Communication Protocols in Substation Automation and IEC 61850 based proposal

J. Horalek, J. Matyska, V. Sobeslav
Department of Information Technologies
University of Hradec Kralove
Hradec Kralove, Czech Republic
e-mail: josef.horalek@uhk.cz, jan.matyska@uhk.cz, vladimir.sobeslav@uhk.cz

Abstract— **The automation of control systems of substations in the energy industry uses a variety of specialized standards, technologies and protocols. Among the most frequently used belong MODBUS, IEC60870, DNP3 and IEC61850 protocols. The present paper analyses and compares approaches to data communication among the abovementioned protocols with the main focus on modern standard IEC61850. The paper was created on the basis of experience while implementing data communications for ČEPS a.s., the national distributor in the Czech Republic.**

Keywords- IEC standards, power system control, substation automation, IP networks, ethernet networks, network topology.

I. Introduction

Substation automation in power industry enables the development of remote monitoring, control and electronic devices coordination. Substation automation encounters the challenge of power distribution reliability and efficiency. Potential risk factors such as lighting, accidents, system faults or financial efficiency leads to development of standardization process [1], [2]. Standards and appropriate technologies help to contribute to the following issues:

- Reduce settings and configuration effort
- Create more capability and flexibility
- Stimulate more interoperability
- Lower installation cost
- Reduce manual effort & errors

Throughout the history, variety of systems, technologies and protocols has been developed. The main problem in this area is the fact that many of these protocols and developed systems are usually vendor depended and cannot be adopted as a complex solution. If we analyse this area from the data networking point of view the most important protocols are Modbus, Modbus Plus, DNP3 and IEC 60870. These protocols still operates at the electronic utility level. Systems usually serve the selected services and cannot be adopted over the standard and high-speed communication technologies like the Ethernet [3]. Ethernet is one of the most important technologies in the networking area. The utilization and interconnection with the industry communication standards is a topical issue and brings many assets. Important Ethernet characteristic is that is part of standardised networking models like ISO/OSI and TCP/IP protocol stack. The independent parts of the substation or the whole substation automation systems can be connected and create the complex system. Furthermore this paper is mainly focused on the modern standrard IEC 61850 and the implementation in complex SAS project in Czech Republic. On the other hand the integrated solution brings the potential risk factors, such as security vulnerabilities and threads.

According to EU direction 96/92/EC, only one operator is responsible for power distribution. Distribution and power production is separated to ensure the competition on the market. In the Czech Republic ČEPS, a.s. serves distribution services. This company, controlled by the government, ensures the allocation of power resources, transformation capacities, management and security issues. Dispatching centre grants neighbouring countries interconnection for international collaboration in Europe, respecting UCTE [6] rules for electricity power exchange. Bilateral cooperation is currently in progress with distribution operators in Germany, Poland, Austria, Slovakia, Hungary and Slovenia.

II. development OF Substation automation standards

Variety of systems, technologies and protocols has been developed throughout the history. The main problem in this area is the fact that many of these protocols and developed systems are usually vendor depended and cannot be adopted as a complex solution. If we analyse this area from the data networking point of view the most important protocols are Modbus, Modbus Plus, DNP3 and IEC 60870. These protocols still operates at the electronic utility level. Systems usually serve the selected services and cannot be adopted over the standard and high-speed communication technologies like the Ethernet [3]. Ethernet is one of the most important technologies in the networking area. The utilization and interconnection with the industry communication standards is a topical issue and brings many assets. Important Ethernet characteristic is that is part of standardised networking models like ISO/OSI and TCP/IP protocol stack. The independent parts of the substation or the whole substation automation systems can be connected to create the complex system.

III. Modbus

The MODBUS protocol has gradually become the standard for creation of automation systems in wide are of industrial applications. Recently Modbus support various set of networking technologies including serial communication,

978-1-4799-0197-5/13/$31.00 ©2013 IEEE

optical or radio networks, RS-232, RS-422 a RS-485 serial communication or the TCP/IP enhancements.

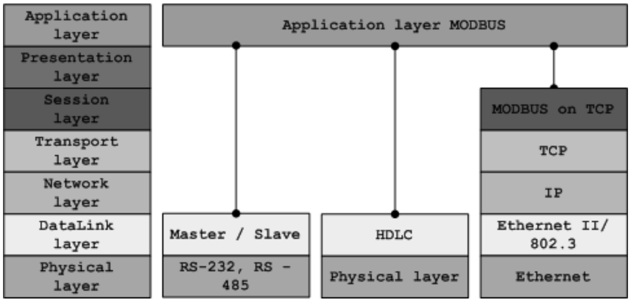

Figure 1. Communication standards MODBUS

According to the transport technologies, MODBUS operates at different layers within the protocol stack model. Following picture presents possible solution. At the operational level, Modbus works in a response/answer manner. Required function is presented by the sequence code listed in protocol documentation. Modbus is suitable mainly for serial data communication and it is not optimized for communication over the Ethernet. Modbus plus is important enhancement of previous protocol version. Modbus plus can be seen as a complex solution for remote communication in industry area. Adoption of TCP/IP protocol stack extends the use of this protocol. For the connection over the internet, Modbus obtained reserved system port 502. Modbus/TCP basically encapsulates a Modbus frame into a TCP frame in a simple manner. Transmission Control Protocol represents the connection oriented and reliable mechanism instead of other industrial or network technologies. Therefore, Modbus can make use of the advantages of internetworking technologies and this fit the master and slave nature of Modbus. There are some disadvantages of this protocol. Modbus for example does not give time stamped events. The sequence of events is missing the time stamp context and also not provides polled report by exception.

IV. IEC 60870-5-101

IEC 870-5-101 is an industrial standard developed by the IEC TC57 for electric utility communication between master stations and remote units. The IEC 870-5-101 consist of five parts, like the DNP3 protocol, which we will discuss in the next chapter. IEC 60870-5-101 is one of the IEC 60870 set of standards, which is focused on remote control in electrical engineering and power system automation applications. The substandard part 5 provides a communication profile for sending basic remote control messages between two systems via directly connected permanent circuit.

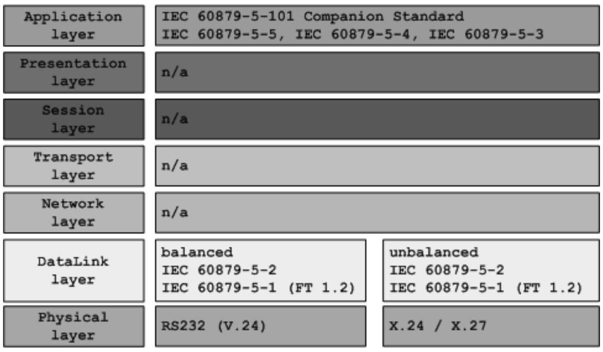

Figure 2. Communication standards IEC 60870-5-101

IEC 60870-5-10 is a structured substandard which provides the definition for the interfaces of RTU (Remote Terminal Units) and IED (Intelligent Electronic Device). It consists of the necessary components and profile definitions for vendor's development and ensures the compatibility with other systems. The communication profiles and mechanisms are technologically independent, according to ISO/OSI relation model. They act mainly on application a data link layer.At the physical layer allows the selection of compatible standards with RS-232 and RS-485, and also support fibre optics interfaces. The frame specification provides the required data integrity together with the maximum efficiency for acceptable implementations. FT 1.2 represents asynchronous way of communication and can be implemented using standard Universal Asynchronous Recover Transmitters ports. This standard also offers fixed and variable block length and single transmission character control procedure. The data link layer specifies if an unbalanced or balanced transmission mode is used together with the link procedures. The selection corresponds with function codes. The address schemas for communication circuit are also provided. The link transmission procedures follow the IEC 870-5-2 standard, like other parts of the protocol stack, and specify the send commands with confirmation and no replay, request and response message. This protocol stack can be implemented in multidrop bus and point to point networks topology.

V. DNP3

DNP3 - distributed network protocol is a protocol stack or a set of communication protocols used for the interconnection of automation systems. Typically is used within the SCADA systems and Intelligent Electronic Devices (IED in the terminology of IEEE TC97 group) in the area of power industry. DNP3 is not widely used in other industries. DNP3 uses the IEC60870-5 defined frame (FT3). FT3 frame is very similar but not strictly identical. CRC checking and optimal enhancements are the main differences. In the networking terminology, according to the ISO/OSI reference model, DNP3 is mostly the layer 2 protocol, which provides multiplexing, error checksum, link control, data fragmentation, basic QoS prioritization and layer2 addressing schemas. From the transport and application layer perspective, the DNP3 packet loses its own logical context, the interconnection with data units and substation transport events. There were some enhancements developed, for example the UCA 2.0 (Utility Communication Architecture developed).

VI. IEC 61850

IEC 61850 is the response of previous standards limits. It brings many assets for technology development and implementation. The standardization process brings the convention for object modelling and programming, the use of modern networking technologies, commands schemas, data representation, data transfer, encapsulation and many more. IEC 61850 is a huge standard and consist of many substandard. It would be impossible to cover all topics; more information can be found here [3], [4], [5].

IEC 61850 communication and data transfers can be realised via serial and modern computer networks technologies using TCP/IP model and Ethernet encapsulation techniques. We recognize two categories of communication: vertical and horizontal [7]. The collection of IEC 61850 standards covers the methodology for devices integration, data encapsulation or network services protocols. Relationships between the specific sub-layers of IEC models are described in the following table. Changes in one part should not affect other relations or elements.

- IEC 61850-10 - Conformance testing
- IEC 61850-6 Configuration language for communication in electrical substations related to IEDs
- IEC 61850-8-x IEC 61850-9-x Specific communication service mapping (SCSM)
- IEC 61850-7-4 Compatible logical node classes and data classes
- IEC 61850-7-3 Common Data Classes
- IEC 61850-7-2 Abstract communication service interface (ACSI)
- IEC 61850-7-1 Principles and models
- IEC 61850-5 Communication requirements for functions and device models

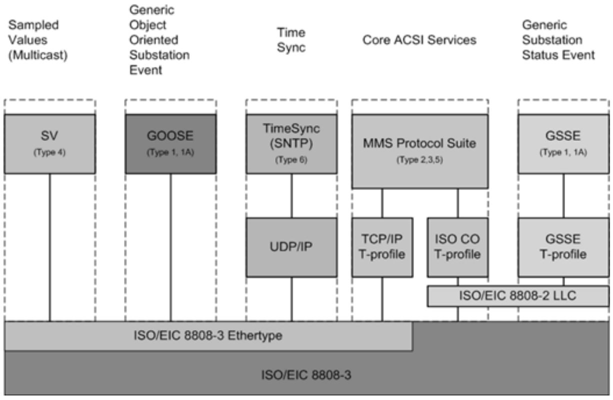

Figure 3. Communication standards

IEC 61850–5 defines the following communication messages with the consequent interpretation:

- Type 1 (Fast messages)
- Type 1A (Shutdown messages)
- Type 2 (Midfast messages)
- Type 3 (Slow messages)
- Type 4 (Prime data messages)
- Type 5 (Data transfer messages)
- Type 6 (Time synchronization messages)

Type 1 and Type 1A are mapped on specific ether-types for decoding optimization of accepted messages. Type 2, 3 and 5 are requested by service oriented messages. ISO 9506 MMS (Manufacturing Message Specification) provides methods and services for ACSI information modelling.

ISO/OSI reference model splits up network communication into seven sub-layers and helps to scale the future development of networking model. IEC 61850 enables utilization of frequently used IP networks; it helps to lower financial costs [8], [9]. The picture bellow illustrates the interconnection between ISO/OSI layers, networking technologies and services. There are three main utilized services: GOOSE, SVM and ACSI basics.

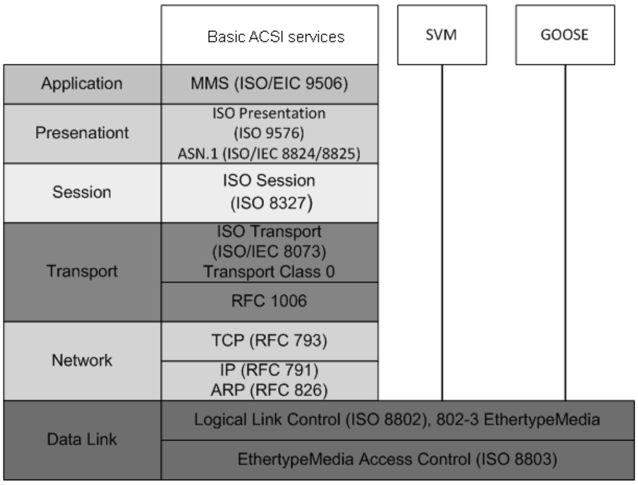
Basic ACSI services
SVM
GOOSE
Application
MMS (ISO/EIC 9506)
Presenationt
ISO Presentation (ISO 9576) ASN.1 (ISO/IEC 8824/8825)
Session
ISO Session (ISO 8327)
Transport
ISO Transport (ISO/IEC 8073) Transport Class 0
RFC 1006
Network
TCP (RFC 793)
IP (RFC 791) ARP (RFC 826)
Data Link
Logical Link Control (ISO 8802), 802-3 EthertypeMedia
EthertypeMedia Access Control (ISO 8803)

Figure 4. Messaging SVM and GOOSE

A. SMV (Sampled Measured Values)

SMV is a method used for passing measured samples from sensor units, like CTs, VTs or digital I/O sharing between IED devices. Lower layers of ISO/OSI model use Ethernet multicast characteristics and unicast communication via serial line. OSI reference model (ISO/IEC 7498-1) describes in detail the conception of each communication layer and networking profiles, application (A-Profile) and transport (T-Profile). A Profile is the collection of specifications and agreements dealing with first three ISO reference model layers. The rest four layers form T-Profile. Services are mapped, according to IEC 61850-7-2 standard, in four different combinations of A-Profile and T-Profile:

- Client/server model
- GOOSE/GSE control
- GSSE services

- Time synchronization

Client/server model is used for relations in conjunction with IEC 61850-8-1 standard and its declaration specified in IEC 61850-7-2.

B. *GSE/GOOSE profiles*

GSE (Generic Substation Events) control model, defined in IEC 61850, provides a fast and reliable mechanism of data transfer [9], [10], [11], [12] over the network. The standard defines more ways for communication in substation. GOOSE and GSE events typically use multicasts for data delivery. Generic Object Oriented Substation Events (GOOSE) mechanism groups data into objects and transmits within them 4 milliseconds. It helps to assure the reliability and transmission speed of communication. (GSSE) mechanism is enhanced by UCA2.0 status messages. In Ethernet networks data are segmented and encapsulated straight into frames and transported as a lower layer multicast over the networks [8]. This might be a bottle-neck in specific implementations, because the feature development depends on GOOSE interpretation, but broadcast domain limitation is not obviously the main problem in implementation.

C. *Time synchronization*

Time synchronization is an important part of IEC 61850 standard and helps to ensure the system homogeneity and action validity. Communication profile is used for relation in conjunction with IEC 61850 8 1 and specifies objects that contains TIME attribute. Special GPS modules with horizontal communication capability are used.

D. *Horizontal and vertical comunication*

The internal topological model separates the communication in horizontal and vertical level, as we mentioned above. Horizontal communication ensures the critically important connection between each IEDs (Intelligent Electronic Devices). From a computer networking point of view it is possible to use serial links or direct encapsulation of Generic Object Oriented Substation Events into Ethernet frames. Serial lines are sometimes offered as a better solution, because of their advantages in direct communication, accessing methods, signalling and finally for security reasons. Big advantage of traditional network utilization in industrial communication purposes are:

- Sharing network resources
- Lower the financial costs
- Faster development of networking technologies
- Creating complex SAS project over internetworks
- Remote access capabilities

On the other hand, IP networks, respectively, Ethernet technologies utilization comes with many limits for IEC 61850 and therefore usually serial links are recommended rather than Ethernet. NBMA (Non-Broadcast Multiple Access) networks were not built for the communication sensitive on delivery order, reliability, constant throughput or quality of services. In case of data modulation in Ethernet frames, it is necessary to grant high quality connection and to overcome some negative aspects, which are not relevant in average networking processes. As a critical factor there can be mentioned communication delay, destination identification interpretation and packet loss on the second OSI layer. TCP/IP stack does not include mechanisms for reliable delivery which will grant frames order and quality of services. This effort historically lays on lower layers or added mechanisms. TCP/IP model is used typically for vertical communication. Connectionless and non-reliable communication over UDP protocol is used for NTP time synchronization. Connection-oriented and reliable communication over TCP protocol is used for ASCI MMS message communication described in previous chapter. In traditional asset the QoS mechanism (Quality of Services) is implemented on logical level and enables services classification and prioritization. IEC 61850 requests reliability, fast data delivery and redundant topology with maximal accepted delivery time of about 10 milliseconds, including network topology convergence. These requirements can be overcome only by the enhancement of Ethernet with special technologies and devices. Analysis and project design has to take these factors into account.

VII. SAS PROJECT IN THE CZECH REPUBLIC

The goal of the Substation Automation System project is to create centralized and interconnected solution within next two years. Finally ČEPS and dedicated suppliers, like ABB or SIEMENS, will be able to connect even with the substation devices via modern IP networks, internet and WAN technologies. This solution opens many questions in security area, data encapsulation techniques, modification of MPLS WAN network or internal substation topology proposal. Following chapters describe the limitation and proposed solution which has recently reached the test phase.

A. *Internal SAS communication level*

Internal substation topology should be designed according to the IEC 61850 requirements described in chapter 2.1. Proposed topology utilizes Ethernet as a main transport technology instead of serial lines, because IP networks allow more possibilities for substation integration. To overcome the limitation of NBMA network type it is recommended [7], [13], [14] to use IEC 61850 certified devices which help to overcome Ethernet limitation with enhanced features.

- Faster spanning tree algorithm calculation
- Optical/metallic links support
- 802.1q VLAN optical rings support
- GVRP (Generic Attribute Registration Protocol)
- Upper layer segmentation
- QoS engine with L2 layer support
- L2/L3 Security integration
- IGM snooping and enhanced L2 multicast features

High availability of the automation system ensures doubled optical rings connected in high capacity switches (Ruggedcom 9100). Data, objects and messages are replicated between two heads of the control system. The main asset of this approach is a system protected against Ethernet broadcast storms with fast convergence time (less than 6 ms against seconds measured in standard RSTP+ protocol implementations). Token GOOSE messages are controlled by L2 filters and logically interpreted by IED devices. The topology was created with the effort to correspond with wide IEEE recommendation for industrial automation (IEEE 1613 level 2, IEC 61850-3, IEC 61800-3, IEC 61000-6-2, NEMA TS-2).

B. External connections to SAS

The external connection to substation automation system serves the access to merge units, legacy IED devices, gathering statistical data or system management. These connections can be divided into three parts:

- Access to dispatching centres
- Intra-substation communication
- Remote connection to WAN or internet

Dispatching centre accesses via serial line encapsulation in to IP datagrams over physical or virtual lines defined in IEC 60870-5-101 industrial standard for data exchange. The communication within substation includes the substation operators and parameterization department access. Demarcation point in these two types of communication lies on the head of automation system. From the security point of view, this might be a bottle neck of network.

Future development and integration with IP networks needs to change this communication means. The first part of the project includes a brand new connection for the third communication type. Remote connection to WAN or internet is used for accounting systems, control and other internal proposes. External access to the IED devices, sensors or head of the substation systems needs to be taken under control and secured. To solve this problem, we offer to use a gateway located on the substation level with the following features and configuration.

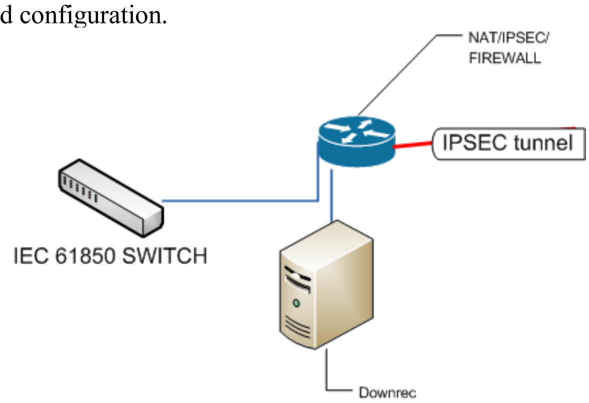

Figure 5. Substation topology control room

There are two types of communication in IEC 61850, horizontal and vertical. The first one is encapsulated directly into the frames and strongly influenced by the network quality. The second one is transported by upper layers of TCP/IP model and it is used for IED device management, connecting to the heads of SAS etc. Downrec is a computer device, controlled by a vendor, with a special control software on the border between substation and WAN part of the ČEPS networks. One the most important goals of this gateway are to manage and filter traffic in both directions and to apply the security rules. Tunnelling techniques help to isolate the traffic between the core of the ČEPS network and vendor internal networks. Another respected requirement is to get the possibility to use the same logical addressing scheme in every substation and therefore this device must be able to perform L3 operation.

C. Remote access and substation interconnection

Remote access and substation interconnection open many security threats. A successful project requires a reliable and secure system with the ability to account, authentic, authorise and monitor the network activity. Every connection to the substation passes through the ČEPS WAN network. In this scenario, vendors, local ČEPS and substation networks are connected together. Communication line violation, listening or DoS attack are pending in transparent networks. Therefore it is necessary to isolate this communication in network. Isolation on physical level is rather expensive and in this case an impossible solution, because of the distance between substations. Virtual private networks are able to encrypt and isolate data.

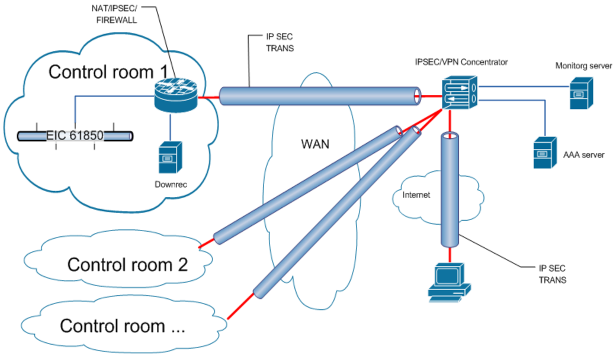

Figure 6. Remote access topology

Proposed network topology is secured in a multilevel way. External communication to substation has to pass CISCO ASA (Advance Security Appliance) connected in failover cluster for high availability solution. This device checks the incoming traffic, the filter against access list, allows to set rules and connects to the AAA system mentioned above. This rule is applied for each type of external communication. The access from internet, WAN or other systems is deeply monitored against viruses, hacking patterns and mirrored. In the next step, data flow is encrypted and routed via OSPF protocol, for internet access packets are translated via NAT mechanism. MPLS networks and firewalls over the rest of the network are allowed to open IPS tunnels authentication process and data flow only.

Each substation is connected (also their substation buses) via gateways with NAT, IPSEC, FIREWALL features. The gateway creates the border between partial SAS automation system and external connection. This place applies further security activities like data decryption, rules for vendors, NAT mappings and many others. Network monitoring and proactive reaction to security threats became necessary part of the security solution [15]. IDS (Intrusion detection system) monitors network activities for malicious activities or policy violations and process the output to the dispatching centre. IPS (Intrusion prevention system) than performs reactions to security threats detected by the IDS system. Security Appliance with IDS/IPS capatibilites will be located in the ČEPS network core, because this point is the last place before data are encrypted in IPSEC tunnels. This device will be responsible for acquiring and recording the information about network utilization. Traffic can be forwarded to the free SPAN port of IPSEC-VPN concentrator and connected to the monitoring server. High availability purpose request more than two ASA device connected and configured as a failover cluster.

Remote access from internet allows operators outside the company or suppliers networks to connect in the substation. SAS project will be examined according to security standards such as ITSEC or FIPS. Remote networking software and Cisco security appliances are FIPS 140-2 certified. The user with remote software connects to IPSEC/VPN concentrator witch filters this traffic and checks the traffic against viruses, malware or potential attacks using signatures, antiviruses and heuristic techniques. All devices or security solutions implemented in the SAS project are certified by security standard FIPS 140 1 or 140-2. Different parts of the system require different security levels defined by FIPS.

VIII. Conclusions

The present paper has analyses and compared approaches to data communication among the abovementioned protocols with the main focus on modern standard IEC61850. The results indicate that remote access to substation automation in power industry can be performed in a different ways. Previous standards like Modbus, DNP3 or IEC 608750-5-101 have limited options of use. IEC 61850 area covers a wide range of problems, solutions and technologies; therefore it is complicated to design. Every project may significantly differ. The IEC 61850 standardization does not offer any method or step by step procedure. Standardization is relatively free and open to modifications. IEC61850 standardizes object definition, communication technologies and requirements. Many settings, such as GOOSE messages, TCP ports settings etc. act as recommendations for system designers.

Acknowledgment

This work and contribution is supported by the project of Specific Science – Analysis of communication protocols and resources in system automation, Faculty of informatics and management and by the project No. CZ. 1.07/2.2.00/28.0327 Innovation and support of doctoral study program (INDOP), financed from EU and Czech Republic funds.

References

[1] DAVID, A. K; WEN, F Market Power in Electricity Supply. In Power Engineering Review, IEEE . Volume: 21: Issue:12 , 2001. p. 67 - 68. <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4311230>. ISSN 0272-1724.

[2] SHIRMOHAMMADI, D, et al Distribution automation system with real-time analysis tools. In Computer Applications in Power, IEEE . Volume: 9 : Issue: 2, 1996. p. 31 - 35 . <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=491517>. ISSN 0895-0156.

[3] ZHANG, Jianqing ; GUNTER, Carl A. . IEC 61850 - Communication Networks and Systems in Substations:An Overview of Computer Science. University of Illinois at Urbana-Champaign 2007. <http://seclab.uiuc.edu/docs/iec61850-intro.pdf>.

[4] BRUNNER, C IEC 61850 for power system communication. In Transmission and Distribution Conference and Exposition. 2008. p. 1 - 6 . ISBN 978-1-4244-1903-6.

[5] YONGLI, Zhu, et al Study on interoperable exchange of IEC 61850 data model. In Industrial Electronics and Applications, 2009. ICIEA 2009. 4th IEEE Conference on. [s.l.] : [s.n.], 2009. s. 2724-2728. ISBN 978-1-4244-2799-4.

[6] Statistical Year Book 2008. 1. Regional Group Continental Europe (former UCTE) : Entsoe, 2008. <https://www.entsoe.eu/fileadmin/user_upload/_library/publications/ce/Statistical_Yearbook_2008.pdf>.

[7] ZHANG, Jianqing ; GUNTER, Carl A. . IEC 61850 - Communication Networks and Systems in Substations:An Overview of Computer Science.

[8] IEC 61850-8-1 Ed. 1.0 en:2004, Communication networks and systems in substations - Part 8-1: Specific Communication Service Mapping (SCSM) - Mappings to 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, ANSI, 2007

[9] IEC 61850-7-2 Ed. 1.0 en:2003, Communication networks and systems in substations - Part 7-2: Basic communication structure for substation and feeder equipment communication service interface (ACSI), ANSI, 2007

[10] IEC 61850-7-1 Ed. 1.0 en:2003, Communication networks and systems in substations - Part 7-1: Basic communication structure for substation and feeder equipment - Principles and models, ANSI, 2007

[11] IEC 61850-7-3 Ed. 1.0 en:2003, Communication networks and systems in substations - Part 7-3: Basic communication structure for substation and feeder equipment - Common data classes, ANSI, 2007

[12] IEC 61850-7-4 Ed. 1.0 en:2003, Communication networks and systems in substations - Part 7-4: Basic communication structure for substation and feeder equipment logical node classes and data classes, ANSI, 2007

[13] Odom W., Hucaby D., Wallece K, CCNP Routing and Switching Official Certification Library, Cisco Press, 2010, ISBN: 978-1587202247

[14] [14] COLE, Robert G. ; RAMASWAMY, Ravi . Wide-Area Data Network Performance Engineering. 1. Boston : Artech House Publishers, 1999. ISBN 978-0890065693.

.