

Electric Power Systems Cyber Security

Zdzislaw Zurakowski
zz@pvd.pl

Outline

1. INTRODUCTION

2. STRUCTURE OF ELECTRIC POWER SYSTEMS

3. POSSIBLE CONSEQUENCES OF THREATS

- Consequences for power stations
- Consequences for substations
- Consequences for an electric power system

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

5. CONCLUSIONS

Introduction

Towards the end of the XX century Electric Power Systems (EPSs) emerged as the most critical infrastructure that is also considered the most vulnerable to physical and cyber attack.

Contemporary EPSs are very complex and highly technologically advanced systems. 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.

Information technology engineers and experts who deal with cyber security in critical infrastructures must at least to some extent understand the nature of these infrastructures, possible consequences of security breaches, etc.

Introduction

The aim of this presentation is to describe in a way comprehensible for all involved in critical infrastructure cyber security:

- physical and organisational structure of an EPS and the concept of an electric power system control;
- possible consequences connected with security breaches in an EPS;
- current state of practice in assuring cyber security in electric power systems.

Introduction

This presentation is based on:

- research carried out in the years 1995-1997 within the EU Joint Research Project *Integration of Safety Analysis Techniques for Process Control Systems (ISAT)*;
- research on cyber security a substation in transmission network carried out in the years 2000—2003 in the Institute of Power Systems Automation (IASE) in Wroclaw, Poland.

A part of the research carried out in the IASE Institute was done in co-operation with EWICS TC7.

Most issues included or mentioned only in this presentation are more extensively described in the EWICS TC7 Briefing Paper entitled *Electric Power Systems Cyber Security: Power Substation Case Study*.

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, 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.

Structure of electric power systems

An increasing tendency is (e.g. in Europe) to build up more and more strong connections between the separate EPSs in individual countries.

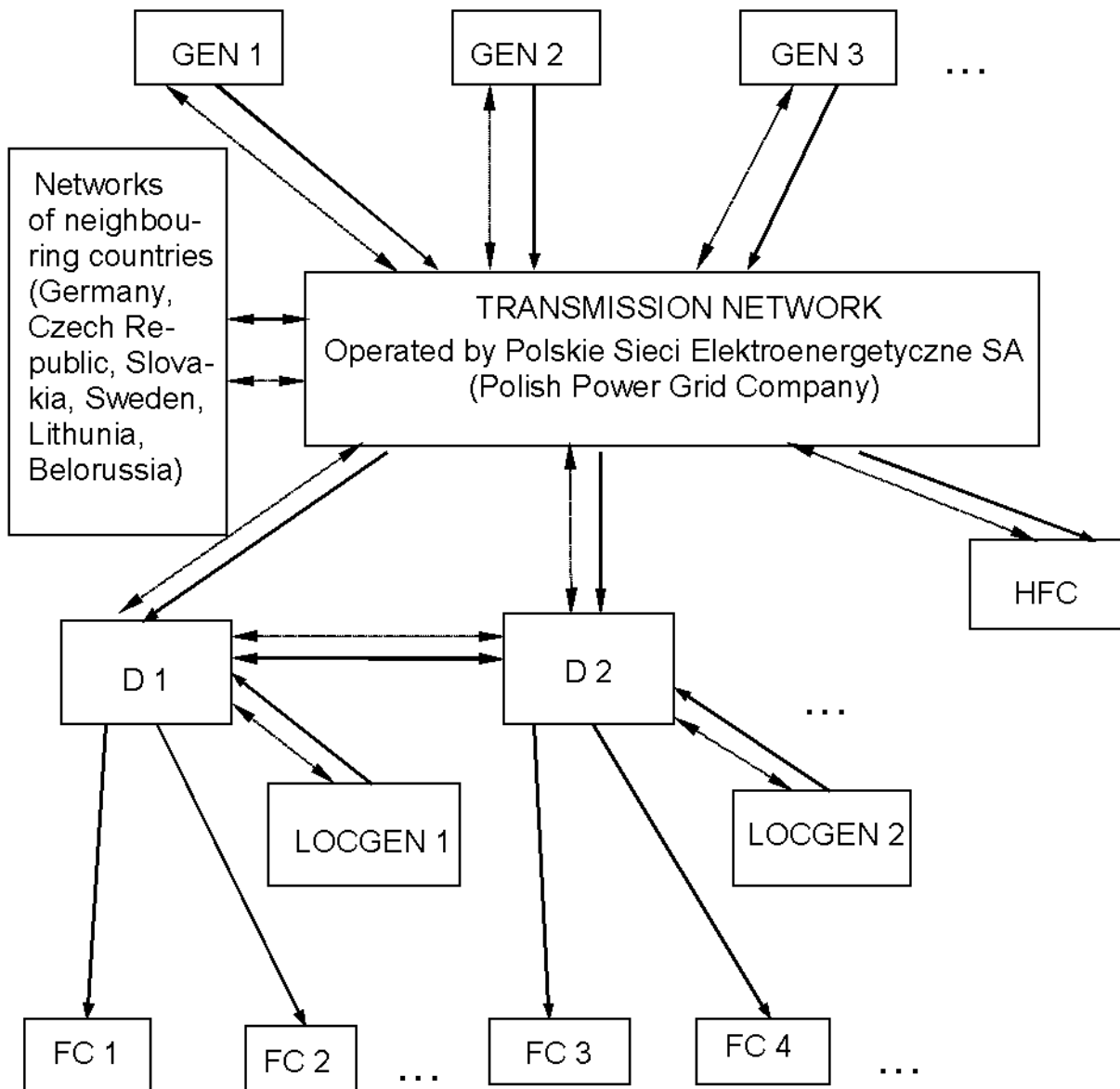
In the most general terms, an EPS can be partitioned into:

- generating stations;**
- transmission network, called Extra-High Voltage (EHV) network, which is used to transmit power from generating stations to main load centres;**
- 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.

Structure of electric power systems

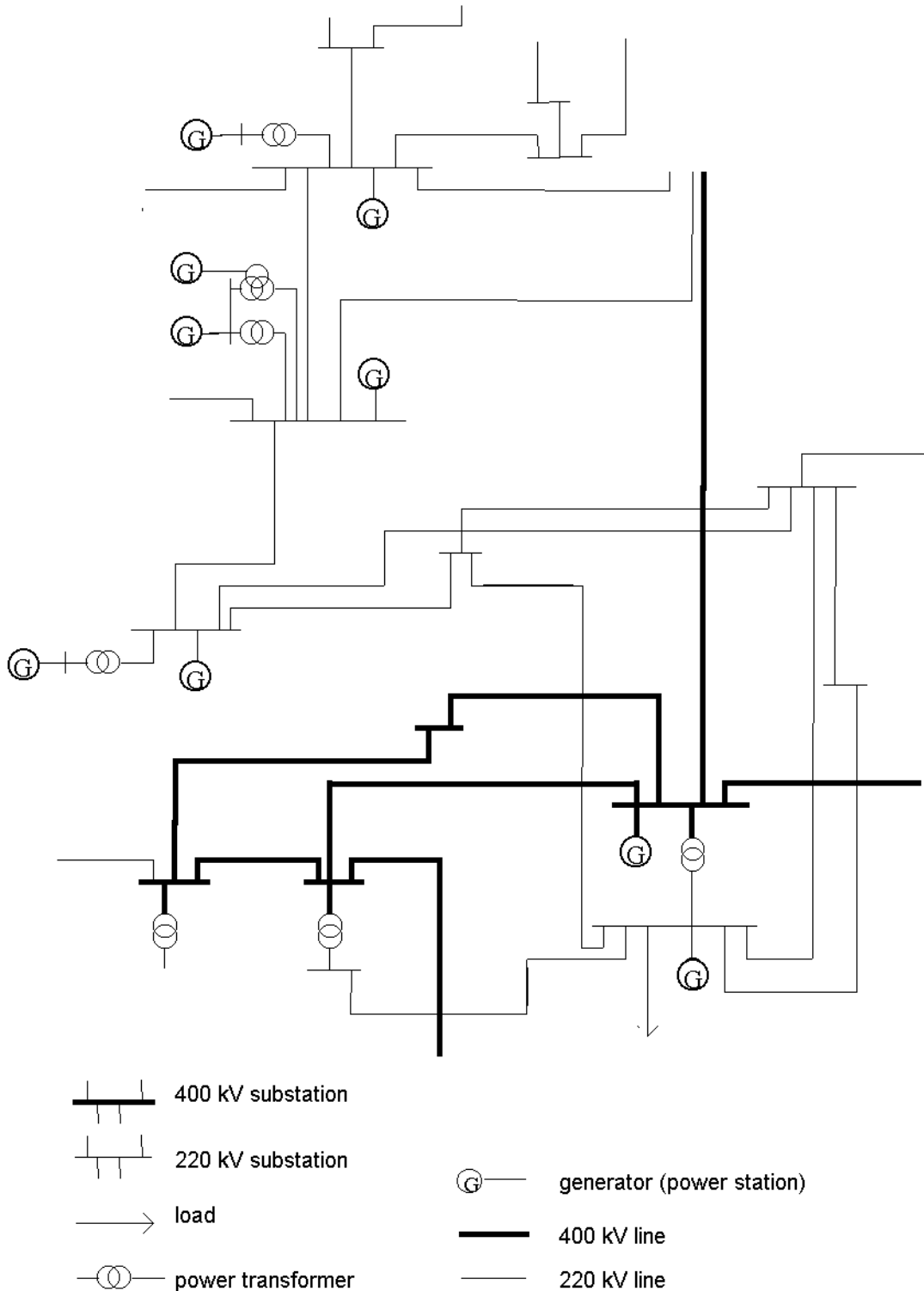
Approximate block diagram of physical and organisational structure of the Polish electric power system



———> - 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).

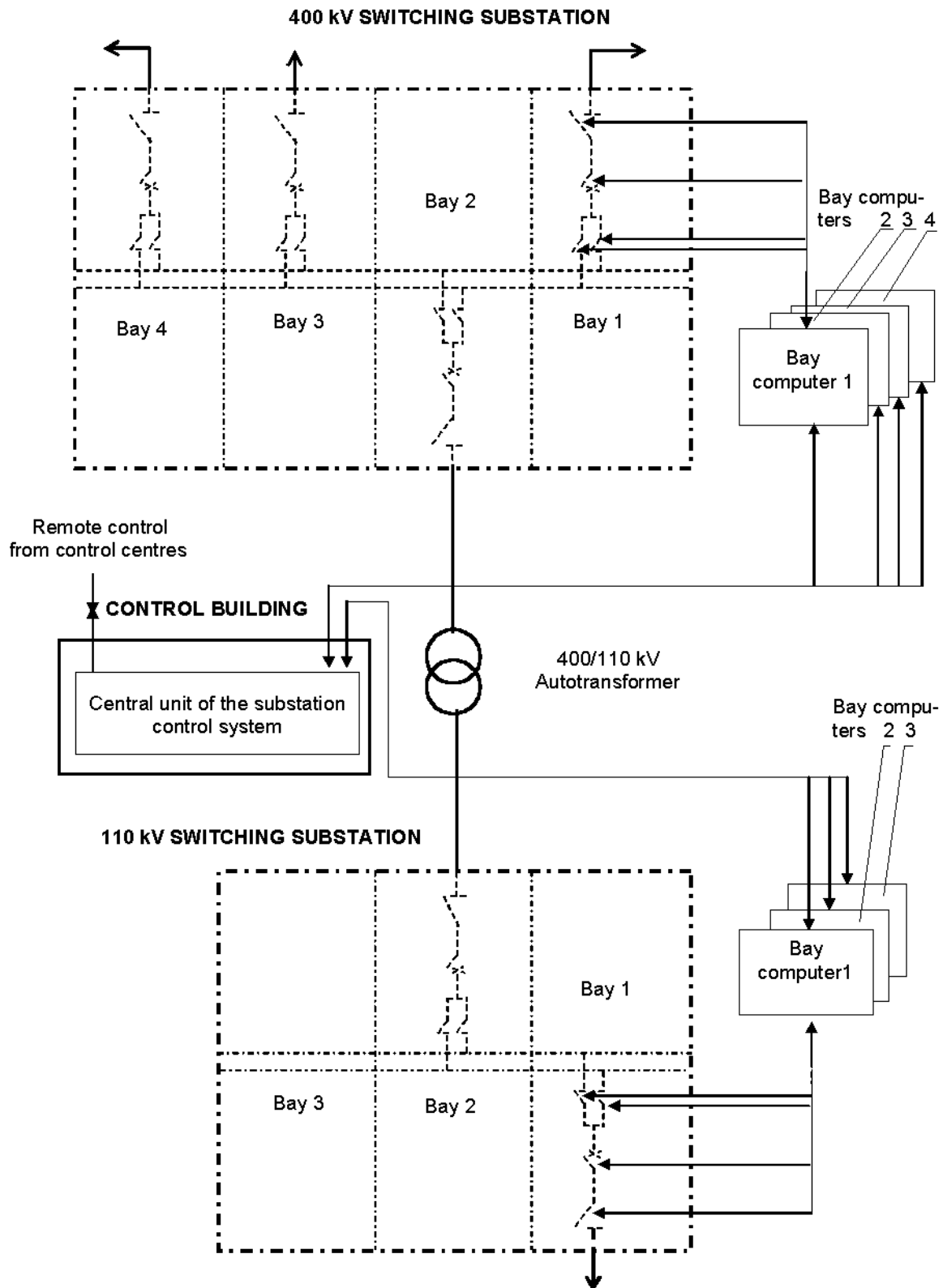
Structure of electric power systems

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



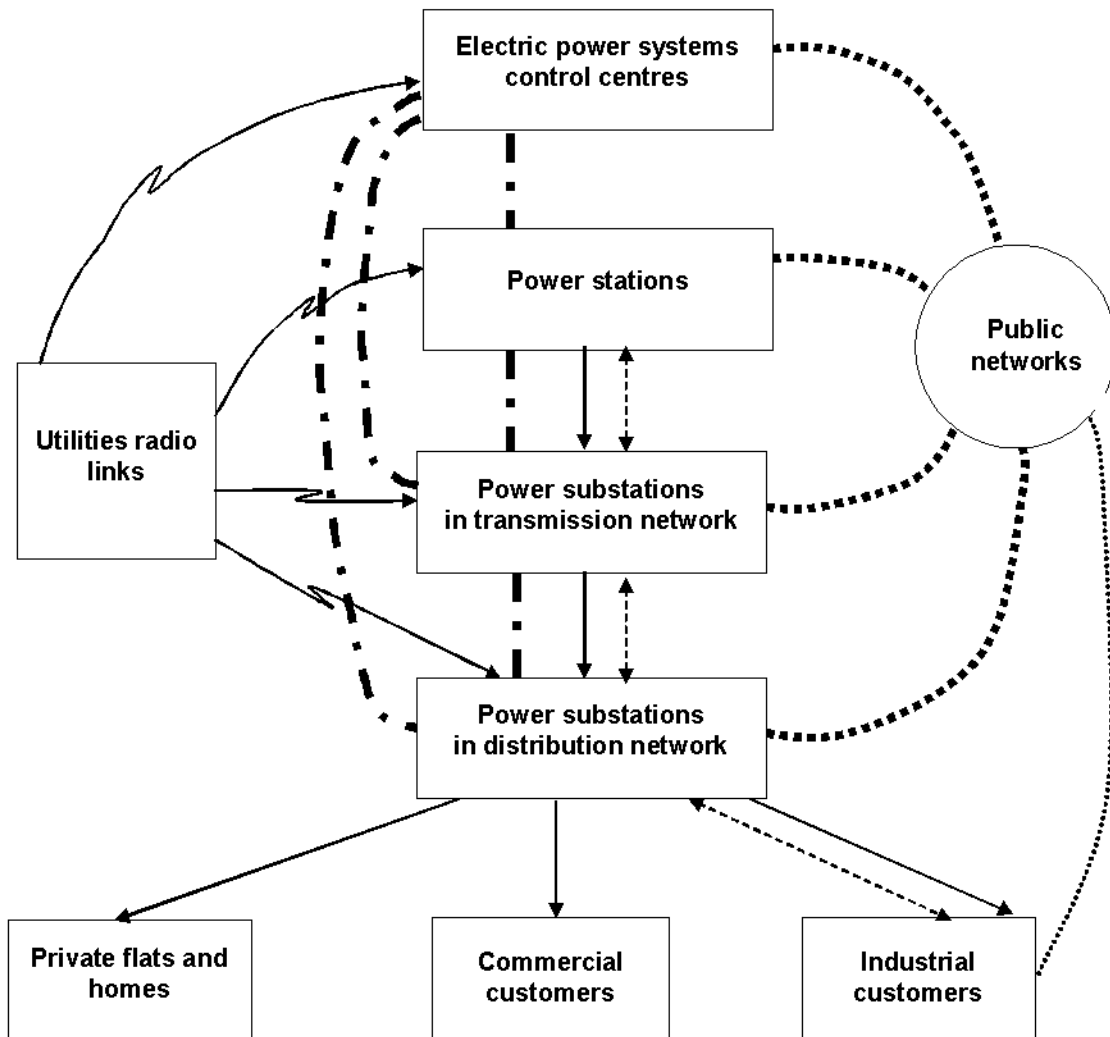
Structure of electric power systems

The concept of switching operations control in a substation



Structure of electric power systems

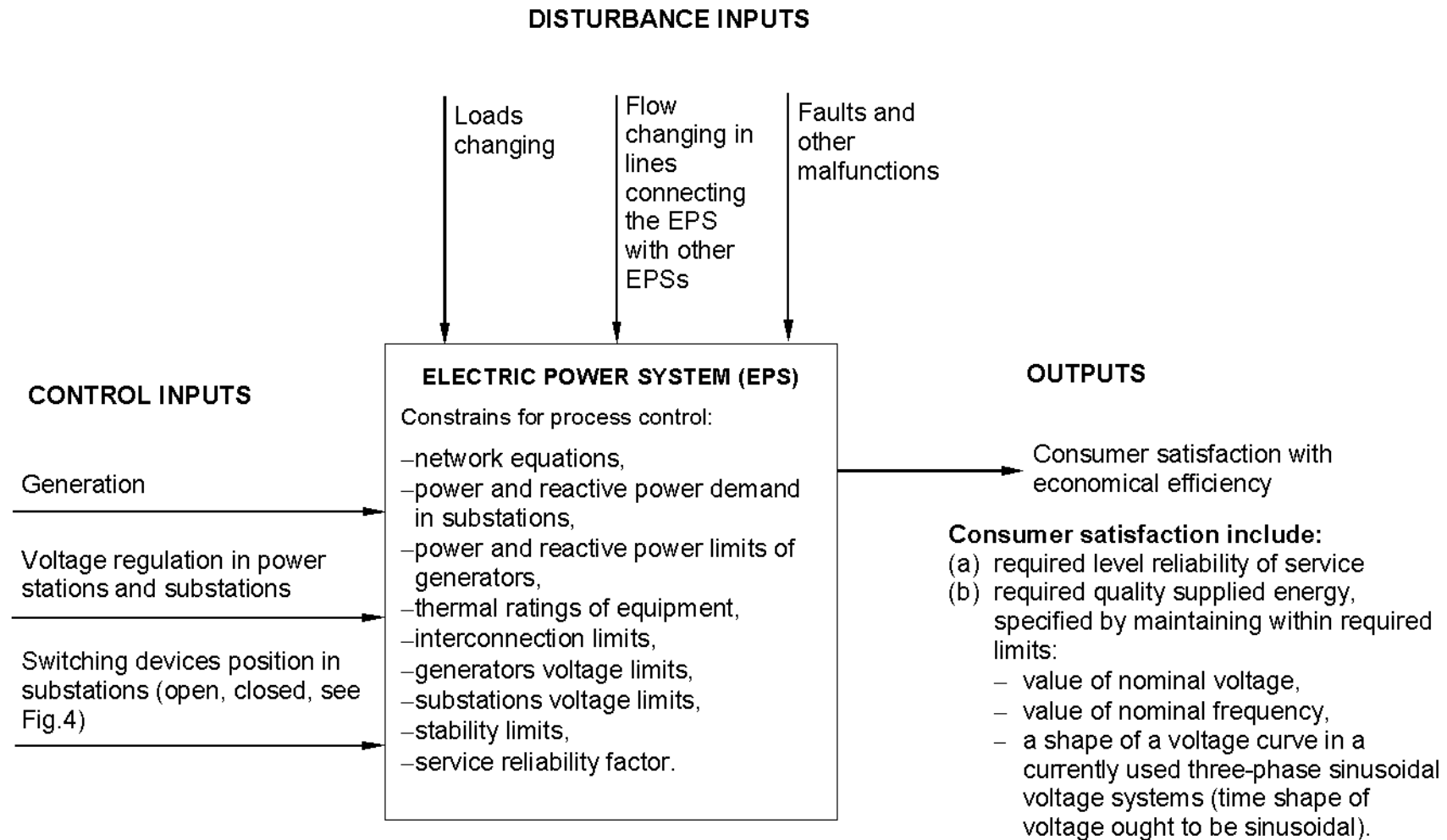
Simplified block diagram of the telecommunication network coupled with an electric power system



- Energy flow in normal operation of an EPS
- - - - - Energy flow in a failure state of an EPS
- Leased lines from public telecommunication network and connections to Internet
- . - . - Private utilities networks
- Connection to an EPS some big industrial consumers by Internet

Structure of electric power systems

The concept of an electric power system control



Possible consequences of security breaches

In EPSs cyber security refers to:

- confidentiality of data and information;
- integrity and availability of data and commands received in substations and control centres;
- authentication of the source of received data and commands.

Potential treats:

- accidental physical damage;
- terrorism and sabotage;
- vandalism;
- disgruntled employees and ex-employees;
- malicious code and viruses, etc.

Possible consequences of security breaches

Main vulnerabilities in EPSs are connected with the ability to remotely access protection, control, automation and SCADA equipment.

Cyber security risks in an EPS concern:

- safety-related computer applications in power stations, substations and control centres;
- applications critical to the power grid-related financial transactions and functioning and interests of the electric power sector organizations.

Possible consequences of security breaches

Consequences for power stations

Most kinds of possible consequences in power stations are similar to the consequences considered in other industry sectors;

An example of safety-related function 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.

Possible consequences of security breaches

Consequences for substations

Main risks of safety-related applications in substations are connected with switching operations control and they can have consequences for

- substation staff;
- substation equipment;
- the EPS.

Consequences for an EPS

The nature of possible consequences for an EPS in case of some security breaches is unique, based on EPS safety concept that is completely different from safety concepts known in others sectors of industry.

Possible consequences of security breaches

Concept of safety of an EPS

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.

The system frequency is a measure for the rotation speed of the synchronised generators.

In the process of synchronisation and next connecting a generator to the EPS, at the moment of connecting, it is coming into step by pull-in torque.

Synchronism of generators connected to the EPS is maintaining by synchro-tie that works like an electric shaft.

cont.

Possible consequences of security breaches

Concept of safety of an EPS

Power generated in an EPS must be maintained in constant equilibrium with power consumed (demanded). If power consumed increase 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.

cont.

Possible consequences of security breaches

Concept of safety of an EPS

In case of sudden disturbances, e.g. sudden increase of the load or switching off a transmission line or a generator in a power station, 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 sectioning of the EPS.

Section/sections that reach balance by disconnection of generation or demand stabilize and work as an island. Sections that do not reach balance collapse and this means collapse of the EPS, which may be partial or total, and this is called a blackout.

cont.

Possible consequences of security breaches

Concept of safety of an EPS

Generators connected to the EPS fall-out of synchronism. 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.

Risk for stability is equivalent to risk for safety (security) of an EPS.

Possible consequences of security breaches

Consequences for an EPS

Most famous blackouts in the United States:

- **The Northeast Blackout of 1965** - about 30 million people and 207 km² in Ontario, Canada, and United States without electricity for up to thirteen hours [D.2, D.3, D.4, D.5].
- **The New York City blackout of 1977** - blacked out the city for 23 hours [D.6]. Losses were estimated at 310 millions USD.
- **The 2003 North America blackout** - affected 10 million people in Ontario, Canada and 40 million people in eight U.S. states. The financial losses were estimated at \$6 billion [D.7].

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

[Source: CIGRE Study Committee publication]

Possible consequences of security breaches

Consequences for an EPS

In the history of the electric power industry safety as it is understood today is a relatively recent concept, which emerged after the Great Northeast Blackout of 1965.

The blackout of 1965 was at that time 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.

The New York City blackout of 1977 is considered in publications the second shock event that shows that there is need to look deeper into electric power systems safety assessment and enhancement.

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 ensuring security of the systems.

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 on EPRI website confirmed to some extent the image.

Current state of practice in assuring cyber security in electric power industry

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 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.

Current state of practice in assuring cyber security in electric power industry

Last years a number of papers on security of computer real-time systems applied in EPSs have been published and made available on websites in connection with critical infrastructures protection programmes applied in many countries.

A number of 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.1, B.2, B.3, B.4].

Current image based on available publications is that the research and developments on ensuring security of electricity infrastructure are most advanced in the United States.

Conclusions

1. Risk analysis for an 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.

In ISAT Project it became clear that such full analysis is very difficult or even impossible.

2. In traditional relay-based technology in Poland 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 are rather not articulated.

Conclusions

3. The shift of the idea how to provide an EPS safety and reliability from robustness of the EPS into control of the EPS during an emergency state will increasingly challenge the state of the art in EPS monitoring, communications, protection and control.

4. The challenge will be also strongly influenced by the emerging free market of electric power and the further increase in requirements of so called digital economy for very high quality of supplied electricity, and especially for reliability.

Conclusions

5. If there is no success in ensuring EPS cyber security more and more of customers with critical power quality needs will find it necessary to self-generate if they cannot get the quality they need from the grid. One can reasonably fear that it might result in the decrease of interest in EPSs development, and consequently in degradation of the distribution systems and even the whole EPS.

6. Differently than in any other 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.

Conclusions

7. As it follows from my experience management of electric power industry seems prefer rather to place orders for research and development on ensuring cyber security of a national EPS in an international experienced company then accept a submission for this research from a research institute from their country. It seems that they believe that in this way they receive ready made and the best solution, and without any risk.

8. It seems worth to consider European legal regulations which would enable to check level of cyber security of electric power infrastructure. Privatisation of the electricity sector should not mean that government will not be able to check if cyber security of this infrastructure is on right level (applied technical measures, technical documentation of security critical systems, security policy, qualification of personnel, etc.).

PUBLICATIONS / BACKGROUND MATERIAL / STANDARDS AND GUIDELINES / WEB SITES

A. Publications

- [A.1] 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.2] Department of Energy: Maintaining Reliability in a Competitive U. S. Electricity Industry. Final Report of the Task Force on Electric System Reliability (1998)
- [A.3] Dy Liacco T., *The Adaptive Reliability Control System*, IEEE Transactions on Power Apparatus and Systems, vol. 85, No. 5, May 1967.
- [A.4] Haase P., *Of Horseshoe Nails and Kingdoms: Control of Complex Interactive Networks and Systems*, EPRI Journal (<http://www.epri.com/journal/details.asp?id=100&doctype=features>).
- [A.5] 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.6] Phadke A.G., Thorp, J.S., *Expose Hidden Failures to Prevent Cascading Outages*. IEEE Computer Applications in Power, pp. 20-23, July 1996.
- [A.7] 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.8] Weedy B.M., *Electric Power Systems*, John Wiley & Sons, 1991.
- [A.9] 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.10] Zurakowski Z., *Safety and Security Issues in Electric Power Industry*. Proceedings of the 19th International Conference SAFECOMP 2000, Rotterdam, The Netherlands, October 2000.

[A.11] Zurakowski Z., *Functional Safety in Electric Power Sector*, SIPI International Workshop on Functional Safety IEC 61508, Gdynia, Poland, 28-29 May 2003 (<http://www.sipi61508.com/> in SIPI Technical Data Resource page).

B. Standards and Guidelines

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

[B.2] IEC 61850: *Communication Networks and Systems in Substations*. Parts 1-9, 2002-2004.

[B.3] IEEE Std 1402-2000: *IEEE Guide for Electric Power Substation Physical and Electronic Security*, IEEE, April 2000.

[B.4] *Security Guidelines for the Electricity Sector*, Version 1.0, June 14, 2002 (<http://www.nerc.com/cip.html>).

[B.5] *UCTE Operation Handbook*, Union for the Co-ordination of Transmission of Electricity, June 2004 (http://www.ucte.org/ohb/cur_status.asp).

C. Electric power systems cyber security web sites

[C.1] Schweitzer Engineering Laboratories, Inc. (<http://www.selinc.com/techpprs.htm>).

[C.2] Electric Power Research Institute (EPRI), Infrastructure Security Initiative (ISI) (<http://www.epri.com/corporate/initiatives/infrastructuresecurityinitiative.asp>).

[C.3] North American Electric Reliability Council (NERC) Critical Infrastructure Protection web page at <http://www.nerc.com/cip.html>.

[C.4] International Institute for Critical Infrastructures (CRIS) (www.cris-inst.com).

D. Famous blackouts web sites

[D.1] A list of famous wide-scale power outages (http://en.wikipedia.org/wiki/List_of_power_outages).

- [D.2] The Great Northeast Blackout of 1965 (<http://www.cmpco.com/about/system/blackout.html>).
- [D.3] 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).
- [D.4] The Blackout History Project – 1965 Blackout (http://www.blackout.gmu.edu/archive/a_1965.html#friedlander_76).
- [D.5] Life Magazine, Vol. 59 No. 2, 19 November 1965 (issue dedicated to the Northeast Blackout of 1965) (http://www.blackout.gmu.edu/archive/life_11_19_1965/life_11_19_65_toc.html).
- [D.6] New York City blackout of 1977 (http://en.wikipedia.org/wiki/New_York_City_Blackout_of_1977).
- [D.7] 2003 US Canada blackout (http://en.wikipedia.org/wiki/2003_U.S.-Canada_blackout).
- [D.8] 2003 London Blackout (http://en.wikipedia.org/wiki/2003_London_blackout). National Grid's report on the blackout available at <http://195.92.225.33/uk/library/documents/pdfs/London28082003.pdf>.
- [D.9] UCTE Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy, UCTE, April 2004 (http://www.ucte.org/pdf/News/20040427_UCTE_IC_Final_report.pdf)