Journal Of Harmonized Research (JOHR)

Journal Of Harmonized Research in Engineering
6(3), 2018, 28-37

ISSN 2347 – 7393

Original Research Article

SMART GRID INFRASTRUCTURE FOR CYBER SECURITY AND POWER SYSTE COMMUNICATION

Rishi Kushwah[1], Rashmi Singh[2], Harsh Pratap Singh[1]

[1]Sri Satya Sai Univeristy of Technology and Medical Sciences, Sehore (M.P.) India
[2]Radharaman Institute of Science and Technology Bhopal (M.P.) India

Abstract: The introduction of "smart grid" arrangements forces that digital security and power framework correspondence frameworks must be managed widely. These parts together are basic for appropriate power transmission, where the data infrastruc-ture is basic. The improvement of correspondence abilities, moving power system from "islands of computerization" to-count coordinated PC situations, have opened up novel possibilities and vulnerabilities. Since a scarce power control frameworks have been secured with "openness" necessities, digital secu-rity dangers get to be distinctly clear. For restoration of a SCADA/EMS framework, a detachment of the operational and regulatory computer system must be acquired. The paper treats digital security concerns, and it highlights get to focuses in a substation. Cyber security concerns are indispensable for "smart gride" arrangements. Broadband communications open up for savvy meters, and the expanding utilization of wind power requires a "smart grid system."

Index Terms—Communication system, control system, digital security, data security, IT security, power system communication, control framework control, control frameworks, SCADA, security, shrewd matrix, wide-territory systems.

I. Introduction: The idea of "smart grid" [1]–[7] has turned into a “hype." It has gotten extensive energy amid the current years, and this is relied upon to grow significantly more. Basic parts here are the digital security issues and the power system communication (PSC) system, which are worried in this paper. The utilization of power is of vital significance to our general public, and the requirement for power supply is expanding. Here, the apprehensions on physical security are somewhat mature and easy to grasp, however now the digital threats are increasing. By method for the PSC abilities, supervisory control and information obtaining (SCADA)

For Correspondence:
rishisinghkushwah@gmail.com
Received on: August 2018
Accepted after revision: September 2018
Downloaded from: www.johronline.com
DOI: 10.30876/JOHR.6.3.2018.28-37

system and substations are presently interconnected with different system. These correspondences occur both over committed line and over the Internet. Likewise in the prior ventures, data and Information Technology (IT) security issues were not considered, as it were, or not under any condition.

For the most part, the patterns are that merchants are utilizing business off the rack (COTS) items as a major aspect of their SCADA/ energy management system (EMS) system, rather than utilizing proprietary arrangements. Here, the expanding utilization of standard items, for example, (PCs), operating systems, and, net-working elements, now opens up new conceivable outcomes and dangers.

The knowledge of security can now be all the more effortlessly known and partitioned on more individuals; the “security-by-obscurity" standard does not make a difference to an indistinguishable degree from some time recently. Rather, the burrow ital dangers emerge and should be taken care of structurally. Here, the consciousness of the new conceivable effects and dangers is essential. All people included must endeavor to take dynamic choices on the decision of sufficient specialized arrangements while conveying another SCADA system, or ensuring a current one.

A. Purpose: The motivation behind the paper is to underscore the part of digital security and PSC system in conjunction with each other, in a smart grid infrastructure, where the data foundation is as basic as the physical. Additionally, a verifiable advancement for each spective is given, clarifying a portion of the actualities of the PSC systems of today, having halfway defenseless structure. The work portrayed in this is created and in view of quite a while of CIGRÉ working collective endeavors inside the field of force system interchanges [8]–[18], where the creator has been effectively included (some portion of the work as a convener). The latest results have been displayed in [8] and [12]. Additionally, the works of [19]–[21] should be considered.

B. Outline

In Section II, the improvement periods of power system communication system are portrayed, together with a classification of various correspondence abilities and necessities. From that point in Section III, the developments of power system control system are given, from "islands of mechanization" to completely coordinated system. Here additionally, a discourse on “open systems" is given. In Section IV, the digital security issues are dealt with. In Section V, digital security highlights regarding to "Smart grids" are given. The paper closes with finishing up comments in Section VI.

II. Development and Classification of Power System Communication Systems

Communication: proficiencies have developed from narrow- band, squat speed communications to high speed broadband “highways” for all sorts of communications. From being exceptionally delimiting variable, new conceivable outcomes have opened up, which have upheld the advancement of PSC system depicted in Section III.

A. Classifications of communications

Correspondence necessities ought to be characterized, since this encourages the treatment of prerequisites and the request of requirements. One path is to characterize prerequisites into three classes, in particular:

- Ongoing operational correspondence prerequisites;
- Managerial operational correspondence prerequisites;
- Managerial correspondence prerequisites.

These three classes were initially presented in 2001/2002 [22], based on works at the Swedish National Grid. Encounters have now demonstrated that this grouping methodology is exceptionally appropriate [23]. It is presently generally utilized both esoteric and outdoor Swedish National Grid.1) Real-Time Operational Communication Requirements: Real-time operational communication comprehends communication in real time that is prerequisite to preserve operation of the power system. The class is in turn separated into real-time operational data communication and real-time operational speech communication.

Constant operational information correspondence incorporates:

- Teleprotection;
- Control framework control.

The correspondence is portrayed by the way that interaction must happen progressively, with hard time prerequisites. The correspondence prerequisites characterize the plan of the technical arrangements.

For teleprotection purposes, messages ought to be transmitted inside a brief timeframe outline. Most extreme permitted time is in the scope of 12–20 ms, contingent upon the sort of insurance plan. The prerequisite has its starting point in the way that blame current disassociation might work inside around 100 ms.

Control System Control predominantly incorporates supervisory control of the power procedure on auxiliary or larger amounts. These systems are of the kind SCADA/EMS.

Constant operational voice correspondence includes customary communication; where voice correspondence has an operational reason, e.g., investigating in an aggravated power operational case, power system island operations. The real plausibility of having voice correspondence is, by the control focus staff, considered as a standout amongst the most imperative instruments, both in ordinary and anomalous operation cases. Continuous operational voice correspondence likewise incorporates copy for exchanging succession orders.

2) Authoritative Operational Communication Requirements: not withstanding ongoing operational correspondence, data is required that, in more detail and subsequently, bolster portrayal of what has occurred in minor and significant power system aggravations. This class is alluded to as administrator iterative operational correspondence. Cases are communications.

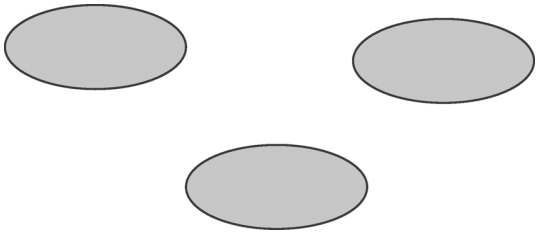

Fig.1. Islands of Automation.

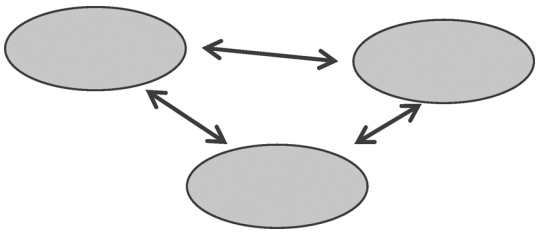

Fig.2. Interconnected system structure.

With nearby occasion recorders, unsettling influence recorders, and power swing recorders. The correspondence is portrayed by that association does not have to occur continuously. Time necessities are moderate.

Additionally, the accompanying capacities are incorporated into this class.

- Asset administration.
- Fault area.
- Metering and exchange of settlement data.
- Security system.
- Substation camera supervision.

3) Regulatory Communication Requirements: Administrative correspondence incorporates voice correspondence and facmetaphor inside the organization (likewise between the workplaces that are at various topographical areas), and in addition to/from the company, where the correspondence has a managerial reason.

III. **Development of power system control systems:** The PSC system has been and will progressively be the life nerve of the power system. It is the need and essential for sufficient operation and control of a power system. Likewise as for new prerequisites in view of data and IT security, the attention will increment on the correspondence system.

Information correspondence system have been created from exclusive answers for institutionalized off-the-rack arrangements, where the sellers more get to be system integrators, as opposed to power control system fashioners. Subsequently, control system that used to be shaped as "Islands of Automation" [21], now have created to interconnected and even coordinated—see Figs. 1–4.

Truth be told, it is the specialized development of interchanges systems and their capacities that have opened up for this between action. Besides in view of these potential outcomes, there were real powers in the 1990s making progress

toward "open system" [24], [25] when obtaining power control system. The utilities required the SCADA/EMS to be more open, and the merchants all guaranteed that their system items were open.

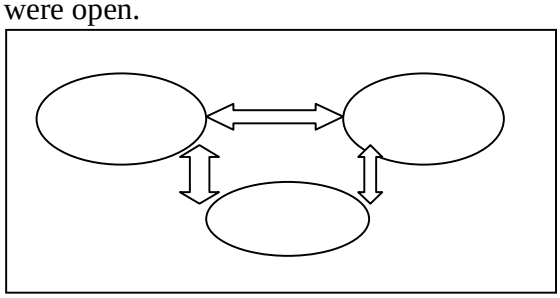

Fig.3.Partially integrated system structure.

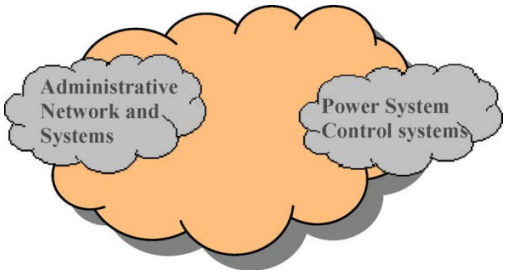

Fig.4.Today full integration system structure.

If the endeavors of obtaining of such framework in the 1990s and mid 2000s are pondered, it can be seen that few of the system were procured with the essential of getting openness in the PCS system condition. For data correspondence system, truth be told some PSC structures parts have opened up [26], while distinctive parts are still in light of prohibitive solutions.

By and by, a client ordinarily gets what he requests from the seller. So in the event that one requests "openness" one may get it. Also, on the off chance that one doesn't request "IT security," one doesn't get that.

Thus, there are a few power utilities around the world that now have introduced SCADA/EMS and modern control systems, which were opened up from the outline stage, however had exceptionally constrained security joined in the system arrangements. It was obviously enticing to require the openness, since new possibilities then emerged. Be that as it may, these utilities now have data and IT security issue to handle. This reality is not kidding, it is a developing concern, and it must be considered for framework every day operation eration and control by every utility.

IV. **Cyber security issues:** In view of the portrayed development of PSC frameworks and constrained worry of digital security in the 1990s, new issues have emerged, which are depicted here.

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

While existing SCADA/EMS system now are being refurbished or supplanted, the data and IT security issues must be considered.

In the event that a SCADA/EMS system is to be restored, the operational SCADA/EMS system part should be protected from the

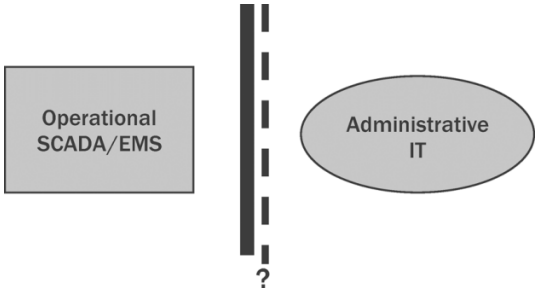

Fig.5.Decoupling among operational SCADA/EMS and administrative IT environments.

Managerial part, with the end objective that the Operational part is shielded from advanced dangers that are plausible over the Internet connection.

In the event that a SCADA/EMS system is to be supplanted, it is then a decent event to reexamine a general system structure, and afterward join IT security on all SCADA/EMS levels.

A path towards this more secure state is to, if conceivable, decouple the Operational SCADA/EMS system and the Administrative IT system. Additionally, an option might be to secure the firewall setup in the middle of operational and administrative parts—see Fig. 5.

B. **Threat and Possibilities**: The way that SCADA/EMS system now is being interconnected and coordinated with outer frameworks makes new possibilities and dangers."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

creator has been a dynamic part. As a major aspect of the JWG endeavors, the different interconnections of a substation were researched [27]; see Fig. 6. All the numbered "get to focuses" (1–10) illustrates the conceivable focuses whereto the substation can be gotten too. As the peruser may see, there is extraordinary number of focuses. What's more, obviously, this number creates an operational situation that infers conceivable advanced en-stupors and consequently computerized vulnerabilities.

C. SCADA Systems and SCADA security

The element that SCADA systems now are, to a prodigious 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 sensitive question, on what to do and how to deal with this new unsecure circumstance, since SCADA system are crucial for a few basic foundations, where a power control system is one such system and open transportation is another. The utilization of SCADA system is cross-sectional and it affects distinctive parts of a general public. Here, the insurance of the computerized structure of a framework commonly alludes to "basic information foundation security" (CIIP).

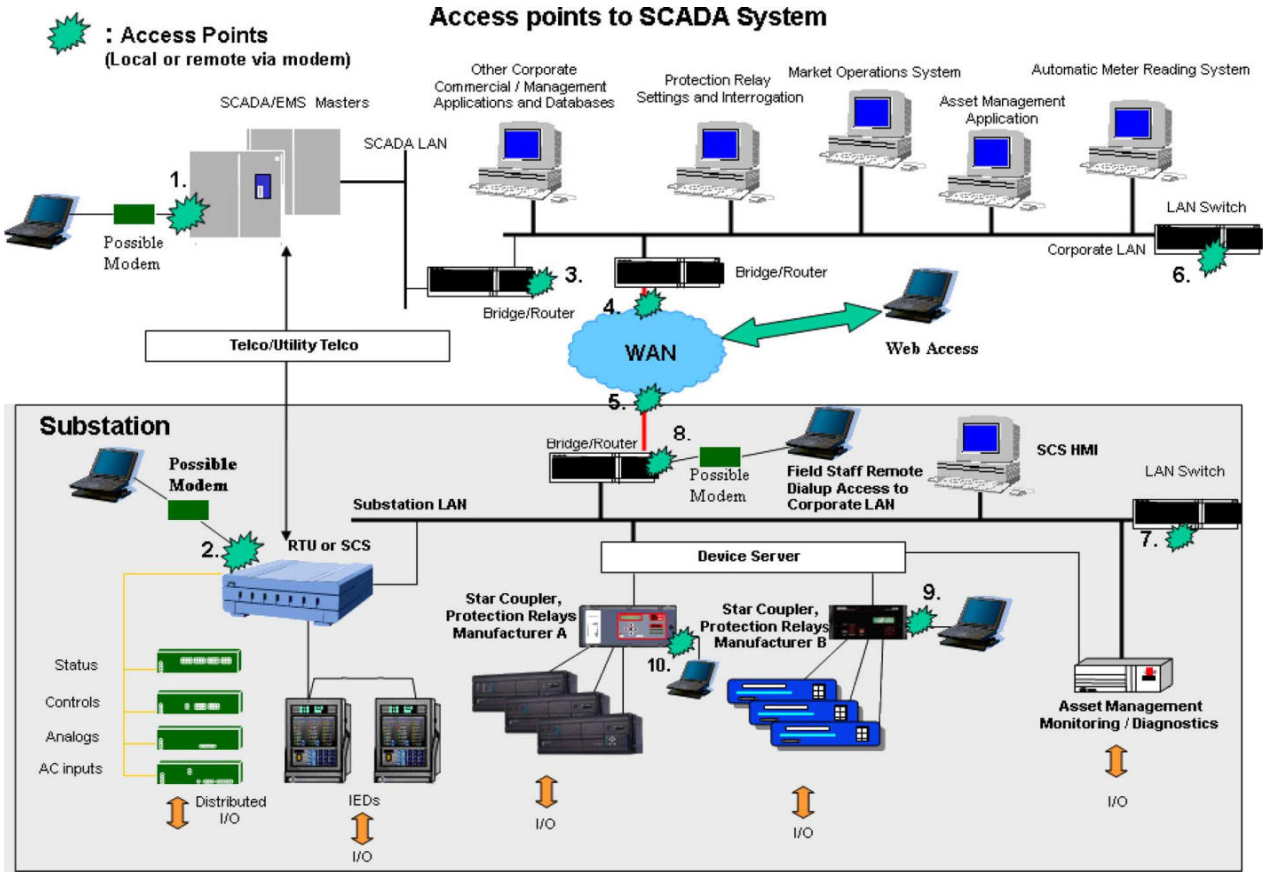

Fig.6.Access points to SCADA system.

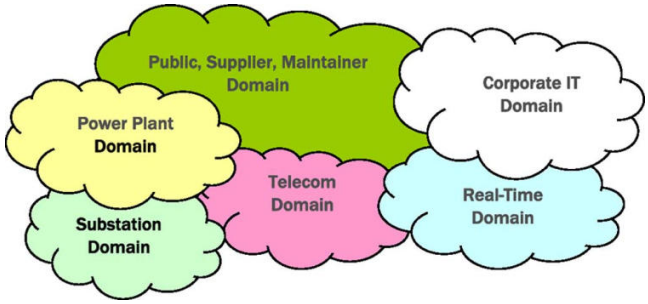

Fig.7. Information security domains.

D. Governmental Coordination in Sweden on SCADA Security: Like in numerous different nations, the issues of securing CIIP systems have been stressed in Sweden. An administrative coordination activity between various specialists and organizations were begun in [28], concentrating on SCADA security. The activity depends on that current associations take an interest, for example, control utilities, water organizations, and railroad, which have SCADA systems as basic piece of operations. Additionally, the security police are spoken to. Here, the aptitude is accumulated and encounters are shared, including both local and global learning; everything with the motivation behind securing the SCADA system being a piece of the basic data foundations of Sweden. As a characteristic stride, the SCADA Security Guideline has been developed [29]. Likewise, specialized rules and managerial recommendations are created which are accessible for nothing down-stacking, that bolster the securing activities of the SCADA systems in the distinctive territories of operation: power, water, and transportation.

E. Information Security Domains—CIGRÉ Developments: Since the SCADA/EMS system have turned out to be progressively coordinated, it turns out to be more hard to treat the system structure as far as "parts" or "subsystems." The physical acknowledgment of different capacities is less clear from a client point of view. In-stead, it turns out to be more normal to concentrate a SCADA/EMS system as far as "spaces." This idea in application to control systems was presented in [11].

A space is a particular range, wherein particular exercises/business operations are going on and they can be gathered together. Here, the accompanying security spaces are presented (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 forevery one 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 in terrelated. The areas portrayed above might be not quite the same as one electric utility to another, contingent upon the utility's operation and assignments.

The security is dealt with inside every space, and there constantly just a single “authority" in charge of security inside the area. Distinctive interests and consistence with authoritative and contractual prerequisites could make it important to characterize a security strategy structure utilizing diverse security areas inside the power utility. Inside one security area, we might depend on just a single security strategy and just a single expert in charge of the security approach inside the space. The expert ought to guarantee a base security level for the frameworks in the space. The security level of the individual frameworks must be ordered furthermore, may really differ.

When conveying crosswise over power utilities, associations, and different organizations, utilizing correspondence arranges, the security spaces ought to be perceived. For instance, a power utility could characterize a security area and related strategies and procedures for its telecontrol action to guarantee consistence with legislative or administrative necessities. On the off chance that comparative definitions, procedures, strategies, and so forth were produced by other power utilities, it is less demanding to talk about and characterize normal standards for the in-arrangement trade or the use of basic assets in a communication organize. However today, there are no basic definitions

including the expressions "security," and "basic resource." Also, there are no normal control system security approaches or procedures, in spite of the fact that gatherings, for example, IEC TC57 [50], ISA [53], and NIST [57], are chipping away at bland strategies and techniques. The peruser is likewise prescribed to allude to other profitable hotspots for data and digital security [30]–[61].

Besides in WG D2.22 [12], the data security do-primary model has been embraced and further utilized, with regards to a data security structure. An Electric Power Utility (EPU) speaking to one security authority could characterize every area as indicated by the level of expert tection required by the association. The space model ought to be characterized in view of the consequences of a hazard evaluation prepare [14], [15]. Fig. 8 demonstrates a model for various sorts of EPUs including cases of interconnections that are expounded [13]. Suitable security controls must be doled out to the areas and bury/intra associations. The EPU frameworks and information systems bolstered by IT segments, for example, servers, customer gadgets, information correspondence foundation, get to and arrange management gadgets, working frameworks, and databases, must be

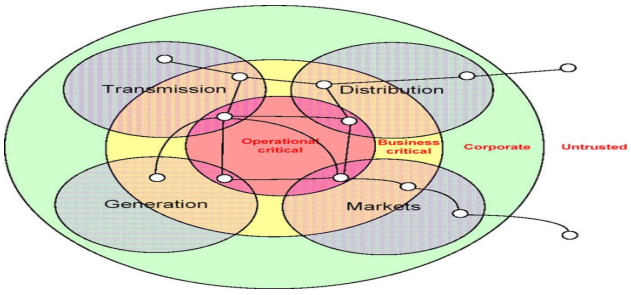

Fig.8.Information security domain model.

Mapped to the space show, also. This model is suited for a "resistance inside and out" technique against digital hazard.

Besides, an EPU needs to characterize its own determination of security controls for SCADA control frameworks, in light of standardizing sources, for example, ISO 27002 [47], NIST SP800-53 [57], NERC CIP [56], or ISA [53]. The controls must be proper for the EPU's administrative administration and appraisal of business dangers.

The security controls should be characterized inside every area and the data streams between the spaces, in view of the concurred hazard appraisals. For instance, the Corporate space and Business basic area controls will rely on upon an intra-business chance appraisal, while the Operational basic do-principle controls are probably going to require related hazard evaluate ments between different administrators and perhaps Government agencies notwithstanding an intra-business chance appraisal. Many sorts of IT parts are required to bolster EPU control frameworks and arrangements of controls ought to be expounded, for example, [13]:

- Framework engineering security controls;
- IT bolster client security control;
- Client get to security controls.

V. **Smart grids:** Amid the most recent couple of years, the expression "smart gride" [1]–[7] has turned into a trendy expression. It is not the creator's aspiration to characterize this here, rather he might want to stress that the improvement of force correspondence frameworks is a key variable for really having a power gride that is "smart." Due to the abilities of having broadband associations, "smart" meters at the family unit premises, and RTUs with computerized insight, together shape a perquisite for a having a matrix that could be viewed as "smart." We will sooner rather than later experience comparative data and IT security contemplations as portrayed before in this paper.

A. **Smart Meters:** The broadband associations make it conceivable to exchange information speedier and of more "massive" kind if necessary. The utilities now utilize the likelihood of remotely perusing the buyers' consumptions at every family unit, without the need to really go to the premises and without informing the clients. This spares time and cash. Be that as it may, the broadband capacities additionally open up better approaches for presenting new usefulness, both at the meters and in the focal framework gathering metering information.

Besides, the utilities are occupied with exchanging information to the family units. Such information could incorporate value data

(USD/kWh) and "uncommon offers." But information could likewise be controls, which then open up new digital security contemplations that should be dealt with. One such case, which is a fragile issue, is to manage "Which gathering will be capable when, by mistake or by deliberate advanced altering, a family is disconnected for two weeks, and that the proprietor of the house gets dam-ages by crushed sustenance or water spillage, when he is away on two weeks of get-away?" The proprietor? The utility? Who? These is-sues are plainly identified with digital security and they should be raised inside the electric power field.

B. Smart Grid Systems—A Way towards the Use of Wind: Power Another rising issue is the presentation of twist power in numerous nations. A few people may assert that is minor, yet truth be told, this is unmistakably apparent. For instance, in Sweden, 20–30 Two out of the aggregate yearly utilization of 150 Two might be founded on twist control inside ten years. This is absolutely not minimal for the transmission framework administrator (TSO) Swedish National Grid. The irregular creation of force by a twist process, in combicountry with keeping up the electrical adjust, for instance by method for expanded utilization of hydro power, is exceptionally fragile.

VI. Concluding remarks: PSC and digital security issues are imperative parts of the basic data foundation, for example, a brilliant framework. Here a noteworthy point of view has been given, tying up PSC and digital security. Likewise, the improvement of disengaged "islands of automation" to completely coordinated PC situations has been de-scribed. The "openness" required in the 1990s has opened up new conceivable vulnerabilities, which makes digital security issues to be tended to and explained, e.g., incorporated SCADA/EMS systems and managerial office IT conditions should now be isolated. Additionally, the creator's encounters from his inclusion in CIGRÉ advancements have been given.

References

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

[2] DOE, "Matrix 2030"— A National Vision for Electricity's Second 100 A long time U.S. Bureau of Energy, Office of Electric Transmission and Appropriation, 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, "Information correspondence over the brilliant network," in Proc. IEEE Int. Symp. Control Line Communications and Its Applications (ISPLC), Mar. 29–Apr. 1 2009, pp. 273–279.

[5] M. Pipattanasomporn, H. Feroze, and S. Rahman, "Multi-specialist sys-tems in a circulated shrewd matrix: Design and usage," in Proc IEEE Power Systems Conf. also, Expo., Mar. 15–18, 2009, pp. 1–8.

[6] P. McDaniel and S. McLaughlin, "Security and protection challenges in the shrewd network," IEEE J. Security and Privacy, vol. 7, no. 3, pp. 75–77, May–Jun. 2009.

[7] A. Ipakchi and F. Albuyeh, "Matrix without bounds," IEEE Power Energy Mag., vol. 7, no. 2, pp. 52–62, Mar.–Apr. 2009.

[8] G. N. Ericsson, "Data security for Electric Power Utilities (EPUs)— CIGRÉ improvements on systems, chance evaluation and innovation," IEEE Trans. Control Del., vol. 24, no. 3, pp. 1174–1181, Jul. 2009.

[9] G. Ericsson, "Towards a system for overseeing data security for an electric power utility—CIGRÉ encounters," IEEE Trans. Control Del., vol. 22, no. 3, pp. 1461–1469, Jul. 2007.

[10] G. Ericsson and Å. Torkilseng, "Administration of data security for an electric power utility—On security areas and utilization of ISO/IEC 17799 standard," IEEE Trans. Control Del., vol. 20, pt. 1, pp. 683–690, Apr.2005.

[11] G. Ericsson, Å. Torkilseng, G. Dondossola, T. Jansen, J. Smith, D. Hol- stein, A. Vidrascu, and J. Weiss, Security for Information Systems and Intranets in Electric

Power Systems Tech. Pamphlet (TB) 317 CIGRÉ, 2007.
[12] G. Ericsson, Å. Torkilseng, G. Dondossola, L. Pietre-Cambacédès, S. Duckworth, A. Bartels, M. Tritschler, T. Kropp, J. Weiss, and R. Pelliz-zonni, Treatment of Information Security for Electric Power Utilities (EPUs) Tech. Handout (TB), CIGRÉ, to seem 2010.
[13]Å.TorkilsengandS.Duckworth,"Securityfra meworks forelectric powerutilities—Some practical guidelines when developing frameworks including SCADA/control system security domains," *CIGRÉ Electra*,Dec.2008.
[14] G. Dondossola, "Hazard appraisal of data and correspondence frameworks—Analysis of a few practices and techniques in the electric power industry," CIGRÉ Electra, Aug. 2008.
[15] M. Tritschler and G. Dondossola, "Data security hazard evaluate ment of operational IT frameworks at electric power utilities," displayed at the CIGRÉ D2 Colloq., Fukuoka, Japan, Oct. 21–22, 2009, Paper D2-01 D03.
[16] A. Bartels, L. Pietre-Cambacédès, and S. Duckworth, "Security innovations rule—Practical direction for sending security innovation inside electric utility information systems," CIGRÉ Electra, Jun. 2009.
[17] L. Pietre-Cambacédès, T. Kropp, J. Weiss, and R. Pellizzonni, "Cy-bersecurity guidelines for the electric power industry—A survival unit," introduced at the CIGRÉ Session 2008, Paris, France, Paper D2-217.
[18] G. Ericsson, A. Bartels, D. Dondossola, and Å. Torkilseng, "Treatment of data security for electric power utilities—Progress report from CIGRÉ WG D2.22," introduced at the CIGRÉ 2008 Session, Paris, France, Paper D2-213.
[19] L. Nordström, "Appraisal of data security levels in powercorrespondence frameworks utilizing evidential thinking," IEEE Trans. Control Del., vol. 23, no. 3, pp. 1384–1391, Jun. 2008.
[20] M. Ekstedt and T. Sommestad, "Endeavor design models for digital security examination," in Proc. IEEE PCSE, Mar. 2009.
[21] T. Cegrell, Power System Control—Technology. Englewood Cliffs, NJ: Prentice-Hall, 1986.
[22] G. Ericsson, "Characterization of force frameworks correspondences needs and necessities: Experiences from contextual investigations at swedish national network," IEEE Trans. Control Del., vol. 17, no. 2, pp. 345–347, Apr. 2002.
[23] G. Ericsson, "On prerequisites determinations for a power framework interchanges framework," IEEE Trans. Control Del., vol. 20, no. 2, pp. 1357–1362, Apr. 2005.
[24] T. Rahkonen, "Client Strategies for Open Industrial IT Systems," Ph.D. thesis, Royal Inst. Technol., Stockholm, Sweden, 1996, ISRN KTH/ICS/R-96/1-SE.
[25] A. M. Sasson, "Open systems procurement: A development technique," IEEE Trans. Control Syst., vol. 8, no. 2, pp. 515–526, May 1993.
[26] G. Ericsson and T. Rahkonen, "Openness in correspondence for power framework control, a condition of-the-practice consider," in Proc. IEEE PowerTech, Stockholm, Sweden, Jun. 1995.
[27] P. Roche, "Digital security contemplations in power framework operations," CIGRÉ Electra No. 218, Feb. 2005.
[28] Swedish Civil Contingencies Agency, SCADA Security Coordi-country [Online]. Accessible: http://www.msbmyndigheten.se/de-fault_138.aspx?epslanguage=EN
[29] Swedish Civil Contingencies Agency, Guide to Increased Security in Process Control Systems for Critical Societal Functions [Online]. Accessible: http://www.krisberedskapsmyndigheten.se/up-load/17915/SCADA_eng_2008.pdf
30] COSO ERM (The Committee of Sponsoring Organizations of the Tread way Commission—Enterprise Risk Management), 2004 [On-line]. Accessible: www.coso.org
[31] COBIT (Control Objectives for Information and related Technology) [Online]. Accessible: 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]. Accessible: www.itil-official site.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 Ex-energetic 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]. Accessible: http://www.irriis.org
[40] CRUTIAL Project [Online]. Accessible: 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, "Digital hazard appraisal in the electric control industry," Electra No 224 pp. 36–43, Feb. 2006 [Online]. Profit capable: http://www.cigre.org/gb/electra/electra.asp.
[43] G. Dondossola, O. Lamquet, and A. Torkilseng, "Key issues and related systems in the security hazard investigation and assessment of electric control frameworks," 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]. Accessible: 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]. Accessible: http://www.iso.org/iso/iso_catalogue/catalogue_tc/cata-logue_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]. Accessible: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_de-tail.htm?csnumber=50297
[48] Information Technology—Security Techniques—Information Secu-rity Risk Management, ISO/IEC 27005:2008 [Online]. Accessible:http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_de-tail.htm?csnumber=42107
[49] L. Piètre-Cambacédès, C. Chalhoub, and F. Cleveland, "IEC TC57 WG15—Cyber security norms for the power framework," in Proc. CIGRÉ D2 Colloq., Luzern, Switzerland, 2007.
[50] IEC, Power System Control and Associated Communications—Data and correspondence Security 62351 section 1-8, TS.