EUROPEAN WORKSHOP ON INDUSTRIAL COMPUTER SYSTEMS TECHNICAL COMMITTEE 7 Reliability, Safety, Security		WP: 5086 V1.1 Date: 2006-01-18 Status: released Classification: public

ACKNOWLEDGEMENTS:
This work was funded by the members' affiliations.

Subgroup Security

BRIEFING PAPER

Electric Power Systems Cyber Security: Power Substation Case Study

INDEX

ELECTRIC POWER SYSTEMS CYBER SECURITY: POWER SUBSTATION CASE STUDY[1]

1. INTRODUCTION

In the report on critical infrastructures protection published in the United States by the President's Commission on Critical Infrastructure Protection in 1997, critical infrastructures are defined as systems whose incapacity or destruction would have a debilitating impact on the defence or economic security of the nation. These systems include [A.17]:

- telecommunications,
- electrical power systems,
- gas and oil,
- banking and finance,
- transportation,
- water supply systems,
- government services and
- emergency services.

The above mentioned Commission was established in 1996. In publication [A.11] it is given that this Commission was established in response to the effects of a number of large-scale blackouts (electric power system failures), in publication [A.19] that in response to terrorist attack in Oklahoma City, but certainly both these facts could contribute to establishing the Commission which has initiated intensive activities on Critical Infrastructures Protection (CIP) in the United States. In January 2000, the National Plan for Information System Protection was published in the US [A.3], which was considered a first approach to national cyberspace protection undertaken by any country. Detailed documentation of results of activities in the field of critical infrastructures protection in the United States can be found at [C.12, C.13, C.14, C.15, C.16, C.17, C.18, C.21, C.22].

At present an increasing number of CIP-related activities exist also outside the US, but – as it follows from publications and was given in the call for papers and invitation for participation of the CIP Workshop 2003 in Frankfurt/M. - one can say that the core concept of CIP which is being now in the process of implementation was developed in US between 1996 and 1999. Current approaches to CIP in other countries can be found in [A.19, C.1, C.2, C.3, C.4, C.7, C.8, C.9, C.10, C.11] and in a considerable number of other websites. EWICS TC7 has produced a briefing paper *Information Operations - Threats, Means and Weapon* on the risks to safety critical systems and organisations. This briefing paper and proceedings of symposia on information security of safety critical systems are available at [C.6].

Critical Infrastructure Protection (CIP) includes cyber and physical measures to secure the systems. Critical Information Infrastructure Protection (CIIP) is a subset of CIP. CIIP focuses on the protection of information technology systems and assets, such as telecommunications,

[1] This Briefing Paper was co-ordinated by Zdzislaw Zurakowski who provided the major input based on his research carried out in the years 1995-1997 within the EU Join Research Project „Copernicus" CP'94 1594 *Integration of Safety Analysis Techniques for Process Control Systems (ISAT)* and his research carried out in the years 2000—2003 in the Institute of Power Systems Automation in Wroclaw (IASE), Poland.

computers/software, the Internet, satellites, fibre optics, etc. and on interconnected computers and networks and the services they provide [A.19].

Towards the end of the 20th century electric power systems (EPSs) emerged as one of the most critical infrastructures in the sense that all other critical and vital infrastructures depend on reliable electricity supply. At the same time they are considered as the most vulnerable to physical and cyber attack. Information technology engineers and experts (in software engineering, information security, etc.) who deal with cyber security in critical infrastructures (also called electronic security in electric power systems) deal only with CIIP but they must at least to some extent understand also the nature of these infrastructures, possible consequences of security breaches, etc. However contemporary EPSs are very complex and highly technologically advanced systems, which appear to be sometimes underestimated by those outside the electric power sector. The vast, highly interconnected North American EPS has been called the „greatest machine ever created". The nature of possible consequences for an EPS in case of some security breaches is unique, based on concepts that are normally not known in others sectors of industry and in information technology. The intended aim of this briefing paper is to describe in a way comprehensible for all involved in critical infrastructure cyber security:

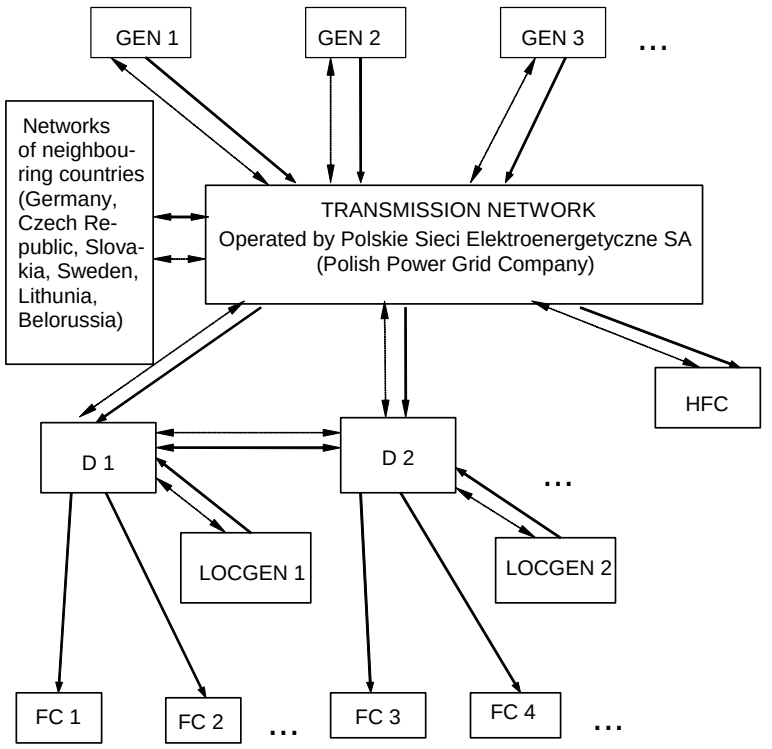
- the structure of electric power systems;
- the possible consequences connected with security breaches in an EPS in general and in an exemplary substation considered in the power substation case study;
- the current practice in assuring cyber security in electric power systems.

This paper is structured as follows. Section 2 presents the physical and organisational structure of an EPS and the concept of an electric power system control. To illustrate the degree of complexity imposed by the structure on the data network of an EPS exemplary data for the Polish EPS are given. Then in Section 3 hazards connected with the current use of computer-based systems in an EPS are described with an emphasis on the description of the concept of safety of an electric power system, whose nature is fundamentally different from the nature of those occurring in the process industry sector and all other sectors of industry. In Section 4 the current state of practice in assuring cyber security in electric power industry is presented. In Section 5 the Electric Power Substation Case Study is described. The aim of this case study was security analysis of a software interlocking system consisting of mutual interlocking disconnectors, circuit breakers and earthing switches to assure safety of switching operations carried out in a substation during operation and maintenance of the substation. Requirements were specified for 400kV 'Mosciska' substation in Warsaw (Poland) treated as an exemplary extra-high voltage substation. In Section 6 references are given. Annex A contains explanations of abbreviations and key terms.

2. STRUCTURE OF ELECTRIC POWER SYSTEMS

The electric power industry in each country consists of many different companies involved in electric power generation, bulk transmission of electricity from power stations to load centres and its distribution to customers. Although usually owned by different companies, in order to perform their functions and to attain suitable effectiveness, all power stations, substations, power lines forming power grids, the related control centres and other components are interconnected forming an EPS. This interconnection is now the strongest at the national level, forming a national power system. However, an increasing tendency can be seen (e.g. in Europe) to build up more and more stronger connections between the separate EPSs in individual countries. Energy related policy of the European Union aims to build Trans-European networks to provide a sound basis for free and competitive electricity market in Europe and strengthening security of energy supply.

An approximate block diagram of the Polish EPS – as an exemplary middle-sized EPS - is shown in Figure 1. A simplified diagram of a small fragment of the Polish EPS transmission network is presented in Figure 2. Figure 3 shows a simplified block diagram of the telecommunication network coupled with an electric power system. The concept of an EPS control is shown in Figure 4.



→ - Power flow in a normal operating condition; ⟶ - Power flow in an emergency condition; GEN - Public utility power stations operated by 17 power generating companies; LOCGEN - Local power generating stations (over 270 power stations of lower power); D - Distribution networks operated by regional distribution companies (33 utility companies); FC - Final customers; HFC - High power final customers connected directly to the transmission network (6 consumers).

Figure 1. Approximate block diagram of the Polish electric power system

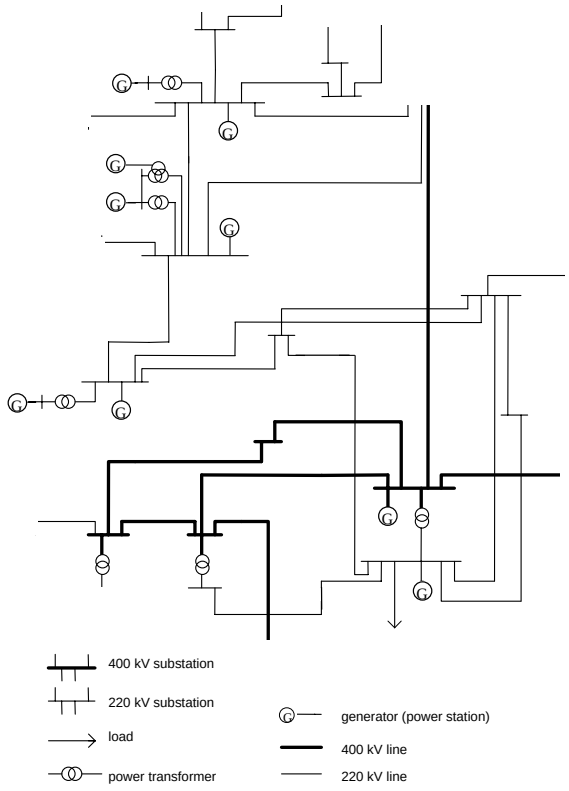


Figure 2. A small part of the transmission network of the Polish electric power system (distribution networks in this area are not shown)

In the most general terms, an EPS can be partitioned into generating stations and high-voltage power networks known as grids. Power networks consist of transmission networks, called Extra-High Voltage (EHV) networks, which are used to transmit power from generating stations to main load centres and distribution networks of lower voltages, also known as High-Voltage (HV) networks, which are used to transmit power to customers. Both, transmission and distribution networks consist of power lines, substations and control centres.

Substations form vital nodes in the HV and EHV networks because they allow configuration changes of networks during the system operation using switching devices in modern substations controlled by computer systems. Initiation of the control procedure may be performed locally by substation operators or remotely from EPS control centres. In generation stations as well as in transmission and distribution networks substations are also used for voltage transformation to minimise transmission losses due to heating of transmission and distribution elements. Transmission losses are proportional to square of current in a line and apparent power transmitted over a line is:

$$S = U \times I$$

where:
U - voltage of a power line;
I – current which flows in the power line when the power S is transmitted over the line.

Output voltage from generators in power stations, which for design reasons is within the range from a few to twenty-odd kilovolts, is transformed to voltage level of transmission network, which is about 220 kV and above, to sent electricity to the distribution centres. In the distribution centres voltage is transformed down to the level of distribution networks which distribute electricity to consumers.

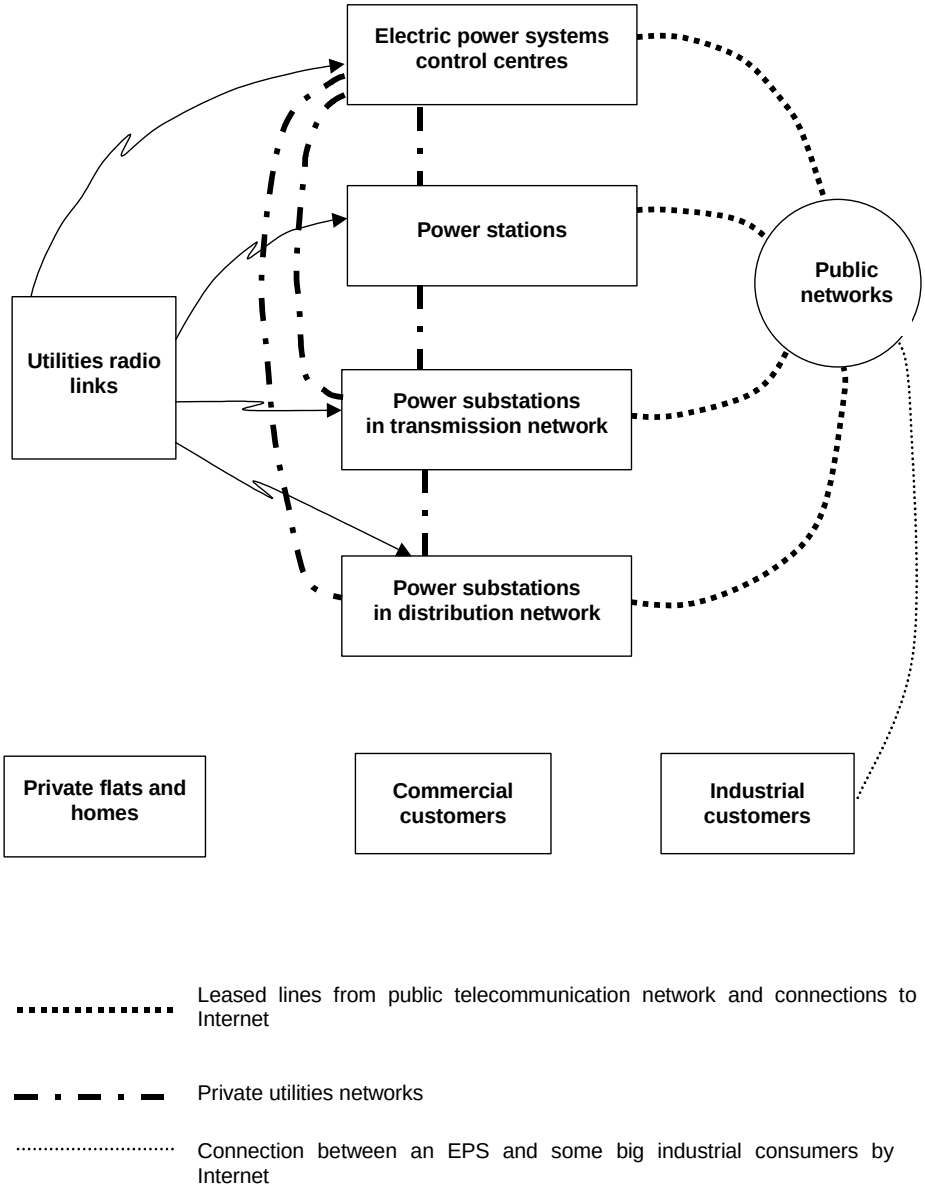


Figure 3. Simplified block diagram of the telecommunication network coupled with an electric power system

The power network of generation, transmission and distribution subsystems forming an EPS is integrated with telecommunication and telecontrol systems used for communication and transmission of data between power generating stations, substations and control centres for remote operation and remote real-time signalling, metering, control and fault protection. Development of these EPS communication systems goes toward an integrated EPS

telecommunication network. In the last decade, due to the process of computerisation of the EPSs, the data network is used on increasingly larger scale for transmitting data critical to safe and reliable operation of an EPS and for the power grid-related financial transactions.

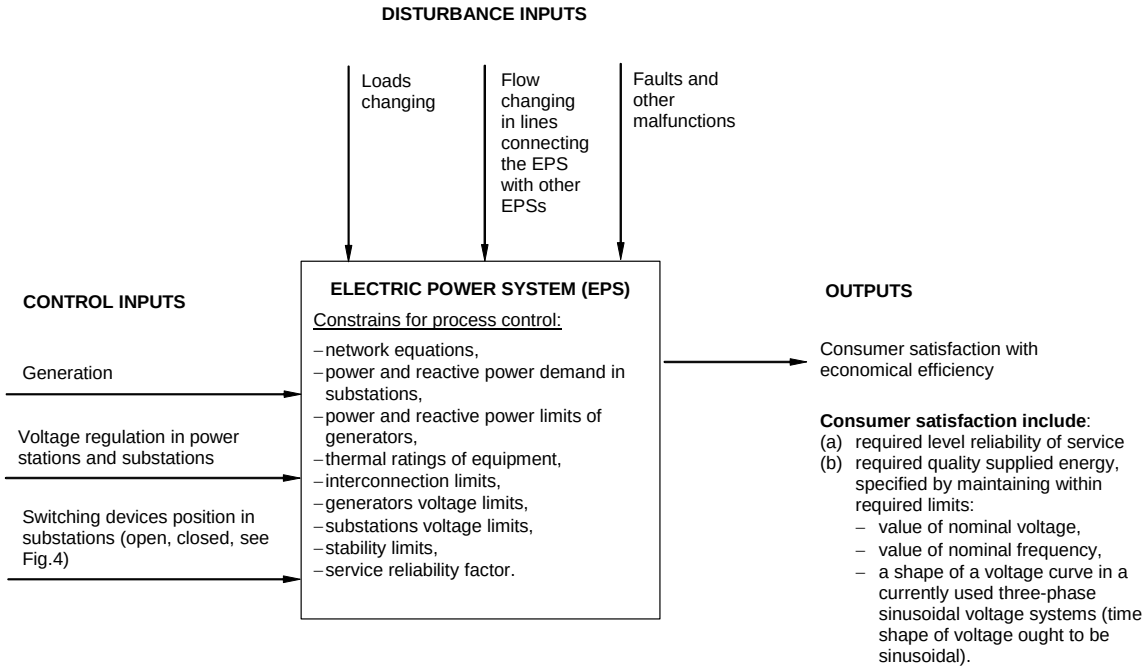


Figure 4. The concept of an electric power system control

Computers have been introduced gradually into the power sector. Initially, they were used for off line computations. The great Northeast Blackout of 1965 affecting Ontario, Canada and Connecticut, Massachusetts, New Hampshire, Rhode Island, Vermont, New York, and New Jersey in the United States, that left around 30 million people without electricity for up to thirteen hours, was a turning point in development of electric power systems and a spur to application of computers to control and monitoring of power systems [C.25, C.26, C.27, C.28]. Dr. Edward Teller, who at that time was the consultant to Governor Rockefeller of New York, describing a situation in the field of control of electric power systems, stated that *"power systems were like dinosaurs, having no nervous system. They needed sensors, communications, computers, displays and controls"* [A.18].

The first, very positively evaluated proposition of an integrated system approach to EPS telecontrol was published in 1967 [A.6]. Although computerization of EPSs progresses quickly the full automatic control of an EPS in normal and emergency states is currently not applied and realization of such idea seems to be rather distant for many reasons. At present, normally, the control function is performed from the area control centre and in many countries most of the substations are unmanned. The area control centre receives information from and controls several substations. A SCADA (Supervisory Control and Data Acquisition) system does this control function. A remote terminal unit (RTU) transmits needed information from each substation to the area control centre. This information is used to draw a complete picture of the supervised network. In the reverse direction RTU transmits commands from the area control centre to the substations. In a large network, with several area control centres, a load dispatching

centre manages and monitors the procurement of energy and the optimal arrangement of the power transmission network. A load dispatching center in turn gets the information from power plants, area control centres, etc.

To illustrate the degree of complexity imposed on a data network in EPS by the physical and organisational structure, it can be given that in the Polish EPS, being a middle–sized system, the transmission network includes 106 extra-high voltage substations (220 kV and above). Within the distribution network, there are 1264 substations of 110 kV and thousands of substations of lower voltages. The majority of the substations in the transmission network and the most important substations of 110 kV are equipped with computer-based control systems or at least with equipment that allows for remote control. There are six control centres to operate the electric power system in the transmission network and several dozens local control centres in the distribution networks. Seventeen power-generating companies operate power stations connected to national transmission system. Most substations are manned.

3. POSSIBLE CONSEQUENCES OF THREATS

The IEEE 1402 standard defines cyber intrusions, called in this standard electronic intrusions, as:

"Entry into the substation via telephone lines or other electronic-based media for the manipulation or disturbance of electronic devices. These devices include digital relays, fault recorders, equipment diagnostic packages, automation equipment, computers, programmable logic controllers, and communication interfaces." [B.5].

A cyber attack can be an electronic intrusion into a station, substation or control centre as defined above or a denial of services attack.

Most potential threats in EPSs are similar to those in other infrastructures, like for example:
- accidental physical damage;
- terrorism and sabotage;
- vandalism;
- disgruntled employees and ex-employees;
- malicious code and viruses;
- insiders and associates;
- labour conflicts;
- economic conditions;
- curiosity and ignorance fraud and theft.

Main vulnerabilities in EPSs are connected with the ability to remotely access protection, control, automation and SCADA equipment. Using vulnerability of a power substation communication an electronic intruder could for example access the substation SCADA system and operate circuit breakers in the substation that could affect the reliability of electricity supply or even cause big EPS failure. The biggest risks for an EPS create SCADA systems. Report [A.12] includes protection of distribution services by improving security for SCADA systems into seven top-priority technical recommendations to immediately apply existing knowledge and technology to make society safer.

In EPSs cyber security refers to confidentiality of data and information, the integrity and availability of data and commands received in substations and control centres, and authentication of the source of received data and commands.

Cyber security risks in an EPS concern safety-related computer applications in power stations, substations and control centres, and transmitting data and information critical to the power grid-related financial transactions (e.g. billing), functioning and interests of the electric power sector organizations. Possible consequences connected with cyber security risks for the financial transactions, functioning and interests of the electric power sector organisations are very similar to those kinds of consequences in other sectors and are not presented in this paper. This paper concentrates on possible consequences for people, equipment and an EPS connected with safety-related computer applications in power stations, substations and control centres.

An example of possible consequences connected with cyber security risks in power stations is presented below in Section 3.1, and connected with risks in substations is presented in Section 3.2. A concept of safety of an EPS and possible consequences for safety of an EPS are presented in Section 3.3. An emphasis is put on description of the concept of safety of an

electric power system, whose nature is fundamentally different from the nature of those occurring in all other sectors of industry.

3.1. Possible consequences in power stations

Possible consequences for people and equipment connected with cyber security risks in power stations are connected with the technological process of energy production. Most kinds of consequences connected with safety-related functions in power stations are similar to the consequences considered in other industry sectors. Their nature is rather obvious and due to the scope of this briefing paper, they will not be analysed in more detail. An example of safety-related function in thermal power stations can be starting the oil burners upon disappearing of flame in the boiler combustion chamber in order to prevent the damping of flame because a very dangerous explosion could take place in case of a repeated ignition of coal dust burned under the boiler to produce vapour.

From cyber security point of view it should only be taken into consideration, that for example adjusting output power of a generating set can be made remotely from the network control or load dispatching centre.

3.2. Possible consequences in substations

Substations form vital nodes in power networks because, among others, they make possible modifications in the configuration of networks during the operation of the EPS by means of switching devices that can be controlled by computer-based control systems. Initiation of the control procedure may be performed locally by substation operators or remotely from the EPS control centres.

Electric power substations consist of two essential parts:
– main (high or extra-high voltage) circuits, also called primary circuits;
– auxiliary circuits also called secondary circuits.

The main circuit of a substation is composed of a busbar system (or busbar systems) and connections of power lines, power transformers, etc. to the busbar system through switching devices. A busbar system is a set of three electric conductors of very low impedance[1)] that serves as a common connection for individual power lines, power transformers, etc. Substations are divided into bays. A bay of a substation is a part of a substation containing extra-high (or high) voltage switching devices and connections of a power line, a power transformer, etc., to the substation busbar system(s) as well as protection, control, and measurement devices for the power line, the power transformer, etc. If it is a bay used to connect a power line to the busbar system, it is called a line bay, if it is used for connecting a power transformer to the busbar system, it is called a transformer bay, etc. (see Figure 5 and 6). Normally, a substation contains a number of line and transformer bays and also other bays. All bays are similar to the line bay. Auxiliary circuits are electrical circuits containing measurement, signalling, control and protection devices.

One of the main safety-related functions connected with consequences for substation staff and equipment is switching operations control. For design reasons, disconnectors used in substations are able to switch on or off only very little currents, and for example they are not

[1)] In high voltage networks transmission lines have three wires, one for each phase. It concerns also busbar systems in substations. Each busbar system in a substation consists of three bars.

able to switch on or off a loaded line, and are only used to ensure the required isolation

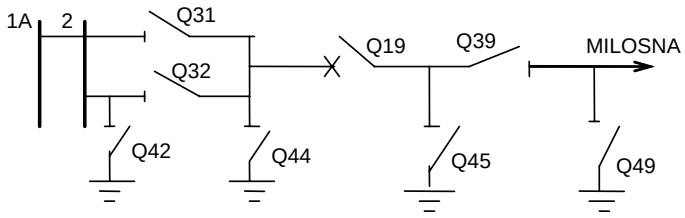


Figure 5. Simplified schematic diagram of the bay number 1 in Mosciska 400 kV substation considered in the Power Substation Case Study

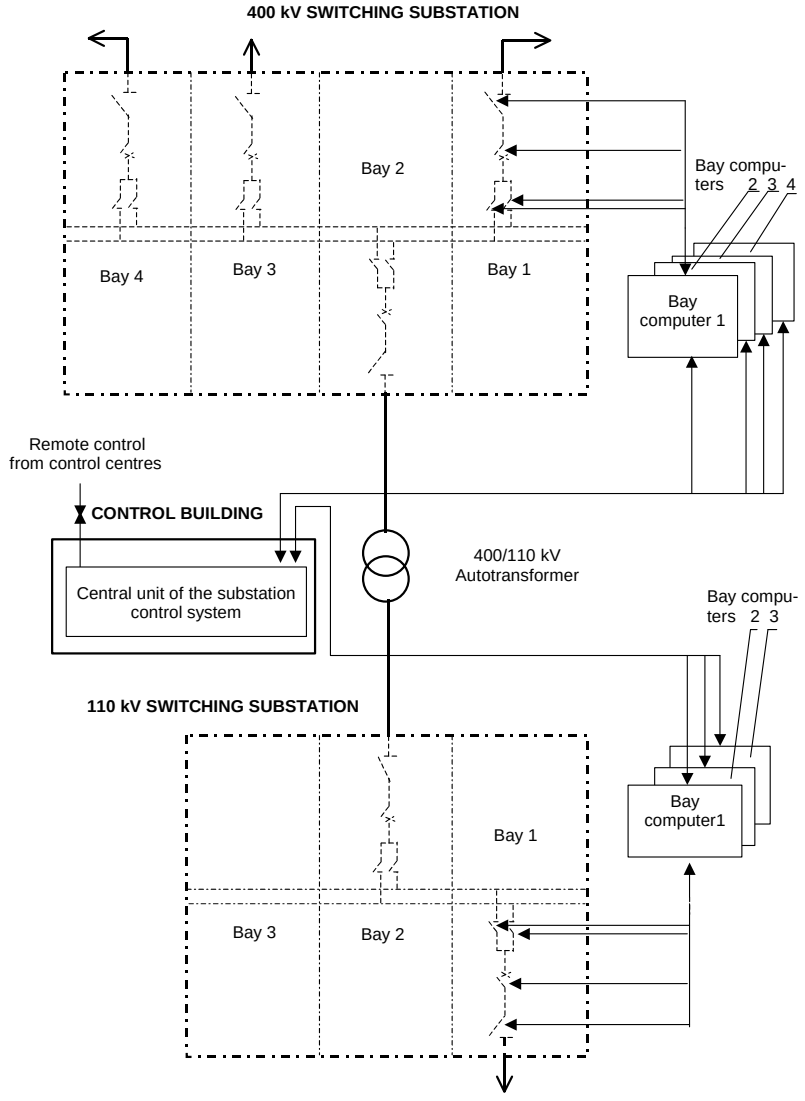


Figure 6. The concept of switching operations control

clearance between disconnected parts of a circuit breaker, which due to design restrictions cannot be ensured by a circuit breaker. Because of these limitations, switching off a line for example must be performed according to the following sequence (see Figure 5):

– breaking of the current using a circuit-breaker (Q19);
– opening of the line disconnector (Q39) to achieve isolation clearance between the disconnected line and the live part of the circuit-breaker;
– opening of the busbar disconnector (Q31 or Q32, depending on which busbar, ”1A” or ”2”, the line is connected to) to achieve the isolation clearance between the circuit-breaker and busbar.

If this sequence is carried out in an incorrect way, and for example the signal for opening would be sent at first to the disconnector (e.g. busbar disconnector), an electric arc would arise between the contacts of the disconnector accompanied by high rate optic and acoustic phenomena, spraying melted metal etc., and resulting in an inter-phase short circuit. It would look like an explosion. This failure would cause considerable material losses because of complete destruction of the disconnector and also partially or complete destruction of other components in the substation, disturbance in substation operation and interruption of energy supply to consumers. Sprayed melted metal could seriously injure personnel if, by accident, someone of the personnel was close to the exploding disconnector. Depending on the state of a given EPS at the moment of performing switching operation, the incorrect sequence of switching operation could also cause a large power system failure resulting for example in a collapse of a part of the EPS called black out, i.e. it could create risk for safety of the EPS.

According to the assessment of risks made during the case study functions, performed by computer-based systems in EHV substations, which vulnerabilities can produce a risk include but are not limited to the following functions:

1. Protection (for the detection and the elimination of faults or of abnormal conditions on power systems and for the restoration of service).
2. Described above control of switching operations which include among others:
   - programmable interlocking;
   - synchronization;
   - checking a continuity of control circuits of circuit breakers and disconnectors.
3. Measurement of analog quantities in an EPS.
4. Voltage regulation (by changing a position of transformer tap-changer).
5. Warning signaling (e.g., reduced SF6 pressure in switchgear).

The functions quoted above are enumerated, mostly, according to the size of consequences connected with error of function performing occurs. Protection and control of switchgears are seen as the most responsible. However, above ordering is only approximate, because, e.g., the error in measurements can also cause very serious results. The consequences ought to be analyzed in each particular case, for each substation. About all substations, we can say only one thing, that the control of switching devices in a primary circuit always plays a critical role because all functions connected with EPS protection, automation and control/operation realized by a substation are realized by switching devices.

Six examples of scenarios of cyber attacks against a substation are given in paper [A.15]. The scenarios show how insiders and outsiders could exploit the vulnerabilities involved in remote access to protective and SCADA equipment that are listed in this paper.

3.3. Possible consequences for safety of an EPS

In electric power systems engineering, safety of an EPS is described using the word ”security”. Because in computer science and software engineering “security” is used in a different meaning to avoid misunderstanding, later the paper refers to the security of EPS by means of the word ”safety”, which according to widely accepted definition given by the North American Electric Reliability Council (NERC) means *the ability of the bulk power electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system components*. IEC definitions of an EPS security are given in Annex 1.

Generally speaking, if all generators connected to an EPS work synchronously and the voltage and the frequency in the EPS are within the required limits, then this is a normal, stable state of an EPS. In case of sudden disturbances, e.g. sudden increase of the load or switching off an important transmission line due to a failure in a substation computer control or protection system, the stable state of operation is disturbed. Each EPS is designed with a certain stability margin. When the disturbance is greater than the stability margin it results in loss of stability and collapse of the EPS, which may be partial or total, and this is called a blackout. The loss of stability is understood in the sense applied in dynamical systems, it means generators connected to the EPS fall-out of synchronism (see also definition of the term “Electric Power System frequency” in Annex 1). This causes an emergency shutdown of the generators by automatic protection devices to protect them against destruction and emergency stop of the power stations. Economic and social consequences of the loss of stability by an EPS are always very serious and can be catastrophic. Thus maintaining stability of an EPS is the main requirement for the EPS planning, operation and control. Risk for stability is equivalent to risk for safety of an EPS.

In publication A.16 it was stated that major blackouts are rare events but their impact can be catastrophic. However, statistics show that the events are not so rare. According to the data published by CIGRE (Conference Internationale des Grands de Reseaux Electriques a Haute Tension) [C.5] numbers of serious power outages outside of the USA in the period 1978-1985 are as follow (see Table 1).

Table 1. Numbers of serious power outages outside of the USA in the period 1978-1985

Years	1978	1979	1980	1981	1982	1983	1984	1985
Number of failures	1	2	2	3	1	5	5	5

The Northeast Blackout of 1965 left about 30 milion people and 207 km^2 in Ontario, Canada, and United States without electricity for up to thirteen hours [C.25, C.26, C.27, C.28]. The New York City blackout of 1977 blacked out the city for 23 hours [C.29]. Losses resulted from the electricity failure were estimated at 310 millions USD. The 2003 North America blackout, the largest blackout in North American history, affected 10 million people in Ontario, Canada and 40 million people in eight U.S. states. The financial losses related to the outage were estimated at $6 billion [C.30]. Data on the 2003 London Blackout, together with links to National Grid's report on the blackout and to media coverage, are available in [C.31]. UCTE Final Report on the 28 September 2003 blackout in Italy is available in [C.32]. A list of famous wide-scale power outages is given in [C.24]. The last large system failure in Poland occurred in January 1987. As a result of this failure north-eastern Poland was without electricity.

Losses of large outages are great. But even in case of minor outages, for example in case of 1000 MW outage resulted in an EPS failure, i.e. rather little outage, financial loses caused by cost of interruption only can amount 4.69 millions USD [A.21, A.22]. The restart of an industrial plant after occurring of an outage with duration time longer than critical one lasts on average 17.4 hours [B.1].

The Great Northeast Blackout, which started 9 November 1965 at approximately 5:16 p.m., in that time it was the largest blackout in history and the first shock event in the electricity industry that influenced the development of modern power systems control and operation. Later that day, in the Memorandum of 9 November 1965 addressed to the chairman of the Federal Power Commission, President Lyndon Johnson wrote [C.25, C.26]:

> *"Today's failure is a dramatic reminder of the importance of the uninterrupted flow of power to the health, safety, and well being of our citizens and the defense of our country.*
>
> *This failure should be immediately and carefully investigated in order to prevent a recurrence.*
> *You are therefore directed to launch a thorough study of cause of this failure. I am putting at your disposal full resources of the federal government and directing to the Federal Bureau of Investigation, the Department of Defense, and other agencies to support you in any way possible. You are to call upon the top experts in our nation in conducting the investigation.*
>
> *A report is expected at the earliest possible moment as to the causes of failure and the steps you recommend to be taken to prevent a recurrence.*
>
> *Lyndon B. Johnson"*

Many organisational and technical initiatives were undertaken to avoid such failures in the future.

In the history of the electric power industry, safety as it is understood today is a relatively recent concept, which emerged after this blackout. In paper [A.2] is given that possibly the first mention in publications of "safety" in its present sense was in the *Proceedings of The Second Power Systems Computation Conference* in 1966. Before this event the term "safety" was not used and the safety of an EPS was subsumed with its reliability and implemented into the system in the system planning process by providing a robust system that could withstand any "credible" sudden disturbances without a serious disruption. Author of the paper [A.2] made the remark that perhaps the epitome of this approach was mid-century American Electric Power system, which in 1974 withstood five simultaneous major tornadoes, losing eleven 345 kV lines, one 500 kV line, two 765 kV lines, and three major switching substations, without interruption of service to customers. The author concluded that such practices even if technically feasible were no longer considered economically or environmentally feasible.

The large failure of 1965 shows a need for safe operation of an EPS. It evidenced inadequateness of dynamical models used at that time and envisaged a need for the on-line control and monitoring. The New York City blackout of 1977 is considered in publications the second

shock event that happened in spite of the major advances in security and emergency control made after the blackout of 1965 and shows that there is need to look deeper into electric power systems safety assessment and enhancement. The focus of the safety concept was shifted from an EPS robustness, which was designed into the system at the planning stage, onto risk aversion, which is based on automatic protection and control devices, and still to a considerably degree on intervention of a system operator in real time in an emergency state.

The following unique physical features of EPSs cause that safe operation and ensuring continuity of electricity supply to customers is very difficult:

- Dispatched power must be equal to the power demand in every moment. At present there is no possibility for accumulation of large amount of electrical energy disposable without delay.
- Differently than in any other infrastructure, for example in telecommunication infrastructure, it is practically impossible to plan the way of electricity flow in power grid with the aim, for example, to maintain continuity of electricity supply to selected customers. Electricity flows according to the physical laws not according to contracts.
- If an EPS is not carefully planned and operated it is very easy to trigger a cascading effect that leads to a great power system failure. For example tripping a line by protection devices can cause overload remaining line/lines in the grid, because of changing the way the electricity flows, and consequently tripping the overloaded line/lines by protection relays. This causes further change of the way the electricity flows with possible further tripping of an overloaded line/lines and cascading development big EPS failure or even totally collapse of the EPS. In EPSs all lines, transformers, generators, etc. are protected by protection devices that operate within fraction of a second or – very rarely - a few seconds at the most. Therefore a very simple event that causes tripping an EPS element by protection devices can initiate very serious power system failure. The Northeast Blackout was initiated by protective relay (set too low) that triggered cascading development the outage.

4. CURRENT STATE OF PRACTICE IN ASSURING CYBER SECURITY IN ELECTRIC POWER INDUSTRY

An extensive review of available publications made in the years 1995-1997 showed that there was almost complete lack of documentation of existing practice with reference to design, validation and commissioning of computer-based control systems applied in electric power sector, including applied methods and techniques for ensuring security of the systems. Opinions about problems related to testing and evaluation of such systems before their exploitation in practice were expressed since the beginning of 1970s [A.8]. But in spite of clear stating that problem there was very few information related to the methods of making the evaluation. Among several hundred papers which described different aspects of computer applications in HV and EHV substations, only a few publications contained some comments and remarks about that problem [A.4, A.9, A.10, A.13, B.6] and very few about security of these systems [A.20]. Published by CIGRE guidelines [B.2] on a software project control for ensuring quality of telecontrol systems focusing on management of the project only and in insufficient way. The general image, which emerged from this review, was that issues of functionality were dealt with only and not of dependability.

Information about Enterprise Information Security (EIS) Project coordinated by the Electric Power Research Institute (EPRI), published at the first period of the project started in the year 2000, confirmed to some extend the image. This information contained among other things a statement that computer-based systems applied in electric power sector have never been designed with security as an important feature implemented into the systems in the process of these systems design. There is significant number of security tools and methods for networks, servers, PCs and other elements of IT however, in most cases, these tools and methods have not been applied in industry, as power plant or substation computer-based control systems, and it is not clear whether they are adequate and effective for these non-IT systems. It also contained a statement that information security and vulnerabilities of real time systems are not widely understood by either IT or the operational organizations, including end-users and vendors or even the research community including universities.

During the last years a number of papers on security of computer real-time systems applied in EPSs have been published and made available on websites. This is connected with critical infrastructures protection programmes applied in many countries. Also security standards and guidelines for the electricity sector have been published as well as some cyber security requirements and guidance have been included into international standards [B.3, B.4, B.5, B.7]. The research and developments on ensuring security of electricity infrastructure are most advanced in the United States and most of available publications on security issues in electric power industry have been published in the US and concern US electric power industry or development of fundamentals for better understanding the complex infrastructure.

The largest number of technical papers published in journals, conference papers, technical reports and other materials on electric power infrastructure protection against cyber threats are available on the following websites: Electric Power Research Institute (EPRI) [C.18], International Institute for Critical Infrastructures (CRIS) [C.20], and Schweitzer Engineering Laboratories [C.22]. Slides from presentations at the EU workshop *Power Security '05* and the workshop report are available at [C.19].

North American Electric Reliability Council (NERC) has developed *Security Guidelines for the Electricity Sector* and a cyber security standard that outlines minimum requirements

needed to ensure the security of electronic exchange of information needed to support grid reliability and market operations. Both these documents are available at NERC webpage [C.21].

On EPRI website there is some information on EPRI and U.S. Department of Defense University research program *Complex Interactive Networks/Systems Initiative (CINSI)* that involved academic researches and experts from 26 leading US universities. The aim of the initiative was to enable critical infrastructures to adapt to a broad array of potential disturbances, including terrorist attacks, natural disasters, and equipment failures. The primary focus of this advanced research program was fundamental understanding of complex interactive systems or development of agent technology to control such systems [A.7].

On EPRI website there is also some information on the Infrastructure Security Initiative (ISI), a research program carried out by EPRI together with electric utility industry centred on the following four major program areas that were assigned the highest priority by representatives of member companies and other industry participants:

1. Vulnerability Assessment (VA)
2. Strategic Spare Parts Inventory
3. "Red Team" Attacks
4. Secure Communications

Research in this program was coordinated with ongoing efforts of the North American Electric Reliability Council (NERC), industry trade associations, the U.S. Department of Energy (DOE), and the Office of Homeland Security [C.18].

5. THE ELECTRIC POWER SUBSTATION CASE STUDY

5.1. Description of the case study

The electric power substation cyber security case study was carried out in the years 2000 - 2003 as a continuation of the safety case study that was carried out from1995 to 1997 as part of the EU joint research project *Integration of Safety Analysis Techniques for Process Control Systems (ISAT)*. The aim of the safety case study was the safety analysis of software interlocking applied in substation control system for assuring safety of switching operations which is carried out in the phase of requirements specification. The requirements were specified for 400kV 'Mosciska' substation in Warsaw (Poland) treated as an exemplary extra-high voltage substation. The 'Mosciska' substation is a new substation, built in the middle of the 1990s, which constitutes an important node of the grid supplying energy to Warsaw.

The case study concerned the software interlocking system applied for mutual interlocking disconnectors, circuit breakers and earthing switches to avoid consequences described in Section 3.2. that is to ensure safety of switching operations carried out in the substation during operation and maintenance. The interlocking system must for example block the opening of a disconnector when circuit breaker interlocked with the disconnector is closed, or closing an earthing switch (e.g. earthing switch Q45 in Figure 5) when the circuit breaker interlocked with the earthing switch (Q19 in Figure 5) is closed, etc. All these requirements are described by the following basic safety-oriented interlocking rules:

(1) load flows must not be switched on or off by disconnectors;
(2) live nodes must not be grounded;
(3) when connecting live nodes the synchronisation conditions must be fulfilled (this rule was not considered in the case study).

Normally such a software interlocking system consists of:

- auxiliary contacts of disconnectors, circuit-breakers and earthing switches which transmit information about the status of main contacts to the computer system (closed or open);
- auxiliary relays, used for the control of switch drives (coils of these relays are connected to the outputs of the computer system, whereas contacts are connected to control circuits of the switch drives);
- wiring system,
- intelligence of the software interlocking system implemented into the target system software.

The intelligence of the interlocking system can include for example:

- the above mentioned safety oriented interlocking rules;
- ability to tolerate a predefined set of failures;
- security or dependability requirements, etc.

The 'Mosciska' substation consists of two busbar systems and eight bays. The case study focused on the bay number 1, to which the line to 'Milosna' substation is connected. A simplified electrical diagram of the bay is shown in Figure 5. The idea how the bay switching devices are controlled by substation control system is shown in Figure 6. All the substation bays are identical and to some extent typical for all extra-high voltage substations in Poland.

The assumed approach to the safety analysis in the safety case study was the same one, which is assumed when a new system is being designed. The starting point was a concept of a target system that would control a considered bay and its definition by a specification of requirements, including safety requirements for a considered interlocking system whose software would be implemented into the target system. Then a system model based on the specification of requirements was designed, and used to analyse the contribution of predefined set of failures, identified constraints (e.g. time constraints), and human factors to the identified hazards. So one can consider that the case study corresponded with first four phases of the Overall Safety Lifecycle in the IEC 61508 standard, namely: (1) Concept; (2) Overall scope definition; (3) Hazard and risk analysis; (4) Overall safety requirements.

The description of the safety case study is given in [A.21] (full description), [A.1, A.22, A.24]. Object oriented models of the bay and results of safety analysis regarding the methods applied during safety analysis are presented in [A.14]. Description of the security case study is given in [A.23].

The electric power substation cyber security case study is considered as a pilot case study and is limited to:
- one kind of functions performed by a computer control system in an EHV substation, namely to software interlocking applied for assuring safety of switching operations controlled by the substation computer control system, and
- one line bay of the substation.

The specification of requirements for the security case study is based on the specification of requirements for the safety case study and results of the case study made within the EU Copernicus Project ISAT and published in the reports [A.20, A.21, A.1]. Full description of the substation bay for the cyber security case study is in [A.23].

The aim of the cyber security pilot case study is to elaborate an example of approach to determination of required level of cyber security and means for assuring the required cyber security level taking into account existing state of the art in this field, including law aspects, existing standards, and technical means.

Examples of problems that, as it was expected, the case study could illustrate are following:
- methods, techniques and tools for risk analysis, including selection of the most appropriate methods and techniques;
- security requirements specification;
- security safeguards that could assure required level of security, including hardware and software security features, operating procedures, security policy, etc.;
- interaction of safety and security requirements;
- methods and techniques for verification of solutions, e.g. for demonstration that applied protective measures can ensure required cyber security level;
- application of existing standards, guidelines, and good practices.

5.2. Final remarks

The case study is not finished and detailed results that could illustrate above problems are not available. General remarks that can be formulated on the basis of the safety case study are the following.

Strict specification of possible consequences in cyber security risk analysis for the considered EHV substation would require full analysis of possible consequences for the whole EPS and the monitoring of possible influence of interconnected EPSs of neighbouring countries and all interdependencies between other infrastructures. Such an analysis has never been carried out in Poland, because in fact such a need rather did not exist. In Poland, the national electric power system has existed only since the beginning of the 1960s (in other countries, germs of first national electric power systems came into being as early as in the 1930s). At the initial period development of electric power industry, there were separated power stations and local systems. Since the 1960s, the EPS in Poland and coupled with it data transmission network have become more and more complex.

In the safety case study it became clear that such full analysis is very difficult or even impossible, because risks in the substation would depend very much on the current situation in the EPS and any other approach must be taken to this problem. For example in the normal state of the EPS switching off a line by a disconnector may cause only destruction of the disconnector and short circuit which would be turned off by the substation protection system. In case of for example shut-down a certain number of power stations (e.g. coal shortage because of severe winter) the same threat may also cause a serious consequence for the EPS, that is a blackout. One of the reasons for the above-mentioned situation is that in spite of the fact that location of the substation in question has not changed, the grid to which the substation is connected has changed. This issue is one of the issues of the CINSI program [A.7].

During the realisation of the safety case study, it has turned out that the existing data on failures of substation components, breakdowns and accidents at substations, and large failures of the national EPS, were insufficient to ensure in an efficient way in the design stage required quality of safety- and security-related systems applied in the EPS. The data on failures of substation components used for traditional relay-based control systems design were insufficient. There were available certain data in foreign publications but they could be used only in a limited way, just to estimate roughly, because each national system has got its own characteristic formed by its history.

In Poland the rules on validation and commissioning of the systems have not been published. In traditional relay-based technology the dependability attributes of computer-based systems were not considered except for reliability. And if they were (like reliability), they were considered in a very simple qualitative manner and rather intuitively. Therefore, requirements for these attributes were not articulated, and assumption of input data for these attributes has also created substantial difficulties. They were assumed roughly on the basis of foreign publications.

The similar remark refers to the lack of analysis of hazards of the whole national EPS and its interdependencies with other infrastructures. The now existing EPSs have been evolving for many years based on another concept of its reliability assurance. Also they have never been designed for the free market of electricity. Hence, in present completely different conditions and with another concept of reliability assurance, their behaviour is to some extent unknown. It has been confirmed to some extend by a study of significant disturbances made in the USA. From the study it follows that relays of EPS protection systems were in one way or another involved in 75% of major disturbances which took place in the USA between 1984 and 1988. A common scenario of these disturbances was that a relay (or a protection system) had an „hidden defect” not detected during normal operation, calibration or maintenance that was

exposed due to conditions created by other disturbances (e.g. nearby faults, overloads, or reverse power flows) [A.16]. The example is given that on December 14th, 1995, a fault occurred on a 345 kV line in southern Idaho, which tripped correctly, followed by an incorrect trip of a parallel line and an overload trip of a third line. As a result:

– the system became unstable and divided into four system islands;
– 3 000 MW load was disconnected.

Similar situation could for example be caused by an incorrectly performed switching operation in a substation. However, as it was mentioned above, results of this study can not be applied to the Polish EPS directly, because the US EPS, similarly like EPSs of other countries, has to some extend different characteristic developed in the historical process of the US electric power industry development from the last decades of the 19th century.

6. REFERENCES

A. Papers

[A.1] Babczynski T., Borgosz-Koczwara M., Zurakowski Z., *Specification of Requirements for Extra-High Voltage Substation Software Interlocking Case Study Using i-Logix STATEMATE*, TR ISAT 97/12. Institute of Power Systems Automation, Poland, April 1997.

[A.2] Balu N., Bertram T., *et al.*, *On-Line Power System Security Analysis.* Proceedings of the IEEE, Vol. 80, No. 2, pp. 262-280, 1992.

[A.3] *Defending America's Cyberspace, National Plan for Information Systems Protection,* Version 1.0, An Invitation to a Dialogue, The White House, 2000 (http://www.iwar.org.uk/cip/index.htm).

[A.4] *Design and maintenance practice for substation secondary systems,* CIGRE Working Group 23.05 Tech. Rep., April 1994.

[A.5] Dolezilek D. J., *Power Systems Automation*, Schweitzer Engineering Laboratories, Inc., Pullman, WA, USA (http://www.selinc.com/techpprs.htm).

[A.6] Dy Liacco T., *The Adaptive Reliability Control System*, IEEE Transactions on Power Apparatus and Systems, vol. 85, No. 5, May 1967.

[A.7] Haase P., *Of Horseshoe Nails and Kingdoms: Control of Complex Interactive Networks and Systems*, EPRI Journal (EPRI Journals are available at http://www.epri.com/).

[A.8] Johnson W.A., Bouchey S.H., *Commissioning Experience and Operating Evaluations of a Consolidated Control Centre Responsible for the Generation, Transmission, and Distribution Systems Serving the Washington, D.C. Metropolitan Area*, International Conference on Power System Monitoring and Control, 24 – 26 June 1980.

[A.9] Labrouhe de G., *Computer-based systems for transmission substations*, Power Technology International, pp. 73-76, 1996.

[A.10] Lilley R.A., Xampeny J., Magnusson B., *The Overall Impact of Digital Techniques for Transmission Systems* (*Substation Control*), Working Group 06, Paris, CIGRE Technical Brochure, No. 19, 1987.

[A.11] Luiijf H.A.M., Klaver M.H.A., *In Bits and Pieces – Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society*, March 2000 (http://www.tno.nl/defensie_en_veiligheid/producten_en_diensten/beleidsstudies/veiligheid/information_operations/downloads_papers/).

[A.12] *Making the nation safer: the role of science and technology in countering terrorism.* Committee on Science and Technology for Countering Terrorism, National Research Council of the National Academies. The National Academies Press, Washington, 2002.

[A.13] Martin O., Messie M., and de Labrouhe G., *The digital monitoring and control of substations,* in Proc. CIGRE Conf., paper no. 23/13-02, 1994.

[A.14] Nowicki B., Górski J., *Object Oriented Safety Analysis of an Extra High Voltage Substation Bay.* In Proceedings of the 17th International Conference SAFECOMP'98. Lecture Notes in Computer Science, Vol. 1516. Springer-Verlag, Berlin Heidelberg, pp. 306-315, 1998.

[A.15] Oman P., Schweitzer E.O., and Roberts J., *Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusions*, Schweitzer Engineering Laboratories, Inc., Pullman, WA, USA (http://www.selinc.com/techpprs.htm).

[A.16] Phadke A.G., Thorp J.S., *Expose Hidden Failures to Prevent Cascading Outages*. IEEE Computer Applications in Power, pp. 20-23, July 1996.

[A.17] President's Commission on Critical Infrastructure Protection (PCCIP) Report, *Critical Foundations: Protecting America's Infrastructures*, October 1997 (http://www.ciao.nrc.gov/ default.htm).

[A.18] Stagg G.W., Adibi M., Laughton M., Van Ness J. E., Wood A. J., *Thirty Years of Power Industry Computer Applications*, IEEE Computer Applications in Power, April 1994.

[A.19] Wenger A., Metzger J., Dunn M. (ed.), *The International Critical Infrastructure Protection Handbook*. Center for Security Studies and Conflict Research Swiss Federal Institute of Technology, Zurich, November 2002 (http://www.isn.ethz.ch/ crn).

[A.20] Zurakowski Z.: Task A2: *Review of Standards and Current Practices: Review of Dependability in EHV Substations*. EC JRP CP94 1594 ISAT, Technical Report TR ISAT 97/20, Institute of Power Systems Automation, Poland, April 1997.

[A.21] Zurakowski Z.: Task B1b: *Identification and Preparation of Case Studies – Extra-High Voltage Substation Software Interlocking Case Study*. EC JRP CP94 1594 ISAT, Technical Report TR ISAT 97/8, Institute of Power Systems Automation, December 1996, Updated: February and April 1997.

[A.22] Zurakowski, Z., *Safety and Security Issues in Electric Power Industry*. Proceedings of the 19th International Conference SAFECOMP 2000, Rotterdam, The Netherlands, October 2000.

[A.23] Zurakowski Z., *Power Substation Case Study*, EWICS TC7 document WP5065/1, January 2001.

[A.24] Zurakowski Z., *Functional Safety in Electric Power Sector*, SIPI International Workshop on Functional Safety IEC 61508, Gdynia, Poland, 28-29 May 2003 (available in 'SIPI Technical Data Resource' page at http://www.sipi61508.com/).

B. Standards and guidelines

[B.1] ANSI/IEEE Std 493-1990: *IEEE Recommended practice for the design of reliable industrial and commercial power systems*, May 1995.

[B.2] *Guidelines for software project control*, CIGRE Working Group 01 of Study Committee 35 Tech. Rep., August 1994.

[B.3] IEC 60870: *Telecontrol Equipment and Systems*, Parts 1-6, 1988-2002.

[B.4] IEC 61850: *Communication Networks and Systems in Substations.* Parts 1-9, 2002-2004.

[B.5] IEEE Std 1402-2000: *IEEE Guide for Electric Power Substation Physical and Electronic Security*, IEEE, April 2000.

[B.6] Schütte H.G., et al., *General Guidelines for the Design of Outdoor A.C. Substations*, Working Group 04, Paris, CIGRE Technical Brochure, No 69.

[B.7] *Security Guidelines for the Electricity Sector*, Version 1.0, June 14, 2002

(http://www.nerc.com/cip.html).

[B.8] *UCTE Operation Handbook*, Union for the Co-ordination of Transmission of Electricity, June 2004 (http://www.ucte.org/ohb/cur_status.asp).

C. Web sites

General information on current activities connected with CIP

Canada

[C.1] Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (www.ocipep-bpiepc.gc.ca).

Germany

[C.2] Bundesamt für Sicherheit in der Informationstechnik (BSI) http://www.bsi.bund.de/fachthem/kritis/kritis_e.htm.

[C.3] Arbeitskreis Schutz von Infrastrukturen/German Group on Infrastructure Protection (AKSIS) www.aksis.de (only in German).

EU

[C.4] Analysis and Assessment for Critical Infrastructures Protection (ACIP) (www.iabg.de/acip/index.html).

International and others non-governmental

[C.5] International Council on Large Electric Systems (CIGRE) (http://www.cigre.org)

[C.6] European Workshop on Industrial Computer Systems, Technical Committee 7 on Reliability, Safety and Security (EWICS TC7), System Security Subgroup (http://www.ewics.org/docs/system-security-subgroup).

[C.7] IWS - The Information Warfare Site: Critical Infrastructure - Essential Documents (http://www.iwar.org.uk/cip/index.htm).

Netherlands

[C.8] TNO-FEL Critical Infrastructures Protection page (http://www.tno.nl/instit/fel/div2/prj/critical-infrastructure-protection.html).

New Zealand

[C.9] Centre for Critical Infrastructure Protection (www.ccip.govt.nz).

Switzerland

[C.10] Swiss Federal Institute of Technology (ETH) www.isn.ethz.ch/crn/.

UK

[C.11] National Infrastructure Security Co-ordination Centre (NISCC) (www.niscc.gov.uk).

USA

[C.12] Critical Infrastructures Assurance Office (CIAO) (http://homelandsecurity.tamu.edu/framework/dhls/iaip/ciao).

[C.13] Homeland Security, Threats and Protection, Critical Infrastructure (http://www.dhs.gov/dhspublic/display?theme=31).

[C.14] Institute for Information Infrastructure Protection (I3P) (www.thei3p.org).

[C.15] National Infrastructure Protection Center (NIPC) http://homelandsecurity.tamu.edu/framework/dhls/iaip/nipc/)

[C.16] National Security Telecommunications Advisory Committee (NSTAC) http://www.ncs.gov/nstac/nstac.html

[C.17] The Infrastructure Security Partnership (TISP) (http://www.tisp.org/).

Electric Power Infrastructure Protection

[C.18] Electric Power Research Institute (EPRI), Infrastructure Security Initiative (ISI) (http://www.epri.com/corporate/initiatives/infrastructure_security_initiative.asp).

[C.19] EU Workshop - "The Future of ICT for Power Systems: Emerging Security Challenges" held in Brussels, 3-4 February 2005 (https://rami.jrc.it/workshop_05).

[C.20] International Institute for Critical Infrastructures (CRIS) (www.cris-inst.com).

[C.21] North American Electric Reliability Council (NERC) Critical Infrastructure Protection web page at http://www.nerc.com/cip.html.

[C.22] Schweitzer Engineering Laboratories, Inc. (http://www.selinc.com/techpprs.htm).

[C.23] The Center for SCADA Security (http://www.sandia.gov/scada/home.htm).

Famous Blackouts

[C.24] A list of famous wide-scale power outages (http://en.wikipedia.org/wiki/List_of_power_outages).

[C.25] The Great Northeast Blackout of 1965 (http://www.cmpco.com/about/system/blackout .html).

[C.26] Northeast Power Failure: November 9 and 10, 1965. U.S. Federal Power Commission Report, 6 December 1965, Washington, DC: U.S. Government Printing Office (http://www.blackout.gmu.edu/archive/pdf/fpc_65.pdf).

[C.27] The Blackout History Project – 1965 Blackout (http://www.blackout.gmu.edu/archive/a_1965. html#friedlander_76).

[C.28] Life Magazine, Vol. 59 No. 2, 19 November 1965 (issue dedicated to the 1965 Northeast Blackout of 1965) (http://www.blackout.gmu.edu/archive/a_1965.html).

[C.29] New York City blackout of 1977 **(**http://en.wikipedia.org/wiki/New_York_City_Blackout_of_1977).

[C.30] 2003 US Canada blackout (http://en.wikipedia.org/wiki/2003_U.S.-Canada_blackout).

[C.31] 2003 London Blackout (http://en.wikipedia.org/wiki/2003_London_blackout). National Grid's report on the blackout available at http://www.nationalgrid.com/uk/library/documents/pdfs/London28082003.pdf

[C.32] UCTE Final Peport of the Investigation Committee on the 28 September 2003 Blackout in Italy, UCTE, April 2004 (available at http://www.ucte.org/publications/library/e_default_2003.asp#id).

ANNEX 1: ABBREVIATIONS AND KEY TERMS

A. List of abbreviations

CIP - Critical Infrastructure Protection

CIIP - Critical Information Infrastructure Protection

EPS - Electric Power System

EHV - Extra-High Voltage (in Poland it relates to substations 220 kV and above)

HV - High Voltage (in Poland it relates to substations from 1 kV to 110 kV)

RTU - Remote Terminal Unit

SCADA - Supervisory Control And Data Acquisition System

B. Key terms

Bay (of a substation) - a part of a substation containing switching and control devices (also called switchgear and controlgear) designed for an electrical supply line, transformer, etc. connected to busbar of the substation. If it is a bay for line it is called line bay, if it is bay designed for transformer, it is called transformer bay, etc. These parts of a substation may be managed by devices with the generic name "bay controller" and have protection systems called "bay protection". The concept of a bay is not commonly used all over the world. The bay level represents an additional control level below the overall station level

Blackout – an unintentional total loss of the electricity supply to an area.

Busbar - electric conductor of very low electrical impedance that serves as a common connection for individual electric circuits (e.g. electrical supply lines).

Critical Infrastructure Protection (CIP) - includes cyber and physical measures to secure the systems [A.19].

Critical Information Infrastructure Protection (CIIP) - is a subset of CIP and focuses on the protection of information technology systems and assets, such as telecommunications, computers/software, the Internet, satellites, fibre optics, etc. and on interconnected computers and networks and the services they provide [A.19].

Circuit-breaker - mechanical device which is able to switch on, switch off and carry the currents in normal conditions as well as to switch on, switch off and carry the currents in other defined conditions (e.g. during short - circuits).

Computer control of substation bay - automatic execution of sequence of switching operations by a computer system which are necessary for normal activities within a substation (e.g. connecting a line to busbar, switching over lines from one busbar to another).

Disconnector (also called isolator) - mechanical device which is able to assure a safe isolating gap in an electrical circuit. Disconnector is able to switch-on and switch-off the circuit with very low currents, or when the voltages between the contacts are

negligible. It is also able to carry the currents in normal conditions and in abnormal conditions during defined period of time, e.g., during short-circuit. Switching off the current in operation of a substation (e.g. nominal load current) by means of a disconnector always leads to complete destruction of the disconnector, short-circuit, and often also to other consequences.

Electric Power System (EPS) – comprises all generation, consumption and network installations interconnected through the network [B.8]. The electric network consists of transmission and distribution networks composed of power lines and substations which are nodes of the networks. An EPS is integrated with telecommunication and telecontrol systems used for communication and transmission of data between power generating stations, substations and control centres for remote operation and remote real-time signalling, metering, control and fault protection. Currently development of these EPS telecommunication and telecontrol systems goes toward an integrated EPS telecommunication network.

Electric power system frequency – the system frequency *f* is a measure for the rotation speed of the synchronised generators. All generators in power stations connected to an EPS are synchronised and they must be synchronised before they are connected to an EPS. Power generated in an EPS must be maintained in constant equilibrium with power consumed (demanded). If power consumed increases the system frequency will decrease. The frequency deviation is initially influenced by the kinetic energy of all rotating generating sets and motors connected to the EPS. Regulating units must then perform rapid automatic action to re-establish balance between power demanded and generated. In European countries in normal conditions the system frequency (nominal system frequency) shall be equal 50 Hz (in US 60 Hz) and maintained within established limits.

Electric system losses – total electrical energy losses in the electric system. The losses consist of transmission, transformation, and distribution losses between supply sources and delivery points. The electric energy losses are mainly because of heating of transmission and distribution elements [B.8].

Event - change of state (status) of EPS or device in a discrete way.

Failure - an event that may limit the capability of EPS or a piece of equipment to perform its function(s).

Intelligent electronic device (IED) - is any electronic device (e.g. numeric Protection Relay, or multifunction electronic meter) incorporating one or more processors, with capability to receive, or send, data/control from, or to, an external source. An IED may have connection as a client or as a server or both with other IEDs [A.4].

Instrumentation and control (I&C) system – collection of devices that monitor, control, and protect the EPS. I&C device built using microprocessors are commonly referred to as intelligent electronic devices (IEDs) [A.5].

Power system automation – the act of automatically controlling the power system via automated processes within computers and intelligent I&C devices. The process relies on data acquisition, power system supervision, and power system control all working together in a coordinated automatic fashion. The commands are generated

automatically and then transmitted in the same fashion as operator initiated commands [A.5].

Power system control – sending command messages to a device to operate the I&C and power system devices. Traditional Supervisory Control And Data Acquisition Systems (SCADA) rely on operators to supervise the system and initiate commands from an operator console on the master computer. Field personnel can also control devices using front-panel push buttons or a laptop computer [A.5].

Power system supervision – computer processes and personnel supervise, or monitor, the conditions and status of the power system using acquired data, collected in the form of measured analogue current or voltage values or the open or closed status of contact points. Operators and engineers monitor the information remotely on computer displays and graphical wall displays or locally, at the device, on front-panel displays or a laptop computer [A.5].

Remote Terminal Unit (RTU) - a compact computer/communication system installed in a substation that acts in a SCADA system as an interface between the communication network and the substation equipment. Typically RTU performs the following functions:

- receive measurements data from the substation and transmits the data to the control centre;
- receives control command from the control centre and executes them in the substation (for example switching operations);
- performs local control independently or in coordination with the control centre.

Safety of an electric power system - in electric power engineering safety of an EPS is described by means of the word ”security” and the term power ***system security*** is used to mean “the ability of the bulk power electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system components.” This is the definition given by the North American Electric Reliability Council (NERC) and accepted by electric utilities.

IEC definitions of an EPS security are following:

security (of an electric power system) - ability of an electric power system to operate in such a way that credible events do not give rise to loss of load, stress of system components beyond their ratings, bus voltages or system frequency outside tolerances, instability, voltage collapse, or cascading.
NOTE 1 – This ability may be measured by one or several appropriate indices.
NOTE 2 – This concept is normally applied to bulk power systems.
NOTE 3 – In North America, this concept is usually defined with reference to instability, voltage collapse and cascading only.
(IEC Vocabulary at http://domino.iec.ch/iev/ iev.nsf/Welcome?OpenForm)

security (structural) - ability of a system to be protected from a major collapse (cascading effect) if a failure is triggered in a given component.
NOTE - Security is a deterministic concept as opposed to reliability which is a probabilistic concept.”
(IEC Glossary at http://dom2.iec.ch/terms/terms.nsf/welcome?OpenForm)

Substation - important node of an EPS, which make possible to change a configuration of a transmission or a distribution network in the EPS. A switching substation contains

busbar and termination of power lines connected to the busbar through switching devices used for switching on or off a line. In case of a transformer substation it contains also one or more transformers which enable for example to connect a line of a HV distribution network to an EHV transmission network. Normally a substation also contains control and protection devices for operation and protection of an EPS (e.g. short-circuit protection relays).

Supervisory Control And Data Acquisition System (SCADA) – consist of a computer system/systems (Master Station) located at the control centre, RTUs located at the power stations and substations, and communication network for data transfer between the RTUs and the Master Station. Depending on complexity of the power station or substation modern RTUs can itself be SCADA systems, called substation SCADA systems. The SCADA Master Station can also communicate with Master Stations in other control centres (more basic information can be found at [C.21]..

———