P07

Information Security in Electric Power Utilities' Environment

Dr RADOSLAV RAKOVIĆ, Dr JASMINA MANDIĆ LUKIĆ, NINA ČUKIĆ
Energoprojekt Entel p.l.c. Belgrade
Republic of Serbia

SUMMARY

The last two decades are characterized by rapid development of information and communication technologies and connection of many devices into computer networks. Advantages of this development in everyday activities of people are significant, but they are followed by problem of information security. The fact that emerging information and communication technologies are widely applied in Electric Power Utility (EPU) networks as corporate ones, requires serious consideration of information security aspects in such an environment. It is clear that any form of threat to basic properties of information transmitted and/or stored within these systems – availability, integrity and confidentiality - could have unforeseeable consequences on system, equipment or people safety. Systematic approach to information security problem resolving asks for application of certain group of standards, both those that establish global framework to this topic (Information Security Management System –ISMS, as per standard ISO 27001) and standards that express specifics of systems in which they are applied, issued by other institutions, which are more or less related to electric power systems – CIGRÉ, IEC, NIST, NERC etc. In this paper, a short review of relevant standards, with particular emphasis put to information security aspects in SCADA systems and intelligent networks (referred to as „Smart Grid") because of the fact that nowadays these industrial control systems are widely aplied in EPU. The topic is illustrated with a practical example of information security solution for a HV SCADA project.

KEYWORDS

Electric Power Utility (EPU), Information security, SCADA, Smart Grid

rrakovic@ep-entel.com

1. INTRODUCTION

The last two decades are characterized by rapid development of information and communication technologies and connection of many devices into computer networks. Main trends are distributed instead of centralized information processing, mobility, wireless technologies, lower prices of computer equipment etc. Advantages of this development in everyday activities of people are significant, but they have also been followed by problem of information security. The fact that emerging information and communication technologies are widely applied in Electric Power Utility (EPU) networks as corporate ones requires serious consideration of information security aspects in such an environment. It is clear that any form of endanger of basic propreties of information transmitted and/or stored within these systems – availability, integrity and confidentiality - could have unforeseeable consequences for system, equipment or people safety.

Information systems applied within EPUs could be classified on different ways ([1],[2]), but classification to three groups is prevailing: *Real-Time Systems* (usually called *Industrial Control Systems* – ICS, in which response time is more critical and large delays could not be tolerated), *administrative-operational systems* (that perform information processing and enable decision making) and *administrative systems* that enable voice and data transmission within EPU, especially because of wide geographic territory. Nowdays, the EPU systems are more vulnerable for several reasons [3]:

- Control systems are not isolated any more, but connected into corporate networks and Internet providing remote access from different sites, as well as devices. Taking into account increase of level of integration and intelligence in networks with development of the „Smart grid" concept [2], the problem becomes even more critical;
- Control systems are operating predominantly on open and widely used platforms (such as Ethernet, TCP/IP, web) and are vulnerable to attack tools which are constantly being developed;
- Many logical components within these systems (electromechanical relays etc) are substituted by microprocessor controlled components with embedded software. These controllers are multipurpose and programmable, and more exposed to external impacts;
- Number of people who could access these systems is becoming more widespread because computer litreracy;
- Size and functionality of the EPU systems is growing up;
- Wireless technologies are being more and more applied.

All these reasons lead to systematic approach to information security problem resolving by applying certain group of standards, both those that establish global framework to this topic and standards that express specifics of systems in which they are applied, issued by other institutions, more or less related to electric power systems [4]. In this paper, particular emphasize has been made to information security aspects in High Voltage (HV) SCADA systems and intelligent networks (referred to as „Smart Grid") because of the fact that this type of ICS nowadays is widely applied. The topic is illustrated with the practical example of information security solution for the HV SCADA project.

2. RELEVANT INFORMATION SECURITY STANDARDS

2.1 ISO 27001

Standard ISO 27001:2013 [5] represents general framework for information security management systems (ISMS). It is based on business risks to which a company is exposed if information important for its activities is available to malicious persons or organizations. Main task in establishing ISMS is to preserve "CIA" information properties - *Confidentiality* (information is not available to unauthorized persons, organizations or processes), *Integrity* (accuracy and completeness of information) and *Availability* (information is available when necessary).

Information assets is exposed to threats that could cause negative consequences, depending on its vulnerability. Combination of likelihood of undesired events and its consequences represents risk for information security. Standard [5] asks for risk assessment and risk treatment (avoiding, transfer, mitigate), to eliminate it or to decrease it up to acceptable level. This standard is related to risk management standard ISO 31000 [6], and requires preparation of *Statement of Applicability* (SoA) that describes way of implementation of information security control from Annex A of the ISO 27001:2013[5]. This Annex consists of 14 areas of security, with 35 control objectives and total 114 controls. The areas of security are related to both technical and organizational actions.

2.2. Recommentdations of CIGRÉ

General approach of International Council on Large Electric Systems (CIGRÉ) and its study committees is to support choice of standard that will be applied based on analysis of possible approaches, not to impose any of them. Several technical brochures are issued based on this approach.

The CIGRÉ brochure TB317 [1] diccusses several elements related to information security in EPU environment. First, except physical intrusion, emphasis is put on logical ones, usually manifested as Denial of Service (DoS). Then, the methodology for Electric Power Cyber Security Assessment (EPCSA) is defined, based on concepts of assets, vulnerability, threats and intrusions. Finally, the „CIA“ concept is tranformed into the „AIC“, because availability is more important in EPUs in comparison with integrity and confidentiality, as information properties.

The CIGRÉ brochure TB 419 [7] considers domain concept from the perspective of information security EPU system model. Basic components of EPU – generation, transmission, distribution and market – are connected with domains which are critical in terms of operations, business activities, corporate level as well as „untrusted“ participants i.e. the third party (suppliers, Internet etc). This brochure defines hierarchical risk assessment model in which lower level reports back up to higher one, and higher level set risk acceptability criteria causing some risk treatment actions and defining security controls per particular domains and applied technology.

The CIGRÉ brochure TB603 [8] provides guidance for application of information security measures for Protection & Control (P&C). It is related to four important segments of EPUs – substation automation, substation-to-substation, substation-to-control centers and remote engineering. Systematization of cyber-attacks per categories was made (blocking, imitation & modification, information gathering and privacy), per type of attacks, possible consequences as well as countermeasures to be taken. Appendices present some „real-world“ examples of impacts of cyber attacks to electic power networks.

Treatment of substation automation connects CIGRÉ brochure TB603 with standards IEC 61850 [9] and IEC 62351-6 [10]. Standard IEC 61850 increase functionality and defines precise interoperability rules among functions and equipment used for protection and control within substation, independently of manufacturers. It is based on Generic Object-Oriented Substation Events (GOOSE) concept. To enable implementation of data and communication security as per this or other standard protocols, the standard IEC 62351-6 has been established that includes security measures such as verification of data transmission digital signatures as form of authentication, prevention methods from eavesdrop attacks or false identity as well as intrusion detection.

2.3 NIST standards

The National Institute of Standards and Technology represents non-regulatory agency within USA Ministry of Commerce. Among large number of standards, particular attention relevant to the topics of this paper should be paid to the standard NIST SP-800-82 [11] related to industrial control systems - ICSs (SCADA, DCS, PLC, ...). This standard covers review of ICS systems, risk management with emphasis to risk assessment, development of security programs, security architecture as well as application of security controls within ICS systems.

Particular publication NISTIR 7628 is related to security in Smart Grid environment [12]. As per NIST concept, within Smart Grid architecture seven logical domain are recognized (see Figure 1 [13]). The first three of them – providers, operations and markets – are related to information collection and energy management, others four – generation, transmission, distribution and consumption – provide two-way flow of energy and information. The network is hybrid and hierachical, backbone structure is predominantly based on fibre optic cables providing connection of domains (using routers) and LANs (over gateways), and LANs provide communication within a domain with gauges, sensors, Intelligent Electronic Devices (IEDs) using wire and wireless communication (WiFi, ZigBee, etc).

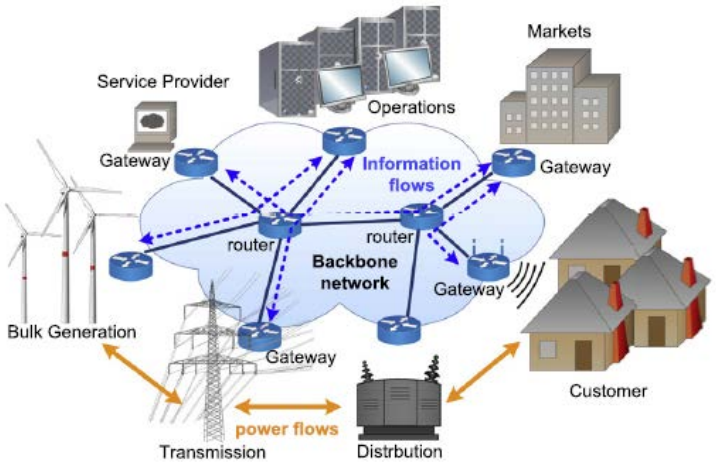

Figure 1: Basic architecture of Smart Grid [12]

2.4 Other standards and recommendations

The North American Electric Reliability Corporation (NERC) deals with reliability of electric power systems in North America (USA, Canada, Mexico), particularly on the level of interconnection, and analyzes all disturbances in network to prevent any problems in the future. Particular attention is paid to systems with „non-continual" generation – Bulk Electric System (BES), such as generation from renewable sources (wind, photovoltaic etc). This standard [14] consists of ten parts - Critical Infrastructure Protection (CIP) 002 to 011 - related to critical assets identification, security controls, personnel and training, electronic security perimeters, physical security, systems security, incident reporting and response planning, recovery plans, configuration management and vulnerability assessment and information protection. These elements are very similar to ISO 27001, Annex A [5] .

The USA Department of Energy (DoE) has developed particular maturity model for information security within energy sector [15]. Model consists of 10 domains – risk management, asset, change and configuration management, identity and access management, threat and vulnerability management, situational awareness, information sharing and communictaions, event and incident response and continuity of operations, supply chain and external dependencies management, workforce management and cyber security program management. Model defines four Maturity Indicator Levels MIL0 to MIL3 applied independently to each domain. Particular document deals with information security risk management [16], with particular segment (Tier 3) devoted to IT and ICS systems. Security problems in SCADA systems are discussed in [17] that defines 21 steps to improve cyber security of SCADA systems. Security of Smart Grid systems is subject of particular study [18].

The European Network and Information Security Agency (ENISA) has issued recommendations for Smart Grid security [19]. Findings of the study are presented in 12 areas, and 10 recommendations for improvement are given. These recommendations are related to need for establishing of referent Smart Grid architecture, approach to security „end to end", taking into account security from the very beginning of design process, developing specific methodology of risk assessment, capability of network to recover after incidents, education of people, etc.

3. INFORMATION SECURITY ASPECTS IN EPU

As mentioned in introduction, information systems applied within EPUs could be classified into three groups ([1],[2]):

- *Real-Time Systems*, with critical time response and low tolerance to delays. Usually, these systems are called „Industrial Control Systems“ (ICS). This group encompasses protection signal transmission, SCADA (Supevisory Control and Data Acquisition) systems, Energy Management Systems (EnMS), Distributed Control Systems (DCS), Programmable Logic Controllers (PLC) etc
- *Administrative-operational systems*, for information processing and decision making. They include applications in which response is not time critical, but high efficiency in data processing is required, since large quantity of data are to be processed (event registers, fault location, video surveillance in substations, assets management etc)
- *Administrative system*s, such as some of ICT services, that enable voice and data transmission within EPU, accross wide geographic territory.

According to the literature [20], there are three rough categories of documented attacks to SCADA, other ICS systems or critical infrastructure:

- *Intentional targeted attacks*, to gain unauthorized access, *Denial of Service* (DoS) or false identity etc. This type of attack usually is performed by hackers or former disgruntled employees to cause material damage or problems to population or system users. It is usually consequence of some weaknesses of the security system (inadequate password control, etc)
- *Unintentional consequences or collateral damage* from worms, viruses or control system failures caused from outside. Effects of these attacks are lower speed of computer work, computer failures, frequent restart of computer, denial of access, „*back door”* approach to computer, disturbance in nuclear plant work, switching off electricity or gas supply etc.
- *Unintentional consequences caused by internal mechanisms or human mistakes*. Effects are similar as in case of external impacts.

4. CASE STUDY: HV SCADA

Application of information security approach is illustrated on example of High Voltage (HV) SCADA system [21]. In this particular case, scope of Terms of Reference was to establish Substation Control Systems (SCSs) in 13 substations for the purposes of local monitoring and control. It was planned to collect all data to SCADA servers in central location to enable remote control of switches (switching on and off). Control of local processes is planned to be done from local SCSs. Communication within substations is based on IEC 61850 standard [9] that assumes several network levels, hierachicaly organized (from the highest to the lowest) as SCADA system – level of monitoring, control network and Human machine Interface (HMI), SCS level, controllers and instrumentation (switches, gauges, sensors). Two SCADA centers are connected to corporate network, to enable access to servers in demilitarized zone (DMZ) from the enterprise level. Communication between SCSs and SCADA servers is based on IEC 60870-5-104 protocol, and data transmission is implemented by Ethernet technology. System solution is presented on Figure 2.

It iss proposed to build an isolated HV SCADA system network infrastructure, reliable and secured by applying the „Defense in depth“ concept [22]. This model is implemented in several layers (physical, network perimeter, security of computer, application and equipment). The network is divided into network segments with different access rights (establishing of DMZ, separating of IT and ICS network). Physical protection at physical perimeter included access control system (biometric check of identity) and video surveillance (CCTV), covering equipment rooms, corridors and entries. Security system is connected through dedicated infrastructure, independent of SCADA network.

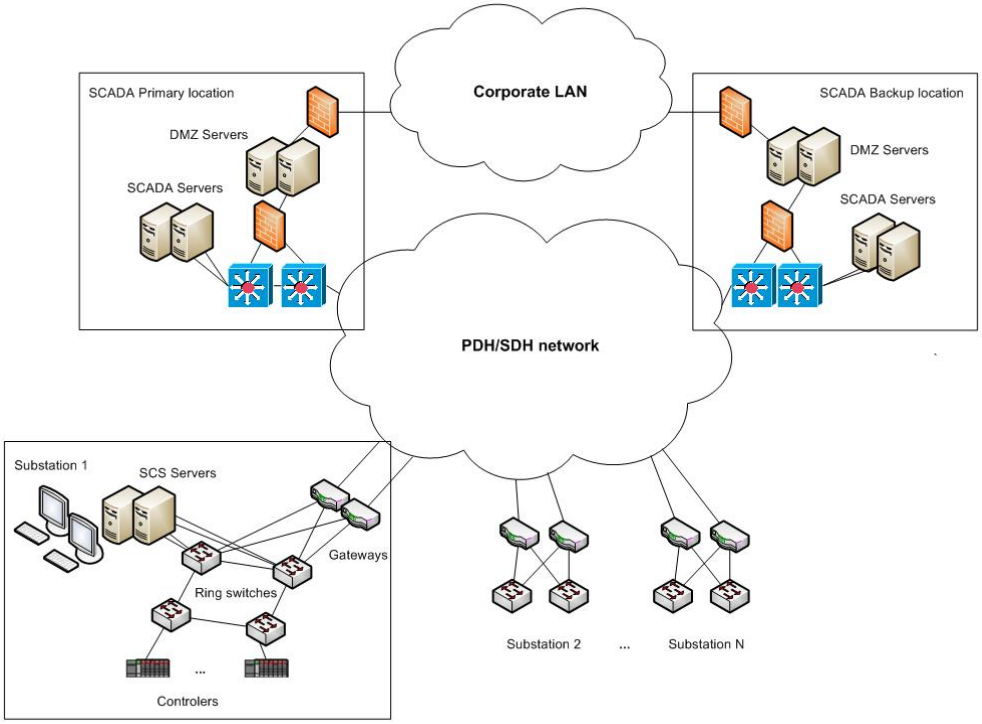

Figure 2: Block scheme of HV SCADA system connection

Equipment is arranged into racks with locks. Unused switch ports are blocked to limit physical access to the network. All equipment is connected to Uninteruptable Power Supply (UPS), that enable its operation even in case of network power supply failure. Equipment rooms are air-conditioned to provide its regular operational conditions.

Taking into account that any information loss in such a system could have serious consequences, a system's availability of 99.999% (five 9) has been proposed. It means that all links and equipment have redundant configuration. Also, two SCADA centers are proposed, one as primary and another as secondary with the role of Disaster Recovery Site, to keep reserve copies of data. Master SCADA servers from both locations receive all information from substations at the same time and in case of failure of any SCADA centre, another continues to provide full service. Segregation of networks provides better protection of information and localization of any problems within the network. All unnecessary services (for example HTTP approach to network equipment) are switched off to decrease system vulnerability.

Segregation of duties as well as areas of responsibility are foreseen within the system by defining of control regimes that prevent dispatchers from substations to do any operations from SCADA level and enable only actions within SCSs, and vice versa. Instrumentation adjustment and configuration is enabled only to authorized person and only using control panel, not through the network.

Protection of operator work-stations is provided by installation of anti-virus application. Intrusion Protection System (IPS) is proposed against maliciuos codes. Control of network equipment and links is provided by Network Management System (NMS). Approach to applications is enabled using authentication system – each particular user enters its username and password. Authentication is based on role that user has within the system, and all actions are subject of monitoring. Access to data from the corporate network is enabled only via firewall, and only to servers within DMZ, that have copy of data necessary for performing of integrated services. Choice of software, updates and use of antivirus applications are strictly controlled, to avoid any loss of information because of slow down of processes.

5. PRACTICAL ASPECTS OF INFORMATION SECURITY

Based on structure of Annex A of standard ISO 27001 [5] it is possible to recognize several practical aspects of information security application within EPU:

- Information assets responsibilities ("owners") and rules of acceptable assets use should be identified;
- Employees at all levels should be permanently educated regarding information security needs as well as how to perform it;
- After termination of employment (contract expire or finishing of activities at the project) all access rights to information as well as information processing equipment should be removed;
- Server rooms should be physically protected. Access should be allowed only to those persons that are directly engaged to work on equipment;
- Availability of information should be provided using all technical measures as per importance of this information (main and standby path, separate electricity supply systems, dual configuration of central units etc);
- Particular attention should be paid to removable devices (USB, External HD, Lap top computers) and to teleworking. This type of media should be kept under control (for example, bring it at hand luggage during travelling, not to leave it into the car etc);
- Control of user access (to the network, operative system and applications) should be defined by rules to provide information necessary to user to perform his/her job, not more or less. Also, rules for passwords should be defined (minimum length, avoiding of birthday date and similar recognizable elements) and periodicity of its change;
- If possible, all situations related to information security should be monitored and registered (information security events) and analysed to prevent its grow into infromation security incident;
- From all these situations it is necessary to make conlusions as „lessons learned" to prevent its recurring.

6. CONCLUSION

In this paper, a short review of relevant standards related to information security aspects within Electric Power Utility is given. Some of these standards establish global framework to this topic (ISO 27001), others express specifics of systems in which they are applied, issued by other institutions, more or less related to electric power systems (CIGRÉ, IEC, NIST, NERC etc.). Particular emphasis has been put to information security aspects in SCADA systems and intelligent networks (referred to as „Smart Grid") because of the fact that these industrial control systems nowadays are widely applied in EPU. Any form of threat to basic properties of information transmitted and/or stored within these systems – availability, integrity and confidentiality - could have unforeseeable consequences for system, equipment or people safety. Finally, the topic is illustrated with practical example of information security solution for the HV SCADA project.

BIBLIOGRAPHY

[1] Technical Brochure TB 317 CIGRÉ "Security for Information Systems and Intranets in Electric Power Systems" (JWGD2/B2/C2.01, April 2007)

[2] G.N Ericsson "Cyber Security and Power System Communication – Essential Parts of a Smart Grid Infrastructure" (IEEE Transactions on Power Delivery, Vol 25, No 3, July 2010, pp 1501-1507)

[3] R.Raković "Revision of standard ISO 27001:2013 for information security" (*16.* Symposium CIGRE-Serbia, STK-D2, Kladovo, October 2014**,** invited paper R D2 08), *in Serbian*

[4] R.Raković, J.Mandić Lukić "Information security standards in Electric Power Utility environment" (*32.* Conference CIGRE-Serbia, STK-D2, Zlatibor, June 2015**,** paper D2 02), *in Serbian*

[5] ISO/IEC 27001:2013 "Information technology - Security Techniques - Information security management systems – Requirements" (ISO, 2013)

[6] ISO/IEC 31000:2009 "Risk management - Principles and guidelines" (ISO, 2009)

[7] Technical Brochure TB 419 CIGRÉ "Treatment of Information Security for Electric Power Utilities (EPUs)" (WGD2.22, June 2010)

[8] Technical Brochure TB 603 CIGRÉ "Application and Management of Cyber Security Measures for Protection and Control" (WG B5/D2.46, December 2014)

[9] IEC 61850: "Communications for Power System Automation" (TC57)

[10] IEC 62351-6: "Power Systems management and associated information exchange: Data and Communication security – Security for IEC 61850" (TC57WG15, January 2007)

[11] NIST SP 800-82 Rev 2 : 2014 "Guide for Industrial Control Systems Security, Special Publication (SP)" (Rev 2, Initial Public Draft, May 2014)

[12] NISTIR 7628:2010 "Guidelines for Smart Grid Cyber Security, Vol 1: Smart Grid Cyber Security Strategy, Architecture and High –Level Requirements, Vol 2: Privacy and the Smart Grid, Vol 3: Supportive Analyses and References" (August 2010)

[13] W.Wang, Z.Lu "Cyber Security in the Smart Grid: Survey and challenges" (Computer Networks Vol 57, 2013, pp 1344-1371)

[14] NERC Cyber Security Standards, Glossary of Terms & CIP-002 do 011 (Ver 5, November 2011)

[15] "Electricity Subsector Cyber security Capability Maturity Model" (ES-C2M2, V.1.1, US DoE, February 2014)

[16] "Electricity Subsector Cyber Security Risk Management Process" (DOE/OE-0003, May 2012)

[17] "21 Steps to improve Cyber Security of SCADA networks" (DoE)

[18] "Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues" (INL/EXT -09-15500, US DoE, April 2009)

[19] "Smart grid Security – Recommendations for Europa and member States" (ENISA, July 2012)

[20] R.Tsang "Cyber threats, Vulnerabilities and Attacks on SCADA Networks" (2010)

[21] R.Raković, N.Čukić "Information protection in electric power systems from the point of view of application of standard ISO 27001:2005" (*15.* Symposium CIGRE-Serbia, STK-D2, Donji Milanovac, October 2012**,** paper R D2 04), *in Serbian*

[22] N.Čukić, S.Kisić, J.Mandić Lukić "Security of SCADA systems" (Infoteh, Jahorina ,March 2012, paper KST-4-1, pp 396-400), *in Serbian*