available for free downloading, that support the securing actions of the SCADA systems in the different areas of operation: power, water, and transportation.

E. *Information Security Domains—CIGRÉ Developments*

Since the SCADA/EMS systems have become increasingly integrated, it becomes more difficult to treat the system structure in terms of "parts" or "subsystems." The physical realization of various functions is less evident from a user perspective. Instead, it becomes more natural to study a SCADA/EMS system in terms of "*domains*." This concept in application to power systems was introduced in [11].

A domain is a specific area, wherein specific activities/business operations are going on and they can be grouped together. Here, the following security domains are introduced (see Fig. 7).

- Public, Supplier, Maintainer Domain.
- Power Plant Domain.
- Substation Domain.
- Telecommunication Domain.
- Real-Time Operation Domain.
- Corporate IT Domain.

The purpose of the domain concept is to emphasize for everyone involved within a specific area the importance and handling of information security issues. Also, one domain X may be using hardware equipment and/or communications that are also used by domain Y. Therefore, the domains are typically interrelated. The domains described above may be different from one electric utility to another, depending on the utility's operation and tasks. The proposed domains in this paper are found to be chosen in a natural way. It is of course up to each utility to choose and implement its domains. The ideas presented here are general and applicable to another set of security domains and their interdependencies.

The security is treated within each domain, and there always only one "authority" responsible for security within the domain.

Different interests and compliance with legislative and contractual requirements could make it necessary to define a security policy structure using different security domains inside the power utility. Within one security domain, we shall rely on only one security policy and only one authority responsible for the security policy inside the domain. The authority should guarantee a minimum security level for the systems in the domain. The security level of the individual systems must be classified and may actually vary.

When communicating across power utilities, organizations, and other companies, using communication networks, the security domains should be recognized. For example, a power utility could define a security domain and related policies and procedures for its telecontrol activity to assure compliance with legislative or regulatory requirements. If similar definitions, procedures, policies, etc. were developed by other power utilities, it would be easier to discuss and define common rules for the information exchange or the usage of common resources in a communication network. However today, there are no common definitions including the terms "security," and "critical asset." Also, there are no common control system security policies or procedures, although groups such as IEC TC57 [50], ISA [53], and NIST [57], are working on generic policies and procedures. The reader is also recommended to refer to other valuable sources for information and cyber security [30]–[61].

A power utility should also discuss and define the policy structure depending on the topology and the importance of resources in the telecontrol network itself. A power utility on a regional level for example, must decide if all substations, all local control centers, and the regional control centre should belong to the same security domain or be split into several domains. This is particularly true when the utility provides electric as well as gas, or water products and services. This becomes more of an issue when utilities share equipments, such as remote terminal units (RTUs).

Furthermore in WG D2.22 [12], the information security domain model has been adopted and further used, in the context of an information security framework.

An Electric Power Utility (EPU) representing one security authority could define each domain according to the level of protection required by the organization. The domain model should be defined based on the results of a risk assessment process [14], [15]. Fig. 8 shows a model for different types of EPUs including examples of interconnections that are elaborated [13]. Appropriate security controls must be assigned to the domains and inter/intra connections. The EPU systems and data networks supported by IT components, such as servers, client devices, data communication infrastructure, access and network management devices, operating systems, and databases, must be mapped to the domain model, as well. This model is suited for a "defense in depth" strategy against cyber risk.

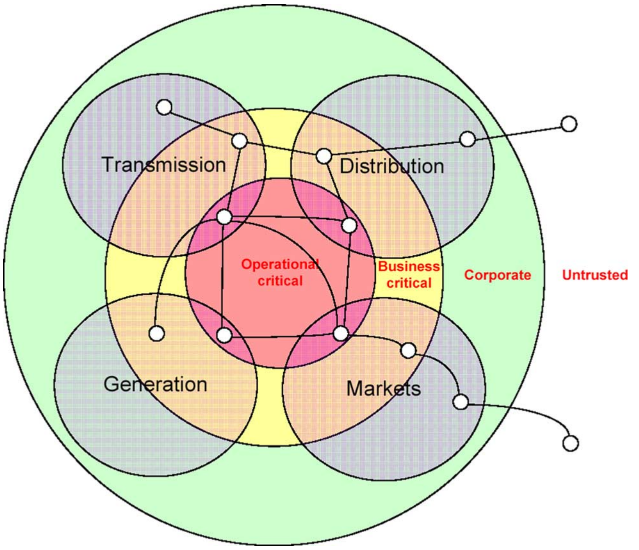

Fig. 8. Information security domain model.

Furthermore, an EPU needs to define its own selection of security controls for SCADA control systems, based on normative sources, such as ISO 27002 [47], NIST SP800-53 [57], NERC CIP [56], or ISA [53]. The controls must be appropriate for the EPU's regulatory regime and assessment of business risks.

The security controls need to be defined within each domain and the information flows between the domains, based on the agreed risk assessments. For example, the Corporate domain and Business critical domain controls will depend on an intra-business risk assessment, whereas the Operational critical domain controls are likely to require interdependent risk assessments between other operators and possibly Government agencies in addition to an intra-business risk assessment. Many types of IT components are required to support EPU control systems and lists of controls should be elaborated such as [13]:

- system architecture security controls;
- IT support user security control;
- user access security controls.

V. Smart Grids

During the last few years, the term "smart grid" [1]–[7] has become a buzzword. It is not the author's ambition to define this here, rather he would like to stress that the development of power communication systems is a key factor for actually having a power grid that is "smart." Due to the capabilities of having broadband connections, "smart" meters at the household premises, and RTUs with digital intelligence, together form a perquisite for a having a grid that could be considered "smart." We will in the near future encounter similar information and IT security considerations as described earlier in this paper.

A. Smart Meters

The broadband connections make it possible to transfer data faster and of more "bulky" kind if needed. The utilities now use the possibility of remotely reading the consumers' consumptions at each household, without the need to actually go to the premises and without notifying the customers. This saves time and money. But the broadband capabilities also open up new ways of introducing new functionality, both at the meters and in the central system collecting metering data.

Furthermore, the utilities are interested in transferring data *to* the households. Such data could include price information (USD/kWh) and "special offers." But data could also be *controls*, which then open up new cyber security considerations that need to be treated. One such example, which is a delicate issue, is to deal with "Which party will be responsible when, by mistake or by intentional digital tampering, a household is disconnected for two weeks, and that the owner of the house gets damages by destroyed food or water leakage, when he is away on two weeks of vacation?" The owner? The utility? Who? These issues are clearly related to cyber security and they must be raised within the electric power arena.

B. Smart Grid Systems—A Way Towards the Use of Wind Power

Another rising issue is the introduction of wind power in many countries. Some people may claim that is marginal, but in fact, this is clearly evident. For example, in Sweden, 20–30 TWh out of the total yearly consumption of 150 TWh may be based on wind power within ten years. This is certainly not marginal for the transmission system operator (TSO) Swedish National Grid. The intermittent production of power by a wind mill, in combination with maintaining the electrical balance, for example by means of increased use of hydro power, is very delicate.

These facts together constitute a challenge, and we here must work with smarter solutions, forming a "smart grid system."

VI. Concluding Remarks

PSC and cyber security issues are vital parts of the critical information infrastructure, such as a smart grid system. Here a historic perspective has been given, tying up PSC and cyber security. Also, the development of isolated "islands of automation" to fully integrated computer environments has been described. The "openness" required in the 1990s has opened up new possible vulnerabilities, which creates cyber security issues to be addressed and solved, e.g., integrated SCADA/EMS systems and administrative office IT environments must now be separated. Also, the author's experiences from his involvement in CIGRÉ developments have been given.

Furthermore, cyber security issues become increasingly important, when the term of "smart grid" has been introduced, and these developments will accelerate. This is evident for the use of smart meters and introduction of wind power, forming a "smart grid system."

References

[1] DOE, *What the Smart Grid Means to You and the People You Serve* U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, 2009.

[2] DOE, "Grid 2030"—A National Vision for Electricity's Second 100 Years U.S. Department of Energy, Office of Electric Transmission and Distribution, 2003.

[3] European Commission, European Technology Platform SmartGrids, Strategic Research Agenda for Europe's Electricity Networks of the Future EUR 22580, 92-79-03727-7. Luxembourg, 2007.

[4] G. N. S. Prasanna, A. Lakshmi, S. Sumanth, V. Simha, J. Bapat, and G. Koomullil, "Data communication over the smart grid," in *Proc. IEEE Int. Symp. Power Line Communications and Its Applications (ISPLC)*, Mar. 29–Apr. 1 2009, pp. 273–279.

[5] M. Pipattanasomporn, H. Feroze, and S. Rahman, "Multi-agent systems in a distributed smart grid: Design and implementation," in *Proc IEEE Power Systems Conf. and Expo.*, Mar. 15–18, 2009, pp. 1–8.

[6] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE J. Security & Privacy*, vol. 7, no. 3, pp. 75–77, May–Jun. 2009.

[7] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power Energy Mag.*, vol. 7, no. 2, pp. 52–62, Mar.–Apr. 2009.

[8] G. N. Ericsson, "Information security for Electric Power Utilities (EPUs)—CIGRÉ developments on frameworks, risk assessment and technology," *IEEE Trans. Power Del.*, vol. 24, no. 3, pp. 1174–1181, Jul. 2009.

[9] G. Ericsson, "Towards a framework for managing information security for an electric power utility—CIGRÉ experiences," *IEEE Trans. Power Del.*, vol. 22, no. 3, pp. 1461–1469, Jul. 2007.

[10] G. Ericsson and Å. Torkilseng, "Management of information security for an electric power utility—On security domains and use of ISO/IEC 17799 standard," *IEEE Trans. Power Del.*, vol. 20, pt. 1, pp. 683–690, Apr. 2005.

[11] G. Ericsson, Å. Torkilseng, G. Dondossola, T. Jansen, J. Smith, D. Holstein, A. Vidrascu, and J. Weiss, Security for Information Systems and Intranets in Electric Power Systems Tech. Brochure (TB) 317 CIGRÉ, 2007.

[12] G. Ericsson, Å. Torkilseng, G. Dondossola, L. Piètre-Cambacédès, S. Duckworth, A. Bartels, M. Tritschler, T. Kropp, J. Weiss, and R. Pellizzonni, Treatment of Information Security for Electric Power Utilities (EPUs) Tech. Brochure (TB), CIGRÉ, to appear 2010.

[13] Å. Torkilseng and S. Duckworth, "Security frameworks for electric power utilities—Some practical guidelines when developing frameworks including SCADA/control system security domains," *CIGRÉ Electra*, Dec. 2008.

[14] G. Dondossola, "Risk assessment of information and communication systems—Analysis of some practices and methods in the electric power industry," *CIGRÉ Electra*, Aug. 2008.

[15] M. Tritschler and G. Dondossola, "Information security risk assessment of operational IT systems at electric power utilities," presented at the CIGRÉ D2 Colloq., Fukuoka, Japan, Oct. 21–22, 2009, Paper D2-01 D03.

[16] A. Bartels, L. Piètre-Cambacédès, and S. Duckworth, "Security technologies guideline—Practical guidance for deploying security technology within electric utility data networks," *CIGRÉ Electra*, Jun. 2009.

[17] L. Piètre-Cambacédès, T. Kropp, J. Weiss, and R. Pellizzonni, "Cybersecurity standards for the electric power industry—A survival kit," presented at the CIGRÉ Session 2008, Paris, France, Paper D2-217.

[18] G. Ericsson, A. Bartels, D. Dondossola, and Å. Torkilseng, "Treatment of information security for electric power utilities—Progress report from CIGRÉ WG D2.22," presented at the CIGRÉ 2008 Session, Paris, France, Paper D2-213.

[19] L. Nordström, "Assessment of information security levels in power communication systems using evidential reasoning," *IEEE Trans. Power Del.*, vol. 23, no. 3, pp. 1384–1391, Jun. 2008.

[20] M. Ekstedt and T. Sommestad, "Enterprise architecture models for cyber security analysis," in *Proc. IEEE PCSE*, Mar. 2009.

[21] T. Cegrell, *Power System Control—Technology*. Englewood Cliffs, NJ: Prentice-Hall, 1986.

[22] G. Ericsson, "Classification of power systems communications needs and requirements: Experiences from case studies at swedish national grid," *IEEE Trans. Power Del.*, vol. 17, no. 2, pp. 345–347, Apr. 2002.

[23] G. Ericsson, "On requirements specifications for a power system communications system," *IEEE Trans. Power Del.*, vol. 20, no. 2, pp. 1357–1362, Apr. 2005.

[24] T. Rahkonen, "User Strategies for Open Industrial IT Systems," Ph.D. dissertation, Royal Inst. Technol., Stockholm, Sweden, 1996, ISRN KTH/ICS/R-96/1-SE.

[25] A. M. Sasson, "Open systems procurement: A migration strategy," *IEEE Trans. Power Syst.*, vol. 8, no. 2, pp. 515–526, May 1993.

[26] G. Ericsson and T. Rahkonen, "Openness in communication for power system control, a state-of-the-practice study," in *Proc. IEEE Power Tech*, Stockholm, Sweden, Jun. 1995.

[27] P. Roche, “Cyber security considerations in power system operations,” *CIGRÉ Electra No. 218*, Feb. 2005.

[28] Swedish Civil Contingencies Agency, SCADA Security Coordination [Online]. Available: http://www.msbmyndigheten.se/default_138.aspx?epslanguage=EN

[29] Swedish Civil Contingencies Agency, Guide to Increased Security in Process Control Systems for Critical Societal Functions [Online]. Available: http://www.krisberedskapsmyndigheten.se/upload/17915/SCADA_eng_2008.pdf

[30] COSO ERM (The Committee of Sponsoring Organizations of the Treadway Commission—Enterprise Risk Management), 2004 [Online]. Available: www.coso.org

[31] COBIT (Control Objectives for Information and related Technology) [Online]. Available: www.isaca.org

[32] *ISO/IEC 20000-1:2005 Information Technology—Service Management—Part 1: Specification*, .

[33] *ISO/IEC 20000-2:2005 Information Technology—Service Management—Part 2: Code of Practice*, .

[34] ITIL (IT Infrastructure Library) [Online]. Available: www.itil-officialsite.com/home/home.asp

[35] *Risk Management—Vocabulary, ISO/IEC CD 2 Guide 73, Concept*, , Apr. 2008.

[36] *Risk Management—Principles and Guidelines on Implementation, ISO/DIS 31000, Concept*, , April 2008.

[37] Generic SCADA Risk Management Framework for the IT Security Expert Advisory Group (ITSEAG), Trusted Information Sharing Network for Critical Infrastructure Protection Dec. 2006.

[38] AS/NZS 4360:2004 Risk Management Standards Australia.

[39] IRRIIS Project [Online]. Available: http://www.irriis.org

[40] CRUTIAL Project [Online]. Available: http://crutial.cesiricerca.it

[41] Risk Assessment of Information and Communication Systems—Analysis of Some Practices and Methods in the Electric Power Industry Giovanna Dondossola CESI RICERCA SpA, Electra, Aug. 2008.

[42] G. Dondossola and O. Lamquet, “Cyber risk assessment in the electric power industry,” *Electra No 224* pp. 36–43, Feb. 2006 [Online]. Available: http://www.cigre.org/gb/electra/electra.asp

[43] G. Dondossola, O. Lamquet, and A. Torkilseng, “Key issues and related methodologies in the security risk analysis and evaluation of electric power control systems,” in *CIGRÉ Session 2006*, Paris 27, Aug. 1–Sep. 2 .

[44] Common Vulnerabilities and Exposures List [Online]. Available: http://www.cve.mitre.org/

[45] *Standards and Projects Under the Direct Responsibility of JTC 1/SC 27 Secretariat*, [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306

[46] *Information Technology—Security Techniques—Information Security Management Systems—Requirements*, ISO/IEC 27001:2005 [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

[47] *Information Technology—Security Techniques—Information Security Management Systems—Code of Practice for Information Security Management*, ISO/IEC 27002:2005 [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

[48] *Information Technology—Security Techniques—Information Security Risk Management*, ISO/IEC 27005:2008 [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107

[49] L. Piètre-Cambacédès, C. Chalhoub, and F. Cleveland, “IEC TC57 WG15—Cyber security standards for the power system,” in *Proc. CIGRÉ D2 Colloq.*, Luzern, Switzerland, 2007.

[50] IEC, Power System Control & Associated Communications—Data & communication Security 62351 part 1-8, TS.

[51] Cryptographic Protection of SCADA Communications AGA Report 12 [Online]. Available: www.aga.org/Committees/gotocommitteepages/gasctrl/AGAReport12.htm

[52] IEEE, Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links Draft 3, 2008-08-16 [Online]. Available: http://grouper.ieee.org/groups/sub/wgc6/wgc6.htm

[53] ISA99 [Online]. Available: http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

[54] Security Technologies for Industrial Automation and Control Systems Technical Report ANSI/ISA-TR99.00.01-2007 [Online]. Available: http://www.isa.org/Template.cfm?Section=Shop_ISA&Template=/Ecommerce/ProductDisplay.cfm&Productid=9665

[55] “The ISA99 Standards Vision, A Roadmap for Developing Secure Industrial Automation and Control Systems,” in *ISA EXPO 2008*, Oct. 2008.

[56] NERC CIP Standards as Approved by the NERC Board of Trustees May 2006 [Online]. Available: ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Cyber_Security_Standards_Board_Approval_02May06.pdf

[57] NIST, Computer Security Division, Computer Security Resource Centre [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html

[58] NIST ICS Security Project [Online]. Available: http://csrc.nist.gov/sec-cert/ics/index.html

[59] CPNI Guidelines [Online]. Available: http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

[60] J. Weiss, Control Systems Cyber Security-The Current Status of Cyber Security of Critical Infrastructures Testimony before the Committee on Commerce, Science, and Transportation, US Senate, March 19, 2009.

[61] A. Jaquith, *Security Metrics—Replacing Fear, Uncertainty, and Doubt*. Reading, MA: Addison-Wesley, 2007.

Göran N. Ericsson (S’90–M’96–SM’06) was born in Huddinge, Sweden, in 1963. He received the Ph.D. degree from the Royal Institute of Technology (KTH), Stockholm, Sweden, in 1996.

In 1997, he joined Svenska Kraftnät (Swedish National Grid), Sundbyberg, Sweden. During 1997–2006, he held expert and managerial positions within the fields of data and telecommunications. During 2007–2009, he was the Chief Information and IT Security Officer. From 2006 to 2009, he was the Convener of the CIGRÉ Working Group D2.22 on information security. As of June 2009, he has been a R&D Manager.

Dr. Ericsson is active in the IEEE Power and Energy Society PSCC and CIGRÉ SCD2.