Hindawi Publishing Corporation
Advances in Electrical Engineering
Volume 2014, Article ID 896296, 13 pages
http://dx.doi.org/10.1155/2014/896296

Research Article

Towards the Smart Grid: Substation Automation Architecture and Technologies

A. Leonardi, K. Mathioudakis, A. Wiesmaier, and F. Zeiger

AGT International, Hilpertstraße 35, 64295 Darmstadt, Germany

Correspondence should be addressed to A. Leonardi; aleonardi@agtinternational.com

Received 29 April 2014; Accepted 29 June 2014; Published 20 August 2014

Academic Editor: Sarod Yatawatta

This paper deals with Industrial Control Systems (ICS) of the electrical sector and especially on the Smart Grid. This sector has been particularly active at establishing new standards to improve interoperability between all sector players, driven by the liberalization of the market and the introduction of distributed generation of energy. The paper provides a state-of-the-art analysis on architectures, technologies, communication protocols, applications, and information standards mainly focusing on substation automation in the transmission and distribution domain. The analysis shows that there is tremendous effort from the Smart Grid key stakeholders to improve interoperability across the different components managing an electrical grid, from field processes to market exchanges, allowing the information flowing more and more freely across applications and domains and creating opportunity for new applications that are not any more constraint to a single domain.

1. Introduction

The electrical grid undergoes a fundamental change with the introduction of the Smart Grid. Installation of end consumer smart meters, deployment of distributed renewable energy generation, and interconnection of operation and information systems require new solutions that can intelligently monitor and manage the infrastructure.

The Smart Grid aims on raising operational efficiencies of operators by increasing the flow of information and automation in order to enable better and faster decisions, hence reducing operational cost. In order to achieve this, utilities are facing some challenges to improve the power delivery methods and utilization, including the integration of control room systems for better workflow, new consumer demands, and security of supply.

Additionally, future trends and developments in operations centers, for example, Supervisory Control and Data Acquisition (SCADA) systems, can be observed.

(i) Integration of operations' centers for smart distribution grids includes the advanced integration of existing IT infrastructure as well as the development of new applications.

(ii) SCADA systems are becoming increasingly ubiquitous. Thin clients, web portals, and web based products are gaining popularity with most major vendors but also introduce additional security aspects.

(iii) SCADA systems become more integrated and connected with existing Enterprise Resource Planning (ERP) systems and other non-SCADA or external applications but require new, tailored architectural approaches to guarantee continuous operation of critical resources.

(iv) Information Technology (IT) and Operational Technology (OT) vendors must prove that their analytics tools have real value at scale in order to integrate their capabilities with new solutions that help utilities extract more value from smart meter data [1].

(v) Current trends in security are related to providing comprehensive protection in order to address security policies, manage user access to critical resources, and the ability to detect and mitigate possible cyberattacks across the entire grid infrastructure, mainly following National Institute of Standards and Technology (NIST) and International Electrotechnical Commission (IEC) recommendations.

Beyond a specific, stakeholder-driven definition (e.g., the Smart Grids European Technology Platform), Smart Grids should refer to the entire power grid from generation, through transmission and distribution infrastructure all the way down to a wide array of electricity consumers. A well thought-out Smart Grid initiative builds on the existing infrastructure, provides a greater level of integration at the enterprise level, and has a long-term focus. It is not a onetime solution but a change in how utilities look at a set of technologies that can enable both strategic and operational processes. Smart Grid is the means to leverage benefits across applications and remove the barrier of silos of organizational thinking.

From a high-level system perspective, the Smart Grid can be considered to contain the following major components:

(i) smart sensing and metering technologies providing faster and more accurate response for the consumer (e.g., remote monitoring, time-of-use pricing, and demand-side management) [2];

(ii) integrated, standard-based, two-way communication infrastructure that provides an open architecture for real-time information and control to every end point on the grid [2];

(iii) advanced control methods monitoring critical components, enabling rapid diagnosis, and precise responses appropriate to any event [2];

(iv) a software system architecture with improved interfaces, decision support, analytics, and advanced visualization enhancing human decision making, effectively transforming grid operators and managers into knowledge workers [2].

The Smart Grid Architectural Model (SGAM) Framework [3] aims at offering a support for the design of smart grid use cases with an architectural approach allowing for a representation of interoperability viewpoints in a technology neutral manner, both for current implementation of the electrical grid and future implementations of the smart grid (c.f., Figure 1). It is a three-dimensional model that is merging the dimension of five interoperability layers (business, function, information, communication, and component) with the two dimensions of the Smart Grid Plane, that is, zones (representing the hierarchical levels of power system management: process, field, station, operation, enterprise, and market) and domains (covering the complete electrical energy conversion chain: bulk generation, transmission, distribution, distributed energy resources, and customers premises).

This work will provide a state of the art of the relevant parts of the Smart Grid, mainly focusing on substation automation in the transmission and distribution domains (c.f., semitransparent cube in Figure 1), as well as relevant protocols, applications, and regulations concerning the control center.

2. Electrical Substation Automation

This section presents the substation types and roles, the electric substation automation (SA) system components, the information flow between different levels of SA, and the SA system architecture.

2.1. Substation Types and Roles. The electrical substation is of paramount importance to the electrical generation, transmission, and distribution system. According to [2] there are four major types of electric substations.

(i) *Switchyard substation* at a generating station connects the generators to the utility grid and also provides offsite power to the plant. Generator switchyards tend to be large installations that are typically engineered and constructed by the power plant designers and are subject to planning, finance, and construction efforts different from those of routine substation projects.

(ii) *Customer substation* functions as the main source of electric power supply for one particular business customer. The technical requirements and the business case for this type of facility depend more on the customer's requirements than on utility needs.

(iii) *System substation* involves the transfer of bulk power across the network. Some of these stations provide only switching facilities (no power transformers), whereas others perform voltage conversion as well. These large stations typically serve as the end points for transmission lines originating from generator switchyards and provide the electrical power for circuits that feed transformer stations. They are integral to the long-term reliability and integrity of the electric system and enable large amounts of energy to be moved from the generators to the load centers. System stations are strategic facilities and usually very expensive to construct and maintain.

(iv) *Distribution substations* are the most common facilities in electric power systems and provide the distribution circuits that directly supply most customers. They are typically located close to the load centers, meaning that they are usually located in or near the neighborhoods that they supply, and are the stations most likely to be encountered by the customers.

A visual representation of how the electrical substations are used within the electric grid is presented in Figure 2. The substation is depicted as a grey box.

The substation roles clearly indicate that it can be considered as critical infrastructure, especially for substations in the transmission grid, interconnecting many systems. As such, it requires proper physical and cyber protection to ensure uninterrupted and smooth operation.

2.2. SA System Components. The SA system uses any number of devices integrated into a functional array for the purpose of monitoring, controlling, and configuring the substation.

The components of the SA system are as illustrated in Figure 3 where VT, CT, and PT stand for voltage, current, and power transformer, accordingly. In the following section, we describe the *remote substation* components and the *operations center* components.

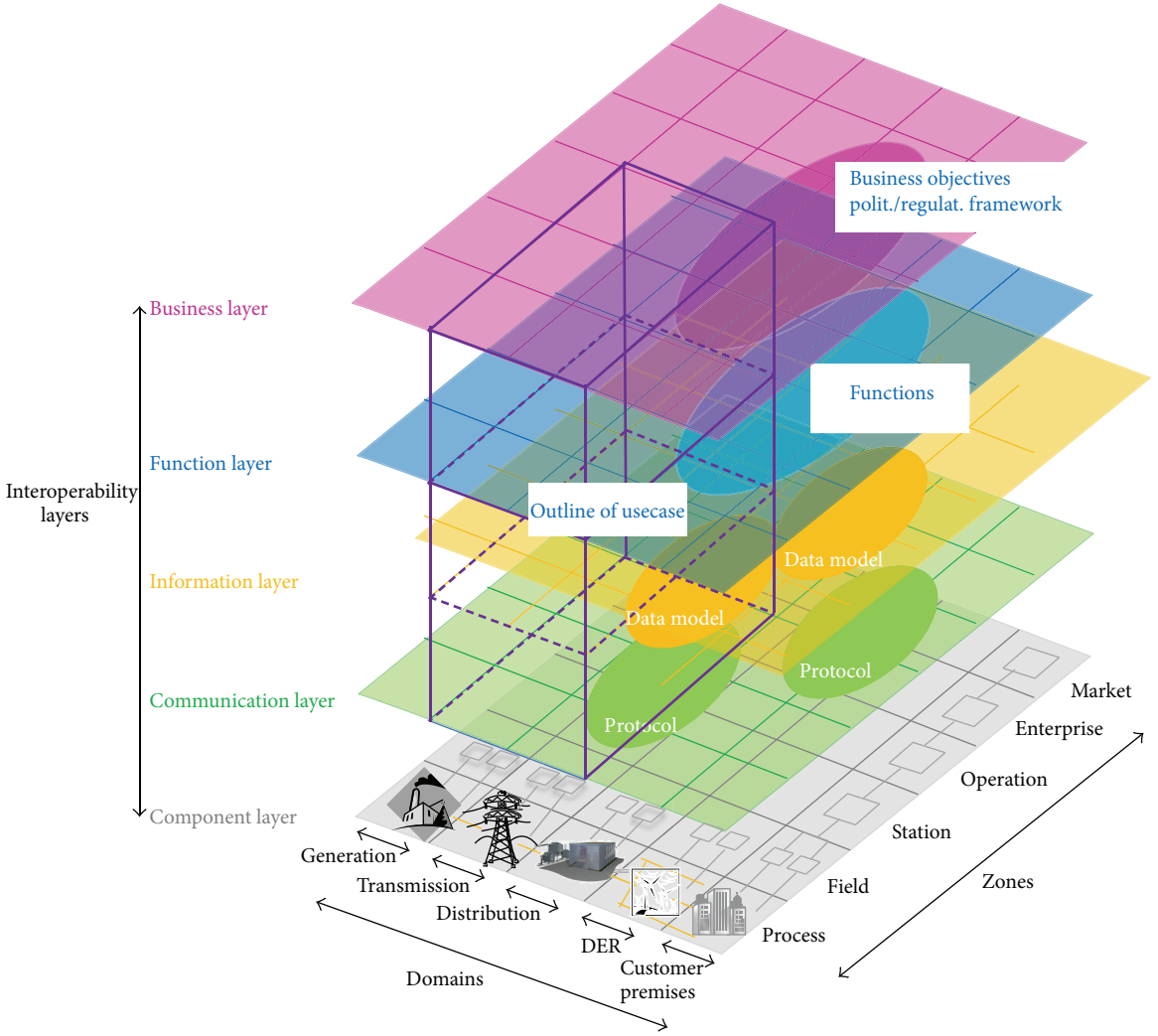

Figure 1: CEN-CENELEC-ETSI Smart Grid plane of domains and hierarchical zones [3].

2.2.1. Remote Substation Components. The SA components present in the substation are as follows.

(i) Microprocessor-based intelligent electronic devices (IEDs), which provide inputs and outputs to the system while performing some primary control or processing service. Common IEDs are protective relays, load survey and/or operator indicating meters, revenue meters, programmable logic controllers (PLCs), and power equipment controllers of various descriptions [2].

(ii) Devices dedicated to specific functions for the SA system like transducers, position sensors, and clusters of interposing relays may also be present [2].

(iii) Dedicated devices often use a controller (SA controller) or interface equipment like a conventional remote terminal unit (RTU) as a means to connect into the SA system [2].

(iv) A substation display or users station (local HMI), connected to or part of a substation host computer (local server), may also be present [2].

(v) Common communication connections to the outer world like utility operations centers, maintenance offices, and/or engineering centers. Most SA systems connect to a traditional supervisory control and data acquisition (SCADA) system master station serving the real-time needs for operating the utility network from one or more operations centers. SA systems may also incorporate a variation of SCADA remote terminal unit (RTU) for this purpose or the RTU function may appear in an SA controller or substation host computer [2].

Other utility users/services usually connect to the system through a firewalled DMZ, which is connected to the SCADA system.

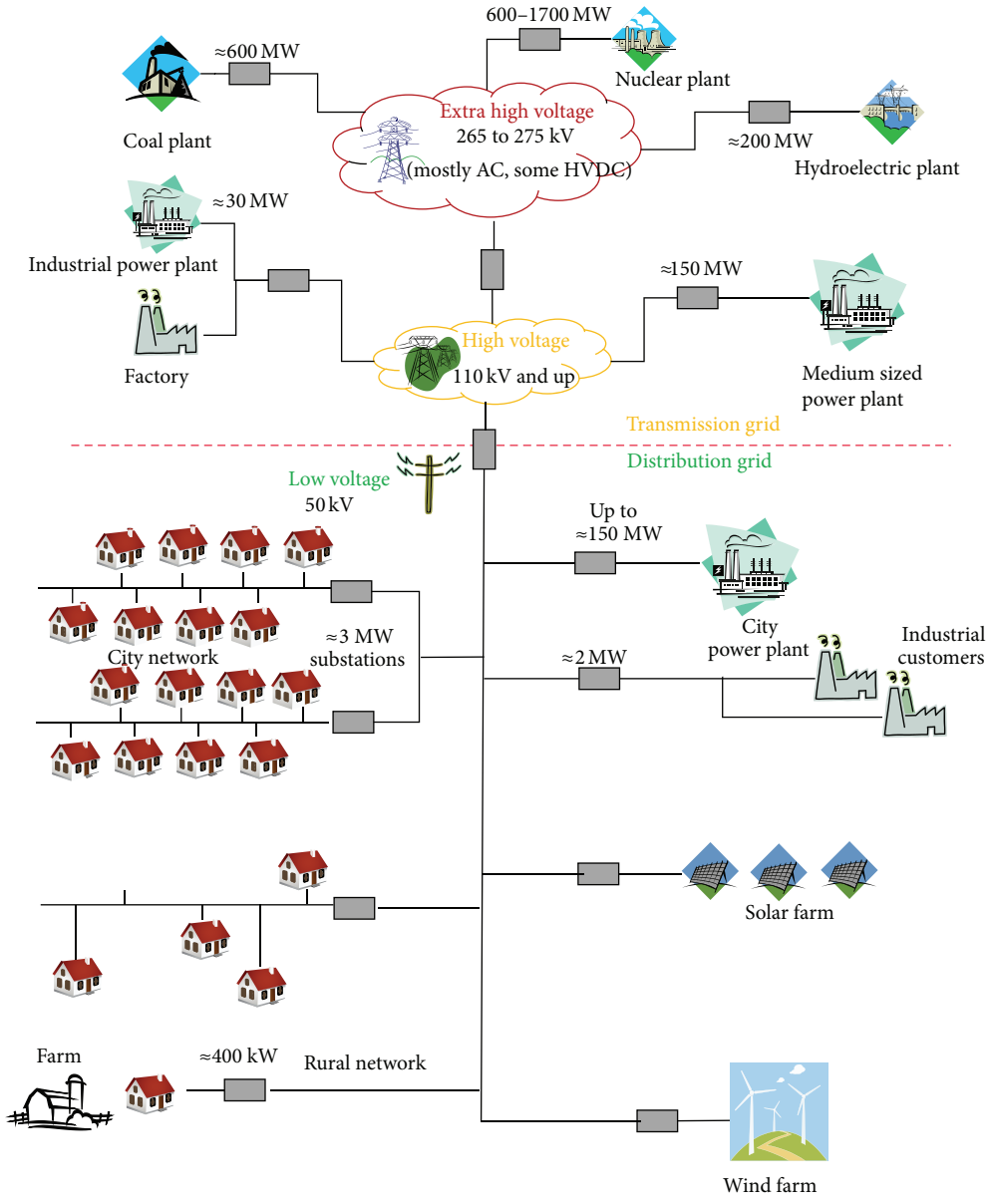

Figure 2: Substations in the electric grid [4].

2.2.2. Operations Center (SCADA Master Station) Components. In electric substation automation, the *operations center* (or *master control center* or *SCADA master station*) receives and processes data from several substations and take appropriate remote substation control actions [5]. The master station system may sometime use an open and distributed architecture. There can also be multiple master stations and accordingly different topologies can be used to interconnect them for synchronizing the grid operational data. Each master station (manned) is supported with a backup/emergency master station (unmanned) and is continuously synchronized with a primary master station database.

The main elements of the SCADA master station (or *SCADA master*) are Human Machine Interface (HMI), application servers, firewall, communication front-end (to communicate with RTU's/data concentrators), and external communication server/M2M gateway (to communicate with other control centers). These elements are networked within the SCADA master via real-time dedicated LAN. The application servers include servers that support all energy management system (EMS) or distributed management system (DMS) applications.

Redundancy is provided for the hardware and software elements of SCADA master (e.g., redundant LAN) and substations (e.g., redundant critical computer) as well as for the M2M communication network.

2.3. SA Information Flow. Substation automation can be broken down into five levels according to [6]. Starting from the bottom we have power system equipment (e.g., transformers,

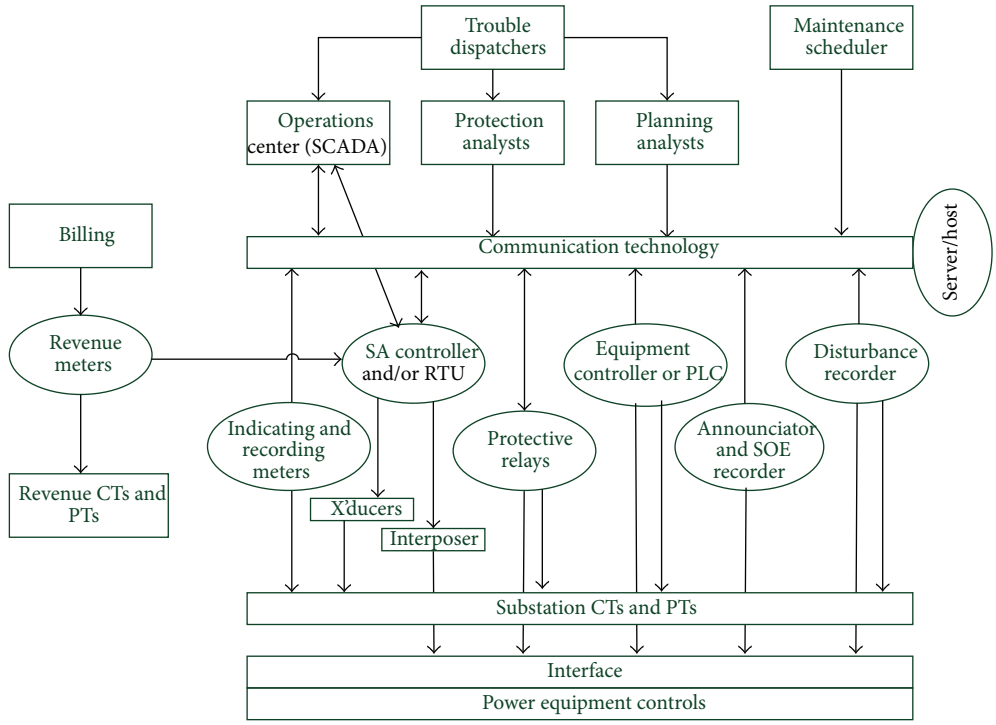

Figure 3: Power station substation automation system functional diagram [2].

circuit breakers); three middle levels: IED implementation, IED integration, and SA applications (usually they are merged as bay level); and finally at the top, the utility enterprise.

In order to interconnect these layers, three functional communication data paths exist from the substation to the utility enterprise.

(i) The *operational data* (e.g., volts, amps) path to SCADA is the most critical and utilizes one of the communication protocols supported by the SCADA system.

(ii) The *nonoperational data* path to utility's data warehouse conveys the IED nonoperational data, like event logs, from the SA to a warehouse.

(iii) Finally, the *remote access* path to IEDs utilizes a two-way network connection.

Figure 4 shows the three functional communication data paths as well as the basic components of SA system. Although it is shown for the energy management system (EMS) case, the data flow is similar for distribution management or SCADA systems.

2.4. SA System Architecture. Figure 5 shows the SA system architecture for remote monitoring, management, security, and maintenance of unmanned energy substations and related sites. As expected, it takes full advantage of the network-based architecture.

The subsystems at remote substation and operation center can be networked via M2M broadband communication network service (fixed and wireless broadband network, satellite links, and secured IP network), a platform to remotely monitor and manage devices and machines [7].

Note that the physical access control system is integrated within the same architecture, providing video surveillance, site monitoring, and access management for the substations.

3. Smart Grid Control Center Applications

The smart electric transmission and distribution grid functionalities are centrally performed at the control center by several control centers or electric utility applications that include SCADA, DMS, EMS, Automated Meter Reading (AMR), Network Integration System (NIS), and Geographic Information System (GIS).

3.1. Concept of Operations. The typical roles of persons involved with SCADA based monitoring and control operations are SCADA Manager, SCADA Information security officer, SCADA system administrator, SCADA operator, SCADA engineer/developer, field maintenance worker, and external user (via remote access). The external users are contractors, consultants, SCADA vendors (maintenance and emergency access), and Managed Security Solution Provider (MSSP). The latter usually performs the SCADA cyber security monitoring which is outsourced to them by the utility. In case of not outsourcing this task, cyber security monitoring is done by the Security Incident Manager.

The SCADA manager is responsible for ensuring that corporate policies are followed. The information security officer is responsible for ensuring that the security policy is followed and performs audits. The administrator is responsible for system activities like maintenance, expandability, and performance. The control center operator is responsible for performing operational functions like electric substation

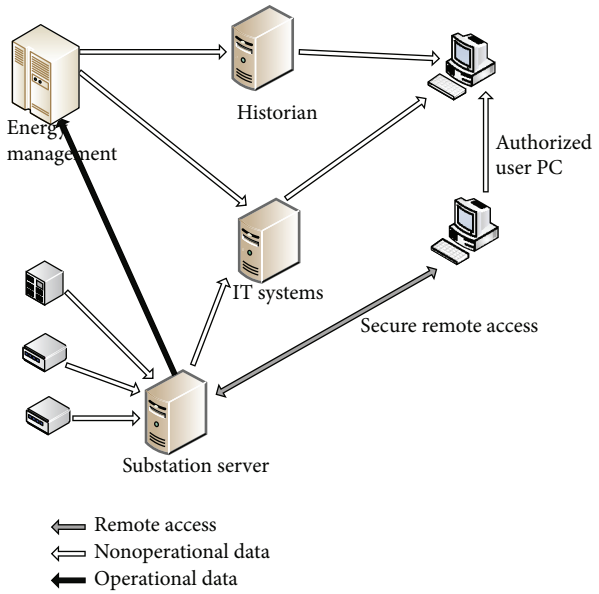

Figure 4: Substation data flow [2].

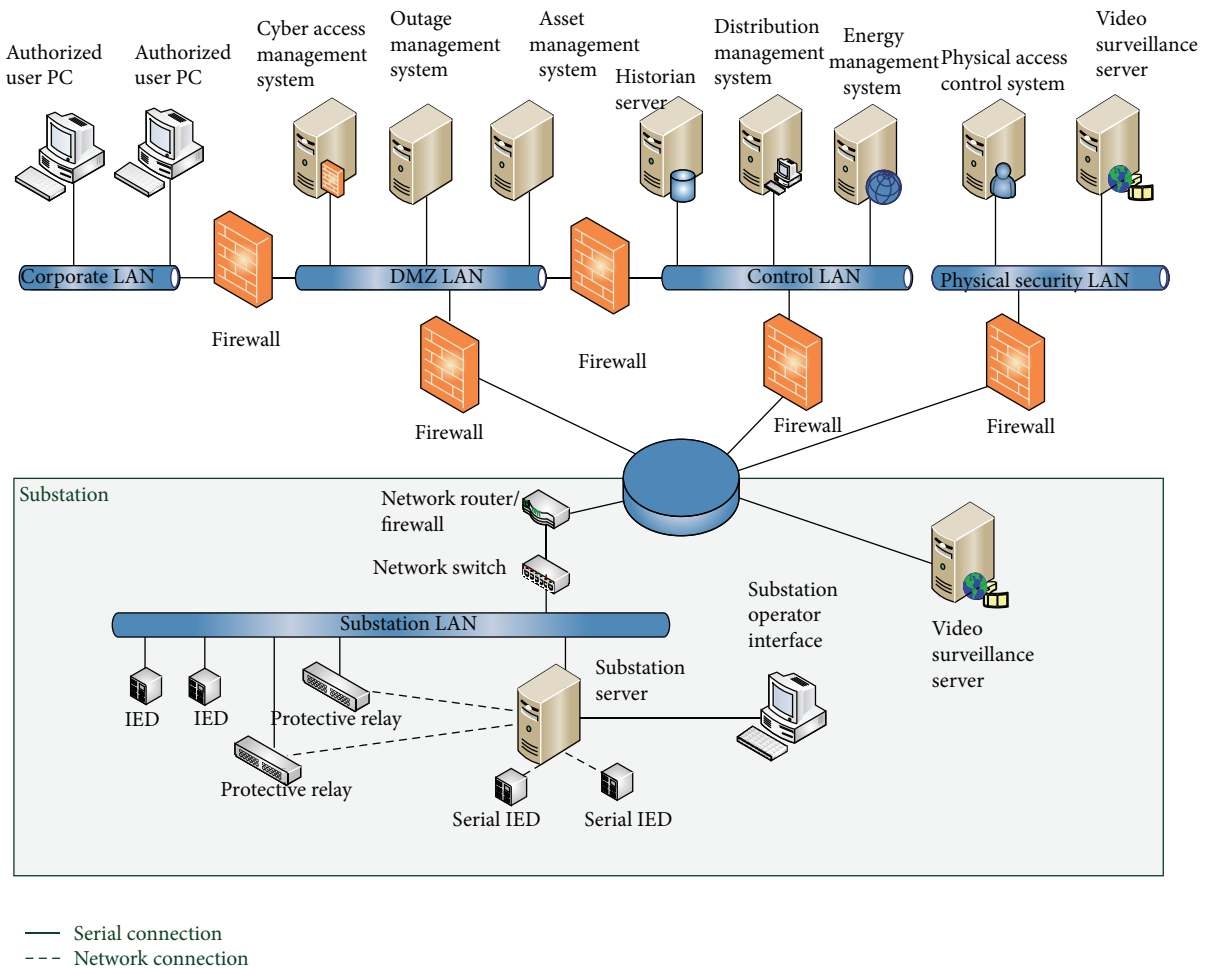

Figure 5: Smart integrated substation [2].

monitoring and control. The maintenance workers perform the field work assigned to them by the control center operator, the scheduler, or the dispatcher.

3.2. System Activities and Performance. In addition to the electric network management system activities, the SCADA also serves as a source of important operating data required for effective management of the utility's business. The SCADA system performance is based on its availability, maintenance, response time, security and expandability. The high availability of the SCADA system and the continuous operation assurance are attained by introducing reliability as well as redundancy of the hardware and software. In case of damage to the primary master station, for example, due to events like natural disasters, the back-up/emergency, master station takes over the system operation.

The system is in normal state when the load and operating constraints are satisfied. In such occasions the main system performances are met. It switches to the emergency state when the operation conditions are not completely satisfied. In the emergency state the response time might be slow and the system performance is allowed to degrade but the basic functionalities (e.g., alarm and status change operations) are retained.

The system's access level is restricted for different group of workers (Access Authorization). For example, the operators are generally provided with complete access to display and control functions for specific Areas of Responsibility (AoR), while the maintenance staff may only have access to display functions.

The system maintenance involves hardware/software repair using diagnostic tools (debugging, corrections), updates (patch management, antivirus protection), tests and preventive maintenance. It can be expanded with new points, functions and equipment depending on the functional and standardization needs. The limitations (e.g., physical space) and downtime are considered important factors during expansion.

3.3. Operational Functions. The main operational functions of the real-time SCADA system includes: data acquisition and processing, basic network monitoring, device and sequence control, network and device tagging, and alarms and events management [8].

Particularly, the DMS includes applications (tools) that perform the following functions: network topology monitoring, demand response and load management, load and generation forecasting, switching procedures, fault management, outage management, trouble call management, work management, crew management, customer information, and asset management [9]. Moreover, the Energy Management System (EMS) performs remote and local control and supervision of transmission systems.

4. Communication Layer

The communication layer in smart grids serves as the core of the entire remote monitoring system. It not only collects operational data from the field devices and sends the data to the SCADA servers, but also transmits commands from the control center to the control units in order to actuate the equipment. The emphasis of the communication layer is to describe appropriate protocols and mechanisms for the interoperable exchange of data between the components of the smart grid.

Key requirements of a fast, robust and reliable communication system include.

(i) Identification of communication traffic flows: source/destination/quantity.

(ii) System topology (e.g., star, mesh, ring, bus).

(iii) Device addressing schemes.

(iv) Communication network traffic characteristics (bandwidth, delay, latency, jitter, reliability, and error handling).

(v) Performance requirements.

(vi) Timing issues.

(vii) Reliability/backup/failover.

(viii) Operational requirements (e.g., security, and management of the network).

(ix) Quantification of electromagnetic interference withstand requirements.

Another critical requirement and recent trend in substation integration and automation architecture is the use of standard communication interfaces to ensure interoperability between different vendors' components as well as with legacy equipment. The lack of standard protocols may lead to communication errors or to incompatibility between different devices. Industries that have invested in proprietary and vendor oriented SCADA communication systems address serious scalability issues, as they are restricted to limited choice of equipment when requirements change.

To mitigate such problems, open communication protocols (e.g., IEC 60870-5-101/104 and DNP 3.0) and control-center-to-control-center communication (e.g., ICCP IEC60870-6/TASE.2) became increasingly popular among SCADA equipment manufacturers and solution providers alike (see Section 4.2).

4.1. Communication Technologies. In conventional substations, serial communication buses or proprietary protocols are used for local HMI, as well as for remote SCADA communication. Modern communication in substation is data transmission inside and between station, bay and process level. Communication between these 3 levels is called vertical communication and is conducted by high-speed Ethernet station bus and process bus. Station bus facilitates communication between station level and bay level. Communication within one level is considered horizontal. Communication networks within the substations often have lower-level data link, physical layer protocols and multiple application layer protocols running on top of TCP/IP.

Traditional SCADA systems had a master-slave communication model. Nowadays, with the availability of networkable communication protocols, such as IEC 61850, it is

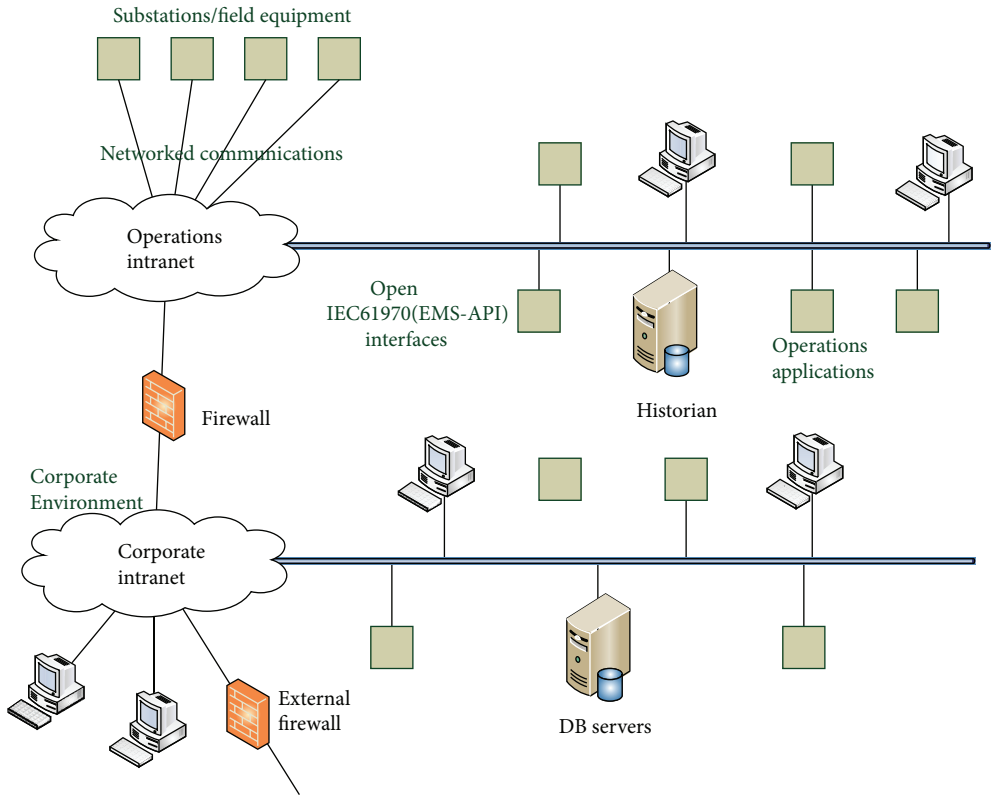

Figure 6: Networked SCADA communications [2].

possible to simultaneously support multiple clients located at different remote locations, although it complicates who has the control of the equipment. Figure 6 shows an example of such a network. These networks allow the integration of both control center and enterprise information systems.

Based on the topology of the distribution network, the appropriate technology has to be chosen among different solutions. Utility communication networks comprise both wireless and wired technologies [2]. Copper wires (e.g., low-rate or broadband DSL signals), fiber optics (e.g., Ethernet signals for broadband MANs), leased phone lines or cellular and satellite communications may be employed for the interconnection of the substation with the control center or between the components of the substation. New development trend is the spread spectrum radio technologies which can operate in unlicensed ISM bands in the 900 MHz, 2.4 GHz, and 5.6 GHz bands or licensed in other nearby bands.

Criteria for the selection of the most appropriate technology are bandwidth and delay requirements for the communication link, and whether a global or a regional solution is targeted or not. Additionally, wireless and satellite systems are subject to eavesdropping, so the use of appropriate security measures is indicated to avoid loss of confidential information.

SCADA communication networks tend to come in line with standard networking technologies in future. Ethernet and TCP/IP based protocols are replacing the older proprietary standards. Migration strategies that are available today have to be identified, in order to move from legacy technology to the standard protocols. It is unlikely that one technology alone will ever provide a complete solution for all communications, thus interoperability and compatibility of different technologies will be the key requirement for all future generations of systems.

4.2. Communication Protocols. One recent effort on communication interfaces of a control center is the OPC protocol [10]. In general, it enables the overall data exchange between automation and control applications, field systems/devices as well as business and office applications. It was developed by the automation industry to standardize the communication of real-time plant data between control devices from different manufacturers. Specifically, OPC is a set of industrial standards for systems interconnectivity, providing a common interface for communications between multi-vendor software applications that is applicable in a wide range of industries spanning from process industries to substation automation and many others. More recently, the OPC UA protocol [11] was introduced in order to support the interoperability and the platform independence.

Communication between control centers is provided via the Inter Control Center Communication Protocol (ICCP) or ELCOM [12], and is based on TCP/IP. The ICCP is an open and standardized protocol based on IEC 60870-6 and Telecontrol Application Service Element Two (TASE.2). The exchanged data is primarily real-time system information like analog values, digital values and accumulator values, along with supervisory control commands [13]. The data transfer

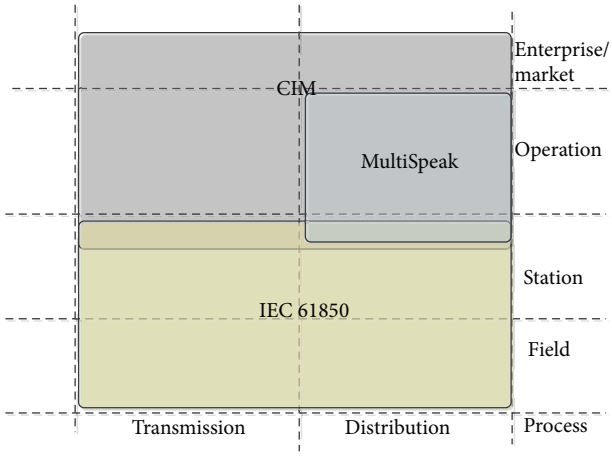

Figure 7: Information model domains.

can take place in both directions between two control centers. Both control centers can initiate interactions/data transfers. The protocol supports spontaneous data transfer, periodic data transfer, and data transfer on request.

For the communication within the substation the IEC 61850 [14] developed by WG 10 [15] is broadly used. It is a standard for electric utility automation, defining communication between IEDs within a substation. It is developed within IEC TC 57 [16] and is composed of 10 parts. It provides communication protocols, data models, security standards, and so forth. Although the scope of IEC 61850 was originally focused on substation automation and the corresponding communication, discussions are underway to look at defining IEC 61850 for the Substation to Master communication protocol. In addition, applications are available using various components of IEC 61850 for wide area substation-to-substation communication.

The DNP3 [17] is a serial communication protocol and specifies the data link layer, the application layer and a transport pseudo-layer. It is used primarily in electric utilities in North America, and offers similar features as IEC 60870-5-104 [18] which is more popular in Europe. Its scope is to enable interoperability among compatible telecontrol equipment.

Modbus [19] is another serial communication protocol which is commonly available for interconnecting electronic devices. Modbus is very well known, easy to implement and widely used in all industries. Nevertheless, as most serial protocols Modbus offers no security and no standard way to provide information about the data it transports.

5. Information Layer

In this Section we present different information models for the power industry, each of them covering specific domains and levels of the SGAM [3]. Figure 7 shows how they fit into our scope.

Note that CIM and IEC-61850 cover further domains such as generation and Distributed Energy Resources (DER) which are out of scope of the paper at hand.

5.1. CIM. The Common Information Model (CIM) enables software applications to exchange configuration and status information of an electric network. It comprises of three standards that are all developed within the IEC Technical Committee 57 (TC 57) [16]: IEC 61970 [20] (transmission) developed by WG 13 [21], IEC 61968 [22] (distribution) developed by WG 14 [23], and IEC 62325 [24] (market) developed by WG 16 [25].

CIM is described using Unified Modeling Language (UML) and is organized in packages, each containing a set of classes along with their inheritance structure, their attributes, and their associations. IEC 69170 further specifies a mapping from UML to Resource Description Framework (RDF), as well as how messages should be serialized in XML (CIM XML).

CIM supports profiles which apply for specific applications only. Profiles are subsets of usually a few dozen classes of the more than 700 CIM classes. IEC 61970 defines a few profiles such as "Schematic Layout Profile" or "Topology Profile".

Currently, CIM is mainly used by EMS applications in order to exchange information about the current transmission states. However, the potential of CIM is much higher as it can be used to describe and exchange data about almost anything related to power systems and its management, including workforce and energy markets.

5.2. MultiSpeak. MultiSpeak [26] defines standardized interfaces among electric utility software applications for distribution only. It offers definitions in the following areas: common data semantics, message structure, and messages required for specific business process steps.

MultiSpeak supports two communication transfer options: file based (batch processing) and web services (real-time data). Further, it offers three different communication modes: batch, request/response, and publish/subscribe.

Currently, MultiSpeak is the most widely applied de facto standard in North America pertaining to distribution utilities. Nearly 70 vendors are using the specification in their products and more than 600 electric cooperatives (from 15

different countries) use MultiSpeak supported products in their daily operations [27].

5.3. IEC 61850. As described before, IEC 61850 provides both an abstract data model and an abstract communication interface. The standard consists of 10 parts. The ones regarding the information layer are

(i) part 61850-6 [28] which defines an XML language called Substation Configuration Language (SCL) and four file formats for describing the configuration of substation equipment and IEDs configurations;

(ii) part 61850-7 [29] which defines the basic communication structure and has multiple parts itself and specifically: IEC 61850-7-2 [30] defines the communication services, which permit to query or send commands to the devices; IEC 61850-7-3 [31] and IEC 61850-7-4 [32] define the object model that describes the equipment of the substation.

All big vendors of power automation technologies and many smaller ones support or even favorite IEC 61850. Within the context of many smart grid projects in North America, Europe, or Asia IEC 61850 is seen as the most important standard.

5.4. Harmonization. There exist semiautomated approaches to create converters between CIM and IEC 61850 models such as in [33].

A direct translation between CIM and MultiSpeak can be achieved using style sheets and readily available tools [34].

IEC TC 57 WG 19 [35] is working [36] on harmonizing CIM and SCL. IEC TC 57 WG 14 [23] is working [37] on harmonizing CIM and MultiSpeak.

In the context of their smart grid interoperability efforts [38] NIST is working [39] on integrating IEC 61850, IEC 61968, and MultiSpeak.

5.5. Comparison. Table 1 shows a comparison of functionalities: market and domain for the presented information models.

6. Security and Regulations

Security in Smart Grids is a crucial factor because disruptions in these systems can lead not only to the destruction of expensive equipment but also interruption of critical operations that can include significant risk to the health and safety of human lives, serious damage to the environment, and financial issues such as production losses and negative impact to a nation's economy.

In a report entitled "Electric Power Risk Assessment" [40], the National Security Telecommunications Advisory Committee (NSTAC) concluded that power substations were "the most significant information security vulnerability in the power grid" mainly because the remotely accessible devices used within substations are largely unprotected against intrusions.

Various regulatory mandates exist or are emerging that requires energy utilities to secure, monitor, and manage their critical sites and data networks in accordance with regulatory requirements and standards. These differ in granularity and scope, ranking from process oriented to technical standards [41–45].

Figure 8 gives an exemplary overview of potential targets for cyber-attacks (indicated by yellow exclamation marks) on the communication infrastructure of SCADA systems. The main problem in most of the existing systems derives from the fact that SCADA systems were not designed to be connected to the outside network infrastructure and consequently security aspects were not considered during the development phase.

The vulnerabilities affecting the SCADA system regard mainly the following components [46].

(i) IEDs and RTUs in the substations;

(ii) Substation LAN and firewall;

(iii) Communication network between substation and control center;

(iv) SCADA LAN and firewall;

(v) Corporate (office) LAN and firewall;

(vi) Computers of vendors that can access the SCADA network for maintenance.

Specifically, concerning IEDs, the security risk is caused by the lack of cryptographic capability because the overhead induced by the extra payload and processing would cause unacceptable delays in time-sensitive applications, especially due to the fact that the microprocessors used in IEDs have little processing capabilities. More recently, IEDs that implement protocols such as IEC 61850 are however able to validate the authenticity of messages.

The messages that IEDs exchange with the outside world are often transmitted over communication channels that are potentially open to eavesdropping or active intrusions. Moreover, the communication protocols most frequently used in substations are well known (Modbus, Modbus-Plus, DNP3, etc.) but security was not an issue when these protocols were designed, and they contain no features to ensure the confidentiality or authenticity of the data transmitted. Hence control messages can be easily spoofed or replayed.

A large potential threat to these systems is derived from unauthorized users on the corporate network or any network that has connection with the SA. Consequently, the first step in securing substation assets should be to ensure that the corporate network is made as secure as possible and has sufficient points of control and isolation from the SA system network using appropriate firewall rules and other known cyber-security measures [1]. Moreover, if wireless technology is deployed at the substation, it can create a new attack vector if no proper security measure such as access control and encryption are in place.

The physical protection of the cyber components and data associated must be addressed as part of the overall security. Having physical access to a control room or control system components often implies gaining logical access to the process control system as well (e.g., through network or USB ports).

Table 1: Information model comparison.

	CIM	MultiSpeak	IEC 61850
Utility domain and interoperability	Transmission, generation, and distribution	Distribution	Substation automation
Markets focus	International utilities	Electric cooperatives in USA	International utilities
Communication/data transfer	Transport independent	SOAP messages using HTTP, TCP/IP	MMS, TCP/IP
Definitions	XML	XML	XML

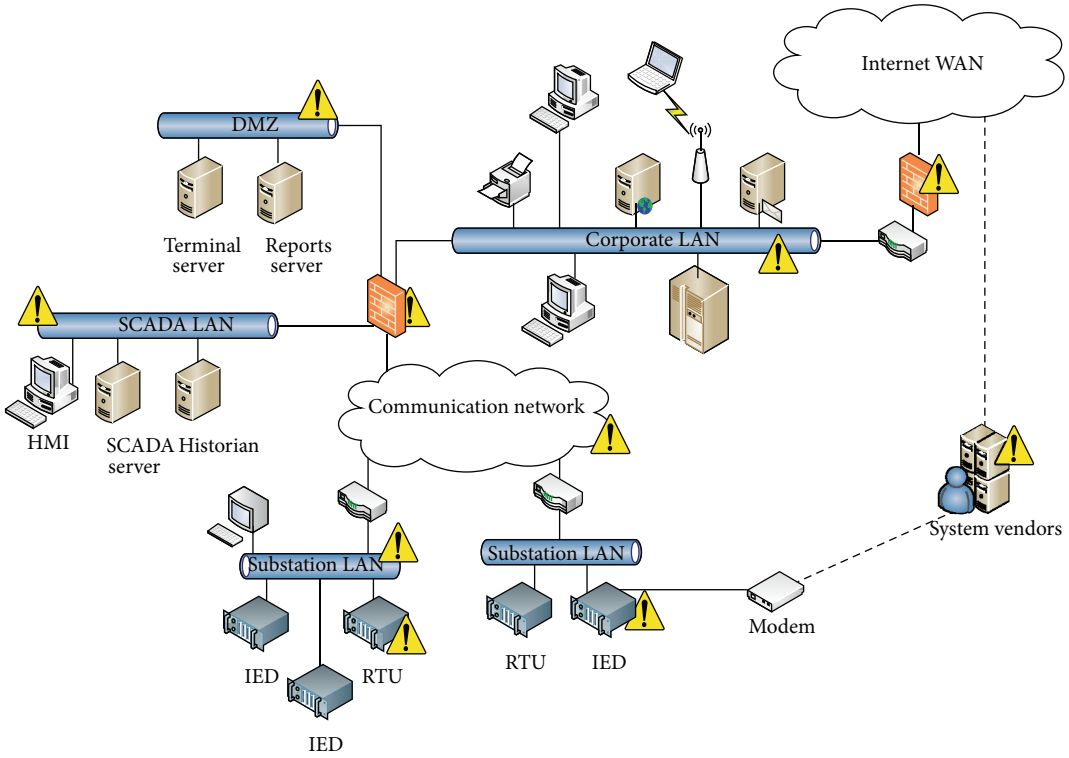

Figure 8: SCADA system vulnerabilities.

IEEE Standard 1402-2000 [43] identifies and classifies the types of "intrusions" into a substation and discusses some security methods to be adopted for mitigating risks.

Also NERC in "Security Guidelines for the Electricity Sector" [44] has developed a comprehensive set of guidelines addressing general approaches, considerations, practices, and planning methods to be applied in protecting the electric infrastructure systems.

Other physical security measures coupled with electronic controls are discussed in NERC-CIP-006 [45].

7. Conclusions

Industrial Control Systems (ICS) have passed through a significant transformation from proprietary, isolated systems with dozens of different vendor specific standards towards open architectures and standard technologies highly interconnected with other applications and systems over corporate networks, as well as wide area networks, or the Internet. This paper focused on the ICS of the electrical sector and particularly on the Smart Grid and provided the necessary background information on SCADA and utility applications that run typically at the control center of transmission or distribution grid operators. This sector has been particularly active at establishing new standards to improve interoperability between all sector players and will continue developing towards the Smart Grid which is needed for an efficient integration of distributed energy generation technologies.

Moreover, a state-of-the-art analysis of the communication and information standards and technologies in transmission and distribution has been presented, ranging from the field devices in electrical substations to the control center. Throughout the state-of-the-art analysis, it can be concluded that there is tremendous effort from the Smart Grid key stakeholders to improve interoperability across the different components managing an electrical grid, from field processes to market exchanges. The information can now flow more and more freely across applications and domains, and there is an opportunity for new applications that are not any more constraint to a single domain.

ICS are very heterogeneous in protocols, applications, and network topologies they use. Therefore the selection of the

communication protocol or technology should be thoroughly investigated. Based on how widespread the adoption of a protocol is, as well as the support of the interoperability, it is observed that approaches like OPC UA as the communication protocol and CIM as the information model show promising results and are more and more adopted by industry.

The observed developments in the Smart Grid domain raise several security aspects which were briefly discussed and most probably will gain more importance in the future.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors thank A.-K. Chandra-Sekaran, R. Gold, A. Hessler, G. Mazarakis, and K. Sasloglou for their valuable contribution to this work.

References

[1] Pike Research, *Smart Grid: Ten Trends to Watch in 2012 and Beyond*, 2012.

[2] J. D. McDonald, *Electric Power Substations Engineering*, CRC Press, Boca Raton, Fla, USA, 2012.

[3] CEN-CENELEC-ETSI Smart Grid Coordination Group, *Smart Grid Reference Architecture*, ETSI, 2012.

[4] "Electric Power Distribution," Wikipedia, http://en.wikipedia.org/wiki/Electric_power_distribution.

[5] IEEE, IEEE standard for SCADA and automation systems C37.1-2007, 2008.

[6] J. D. McDonald, "Substation Automation Basics—The Next Generation," Electric Energy T&D Magazine, 2007.

[7] T. Ihonen, "LNI Verkko- Smart Grids in Practice," Presentation.

[8] ABB, "ABB Network Manager SCADA/DMS," Application Brochure.

[9] SMB Smart Grid Strategic Group (SG3), "IEC Smart Grid Standardization Roadmap," 2010, http://www.iec.ch/smartgrid/downloads/sg3_roadmap.pdf.

[10] OPC Foundation, "OPC—The Interoperability Standard for Industrial Automation & Other Related Domains," 2013, http://www.opcfoundation.org/Default.aspx.

[11] S. Lehnhoff, S. Rohjans, M. Uslar, and W. Mahnke, "OPC unified architecture: A service-oriented architecture for smart grids," in *Proceedings of the 1st International Workshop on Software Engineering Challenges for the Smart Grid (SE-SmartGrids '12)*, pp. 1–7, IEEE, June 2012.

[12] J. Hegge and A. Larsen, "The ELCOM utility communication concept," *IEEE Transactions on Power Systems*, vol. 6, no. 4, pp. 1411–1417, 1991.

[13] Siemens, "Power Engi neering Guide Edition 7.0—Communication Network Solutions for Smart Grids".

[14] IEC, "Power Utility Automation," IEC 61850.

[15] IEC, "WG10 Power system IED communication and associated data model," http://www.iec.ch/dyn/www/f?p=103:14:0::::FSP_ORG_ID,FSP_LANG_ID:2400,25. [22 Jan 2014].

[16] IEC, *Technical Committee 57*, 2014, http://tc57.iec.ch/index-tc57.html.

[17] ABB, "650 Series DNP3 Communication Protocol," Manual, 2011.

[18] ABB, "IEC 60870-5-101/104 Communication Protocol," Manual, 2011.

[19] Modicon, *Modbus Protocol Reference Guide*, 1996.

[20] IEC, "Common Information Model (CIM)/Energy Management," IEC 61970.

[21] IEC, "WG 13 Energy management system application program interface (EMS-API)," 2014, http://www.iec.ch/dyn/www/f?p=103:14:0::::FSP_ORG_ID,FSP_LANG_ID:2392,25.

[22] IEC, "Common Information Model (CIM)/Distribution Management," IEC 61968.

[23] IEC, "WG14 System interfaces for distribution management (SIDM)," http://www.iec.ch/dyn/www/f?p=103:14:0::::FSP_ORG_ID,FSP_LANG_ID:2393,25.

[24] IEC, "Standards related to energy market models & communications," IEC 62325.

[25] IEC, "WG16 Deregulated energy market communications," http://www.iec.ch/dyn/www/f?p=103:14:0::::FSP_ORG_ID,FSP_LANG_ID:2388,25.

[26] NRECA, *The MultiSpeak Specification*, 2014, http://www.multispeak.org/about/Specification/.

[27] NRECA, "MultiSpeak," 2014, http://www.multispeak.org/Pages/default.aspx.

[28] IEC, "Configuration language for communication in electrical substations related to IEDs," IEC 61850-6.

[29] IEC, "Basic communication structure for substation and feeder equipment," IEC 61850-7.

[30] IEC, *Abstract Communication Service Interface (ACSI)*, IEC 61850-7-2, 2010.

[31] IEC, "Common Data Classes," IEC 61850-7-3.

[32] IEC, "Compatible logical node classes and data classes," IEC 61850-7-4.

[33] T. Kostic, O. Preiss, and C. Frei, "Towards the formal integration of two upcoming standards: IEC 61970 and IEC 61850," in *Proceedings of the Large Engineering Systems Conference on Power Engineering (LESCOPE '03)*, pp. 24–29, May 2003.

[34] R.-M. Keski-Keturi, *Implementing the IEC common information model for distribution system operators [M.S. thesis]*, Tampere, Finland, Tampere University, 2011.

[35] IEC, "WG 19 Interoperability within TC 57 in the long term," http://www.iec.ch/dyn/www/f?p=103:14:0::::FSP_ORG_ID,FSP_LANG_ID:2402,25.

[36] EPRI, "Harmonizing the international electrotechnical commission Common Information Model (CIM) and 61850," EPRI 1020098, 2010.

[37] IEC, "Application integration at electric utilities—system interfaces for distribution management—Part 14: multiSpeak—CIM harmonization," IEC 61968-14 .

[38] NIST, *Framework and Roadmap for Smart Grid Interoperability Standards*, Special Publication 1108, 2010.

[39] NIST, "PAP08: CIM/61850 for Distribution Grid Management," http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP08DistrObjMultispeak#Other_CIM_61850_MultiSpeak_Event.

[40] P. Oman, E. O. Schweitzer, and D. Frincke, "Concerns about intrusions into remotely accessible substation controllers and SCADA systems," Tech. Rep., Schweitzer Engineering Laboratories, 2000.

[41] NIST, "Guide to Industrial Control Systems (ICS) Security—Special Publication 800-82," 2011.

[42] NIST, *NISTIR 7628—Guidelines for Smart Grid Cyber Security*, vol. 1 of *Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*, 2010.

[43] IEEE, "IEEE 1402-2000," http://standards.ieee.org/findstds/standard/1402-2000.html.

[44] NERC, "Security Guidelines for the Electricity Sector," http://www.nerc.com/docs/cip/sgwg/Physical_Security_Guideline_2012_01_05_V1_9_45_day_review.pdf.

[45] NERC, "CIP," http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[46] VIKING Consortium, "REPORT D2.3 SCADA system architectures," VIKING Consortium, 2010.