

Rapporto tecnico N.56



Polish case study. Scenario based
assessment of costs and benefits
of adoption of comprehensive CIP standards.

Hanna Bartoszewicz-Burczy, Clementina Bruno,
Fernando García, Tadeusz Włodarczyk



RAPPORTO TECNICO CNR-CERIS

Anno 9, N° 56; Dicembre 2014

Direttore Responsabile

Secondo Rolfo

Direzione e Redazione

CNR-Ceris

Istituto di Ricerca sull'Impresa e lo Sviluppo

Via Real Collegio, 30

10024 Moncalieri (Torino), Italy

Tel. +39 011 6824.911

Fax +39 011 6824.966

segreteria@ceris.cnr.it

www.ceris.cnr.it

Sede di Roma

Via dei Taurini, 19

00185 Roma, Italy

Tel. 06 49937810

Fax 06 49937884

Sede di Milano

Via Bassini, 15

20121 Milano, Italy

tel. 02 23699501

Fax 02 23699530

Segreteria di redazione

Enrico Viarisio

e.viarisio@ceris.cnr.it



Copyright © Dicembre 2014 by CNR - Ceris

All rights reserved. Parts of this paper may be reproduced with the permission of the author(s) and quoting the source.

Tutti i diritti riservati. Parti di questo rapporto possono essere riprodotte previa autorizzazione citando la fonte.

ESSENCE

Emerging Security Standards to the EU power Network controls and other Critical Equipment

A project financed under the programme "Prevention, preparedness and consequence management of terrorism and other security-related risks" HOME/2011/CIPS/AG

The Essence project is a study to evaluate costs and benefits of the implementation of security standards to critical electric infrastructure, based on two case studies.

Networked computers reside at the heart of critical infrastructures, these are vulnerable to cyber attacks that can inhibit their operation, corrupt valuable data, and expose private information. Such attacks might affect large portions of the European power system, make repair difficult and cause huge societal impact, so that pressure to ensure cyber security of control and communication systems is now very strong worldwide. To that aim, several frameworks have been developed or are under development at present, both in the form of guidelines and proper standards, but it is difficult to evaluate costs and benefits of their adoption, although experimentation so far has shown that they may be huge.

In this scenario the key objectives of ESSENCE include:

1. Developing a common understanding of industrial needs and requirements regarding the security of control systems and the related standardisation efforts;
2. Identifying power system vulnerabilities induced by control systems, and estimating the likely socio-economic impact of failures due to faults and attacks exploiting those vulnerabilities;
3. Evaluating emerging frameworks for ensuring industrial control systems security, and establishing the costs of their adoption on an objective basis;
4. Recommending a pathway towards adoption of one or more of the above frameworks to the European power system infrastructure, having specific regard to EU transnational infrastructures as defined by the Directive 2008/114/EC.

The results of the project have been published in the "Special Essence series on security standards for critical infrastructures", hosted in the "Ceris Technical reports series". The published titles, available at <http://essence.ceris.cnr.it/index.php/documents/2-uncategorised/14-reports>, are:

1. Considerations on the implementation of SCADA standards on critical infrastructures of power grids.
2. Attack scenarios. Threats, vulnerabilities, and attack scenarios along with their selection criteria.
3. Terms of reference for the trials.
4. Benefit analysis. Assessing the cost of blackouts in case of attack. Evaluation based on Italian and Polish case study.
5. Cost analysis of standard implementation in the SCADA Systems of electric critical infrastructures.
6. Italian Case Study: socio-economic impact analysis of a cyber attack to a power plant in an Italian scenario. Cost and benefit estimation of CIPS standard adoptions. A reduced version.
7. Polish case study. Scenario based assessment of costs and benefits of adoption of comprehensive CIP standards.
8. Trial evaluation: conclusive lessons from Essence case studies.



Partners of the project are:

CNR-Ceris (*Coordinator*) (*Italy*); Università del Piemonte Orientale Amedeo Avogadro (*Italy*);
Deloitte Advisory S.l. (*Spain*); Antonio Diu Masferrer Nueva Empresa SLNE (*Spain*);
Enel Ingegneria e Ricerca S.p.A. (*Italy*); Abb S.p.A. – Power systems division (*Italy*);
IEN - Institute of power engineering (*Poland*); PSE – Operator SA (*Poland*).



*With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme European Commission - Directorate-General Home Affairs
The Commission is not responsible for any use that may be made of the information contained therein,
the sole responsibility lies with the authors.*

Polish case study. Scenario based assessment of costs and benefits of adoption of comprehensive CIP standards.

Hanna Bartoszewicz-Burczy ^a, Clementina Bruno ^{*},
Fernando García ^b, Tadeusz Włodarczyk ^c

*Corresponding author: Dipartimento di Studi per l'Economia e l'Impresa
Università del Piemonte Orientale
28100 NOVARA – ITALY
Mail: clementina.bruno@eco.unipmn.it

ABSTRACT: The Polish case study describes results of simulations of cyber-attacks on the Polish transmission system of electricity and compares the economic and social impact of these attacks, assumed to occur in situations where the system is working in normal operation, versus situations where standards are implemented as additional security countermeasures and the same incident arises. This work analyses security measures defined in selected documents, standardization, evaluates their effectiveness relative to attack scenarios, as well as implementation costs in comparison to weight of potential losses resulting from non-implementation. On this basis, a list of recommended safety measures, which guarantee high level of security and the highest level of return, has been prepared.

KEYWORDS: cyber security, malicious attack, power control centre, hardware breakdown, security standards, power threats, scenarios definition.

JEL CODE: D12, D61, L94.

^a IEN - Institute of Power Engineering, 9 Mory str., 01-300 Warsaw, Poland

^b Deloitte Advisory SL, Plaza Pablo Ruiz Picasso, 1, Torre Picasso, 28020 Madrid Espana

^c PSE Operator SA, Warszawska 165, 05-520 Konstancin-Jeziorna, Poland

TABLE OF CONTENTS

1	Polish Power Sector.....	8
1.1	Key data of the Polish Power Sector	8
1.2	Structure of energy generation	9
1.3	Polish Transmission System.....	13
1.4	Structure of Information and Communication Technologies in PSE	16
1.4.1	Communication protocols for operating cooperation with power plants.....	18
1.4.2	Communication protocols to energy market information exchange system.....	18
1.4.3	Communication protocols for substations	19
1.5	Polish National Power System cross border interconnections.....	20
1.6	Development of the Polish transmission system	22
1.7	Distribution sector	24
2	System reliability and average system interruption.....	27
3	Standards and regulations	30
3.1	CIP Directive and other national regulations.....	30
3.2	ENTSO-E Policy	32
3.3	Introducing the ENTSO-E Operation Handbook	33
4	Standards and regulations in Polish law	35
4.1	Energy Policy	36
4.2	Instruction of Transmission System Operation and Maintenance	37
4.3	Conclusion.....	38
5	Attack scenarios.....	39
5.1	Attack source (type of attacker, knowledge and recourses)	42
5.2	Reasons and objectives of attacks	43
5.3	Types of attacks (cyber, damage to the active network elements)	46
6	Vulnerabilities characteristics of TS elements (physical network elements, ICS)	49
6.1	Generation power plants.....	49

6.2	TSO.....	50
6.2.1	Substation	50
6.2.2	Power lines and interconnection lines	52
6.2.3	Control centres.....	53
7	Polish case study.....	55
7.1	Description of the cyber attack case and effects on power plants and electric grid of capital city Warsaw	55
7.1.1	7.1.1 Description of the method to simulate attacks.....	56
7.2	Energy generation and distribution system in Warsaw	57
7.3	Specification and statistical data of Warsaw electricity customer groups.....	61
7.3.1	7.4 Daily load profile for Warsaw city	63
7.4	Standard implementation.....	66
7.4.1	Cost of standards implementation	67
8	Polish case study – benefit analysis.....	71
8.1	Evaluating cost of blackouts.....	71
8.2	Damage for non-households.....	72
8.3	Damage for the electricity sector.....	75
8.4	Damage for households	76
9	References	83

1 POLISH POWER SECTOR

1.1 Key data of the Polish Power Sector

Availability and security of electricity supply, due to the important role energy plays in any society, have impact on economic growth, industrial competitiveness and well-being of individuals. Growing importance of information technology and communications leads to costs increase to national economies in case of electricity interruptions.

It is evident that Polish society and industry are fundamentally dependent on secure well-functioning energy network.¹

In 2012 (the year of simulation), the Polish power system presented the following characteristics:

- Total installed capacity of the Polish electric system amounted to 38 203 MW, of which:
 - Installed capacity of public power plants with RES – 36 344 MW
 - Installed capacity of industrial power plants (auto-producers) – 1 859 MW
- Available capacity amounted to 38 001 MW, of which:
 - Public thermal plants with RES – 33 475 MW
 - Industrial power plants (auto-producers) – 1 729 MW
- Maximum power demand amounted to 25 845 MW (evening peak, 7th February, 2012)
- Evening minimum of national demand amounted to 18 227 MW (13th July, 2012)
- Gross electricity production in the country reached 162 139 GWh, of which:
 - Thermal power plants – 148 639 GWh
 - Industrial power plants – 7 842 GWh
 - Renewable energy sources – 5 658 GWh
- Electricity production per capita amounted to 4 208 kWh/p
- Domestic electricity supplied reached 159 299 GWh
- Number of electricity consumers (thousands) – 16 743, of which:
 - High-voltage supplied consumers - 0,3 thousands
 - Medium-voltage supplied consumers – 33,3 thousands
 - Low-voltage supplied consumers – 16 709 thousands, of which:
 - Households and agriculture – 14 345 thousands

¹ The terms energy security is broadly defined in EU documents and literature. The terms of security of supply, network of security, as well as other were defined in the Directive 2005/89/EC of the European Parliament and of the Council of 18 January 2006 concerning measures to safeguard security of electricity supply and infrastructure investment. According to Article 2 of this Directive security of electricity supply means the ability of an electricity system to supply final customers with electricity and operational network security means the continuous operation of the transmission and, where appropriate, the distribution network under foreseeable circumstances.

- Electric lines length, total (km) – 572 487
- Electric cable lines length, total (km) – 215 252
- Number of transmission lines - 245, with a total length of 13 445 km
- Total high and medium voltage substations – 250 568
- Number of network transformers – 254 204
- Network transformers capacity (MVA) – 143 504
- Balance of electricity exchange with neighbouring countries amounted to 2 840 GWh.

1.2 Structure of energy generation

The Polish generation subsystem includes thermal power plants, industrial power plants, hydro and renewable power plants (wind power, biomass, biogas), as well as any other equipment essential to generate electricity properly, including protection monitoring and control systems.

In 2012 the Polish electric system worked on the basis of 123 thermal power plants, 136 hydro power plants and 72 industrial power plants.²

In the above power plants, 99 turbosets have been installed with the following specifications: one 850 MW unit, four 500 MW units, sixteen 360 MW units, fifty-nine 200 MW units and nineteen 120 MW units.

The Polish generation sector has been historically based on coal, and majority of power generation capacity is based on coal and lignite power plants, i.e. 20 GW of coal (52.9%) and 9,6 GW of lignite (25.3%). Maximum capacity of gas fired power plants stands at 0.9 GW (2.5%). Capacity of hydro power stations amounted to 2.2 GW (5.8%) and

2.6 GW of renewable power plants (6.9%) in 2012.

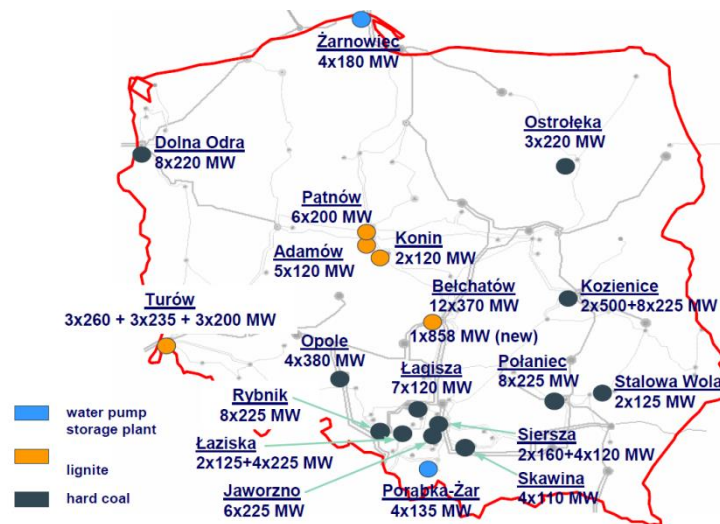
Installed capacity and production of public coal and lignite power plants in Poland in 2011 are presented in Table 1. and Figure 1.

² According to Energy Regulatory Office 1332 entities had concessions for electricity generation in 2012.

Table 1. Installed capacity and energy production in public thermal power plants in 2011.

No	Item	Installed capacity MW	Energy production GWh
<i>Coal public power plants</i>			
1.	TAURON WYTWARZANIE SA	5 011	21 696
1.1	El. Jaworzno III	1 345	6 716
1.2	El. Łaziska	1 155	5 655
1.3	El. Łagisza	1 060	4 076
1.4	El. Siersza	666	2 590
1.5	El. Stalowa Wola	330	1 169
1.6	El. Jaworzno II	190	778
1.7	El. Blachownia	165	561
1.8	El. Halemba	100	151
2.	PGE SA	3 264	14 432
2.1	El. Opole	1 492	7 794
2.2	El. Dolna Odra	1 772	6 639
3.	ENEA WYTWARZANIE SA	2 845	11 889
4.	El. Rybnik SA	1 775	10 107
5.	El. Połaniec	1 600	8 445
6.	ENERGA Elektrownia Ostrołęka	647	3 379
6.1	El. Ostrołęka B	647	3 379
7.	El. Skawina	490	1 128
<i>Lignite power plants</i>			
8.	PGE SA	7 197	42 417
8.1	El. Belchatow	4 440	29 123
8.2	El. Belchatow bl.14	858	1935
8.3	El. Turow	1 899	11 358
9.	PAK SA	2 457	11 200
9.1	El. Patnow	1 664	8 320
9.2	El. Adamow	600	3 461
9.3	El. Konin	193	451
10.	<i>Coal and lignite power plants</i>	25 286	124 692

Source: Minister Gospodarki, Sprawozdanie z wyników monitorowania bezpieczeństwa dostaw energii elektrycznej, Warszawa 2013.



Source: Ministry of Economy, Energy Department.

Figure 1. Major power stations in Poland

Gross electricity generation amounted to 162 139 GWh in 2012, and was ca. 0.6% lower than in 2011, partly as result of financial and economic crisis, the fall of GDP growth which grew by 2% in 2012 (in comparison with 4.3% registered in 2011) and decreasing energy demand.

In 2012 electricity generation from coal power plants amounted to 140 087 GWh (87.6% of total electricity generation), and gas fired generation produced 4 485 GWh (2.8%). Electricity generated from hydro and renewable energy sources amounted to 6 291 GWh, representing 7% of total output. Such coal-based structure of electricity production results from abundance of domestic coal resources located in 3 basins of different size: Upper Silesian, Lower Silesian and Lublin, and advances technologies for its exploitation, preparation and combustion. Coal is the most important primary source of energy and shall maintain its dominance position for next decades.

New source of energy will be nuclear power plant, whose launch is planned for 2022.

It is estimated that ca. 55% of all power plants are over 30 years old. Both the Large Combustion Plants Directive (LCPD) and the Industrial Emissions Directive (IED) will lead to closure of several existing coal power plants, and loss in output which is estimated to be around 5.8 GW by end of 2020; in this ca 4.117 GW by PSE Transmission Operator disposal). Such values are likely to increase to 9.45 GW and 7.41 GW, respectively, by 2028. Such situation can create risk of capacity deficit in the electric market.

Reforms of energy utility market and privatisation processes started since 1998, as well as governmental consolidation policies (occurred in 2000, 2004 and in 2006 - programme for electricity sector) generated the current market situation, with five leading companies operating in the power generation sector.

The biggest generation companies are:

- PGE Polska Grupa Energetyczna SA (Eng.: Polish Energy Group) - operating in the eastern part of Polish energy system; 12.9 GW of installed capacity, 57.05 TWh of energy production in 2012;
- TAURON Polska Energia SA - operating in southern part of the Polish energy system; 5.6 GW of installed capacity, the group produced 21.4 TWh of energy in 2012;
- ENEA - operated in Western part of Polish energy system; total installed capacity of the group is 2.9 GW, the group produced 12.3 TWh of energy in 2012;
- ZE PAK – 2.9 MW of installed capacity, sold 7.9 TWh of electricity in 2012;
- ENERGA SA - operated in the northern part of Polish energy system; operator of 47 hydro plants and the coal-fired plant in Ostrołęka, the group produced 4,7 TWh of energy in 2012.

The biggest foreign investors in the energy generation and distribution sector are: the French group EDF (operator of power plant in Rybnik and CHP in Wrocław, Kraków, Wybrzeże, Zielona Góra, installed capacity to supply is amounted to 3 GWe of electricity and ca. 3.5 GWt of heat), GDF SUEZ (operator of power plant in Połaniec, sold 1 GWh of electricity in 2012) and Dalkia (installed capacity to supply amounted to 0.820 GW of electricity and 4.290 GW of heat). Other active entities include: Czech group ČEZ, Finnish company Fortum, German companies E.ON, RWE, and Spanish company Iberdrola specialising in wind energy.

Balance of electricity production in Poland in 2000 - 2012 years are presented in Table 2.

Table 2. Balance of electricity.[GWh]

	2000	2005	2010	2011	2012
Gross electricity generation	145183	156935	157658	163548	162139
- of this thermal power plants	137798	148426	147696	151695	148639
- of this hydro plants	3967	3528	3155	2453	2159
Electricity import	3290	5002	6310	6780	9803
Electricity consumption	138810	145749	156304	158306	159299
Domestic consumption	124576	131186	144453	147668	148415
Distribution losses and statistical difference					
Electricity exports	14234	14563	11851	10638	10884
	9663	16188	7664	12022	12643

Sources: Statystyka elektroenergetyki, Agencja Rynku Energii 2012.

Domestic consumption of electricity in 2012 reached 148 415 GWh and was higher than consumption in 2011 by ca. 747 GWh.

Since 2006, renewable energy sources (RES) have been emerging in the system and in 2012 energy production of RES reached 16 879 GWh, amounting to 10,4% of total primary energy production. Total installed capacity was equal to 4129.41 MW, of which 2583.67 MW belonged to wind energy, 950.85 MW

to hydro energy, 593.6 MW to bio-energy³ and 1.3 MW to photovoltaic. Total electricity production from RES with biomass co-firing reached 16.8 TWh in 2012. According to data from the PSE, in the middle of 2013 total installed capacity of wind energy increased to 3 300 MW, but additional ca 21 000 MW were subjects to procedures for connecting transmission and distribution grids. This new RES capacity will replace capacity losses due to closure of old coal power plants and will contribute to security of energy supply.

European Union membership is key driver of increase of share of renewable energy sources in the energy mix and reduction of the greenhouse gas emission in Polish energy system. Development of RES will contribute to proper functioning of the energy system and energy security by improving energy supplies and increasing flexibility of operation. New RES capacities will replace lost capacities mainly due to least efficient coal power plants closing.

Structure of electricity generation is presented on Figure 2.

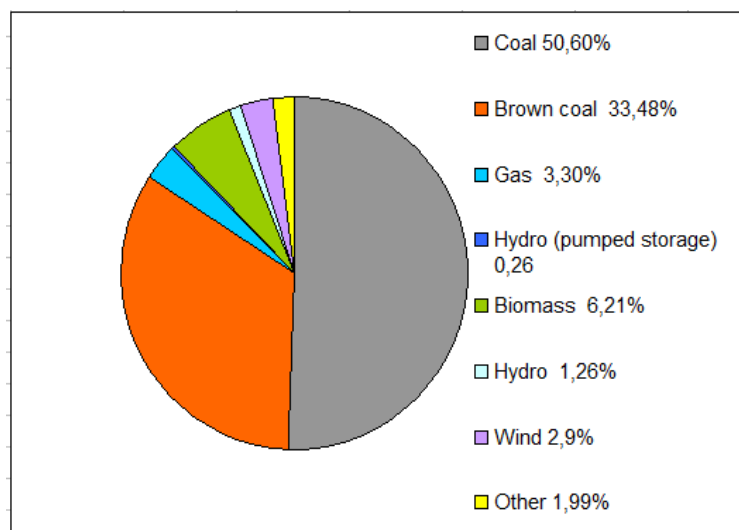


Figure 2. Electricity generation in Poland, 2012 (total: 161.957 GWh)

Energy trade was conducted on the Polish Power Exchange (Towarowa Gielda Energii) - 131.997 TWh (82,6% of domestic electricity production) and on Warsaw Stock Exchange Platform for Trading Electricity (POEE GPW SA) in 2012.

1.3 Polish Transmission System

Polskie Sieci Elektroenergetyczne SA - PSE Operator SA (since 9 January 2013 under a changed name PSE SA) was designated Transmission System Operator for high voltage electricity system in Poland, by decision and the license issued by the President of Energy Regulatory Office (ERO), of 15 April 2004 for period from

³ Without co-firing.

1 July 2004 to 1 July 2014, and decision of the President of ERO of 28 May 2013, extending that period to 31 December 2030.⁴

PSE SA is owned by the State Treasury. Ownership supervision over PSE SA is executed by the Minister of Economy. PSE is the owner of transmission assets and manages the system, being responsible for current and long term safe technical and operating service, system balancing, operational security of the system, maintenance, repairs, and development of the transmission grid including interconnection with neighbouring countries systems.

The PSE objective is to supply electricity of appropriate quality to all regions in Poland, respecting natural environment, third party access principle and the lowest possible cost. PSE has strategic significance to Poland energy security.

The high voltage transmission network owned by PSE consists of 245 lines with a total length of 13 445 km, 100 power stations, 101 high voltage substation and 183 transformers.

Below a detailed list of PSE operational assets is provided:⁵

- Length of transmission power lines:
 - 750 kV - with a total length of 114 km,
 - 400 kV - 77 of power lines with a total length of 5 383 km,
 - 220 kV - 167 lines with a total length of 7 948 km,
 - 101 extra-high voltage (EHV) substations, (750 kV – 3 units, 400 kV – 27 units, 220 kV – 63 units),
 - 450 kV DC under-sea connection between Poland and Sweden, with total length of 254 km.
- Transformer stations of total capacity amounting to 143 504 MVA :
 - 750/400 kV - 6 units,
 - 400/220 kV - 19 units,
 - 400/110 kV - 39 units,
 - 220/110 kV - 116 units,
 - 110/15 kV - 3 units.
- IT infrastructure:
 - 63 optic fibres and ICT lines,
 - 6 007 IT devices,
 - 2 455 teletransmission and telephone devices,
 - 466 AC/DC switching stations, measurement devices, air-conditioning devices, installed in substations..

⁴ PSE Annual Report, 2012.

⁵ PSE Annual Report, 2012.



Source: PSE Annual Report 2012.

Figure 3. Scheme of the high voltage power grid.

400 kV lines are basis of transmission network of the country, with greater transmission capability than network of 220 kV, and transformer stations of voltage of 400 kV are sources of greater efficiency for 110 kV lines.

Control and communications systems consist of facilities necessary to monitor and control all components of electric networks.

In 2012 yearly peak load took place during the winter season. Maximum domestic power demand in evening peak on workdays reached 25 845 MW, it took place on 7th of February, 2012. The lowest demand during night peak-off period occurred on 13 July and reached 18 227 MW. Generation capacity under disposal of the transmission system operator was 25 876 MW ie. 69% available capacity, compared with 31% i.e. 11 844 MW of non-centrally dispatched generating units.

Power reserve available to the TSO amounted to 3 652 MW, slightly increasing (by 0.25%) in comparison to 3 538 MW in 2011. It should be noted that, in previous years, the level of available reserves adjusted for necessary losses of capacity had been systematically falling. It is estimated that in coming years, as result of decommissioning caused by IE Directives coming into effect, as well as limitation of units lifespan, reserve margin will significantly decrease, particularly after 2015. In order to avoid shortage of reserve margin, from January 2016 capacity mechanism intervention “cold reserve” will be applied. “Cold reserve” will include units that will be temporally exempted from compliance with emission limit values under Article 33(1) of Directive 2010/75/EU, ready to operate with a view to cover peak demand. They will be permanently

excluded from competitive mechanisms and the costs of their activity will be covered by the TSO (they are included in a quality charge that is a component of the TSO tariff).⁶

1.4 Structure of Information and Communication Technologies in PSE

Effective communication has become ever more critical today playing basic role in real-time communication, operation and control. Significant development of information technology and communication tools have been implemented in PSE trough last decade, too.

In 2011 and 2012 further development of telecommunication network based on SDH (Synchronous Digital Hierarchy) technologies took place, ensuring control over power grid dispatch communication and data transfer.

In 2012, IT systems were continuously upgraded and consolidated including migration from an AMS (Asset Management System) and SOT (Technical Protection for the Stations, in Polish: System Ochrony Technicznej - SOT) to joint virtual hardware-software platform, implementation of virtual workstations and implementation of consolidated system of back-up copies, as well as introducing new standard of technical infrastructure of IT systems.

The teletransmission grid of PSE was further expanded. Teletransmission devices were installed and launched in 43 locations of PPS (e.g. a DWDM connection was launched between the data processing centres, with the total capacity of over 70 Gb/s). 110 leased lines were switched to PSE's own teletransmission grid, thus reaching independence level in demand for lines at 86 %.

The telecommunication system used for collection, transmission and exchange information includes:

- ✓ Operation and Control System for National Transmission Network - SCADA (in Polish: System Prowadzenia Ruchu i Sterowania Pracą Systemu),
- ✓ Control and Supervisory Systems for Substations - SSiN (in Polish: System Sterowania i Nadzoru Pracy Stacji Elektroenergetycznych),
- ✓ Market Information Exchange System - WIRE (in Polish: System Wymiany Informacji o Rynku Energii),
- ✓ System for Operating Cooperation With Power Plants - SOWE (in Polish: System Operatywnej Współpracy z Elektrowniami),
- ✓ System for Monitoring the Operating Parameters of the Units - SMPP (in Polish: System Monitorowania Parametrów Pracy Jednostek),
- ✓ Central Metering-Settlement System - CSPR (in Polish: Centralny System Pomiarowo - Rozliczeniowy),
- ✓ Automatic Load Frequency Control System, System – LFC.

These systems are built in two redundant Dispatching Centers. For remote monitoring and control energy network in a dispatching center SCADA/EMS system has been used. SCADA/EMS system (Supervisory

⁶ Energy Regulatory Office Report from 2010-2012.

Control and Data Acquisition/Energy Management System) supervises, controls, optimises and manages generation (load forecast, automatic generation control, monitoring and schedules, economic dispatch, balancing market and transmission systems functions, such as dispatcher power flow, contingency analysis, optimal power flow etc).

ICS SCADA/EMS for TS dispatching center is connected to:

- 5 regional TS dispatching centers,
- 101 substation ICS Scada,
- 20 generation plants,
- 5 DSO's ICS Scada,
- 9 European ICS Scada EMS, from ENTSO-E Members TSO's,
- ENTSO-E AES,
- management systems in PSE.

Operation ICS Scada for substations dispatching center is connected to:

- 5 regional substations dispatching centers,
- 60 operation substations ICS Scada,
- substation ICS Scada,
- up to 15 different (by vendors) mini Scada ICS systems per substation,
- local connections to generation plants ICS Scada.

Data exchange with TSO takes place with support of the primary link using power sector extranet network, including network mechanisms based on Transmission Control Protocol/Internet Protocol (TCP/IP protocol). The data transmission subsystem of TSO ensures guaranteed communication under TCP/IP protocol between all servers which are part of SCADA system. TCP/IP Standard is supported by hardware and software vendors which allows operate easily and inexpensively with multiple systems.

Acquisition of data from power facilities takes place with support of UTJ, DNP 3.0, IEC 870-5-101, IEC 870-5-104 protocols. ICCP/TASE.2 protocol is used for data exchange with DSO's SCADA systems.

TSO's SCADA system enables assembly of link with external systems through a dedicated access router. The router is equipped with function of protection against access to servers by unauthorised personnel.

The data transmission subsystem at TSO ensures reliable and secure data transmission between SMPP - systems of monitoring of units operating parameters, servers through separation of the transmission sub-network used only for the SMPP system needs. Data transmission is executed with support of ICCP/TASE.2 protocol (blocks 1 and 2) based on TCP/IP protocol according the following standards: IEC 870-6-503, IEC 870-6-802, IEC 870-6-702, ISO/IEC 9506, while supplementation of archive data is available through https protocol.⁷

⁷ Instruction of Transmission System Operation and Maintenance. PSE Operator, 2006.

1.4.1 Communication protocols for operating cooperation with power plants

System for Operating Cooperation with Power Plants (in Polish: System Operatywnej Współpracy z Elektrowniami - SOWE) is dedicated to exchange technical information between TSO's dispatching services and operating services of managing by TSO units. SOWE provides communication among TSO and with operation departments of power plants concerning load plans of dispatching units for 15 minute periods, availability of generating units, operating orders, as well as exchange information on operational events and network events.

TSO data transmission subsystem provides communication under TCP/IP protocol, with support of redundant link using power sector extranet network, with any SOWE/EL server at guaranteed 64 kB/s rate for each channel and has permanent IP address and available communication ports.

Encryption and authorization mechanism based on SSL protocol is used for the communication between SOWE/EL and SOWE systems of TSO. Transmission and reception of documents is provided through WebSphere MQ tools, while distribution of documents is executed with support of JMS libraries in JAVA environment.

Protection of communication between SOWE/EL servers is executed at level of a SSL WebSphere MQ channel. The SSL channel is assembled with support of certificates of queue managers WebSphere MQ and based on the name of a channel and IP address.

Information exchange under SOWE system takes place through appropriate preparation of electronic documents according to determined format and recording method under XML standard.⁸

1.4.2 Communication protocols to energy market information exchange system

Market Information Exchange System (in Polish: System Wymiany Informacji o Rynku Energii WIRE) is dedicated to exchange trade, technical, metering and settlement data of the balancing market and control system services, between trade departments and technical departments of TSO and Market Operators.

Data transmission subsystem provides communication under TCP/IP protocol with any WIRE/UR server (UR- market operator) at guaranteed 64 kB/s rate for each channel and has permanent IP address and available communication ports.

Encryption and authorization mechanism based on SSL protocol is used for communication between WIRE/UR and WIRE systems of TSO.

Transmission and reception of documents is provided through WebSphere MQ tools, while distribution of documents is executed with support of JMS libraries in JAVA environment.

Protection of communication between WIRE/UR and WIRE servers of TSO is executed at level of SSL WebSphere MQ channel. The SSL channel is assembled with support of certificates of queue managers WebSphere MQ and based on name of the channel and IP address.⁹

⁸ Instruction of Transmission System Operation and Maintenance. PSE Operator, 2006.

⁹ Instruction of Transmission System Operation and Maintenance. PSE Operator, 2006.

1.4.3 Communication protocols for substations

PSE SA for operating substation are running different teleinformation systems grouped into the following logical segments:

- office system for communication with ICT business systems of PSE, in this: e-mail, file servers, Internet,
- system of technical protection, covering physical security such as burglary and robbery system, fire alarm system, satellite usable CCT, access control system,
- subsidiary technological systems to monitor selected parameters of substation, disturbance recording, quality system of electricity monitoring, remote meter reading, internet engineering, WAMS - Wide Area Measurement System,
- substation automation system, under which operate station and supervisory control system based on IEC 61850 and IEC 870-5-104 automation, monitoring system voltage transformers, automatic frequency control and power, automatic power adjustment settings,
- TELCO system, designed to support voice, chat loggers and supervision of telecommunications equipment, air-conditioning and 48V generators,
- systems of external entities such as wind farms, power plant control systems.

Communication is implemented using popular communication protocols, such as HTTP (Hyper Text Transfer Protocol), SMTP (Simple Mail Transfer Protocol), RDP (Remote Desktop Protocol), and specialized technological protocols, IEC 870-5-104, synchronizer protocol, ICCP/TASE.2, counters protocol. Communication between logic segments of power stations is performed only when required by operation of automatic data, and it is assumed total separation of office systems from remaining logical segments on the substation. Communications between SSiN in substation and SSiN in power station are also authorized, and their implementation is made using IEC 61850 or IEC 870-5-104 protocols.

First implementation of IEC 61850 protocol in PSE took place in 2006 at Łośnice substation. Currently, devices supporting IEC 61850 protocol are installed on all substations, but GOOSE communication is performed only on selected objects for testing this standard.

Special system for the substation is an engineering link, through which operational services operating in control centres gain access to automatic substation engineering interfaces. This system works in a star topology, i.e. dispatch centres staff communicate via secure proxy and RDP protocol to computer engineering link, on which is running software for automatic communication. For computer engineering link is connected communications module that provides connectivity running using variety of technologies (links serial, parallel, Ethernet and TCP/IP) to automatic. All interfaces and links within communication between computer engineering and automation are galvanically isolated from rest of network substation infrastructure.

1.5 Polish National Power System cross border interconnections

The Polish national power system is connected synchronously (220 and 400 kV alternating current connections) with power systems of Czech Republic, Germany and Slovakia and asynchronously (using direct current cable) with the Swedish power system. Total capacity of connections of the Polish power system with EU member states is 3000 MW.

In 2012, the PSE provided transmission capacity on interconnections between 8 transmission system operators from 7 countries of the central-eastern Europe area, within a mechanism of coordinated explicit auctions organised for yearly, monthly and daily (a day-ahead market) negotiations, as well as within an intraday mechanism on conditions agreed upon with other operators from the region. Auctions for transmission capacities were organised and conducted by a Central Allocation Office (CAO) in Freising (Germany).

Transmission capacity for export offered by the TSO in 2012 on yearly auctions ranged from 100 MW to 400 MW, in monthly auctions it amounted to maximum 304 MW (on average 116 MW in the year) and during daily auctions to maximum 1.368 MW. The transmission capacity for import offered by the TSO in daily auctions reached a maximum of 425 MW (on average 118 MW in the year).

Transmission capacity was also allocated to a high-voltage direct current link with Sweden - the SwePol Link - within day-ahead market coupling mechanism (implicit auctions) through power exchanges (POLPX and Nord Pool Spot). Average daily capacity available for export from Poland amounted to 110.5 MW and for import to 394.9 MW. Average hourly flow from Poland to Sweden was at the level of 14.3 MW and from Sweden to Poland at the level of 304.3 MW. Total electricity exports from Poland to Sweden amounted to 187.8 GWh in 2012, while the total import amounted to 1 686.1 GWh.¹⁰

Interconnections:

- In the north
 - 450 kV DC undersea cable connecting Polish and Swedish systems from Słupsk to Stårnö (capacity 600 MW) 254 km,
- In the south with the Czech Republic and Slovakia (transmission capacity 6 300 MVA)
 - line 400 kV Wielopole - Noszowice (Czech Republic),
 - line 220 kV Kopanina - Liskovec (Czech Republic),
 - line 220 kV Bujaków - Liskovec (Czech Republic),
 - line 400 kV Dobrzeń - Albrechtice (Czech Republic),
 - double circuit line 400 kV Krosno Iskrzynia - Lemesany (Slovakia).
- In the east connections with two non-EU electricity systems - Belarusian and Ukrainian.
 - line 220 kV line connecting the Polish and Belarusian systems (line out of operation since 2004),
 - line 220 kV from Zamość to Dobrotwór (Ukrainian systems, capacity 180 MW),

¹⁰ Energy Regulatory Office Report 2013.

- line 750 kV joining Polish and Ukrainian systems from Rzeszów to Chmielnicka (disconnected in 1993, at the end of 2015 re-start is planned).
- In the west with Germany (transmission capacity 3 700 MVA)
 - two 400kV double-circuit transmission lines connecting Polish and German systems from Krajnik to Vierraden (line temporarily operating at 220 kV),
 - two line 400 kV Mikułowa – Hagenverder.

The biggest volume of actual power flows was directed from Poland to the Czech Republic and Slovakia, while most of physical flows came from Germany.

Poland was net electricity exporter in 2012. Balance of electricity cross-border exchange between Poland and neighbouring countries amounted to 2 840 GWh.

In 2012 there were no cases of limiting available cross-border transmission capacity due to lack of capacities or network failures.

There are planned next interconnection projects between Germany and Poland: GerPol power bridge between Plewiska and Eisenhüttenstadt - AC 380 double circuit OHL of 252 km with capacity of approximately 3 750 MVA (final stage after 2022), and the construction of a new internal line between Krajnik and Baczyna, as well as Mikułowa and Swiebodzice to extend existing line and upgrade their limitation.

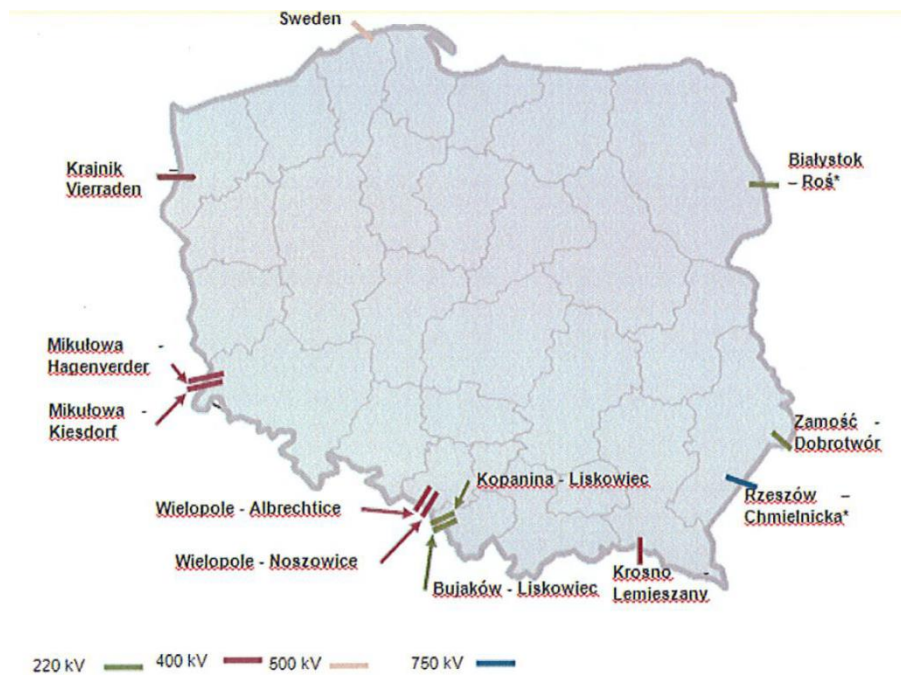
Also upgrade are planned on the existing interconnection between Vierden and Krajnik to 380 kV, and on the interconnection between Mikułowa and Hagenverder (installation of phase shifting transformers).

In the North: Baltic ring, construction of power bridge, cross-border interconnection linking Poland (Elk) and Lithuania (Alytus) is most advanced, planned to start in the end of 2015.

The cross-border connection with Belarus, due to poor technical condition, was excluded from operation (the line has been deactivated).

There is one synchronous connection between Polish and Ukrainian systems. It is a single-track 220 kV line between Zamość and Dobrotvir with dedicated generation units of the Dobrotvir Power Station. From September 2011, a mechanism for transmission capacity allocation was introduced. Capacity provided from Ukraine to Poland is allocated to market participants by explicit monthly auctions.

The cross border electricity interconnections between Polish system and German, Swedish, Slovak, Czech, Belarus and Ukrainian systems are illustrated on Figure 4.



Source: Energy Regulatory Office

Figure 4. The cross-border electricity interconnections between Polish system and neighbouring countries systems.

1.6 Development of the Polish transmission system

There is a significant programme of investment in Polish electricity networks. PSE plans to conduct over 2870 tasks including funding for replacement and maintenance of network assets (stations, lines) and cross border interconnections in period 2014-2025. Big share of investment ensures development and modernization of the telecommunication network, including control centres, dispatch communication, power grid control and data teletransmission.

Planned expenditures on investment tasks and projects totalled 22.9 billion PLN.¹¹

Increase in transmission capacity may provide important security, reliability and quality benefits to electricity supply, decreasing the probability of failures and power cuts in future. Increased interconnection may also provide important security advantages, such as access to additional power supplies, on condition that power flows can be controlled.

A detailed list of planned investments projects related to cross-border interconnections included in development plan of the PSE SA for years 2010-2025 is provided below:

¹¹ Energy Regulatory Office Report 2013.

1. Construction of a 400/220/110 kV Ołtarzew substation
2. Installation of TR 400/220 kV 500 MVA in Ołtarzew substation
3. Installation of TR 400/220 kV 500 MVA in Ołtarzew substation
4. Installation of TR 400/110 kV 330 MVA in Ołtarzew substation
5. Construction of a 400 kV Narew /Łomża /Ostrołęka line
6. Construction of a 400kV switchboard at the 220/110 kV Ostrołęka substation
7. Installation of TR 400/220 kV 500 MVA in Ostrołęka substation
8. Installation of TR 400/110 kV 450 MVA in Ostrołęka substation
9. Construction of a 2-track 400 kV Ełk /Łomża line
10. Construction of a 400kV switchboard at the 220/110 kV Ełk substation
11. Installation of TR 400/110 kV 330 MVA in Ełk substation
12. Construction of a 400 kV Siedlce Ujrzanow /Miłosna line
13. Construction of a 400/110 kV Siedlce Ujrzanow substation stage I
14. Extension of a 400 kV switchboard at the 400/110kV Narew substation
15. Construction of a 400 kV Płock /Olsztyn Mątki line
16. Extension of a 400/110 kV Olsztyn Mątki substation
17. Construction of a 400 kV Łomża substation
18. Construction of a 2-track 400 kV Ostrołęka /Stanisławow line with a partial use of the route of the existing 220 kV Ostrołęka /Miłosna line
19. Construction of a 400 kV or 400/110 kV Stanisławow substation
20. Construction of a 1-track 400 kV Kozienice /Siedlce Ujrzanow
21. Construction of a Ełk - Polish border line
22. Installation of phase shifters on Krajnik/Vierraden line
23. Installation of phase shifters on Mikułowa /Hagenwerder line
24. Construction of a line of relation Plewiska / Polish border towards Eisenhuettenstadt executing preliminary works
25. Modernisation and extension of a 400/220 kV Krajnik substation
26. Construction of a 400/220/110 kV Kozienice substation
27. Modernisation and extension of a 400/220/110 kV Mikułowa substation
28. Extension of a 400/110 kV Płock substation.¹²

As a result of completion of the above listed investment projects, cross-border transmission capacity between Poland and Germany is expected to rise by 2 000 MW and between Poland and Lithuania by 1 000 MW. By 2020, total export capacity shall increase to 4 600 MW and import capacity to 3 820 MW, including:

¹² Source: PSE Operator SA development plan. PSE Operator 2010.

- with ENTSO-E group (Germany, Czech Republic and Slovakia),
 - export capacity - minimum 3 000 MW,
 - import capacity - minimum 3 000 MW,
- with Lithuania and IPS/UPS (former Soviet Union countries,)
 - export capacity - 1 000 MW (Lithuania), 600 MW (Belarus) and 1 200 MW (Ukraine),
 - import capacity - 1 000 MW (Lithuania), 600 MW (Belarus) and 1 200 MW (Ukraine),
- with ENTSO-E Nordel (Sweden),
 - export capacity - 600 MW,
 - import capacity - 600 MW.¹³

TSO plays key role in prevention and elimination of failures and hazards to safe operation of Polish electric network.

Polish network has been connected to the UCTE system since 1995, than since 2008 PSE has cooperated with European TSO's, within the European network of transmission system operators (ENTSO-E).

PSE SA has cooperated with distribution system operators coordinated part of 110 kV network, and according to the instruction of the transmission system operation and maintenance, TSO dispatch services cooperate directly with DSO dispatch services.

1.7 Distribution sector

In Poland, electricity distribution is managed by 148 different DSOs. There are five legally unbundled distribution companies (PGE Dystrybucja, Tauron Dystrybucja, Enea Operator, Energa Operator, RWE Stoen - Warsaw agglomeration) and 143 DSOs which are not subject to legal unbundling .

Ownership supervision over these groups is performed generally by the State Treasury, while over DSOs indirectly by its holding or parent companies which have not been subject to unbundling process. There is only one DSO that is owned by a company whose main stakeholders are not connected with the State Treasury (RWE).

Distribution systems include 110 kV networks, and below 100 kV, mostly 60 kV, 30 kV, 15kV and low voltage, substations, other installation for delivering electricity to customers.

The Polish medium and low voltage grid consists of :

I. Overhead lines:

- 110 kV line - 32 486 km (some of the lines 110 kV perform functions of transmission lines, complying criterion of n-1),
- 40-60 kV line - 24 km,
- 30 kV line - 3 258 km,
- 15-20 kV line - 230 096 km,

¹³ Minister Gospodarki, Sprawozdanie z wyników monitorowania bezpieczeństwa dostaw energii elektrycznej, Warszawa 2013. . (Eng. Report on the results of the monitoring of security of electricity supply from 2011 to 2012. Ministry of Economy, 2013.

- below 15 kV - 1 354 km,
- low voltage - 144 307 km.

II. Cable lines:

- 215067 km,
- medium voltage - 70 760 km,
- 30-60 kV - 197 km,
- 14-20 kV - 62 651 km,
- low voltage - 144 307 km.

III. Substation:

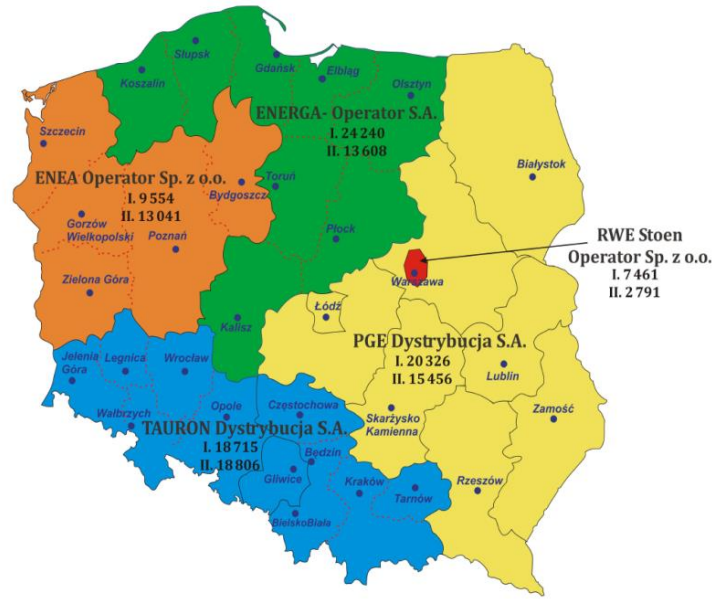
- 110 voltage substation - 1 426,
- medium voltage substation - 249 040.

Characteristic of main distribution company¹⁴:

1. ENEA Operator : area of activity - 58 200 sq. km, 111 100 km of electricity line length, 2392 000 consumers and 17 789 GWh energy sales,
2. ENERGA Operator: area of activity - 74 600 sq. km, 189 300 km of electricity line length, 2892 000 consumers and 22 475 GWh energy sales,
3. Tauron Dystrybucja: : area of activity - 57 100 sq. km; 219 400 km of electricity line length, 5275 000 consumers and 53 093 GWh energy sales,
4. PGE Dystrybucja - area of activity - 122 400 sq. km; 272 400 km of electricity line length, 5132 000 consumers and 34 873 GWh energy sales,
5. RWE Stoen - area of activity - 500 sq. km; 13 500 km electricity line length, 924 000 of consumers and 9 642 GWh energy sales.

Operating activities on main distribution companies are presented on Figure 5.

¹⁴ Agencja Rynku Energi, ARE SA



Sources: Energy Regulatory Office

Figure 5. Main distribution companies operated in Poland in 2012.

Basic network infrastructure, including transmission and distribution grids, was constructed over 30-40 years ago. The average age of distribution network is 30 years, while losses in transmission network in 2011 amounted to 10 774 GWh i.e. 7,3% supplied energy to the system.

2 SYSTEM RELIABILITY AND AVERAGE SYSTEM INTERRUPTION

Reliable and secure energy supplies to all regions in Poland is vital for industrial, transport and domestic customers.

Electricity security of supply depends on many factors, especially the level of electric infrastructure development, the technical condition of electric grids and entities, as well as the amount of generation capacity available to produce electricity to meet demand at any point in time, sufficient security operating reserves and cross-border transmission capacity exchange.

In 2011-2012 years, power system breakdowns mostly related to atmospheric events such as: freezing rain, snowfall, strong wind, which are more frequent and occur with greater intensity nowadays in Poland.

Total unsupplied energy as result of system failure and exceptional weather conditions amounted to 10.01 GWh in 2012 and was lower by 6.62 GWh than in 2011 (and by 16.31 GWh than in 2010).¹⁵

In 2012, the biggest supply interruptions of electricity related to failures occurred in July and amounted to 4.09 GWh. Volume of restrictions on distribution network was caused by high temperatures peak (July 2012) and strong wind (April 2012) and this accounted for 86% of annual volume of supply constraints.

In 2011, the biggest limitation of electricity supply occurred in November amounted to 5.22 GWh. These limits were mainly related to damaged high voltage and medium voltage transmission lines due to intensive wet snowfall. In the Lower Silesia province about 90 thousands households were deprived of power supply, while in Opole province about 10 thousand households remained without power supply for several hours. Also during winter 2009/2010 snowfall, frost, and strong wind damaged many transmission and distribution lines. About 120 000 people had no access to energy supply (about 20 000 of them were deprived of power supply for a period of two weeks).¹⁶

The greater risk of network failure and blackout refers to the northern part of the Polish electric system. This situation is caused by small amount of generation sources and lower density of networks in this area. Unfavourable factor is also an excess of reactive power generated relative to demand, which may result in necessity off on lightly loaded lines. A further major problem of the system is the increasing number of applications for renewable energy connections in the northern part of the system, mainly unstable wind sources.

Additionally, ageing of electrical infrastructure is becoming an increasingly significant factor increasing the risk of interruption.

Basic indicators for measuring duration and continuity of supply reported in Poland for number and duration of outages are: system average interruption duration index (SAIDI), system average interruption frequency index (SAIFI) and momentary average interruption frequency index (MAIFI).

¹⁵ Sprawozdanie z wyników monitorowania bezpieczeństwa dostaw energii elektrycznej 2011-2012. Ministerstwo Gospodarki 2013. (Eng. Report on the results of the monitoring of security of electricity supply from 2011 to 2012. Ministry of Economy, 2013.

¹⁶ M. Tomaszewski, B. Ruszczak Analysis of frequency of occurrence of weather conditions favoring wet snow adhesion and accretion on overhead power lines in Poland. Elsevier, 2013.

The “SAIDI” index shows in units of time average outage duration for each customer, separately for scheduled and unscheduled interruptions, considering grid breakdowns due to disastrous events and without them. It indicates how long, in a given year, energy is not supplied.

The “SAIFI” index is defined as average number of times that a customer’s power is interrupted during a specified time period. Units for “SAIFI” index are “interruptions per customer”. “SAIFI” index is calculated by dividing the number of customer interrupters by total number of customer. There is distinction between long and short interruptions. Long interruption is defined with duration longer than 3 minutes ($T > 3$ min), and short interruption with duration shorter than 3 minutes ($T \leq 3$ min).

“MAIFI” index shows number of customers that can be influenced by effects of all short interruptions during a year. We should have in mind that also short interruptions even up to several second can caused unacceptable high costs.

Indicators for supply interruption in transmission system in 2009-2012 are summarised in Table 3.

Table 3. The indicators for supply interruption in transmission system in 2009 – 2012.

	Unit	2009	2010	2011	2012
SAIDI an unplanned interruption	min/ customer	341,6	316,1	309,1	254,0
SAIDI an unplanned interruption with exceptional events included		408,6	385,5	325,8	263,2
SAIDI planned		145,8	129,8	153,0	147,3
SAIFI an unplanned interruption	no/ customer	4,0	3,7	4,1	3,4
SAIFI an unplanned interruption with exceptional events included		4,1	3,8	4,2	3,4
SAIFI planned		0,8	0,7	0,8	0,7
MAIFI – short interruption	no/ customer	3,3	3,6	3,5	7,7

Source: Statystyka elektroenergetyki Polskiej. Warszawa 2013 r.

The value of the indicators for supply interruption in distribution system in 2012 for 5 main Polish distribution operators are presented in Table 4.

Table 4. Number and duration of distribution network interruption in 2012.

	Unit	Distribution System Operator				
		PGE	Tauron	ENEA	Energa	RWE
Customers number		5164,7	5301,5	2421,1	2916,8	938,5
SAIDI an unplanned interruption	thousand	318,09	197,51	356,25	221,10	58,92
SAIDI an unplanned interruption with exceptional events included	min/ customer	334,50	199,78	374,68	225,10	59,73
SAIDI planned		196,02	164,63	133,09	83,70	16,04
SAIFI an unplanned interruption		3,70	3,07	4,49	3,39	1,27
SAIFI an unplanned interruption with exceptional events included	no/ customer	3,72	3,08	4,50	3,39	1,27
SAIFI planned		0,84	0,88	0,57	0,43	0,15
MAIFI – short interruption	no/ customer	3,97	3,60	2,11	4,78	0,37

Sources: DSO data.

Planned interruptions are designed, informing each network user in advance, to allow execution of scheduled works on the distribution system. Minutes lost over the 2009-2012 period, for planned interruption, range between 129.8 in 2010 to 153.0 in 2011.

Unplanned interruption is defined as an accidental fact, caused by permanent or transient faults, mostly related to external events, equipment failures or attacks made by insiders or outsiders, without notice in advance to the customers. In years 2010-2012, “SAIDI” indicator decreased by about 20%, ranging between 341.6 minutes in 2009 to 254.0 minutes in 2012.

Energy interruptions caused by extreme weather events have occurred in Poland most frequently in 2008-2012 years. Strong wind and high temperature in summer time, and intensive snowfall and icing in winter time, damaged power transmission and distribution line elements, constituting more than 80% of all annual volume of supply constraints.

To cover increasing demand for electricity and improve transmission system security, major new investments in generating and in transmission capacity have been planned foreseen in coming years.

3 STANDARDS AND REGULATIONS

3.1 CIP Directive and other national regulations

Stability of European economy and welfare requires that the energy infrastructure works properly. National authorities are responsible for policies regarding protection of energy facilities and infrastructures in their territories, involving measures oriented to prevent disruptions, mitigate damages and restore supply under the best conditions.

Recently, new international threats have emerged. Intensification of capability in awareness raising, prevention and response is necessary to face this menace. Furthermore, evolution of the energy networks in Europe results on more cross-border infrastructures, creating interdependencies among different countries. In the European vision, dealing with all risks, which could affect energy infrastructures in different sorts of scenarios, is a totally necessary task.

In 2004, European countries took initiative on this issue: the “European Programme for Critical Infrastructures Protection” had been developed to work towards common European approach. This mutual effort has as key tasks the followings themes:

- ✓ Establishment of legal instruments for implementation of EPCIP considering a sectorial dimension,
- ✓ Identification of European Critical Infrastructures in different energy sub-sectors: oil, gas, electricity,
- ✓ Elaboration recommendations and technical assistance to Member States,
- ✓ Follow-up of national critical infrastructure programs,
- ✓ Creation of networks among member states, security technology companies and energy infrastructure operators,
- ✓ Coordination with relevant international organizations.

Elaboration of the Directive was originally launched in June 2004, when the European Council asked for preparation of an overall strategy to protect critical infrastructures. In response, on 20 October 2004, the Commission adopted a Communication on critical infrastructure protection in fight against terrorism, which put forward suggestions as to what would enhance European prevention of, preparedness for and response to terrorist attacks involving critical infrastructures.

In November 2005 the Commission adopted a Green Paper on European program for critical infrastructure protection, which provided policy options on the establishment of the program and the Critical Infrastructure Warning Information Network, where The Commission expressed the need to increase critical infrastructure protection capability and reduce its vulnerabilities.

In December 2005, the Justice and Home Affairs Council called upon the Commission to make proposal for a European Program for Critical Infrastructure Protection “EPCIP”. This Program was based on all risks approach, but giving priority to the fight against terroristic threats.

Efforts of the Commission to develop a European procedure for identification and designation of European critical infrastructures (‘ECIs’), and assessment of the need to improve their protection, had been reflected in a council directive. Under European Legal framework, the Directive 2008/114/EC represents first legal pan-

European instrument regarding critical infrastructure protection. This directive is mainly focused on energy and transport sectors. Complementary to the Directive, the Council has also adopted a set of “Non-binding Guidelines” for its application.

Directive 2008/114/EC constitutes the first element of a step-by-step approach to identify European Critical Infrastructures (ECIs) and assess the need to improve their protection. As such, this Directive focuses on energy and transport sectors and should be reviewed in order to assess its impact and to account for the need to include other sectors within its scope. Each member state shall identify potential ECIs which both satisfy cross-cutting (casualty criterion, economic effects criterion and public effects criterion) and sectorial criteria (energy and transport sectors).

EU critical infrastructure is an asset, system or part located in member states which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, which would have a significant impact in a member state as a result of the failure to maintain those functions.

Each member state shall conduct a threat assessment in relation to ECI subsectors within one year following designation of critical infrastructure on its territory as an ECI within those subsectors.

Figure 6. List of European Critical Infrastructures sectors.

Sector	Subsector	
I Energy	1. Electricity	Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity
	2. Oil	Oil production, refining, treatment, storage and transmission by pipelines
	3. Gas	Gas production, refining, treatment, storage and transmission by pipelines LNG terminals
II Transport	4. Road transport 5. Rail transport 6. Air transport 7. Inland waterways transport 8. Ocean and short-sea shipping and ports	

Source: Commission staff working document Brussels, 28.8.2013

The energy sector remains at core of EPCIP, while both the gas and electricity transmission networks are highlighted as priorities for specific projects under the future EPCIP. As result of work carried out during the following years, the European Union published a commission staff working document, on new approach to the European programme for critical infrastructure protection, making European critical infrastructures more secure (Brussels, 28.8.2013).

This document sets out revised and more practical implementation of EPCIP. It provides analysis of elements of current programme and proposes a reshaped EU CIP approach based on practical implementation of activities under prevention, preparedness and response work streams.

Following this new approach, the EU (led by the European Commission) can play supporting role for member states in their own CI protection and resilience work, and facilitate better cooperation on CI protection and resilience within the EU. Given that many critical infrastructures are privately owned, better cooperation includes supporting development of private-public structured dialogues.

3.2 *ENTSO-E Policy*

System security is one of main goals in operation of interconnected network. In interconnected system (electric power network), there are impacts attributable to the usage of the system by players involved.

Operation of interconnected network is founded on the principle that each partner is responsible for its own network (coordination at regional and European levels, interference of national system and corresponding inter-TSO coordination that requests more and more coordination).

In order to give practical application to basic principle of interconnection that each TSO is responsible for its control area, one of purposes of the ENTSO-E Operation Handbook is to define methods of co-operation. In order to harmonise operating methods for the interconnected network, ENTSO-E has worked out rules, instructions and suggestions, to which the operator of each network has to make reference in order to ease inter-operability.

ENTSO-E has established, through the Operation Handbook, a communication network, that provides necessary infrastructure to support all data exchanges among TSOs. Minimum requirements, rules for implementation, extension, operation and maintenance of the Communication Network of European Transmission System Operators (Electronic Highway, EH) and main application services are explained in this document.

Applications themselves, along with specification of application data for exchange, are described in appropriate policies of the ENTSO-E RG CE Handbook. All relevant data exchanges between TSOs shall be communicated using application services of the EH. If any additional application services are required, ENTSO-E will decide how to build, operate and maintain these services.

ENTSO-E security policy specifies requirements for operating the TRANSMISSION system to protect TSO's physical and information technology assets. Each TSO is responsible of procedures for reliable operation over a reasonable future time period in view of real time conditions and of their preparation.

Therefore N-1 principle has been developed with goal for each TSO to prevent any propagation of one incident, with meaning of "no cascading with impact outside my borders". (N-1) principle is then to prevent emergency condition that appears as result of combination of events. Coordination between TSOs contributes to enhance the common solidarity resulting from operation of interconnected networks, to prevent disturbances, to provide assistance in event of failures with view of reducing their impact and to provide resetting strategies after collapse. This coordination is intensively developed, covering today new aspects related to market mechanisms.

Second edition of this policy focuses mainly on the N-1 rules. The in-deep definition of N-1 is based on:

- ✓ risk assessment considered by each TSO,
- ✓ contingencies and their gravity in terms of consequences for the system to be considered in security calculations, whose goal is to detect constraints of network,

- ✓ area to observe the system by each TSO, in order to get the best survey of constraints to come,
- ✓ operating limits accepted by TSOs with minimum risks for the system,
- ✓ remedial actions to cope with and relieve constraints in due time with simulations of their efficiency in advance,
- ✓ strengthened coordination between TSOs to implement such stronger commitments.

The policy philosophy is the following: TSOs have to be aware

- (i) of risk in their own system due to inside or outside contingencies; they inform or are informed by neighbours and prepare coordinated appropriate remedial actions in order to avoid uncontrolled cascading with impact across borders in operational planning and real time,
- (ii) of the domestic decisions or actions can have influence on neighbouring systems, therefore coordination is obligation.

N-1 principle as described herewith can be summarized as follows:
 “No cascading with impact outside my border”

3.3 Introducing the ENTSO-E Operation Handbook

The main aim of the ENTSO-E Operation Handbook is:

- ✓ To create comprehensive set of technical standards and recommendations
- ✓ To ensure continued secure operation of the ENTSO-E Continental European Grid

Since the end of 2004, the binding nature of the Operation Handbook has been governed by a multilateral agreement.

The Operation Handbook contains the following:

- Currently valid rules and recommendations
- Rules governing critical grid situations
- Rules for communication or data exchange

The Operation Handbook governs collaboration between TSOs, but does not make any statements regarding national grid codes. National regulations that define grid access and adhere to market rules, for example, are complementary to the ENTSO-E Operation Handbook. Regarding Communication Infrastructure, ENTSO-E establishes, on the Policy 6 of the Operation Handbook minimum requirements, rules for implementation, extension, operation and maintenance of the Communication Network of European Transmission System Operators. Attack or failure in the IT system to manipulate part of infrastructure could produce cascading effect in other parts of network. Bases for secure ITC procedures are described in the following definitions:

A-S3. Connection to Internet. There must not be any direct physical or logical connection between EH and Internet. Data exchange between EH and the outside world should be done under full security procedures. Separation of EH from insecure networks must be guaranteed by use of intermediate gateways. These gateways must be located in Demilitarized Zone (DMZ) separated by different firewalls from both Internet and EH.

A-S4. Private Network. Electronic highway:

A-S4.1. Shall use only protocols and applications as specified in the TRM.

A-S4.2. Must not have direct connection to Internet.

A-S5. Dedicated network for data exchange. The EH is main and preferred communication media for data exchanges among TSOs related to operation. The EH should also be used as communication media for data exchanges among TSOs related to market.

A-S6. Incorporation of new protocols and applications: Procedure for requesting new protocols and applications is described in TRM.

A-S7. Requirement for EH interconnections

4 STANDARDS AND REGULATIONS IN POLISH LAW

National legal regulations concerning rules of functioning of the Polish power energy sector are defined in the Energy Law Act, dated 10 April 1997, as amended, and related executive regulations issued under that act by the Ministry of Economy or the Council of Ministers.

The Energy Law Act defines principles of development of energy policy, rules of supply and use of fuels and energy, and operation of energy entities, as well as determines bodies in charge of energy economy.

Energy Law regulates the functioning of the whole energy market and the security of system operation, as well as creates conditions for sustainable energy sector development.

Energy security issues, concerning security of power supply by securing operation of the power system, are regulated by:

- allocation for TSO obligation to maintain equipment, installation and network to carry out supply continuously and reliably (Article 4.1),
- definition of financial penalties for failure to comply with obligation to ensure continuity of supply (Article 11e.1 - 11e.4),
- determination of eligibility requirements (only in field of electrical qualifications) in respect of persons engaged in construction, operation and maintenance of equipment, installations and networks of power (Article 54),
- identify financial penalties for not maintaining proper condition of facilities, installations and equipment (Article 56.1).

Energy Law does not contain separate requirements with respect to operation of computer control systems (ICS SCADA) and other ICT systems to support the operation and maintenance of transmission system operation. It must therefore be assumed that they are integral part of the transmission network as its equipment and installations.

Key actors on the Polish energy sector are: The Ministry of Economy, The Ministry of Environment, The Ministry of Treasury and The President of Energy Regulatory Office (ERO).

There are also several governmental agencies under the supervision of the Ministry of Economy and Environment, working in energy sector development.

The Ministry of Economy is responsible of energy policy and tasks in energy security. The Ministry of Treasury represents government as owner of companies fully or partly owned by the State. The Ministry of Environment is responsible for environmental aspects of energy production and utilization, including CO₂ and other greenhouse gas emissions, and environmental fees.

In reference to Article 4 of Directive 2009/72/EC, President of “ERO” has responsibilities for monitoring and regulating the energy system, controls method of fulfilling statutory responsibilities by the energy system operators and assess their actions in terms of ensuring proper functioning of network, according to criteria described in grid codes. Moreover, possibilities of covering demand for energy and peak capacity in the electricity system, as well as level of necessary capacity reserves are also assessed by “ERO”. These tasks are performed ex post and relate to assessment of operational security of electricity system in context of

meeting obligations by electricity system operators. Annually assessment on energy security is presented to the Minister of Economy.¹⁷

4.1 Energy Policy

According to Polish Energy Law, the Polish Government (the Ministry of Economy) is obliged to publish, every 4 years, a document on Energy Policy.

Current document “Energy Policy of Poland until 2030”, was adopted by the Council of Ministers on 10 November 2009, presents strategy of the state which aims to address the most important challenges that the Polish power industry must face, both in short and in long run, until 2030.

Energy Policy specifies that strategic objectives of this policy are as follows:

- to enhance energy security of the country,
- to reduce environmental impact of the power industry, environmental safety of the country,
- to improve of competitiveness and energy efficiency of the economy.

Energy security is defined as state of economy, which enables to cover current and future fuels and energy requirements of consumers, in way technically and economically justified, with minimisation of negative impacts of the energy sector at environment and at living conditions of the nation.

Environmental safety is a condition in which influence and pressure of economy, including the energy sector, on environment is decreasing. Such condition allows to maintain - at least at current level - biodiversity, enables effective protection of people’s health and lives, as well as effective preservation of natural and landscape values, and ensures also effective compliance of the country with the international obligations in the field of environment protection.

Improvement of energy efficiency of economy means reduction of primary energy consumption per unit of Gross Domestic Product and is a significant element of sustainable development of the country. It also means reduction of energy intensity of products, and energy intensity of industrial processes, increase in energy production efficiency, reduction of energy losses in its transmission and distribution etc.

Long-term forecast of energy economy development is an integral part of energy policy. This forecast includes the following components:

- forecast of primary energy and final energy requirements (included energy from RES),
- forecast of electricity requirements and of its coverage,
- forecast of energy intensity and electricity intensity of economy,
- forecast of the atmospheric pollutants emissions.

Poland, as member state of the European Union, implements Community legislation, energy goal and programs, including the "20-20-20" goal, which are reflected in energy policy.

¹⁷ Energy Regulatory Office Report from 2010-2012.

The energy policy specifies also strategic objectives of the RES as follows:

- achieving 15% RES in 2020 in final energy use,
- achieving 10% share of biofuels in liquid fuels market by 2020, and increase use of second generation biofuels,
- forest protection against excessive exploitation for biomass, and sustainable use of arable land for RES.

4.2 *Instruction of Transmission System Operation and Maintenance*

Fulfilling obligation resulting from article 9 g of the Energy Law Act, transmission system operator developed an “Instruction of Transmission System Operation and Maintenance” - the terms of use, operation, maintenance and planning of network development (Polish abbreviation IRiESP).¹⁸

“Instruction of Transmission System Operation and Maintenance” defines detailed rules of using transmission networks by system users and consumers and terms and methods of operation, maintenance and planning of development of electric networks, including:

- ✓ terms of connecting the generating facilities, distribution networks, final customers facilities, inter-system connections and direct lines,
- ✓ technical requirements for facilities, installations and networks including necessary auxiliary infrastructure,
- ✓ security criteria for operation of the power system including reconciliation of actions plans in case of occurrence of significant disturbance in the power system and restoration of such system after disturbance,
- ✓ terms of cooperation between power systems operators, including area of coordinated 110 kV network,
- ✓ terms of exchanging information between electric utilities and the customers,
- ✓ power quality parameters and quality standards of service of system users and customers.

Rules concern balancing and management of system limitations are specified in separate part of IRiESP - system balancing and management of system constrains (Transmission Grid Code) and defines specifically:

- ✓ terms which should be met in area of balancing of the system and management of system constraints,
- ✓ procedure of submitting and accepting by the TSO for execution of electricity sale contracts and electricity delivery and collection programs,
- ✓ procedure of notification to TSO about contracts regarding provision of transmission services,
- ✓ procedure of balancing the system, including method of settlement of costs of its balancing,

¹⁸ Official Journal of 2003 No 153 item 1504 as amended.

- ✓ procedure of management of system constraints, including method of settlement of costs of such constraints,
- ✓ emergency procedures,
- ✓ operating procedure under conditions threatening security of electricity supply,
- ✓ procedures and scope of exchange of information necessary to balance the system and manage system constraints;
- ✓ criteria for dispatching capacity of the generating units and managing power system connections.

The “Instruction of Transmission System Operation and Maintenance”, also contains: dispatching instructions, instructions for operation of facilities, circuits, equipment and installations, organisational and technical standards and procedures . Balancing rules of distribution systems are consistent with rules given in the Transmission Grid Code. Both Transmission and Distribution Grid codes are approved by the President of Energy Regulation Office. The regulator is the authority that monitors the operation of transmission and distribution companies and gives incentives for companies to compete with each other.

Activity of TSO as the most important entity in energy security area is defined by the Energy Law.

The Instruction of Transmission System Operation and Maintenance is a mandatory document drawn up by the TSO and approved by the Energy Regulatory Office, governing conditions of use, operation and planning of network development (technical part) and principle of balancing and congestion management.

Technical parts of the IRiESP defined security requirements:

- chapters 2.1.2.3.6-2.1.2.3.10 defined parameters of reliability of transmission network, in particular parameters determined by boundary beyond which is failure of this network,
- chapters 6.3-6.6 described computer control systems for managing work of transmission network and exchange control information with installations, equipment and networks connected to transmission network. These chapters, however, does not describe safety requirements of these systems in both the TSO, as well as requirements for entities exploiting ICS connected to ICS TSO.

4.3 Conclusion

After this analysis above law and regulations, according to which operation and maintenance of transmission networks is conducted, it must be emphasized that they do not define precise requirements for IT security information control systems, as well as computer networks, telecommunications and other systems supporting operation of the transmission.

There is no indications in the above mentioned regulations regarding obligation to conduct risk analysis in the field of IT security, nor respect norms and standards that can be used in selecting securities.

In this situation, the process of ensuring security of ICT by the TSO may potentially be of interest only at moment of failure of transmission network, while the recovery depends on whether the TSO kept it in good condition. This means that due to lack of formal security requirements, risk in operation of the ICS can be continuously high, because definition of scope of costly operations to maintain safety of ICS is sole responsibility of the TSO and his will.

5 ATTACK SCENARIOS

Analysis observed in recent years on cyber-attacks indicates that in this area methods for their implementation have been standardized. The reason for structuring harmful activity is profitability, which is associated with cybercrime, while what remains still weak is detectability. A poor protection of victims (institutional and private), their low awareness of cyber security, the lack of definition of international organized cybercrime and cyberwar, and a limited cooperation of many countries in prevention and criminal activities, contributed to make cybercrime a very profitable branch of crime. Application engineering attacks increases likelihood of achieving target, while minimizing risk of being detected.

In addition, degree of quality of organization of crime has been raised by inclusion of cyber-war governments of some countries.

Currently, the most effective method of carrying out attacks is through targeted attack techniques (advanced techniques of attack), which consist in the fact that attack is conducted against a specific victim and with specific purpose.

In targeted attacks, the first step is identification, consisting of the following phases:

- Terms of expected effect of attack - can it be stealing data, embarrassment, business interruption, blackmail, calling for riots earnings. In addition, they can come into play political motives.
- Search for victims of attack - after determining goal methods of its achievement are analyzed, if goal is to disrupt work of transmission system, searches may be information about his previous failures. Methods of operation analyse potential victims, technical aspects related to business activity. It narrows down a group of victims.
- Gaining knowledge about victims - after lists of potential victims are identified, their websites are searched, employees and collaborators are identified, as well. Intelligence methods are used in order to develop the most precise plan of attack. Identified victims are recognized and developed by operating systems, applications, types of servers, IP address pools, operated web sites, e-mail addresses. In this phase, knowledge about victims of attack is ordered and tools such as mind mappery are used in standard IT projects and research.

These preparatory phases of attack are often implemented without any interaction with a victim, so there is practically zero chance of detecting threats. Moreover, the situation is complicated due to fact that normal methods of operation of some online services such as search engines, which are continuously searching the internet and index your content, are obscure and conceal fact of performing preparatory action.

Next stage of attack is linked to performance of intrusion. It consists of the following phases:

- Search for vulnerabilities - by scanning internet computers available in attacked company, its suppliers, employees and exploration of potential holes that can be used to implement attack. In case you cannot find simple methods to introduce malicious software to a victim's system, for example through exploration of potential holes in the website, purchased or developed are 0-day vulnerability types and are referred to lists of potential people to whom they will be delivered.

- Provide malware - by using anonymizing services such as TOR networks or computers not connected with other victims of attack, malicious code is delivered to victims. Method may be sending an electronic message, to encourage online forum to open link, and if you find ready susceptibility it is easy to break security of servers.
- Hiding possible to detect traces of tampering - striker often in this phase alone removes susceptibility servers and computers that were used to break (motivation may be fact that at moment of use by someone else he would lose control over the victim), and obscures its presence in a victim's computer system.

Because at this stage there is no longer direct interaction between computer systems of a victim and an attacker, as well as between the subject carrying out attack and employees or co-operators of a victim, extremely important for success of burglary is quality of activities carried out in phases prior to burglary. List of affected people may not be long, just as it is not advisable to attack a large number of computers. Important for success of this phase are aspects such as correct use of language of victims, ability to establish its operations and current activity. A victim could not suspect that something strange is happening.

Next phase is attack phase:

- Reconnaissance on a victim system - in this phase an attacker acting out of closet, searches available, on a victim system, sources of information such as network shares, email, internal corporate portals, in order to gain information about network structure, used systems and applications used naming structure accounts users and computers. These actions may be extended in time, stolen data portions are often sent at irregular intervals. Particularly important in this phase is delicacy of conducting attack, which minimizes likelihood of being detected, as any mass or violent actions will be in fact detected even by not well-prepared organization. In this phase, an attacker will try to get to know victim's safety systems and preparation of defence. Special-purpose attack may be implemented, where test will check effectiveness and time it was discovered and use procedures for responding to incidents.
- Conduct proper attack - action may include immobilization of victim's ICT system, stealing large amounts of data (eg. financial), disruption of business processes and such activities as publication of undesirable content on the website. Often action is carried out in time in which most employees have already left the victim from work (unless it is for example necessary that victim equipment were turned on during attack). Depending on course of previous phases, as well as expected effects, logical malware bombs, malware triggering their actions in certain time or after fulfilment of defined conditions.

Success of this phase depends largely on whether methods used on the victim side regarding safety monitoring will help to identify the fact that an attacker operates inside the system.

Last step is removing traces of attack. An attacker deletes logs from computers that are used to attack, eliminate, where possible, malicious code used to attack. Errors made at this stage could delay detection of perpetrators of attack, so it's important for an attacker to observe diligence in removing traces of attack.

Analyzing profiles of attackers and their motives highlights some relationships:

- The degree of severity of attack is proportionally dependent on knowledge and resources (financial and intellectual) of an attacker: in case he has sufficient knowledge and financial resources (eg. need to buy 0-day vulnerability with almost 100% efficiency), he would be able to attack victim's computer system,
- The moment selected for the attack is dependent on its expected effects.

From the perspective of an attacker, the most convenient moment will be a time that may result in achievement of the greatest chaos, and the most negative effects of media for a victim, which from perspective of an attacker may be more important than resulting damage.

From the above information, we can deduce two theses :

1. Providing malicious software to victim's ICT system will be probably highly efficient. The success of this phase is determined by the quality of recognition of victim, possession of malware which uses vulnerabilities for which no vaccines yet announced or use of obfuscation techniques malicious code.

A victim at this stage has probably no knowledge about activities that are carried out with respect to hostile actions;, the victim will not get support from software and protective systems, which will not be able to identify hazards because they do not understand.

In addition, attacks do not have to be directly carried out against employees of victims in their workplace. They can be carried out against subcontractors and their employees, and employees of a victim can be attacked on their profiles or private computers where their vigilance can be reduced.

2. The freedom of action of a striker in the reconnaissance phase, at stage of attack, allows propagation of incidents and achievement of his objectives. It is also at the first stage of the attack that a victim is able to detect incident.

At the same time the last phase of which will not be forensic analysis.

There are many documents and publications describing different methodologies to define attack scenarios in general and particularly for both, protecting power network targets and defining security during the design of information systems. As it is mentioned by Jie Feng in the paper "*Generating Attack Scenarios for Attack Intention Recognition*"¹⁹, published in the International Conference on Computational and Information Sciences (ICCIS) in 2011:

"The common methods of modelling attack scenario are attack tree and attack graph, but these methods are not suitable for attack intention recognition."

It is important to take into account that the paper was focused on attack intention recognition.

Main objective of the current document, in addition to being one of the key ESSENCE project goals, is to elaborate base scenario that will be used in cost-benefit assessment of adoption of comprehensive Critical Infrastructure Protection standards.

It is also worth recalling that security standards introduced into the ESSENCE project evaluation were: ISO 27002, ISO 27035, ISO 27036, NIST 800-53, NERC CIP, ANSI/ISA 99, IEC 62443 and IEC 62351. All

¹⁹ Generating Attack Scenarios for Attack Intention Recognition. Feng, Jie *et al.* International Conference on Computational and Information Sciences (ICCIS). October 2011. 10.1109/ICCIS.2011.156

these security standards share a common framework, security awareness regarding information and communication systems in industrial environment (more specifically power networks). In other words, security in power network systems is the focus of the ESSENCE project.

In order to elaborate complete scenario definition, a set of layers has to be identified, described and featured. In the next sections of this chapter, the following points regarding a power network system will be described, providing the reader with certain knowledge about how the subsequent questions can be solved:

- a) Attack source (type of attacker, knowledge and recourses):
 - Who can proceed with attack to power network?
 - What is potential knowledge?
 - What are available resources?
- b) Reasons and objectives of attacks:
 - How are attackers motivated? (reasons for the attacks)
 - What are goals of potential attackers?
 - How are facilities identified as target?
- c) Types of attacks (cyber-attack, damage to the active network elements):
 - What are likely forms of attack against the power network infrastructure?

5.1 Attack source (type of attacker, knowledge and recourses)

Determining the best security practices for ICS/SCADA systems and tackling backdoor interface vulnerabilities in SCADA systems are two of current issues studied in this document. Identification of attack sources enables mitigation of potential infrastructure threats.

Generally, attackers intend to generate impact, the greater the better. A common example of this would be attack against infrastructure by a terrorist group in order to generate global impact at country level, or even on international basis.

However, not only terrorist groups are interested in causing impact on infrastructure. Ecologist groups, other protest sectors, or just hackers trying to show off their own abilities could carry out actions against IT infrastructure in the power network, compromising its well-functioning.

Insiders, people with legitimate access to the system, have to be considered in addition to possible attackers previously mentioned. Insiders are type of attacker very difficult to control, network might be secured against threats according to the state-of-the-art and insiders might still be able to find ways to breach security measures. The following quote from the official website of the Federal Bureau of Investigations (FBI) in the U.S.A. highlights this problem²⁰:

“A company can often detect or control when an outsider (non-employee) tries to access company data either physically or electronically, and can mitigate the threat of an outsider stealing company property. However, the thief who is harder to detect and who could cause the most damage is the

²⁰ Federal Bureau of Investigations (FBI). The insider threat. <http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat>

insider—the employee with legitimate access. That insider may steal solely for personal gain, or that insider may be a “spy”—someone who is stealing company information or products in order to benefit another organization or country.”

The FBI also provides set of recommendations to protect ITC infrastructures from this kind of threats²¹:

- ✓ Protect the intellectual property.
- ✓ Beware of personal factors.
- ✓ Control organizational factors.
- ✓ Monitor behavioural indicators.

In addition, the FBI suggests a list of measures for organizations to do their part to stop intellectual property theft:

- ✓ Educate and regularly train employees on security or other protocols.
- ✓ Ensure that proprietary information is adequately, if not robustly, protected.
- ✓ Use appropriate screening processes to select new employees.
- ✓ Provide non-threatening, convenient ways for employees to report suspicions.
- ✓ Routinely monitor computer networks for suspicious activity.
- ✓ Ensure security personnel have the tools they need (including computer network security).

5.2 *Reasons and objectives of attacks*

In general, power infrastructure attackers want to achieve their objectives for getting either personal satisfaction or reward. For example, regarding ITC systems, malicious attackers who delete or alter information normally do it in order to show security breach or take revenge for something. Therefore, commonly, terrorist groups commit acts of violence to²²:

- ✓ Produce widespread fear.
- ✓ Obtain worldwide, national, or local recognition for their cause by attracting the attention of the media.
- ✓ Harass, weaken, or embarrass government security forces so that the government overreacts and appears repressive.
- ✓ Steal or extort money and equipment, especially weapons and ammunition vital to the operation of their group.
- ✓ Destroy facilities or disrupt lines of communication in order to create doubt that the government can provide its citizens with protection.

²¹ Federal Bureau of Investigations (FBI). The insider threat brochure. http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure

²² Terrorism research. Goals and Motivations of Terrorists. <http://www.terrorism-research.com/goals/>

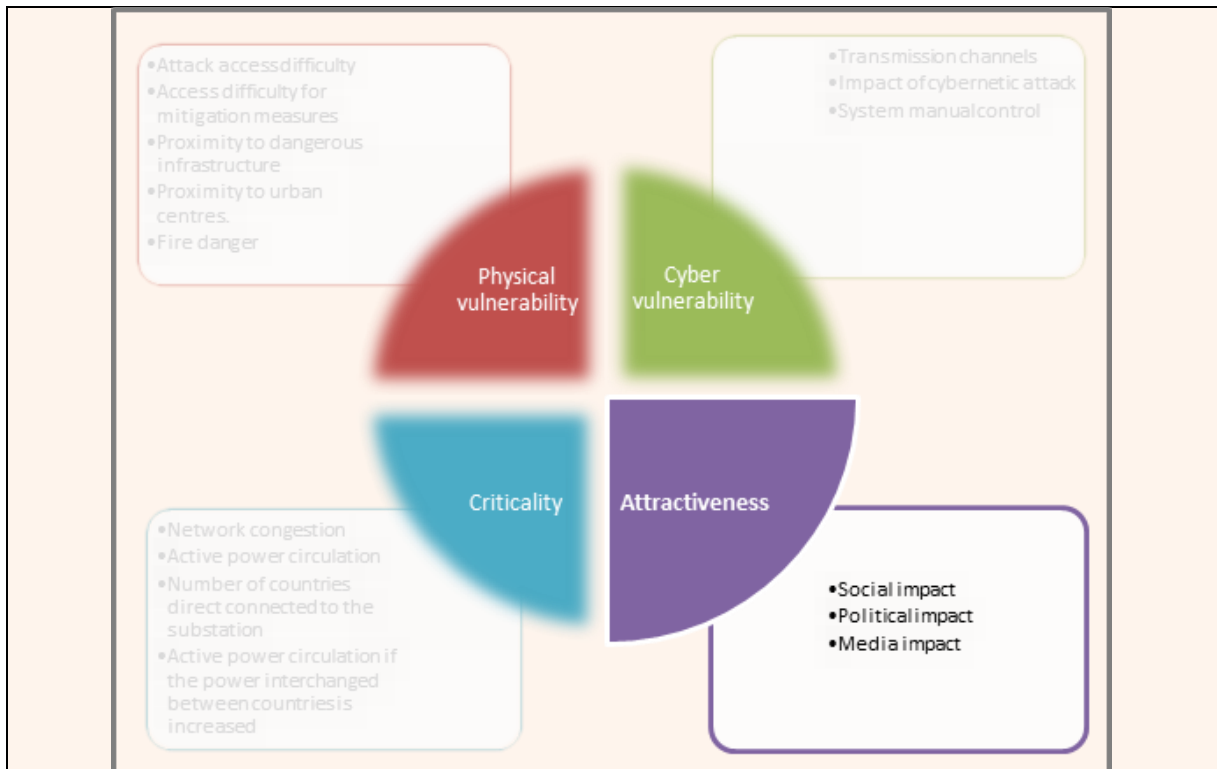
- ✓ Discourage foreign investments, tourism, or assistance programs that can affect the target country economy and support the government in power.
- ✓ Influence government decisions, legislation, or other critical decisions.
- ✓ Free prisoners.
- ✓ Satisfy vengeance.
- ✓ Turn the tide in a guerrilla war by forcing government security forces to concentrate their efforts on urban areas. This allows the terrorist group to establish itself among the local population in rural areas.

“Guidelines to define standards and procedures, and protection government schemes” is a document published in April 2010 as part of the project “Net Protection - EU Interconnected high voltage electricity grid security approach” (project funded by the European Commission, Directorate of General Justice, Freedom and Security). The document defines elements that take part directly in evaluation of security of each component of the electricity network. These elements are related to physical and cyber vulnerability, criticality and attractiveness of assets.

One of major motivations for attempting against power network infrastructures is behind concept of attractiveness; an attacker might see it as challenge. The following text supports this assertion and recovers part of the Guidelines established in Net Protection project, which drive perfectly possible motivations in terms of attractiveness of target infrastructure.

Elements that take part directly in evaluation of security of each component of the electricity network have been divided into four security aspects:

- ✓ Physical vulnerability.
 - ✓ Cyber vulnerability.
 - ✓ Criticality.
 - ✓ Attractiveness.
- (...)



(...)

Attractiveness

This concept measures consequences of malicious attack in terms of social, political and media impact. Attractiveness of infrastructure can sometimes be related to criticality, as mentioned impact may be directly dependent on importance of infrastructure in the system.

Attractive infrastructure is one whose disconnection implies political relevance, or has media impact or is considered as critical by society. Infrastructure can have some critical importance in terms of system operation, but not implying social, political or media impact.

Security characteristics of the attractiveness are detailed below.

Security aspects	Maximum score	Standard	Security characteristics
Social impact	9	3	<ul style="list-style-type: none"> ▪ Social visibility of the attack ▪ Number of people with cut off energy ▪ Facilities affected (hospital, educational centres, etc.)
Political impact	6	3	<ul style="list-style-type: none"> ▪ Industries affected ▪ Interconnections affected ▪ Political organisms affected
Media impact	4	2	<ul style="list-style-type: none"> ▪ Policemen needed ▪ Firemen needed ▪ Location of the attack ▪ Impact on other sectors

Social impact is related to interest of an attacker to select one location instead of another to carry out malicious attack. This selection will depend, among others, on negative impact caused to society. Therefore, the attacker would prefer to plan attack against specific location where his/her action leads to greater chaos; affecting higher number of citizens, destroying emblematic buildings, etc.

Political impact is also one of reasons that attract attackers. Interest of the attacker (most likely, terrorist groups in this particular case) could be, for instance, to influence on political life, resulting in damages on international agreements or political bodies.

Lastly, media impact is one of major ambitions of attackers. Aim is to draw attention of mass media, which can be seen as means of showing impact of their malicious acts around the world, since attackers take advantage of mass communication tools that keep citizens informed. Degree of attractiveness would be directly related to mass communication.

5.3 Types of attacks (cyber, damage to the active network elements)

As it was mentioned in the document “Attack scenarios - Threats, vulnerabilities, and attack scenarios along with their selection criteria” of ESSENCE project:

“The ease and speed of access is then a double-edged knife as it allow individuals and organisations to interfere with these operations from remote locations for malicious purposes, such as sabotage and fraud.”

Typical methods of cyber-attack against energy systems include:

- ✓ Social engineering.
- ✓ Malware: viruses, Trojan horses, worms and spyware.
- ✓ Denial of Service (DoS), distributed Denial of Service, and permanent Denial of Service.
- ✓ IP spoofing or stealth of Domain Credential.

- ✓ Replay attack.
- ✓ Man-in-the-middle.
- ✓ Cross-site scripting.
- ✓ Phishing attacks and local DNS poisoning.
- ✓ Logic bombs.
- ✓ Passive wiretapping.
- ✓ Structured Query Language (SQL) injection.
- ✓ War dialing and war driving.
- ✓ Scanning.
- ✓ Zero-day exploit.
- ✓ Password cracking.

Retaking previous points, electric systems are becoming more dependent on ICT infrastructure, which monitors distributed components (Remote Automation Solutions, RTU) and computer environment. This fact results in large amount of advantages, such as real-time information on the system that can be used to detect problems, as well as to ensure its correct operation. Besides, Internet allows for controlling the system and communicating with it from anywhere using SCADAs. However, this ease of access to systems might pose an important threat: individuals and organizations are able to attack systems from remote locations and in a secure manner as it is difficult to identify and arrest them.

There are a large number of potential methods of attack, depending on the used tools and techniques, as explained before in section 4 of this document. However, from point of view of electric networks, it is more important to identify effects of attack on the system than their origin or source. Main effects are the following:

- ✓ Steal of confidential information.
- ✓ Manipulation and remote control of the system.
- ✓ Change or loss of information: Modify, erase or corrupt files.
- ✓ Hindering or slowing down of operations.

Steal of confidential information

Some attacks are intended for getting some confidential information, such as passwords or logins. Sometimes, passwords are used to enter the system and cause further damages, such as loss or change of information or loss of control of the system. In these cases, this attack is only a way to get real objective of the attacker.

However, stolen information can be used directly to cause damage. Attackers can steal confidential information on a company to steal money, to impersonate the company, to commit fraud or forgery, or simply blackmailing the company by threatening it to make public confidential or sensitive information if the company does not pay a ransom or take action.

Manipulation and remote control of the system

When the attacker takes over the system, he can cause big damages. He could control and hinder communications with the system, and make it uncontrollable for legitimate users. It is easy to imagine damages an attacker could cause: get information on the system and data on people, hinder maintenance and operation activities, disturb power supply, cause blackouts, slow down control in emergency situations and even destroy the system (and related assets).

Change or loss of information: Modify, erase or corrupt files

Viruses and other types of attacks can change historic or current data, corrupt or erase files, or all hard disks. Maybe change of information can be more dangerous, as it is more difficult to detect, unless somebody looked into data and discovered changes. Another option would be controlling communication between parties by means of changing messages they receive and send (this attack can be used to steal information, too).

Hindering or slowing down of operations

Some attacks are intended to disrupt communications and avoid control of the system or exchange of information between people. This can be done in order to control or manipulate the system, but sometimes, objective of the attacker is simply avoiding communications or making operators lose control of their systems. In these cases, system operation is not controlled, and possible breakdowns, accidents and emergencies (not directly caused by the attacker) would not be discovered.

Typical way to get this is Denial of Service (DoS). The attacker prevents legitimate users from entering systems using variety of methods: forcing repeatedly the system to reset or saturating a computer with external communication requests in such way that it cannot respond legitimate requests. Other possibility would be using programming flaws which, if activated, consume large amounts of memory.

6 VULNERABILITIES CHARACTERISTICS OF TS ELEMENTS (PHYSICAL NETWORK ELEMENTS, ICS)

After reviewing attack sources, reasons to attack and way to measure risk to be attacked, as well as types of attacks, it is time to study different elements which can be attacked in an electric grid.

In the following sections configuration of information and communication systems of different transmission network elements is described in high detail, as well as their vulnerability.

First of all, it is important to consider some ideas about these assets:

- ✓ Many parts of the transmission system cannot be effectively protected, as they are in field. For example, cables or tubes are easy to locate and access because they can be seen, and they are not protected.
- ✓ Other parts, such as substations and many control points are isolated, only protected by fences, or electronic systems such as cameras, and controlled by means of control centres far from a facility. As there are no personnel to guard them, they can be easy to access to produce damages.
- ✓ The biggest power plants, like thermal or nuclear ones are carefully controlled, but minor facilities, like smaller thermal plants, hydro or wind power are not closely attended, and so they are easy to attack.
- ✓ When a facility is designed, some redundancy is included to fight normal incident with minor disturbances. This is called the “n+1” redundancy: “n” essential components plus another backup one. This backup component normally does not take action in process, but it can replace a failing component. However, malicious attacks normally make too many components fail, so this redundancy cannot avoid damage.
- ✓ Communication is essential to control electric infrastructures. There is network of control centres, which are connected to all assets, and operators have to keep in contact. Thus, variety of Internet private and public protocols are used to communicate with the company staff (operators and management staff), other facilities or administrations.

6.1 Generation power plants

According to the ease to be attacked, they can be classified as follows:

- ✓ Attended power plants: There are operation and maintenance personnel in the plant. They are the biggest plants, such as big thermal ones or nuclear plants.
- ✓ Unattended power plants: These plants, including small thermal, wind or hydraulic ones, are remotely operated. Then, normally there is nobody in, except for control and maintenance actions.
 - (i) Attended power plants: They include the biggest plants, where there is a control room from where the whole plant is controlled, by means of IT equipment which connects this room with all elements in the plant.
Control room uses SCADA systems with internal cable connections difficult to be accessed. The plant is also connected to the generating company control centre, where information can be received but the plant cannot be operated.

These plants need a number of auxiliary equipment, like a substation, or lines connecting the power plants and the grid, or transformers. This equipment is spread along big extensions, and can be easily accessed. Thus, the power plant itself is highly protected, but auxiliary elements keep vulnerable.

A power plant can be put out of operation not only by directly attacking it, but also damaging substation or cables which connect it to the main power grid.

Finally, it is possible to produce cyber-attack on the power plant, taking control and operating it with malicious intentions. Normally, the power grid is designed to withstand loss of a single unit, but if more units are affected, local or regional blackouts can arise.

- (ii) Unattended power plants: These plants are normally smaller than attended plants, and so impact of attack on the power system will be smaller than attacks on bigger plants. These plants are, however, more vulnerable, as there is no personnel controlling them directly, and they depend deeply on communication systems which connect them to control centres.

Many of these plants are hydro power plants. Physical attacks can affect their structure (dams, channels, etc.), and produce big damages to other infrastructure or citizens. On the other hand, cyber-attacks can take control over the electric infrastructure (for example, water flows can be opened or closed by the attacker).

These attacks can produce variety of events on a power plant:

- ✓ Generator trip: If there is loss of demand, the generator cannot use all the electric supply, so unless an automatic system reduces supply, there can be an over voltage. This can produce fires or explosions.
- ✓ Break of the generator: This event will lead to stop of the power plant, which will be out of service until the generator is repaired or replaced. If attack is produced only in a plant, redundancy of the system can avoid major disturbances, but if many power plants are stopped, blackouts are likely to happen.
- ✓ Backup generator failure: The backup generator is put into operation if other generators fail. For this reason, normally failure of this element has not very severe consequences, but if other generator fails, there will be no alternative to keep the power system on.
- ✓ Turbine malfunction: In power plants, turbine is the first step to produce electricity. They are moved by fluid, which is put into movement by a variety of means. Then the generator transforms movement into electricity using electromagnetic induction. As can be understood, if blades do not rotate, electricity cannot be produced.

6.2 TSO

6.2.1 Substation

Electric substations are well distributed on territory, and they are easy to see and attack. It is true that single attack cannot produce big disturbance in the electric system, as this system has been designed to be redundant, following the “n+1” criterion. However, coordinate attacks can produce damages to a number of elements, leading to local, regional or national blackouts.

Besides, single attack to a substation can affect number of parts, for example attack on bus-bars can damage multiple lines and transformers. For this reason, each attack on a substation will make different effects, very difficult to be foreseen.

Many substations are electronically protected, and intrusions can be detected. However, as they are isolated, defenders cannot reach them immediately, and attackers can produce damage. Apart from it, it is possible to destroy the substation without entering it.

Some examples of vulnerabilities affecting the substation are the following:

- ✓ Insulator failure: If insulators are destroyed or damaged, the substation can suffer short circuit. Short circuits, if not repaired, are likely to produce heating of the parts of the system which conduct poorly electricity, what can lead to fires. Besides, electric arcs can be produced, and generate heat and the ignition of combustibles.
- ✓ Busbar malfunction: Busbars are bars of copper, brass or aluminium that conduct electricity and connect parts of an electric facility. They are used only to conduct electricity, but are not structural parts. They connect multiple parts of the electric circuit, so damages made to busbars can lead to multiple destruction of the system.
- ✓ Transformer trip: Transformers can be damaged because of transient currents which appear due to sudden changes in the exciting voltage. These currents appear, for example, when the transformer is energized, after solving a problem which made the transformer work out with problems, or when another transformer is started.
- ✓ Transformer break: The transformer can be broken by attackers using variety of means, like shooting it or making it explode.
- ✓ Switch malfunction: If a switch does not work properly, the operator will be unable to stop or start any of the elements of the substation. Normally, all elements have an emergency switch, but disturbances can be important.
- ✓ Control malfunction: There are a number of devices controlling the performance of the transformer, like its voltage, power factor or the power flow. Any failure of these devices can produce loss of control over the transformer behaviour, and future more severe problems.
- ✓ Lightning arrester failure: Lightnings are major danger for transformers, as if they strike the transformer, the latter suffers a voltage surge. The over voltage can cause fires and explosions in the transformer.
- ✓ Circuit breaker malfunction: A circuit breaker is used to protect an electric circuit from an overload or short circuit. Thus, if the circuit breaker fails and there is fault in the circuit, it will suffer excess of current, what can lead to fires and explosions.
- ✓ Current transformer malfunction: Current transformers are used to measure alternating currents circulating in a circuit. They are transformers which reduce the current when it is too high to be directly measured by instruments. Thus, malfunction of this element means that real current in the circuit is not known.
- ✓ Control and protective relay malfunction: Relays are used to control circuits using low-power signal, with electrical isolation between control and controlled circuit. Thus, if an operator loses control of the relay, he will be unable to stop or start circuit.

- ✓ Fuse malfunction: A fuse is low resistance resistor which protects circuit from overcurrent or overload. This element is made from metal wire or strip which melts when too much current flows in the circuit, interrupting it. If the fuse does not work properly, circuit can be damaged by too much electric current, or it can be interrupted without need.

There are ICT systems within levels 1-3 according to the logical architecture described in section 1.4.4. on substations.

6.2.2 Power lines and interconnection lines

Similarly to substations, power lines can be easily located and attacked, indeed, in the past most attacks on electric systems were focused on high voltage towers which hold electric cables.

Unlike substations, power lines are not protected at all, and attackers can use explosives, or dismantle the towers with few risk.

Power substations and lines are very easy to locate, moreover companies publish maps showing where their facilities are located. Thus, an attacker can plan the best way to make a big disturbance, choosing the most critical elements.

Sometimes, facilities can be located using Internet tools, such as maps, which are accessible for all Internet users (e.g. Google Maps).

Whereas substations can be protected up to a point, power lines are too widespread, and too long to be effectively defended. Thus, they are prepared to withstand attack affecting a single part, but combined attacks can lead to local or regional blackouts.

Some of main vulnerabilities of power and interconnection lines include:

- ✓ Transmission or distribution line trip: Fail in transmission line can produce dynamic voltage instability, and cut electric supply to affected area.
- ✓ Transmission or distribution line short circuit: Short circuit is produced when electric current travels along part of circuit where it should not, because few or no resistance is found. This leads to transient voltage instability, and cut of electric supply.
- ✓ Transmission or distribution line break: If the attacker cuts cable, electric current cannot circulate by it. Thus, outages can arise, and affect big or small populations depending on importance of line.
- ✓ Power tower collapse: The attacker can dismantle, tumble or destroy (using bombs) the power tower which holds electric cables. These cables would be broken, and electric supply would be cut. Effects are similar to former vulnerability, although problem can be harder to be solved.
- ✓ Underground cable malfunction: Attackers can look for buried cables to disrupt electric supply. Effects are similar to transmission or distribution line break.

Good example of terrorist attacks aimed at cutting supply by destroying elements of distribution system can be wave of attacks that the terrorist group FARC carried out in Tumaco (Colombia). This poor zone, where guerrillas and drug are common, has suffered these attacks since August 2012. Terrorists tumble power towers to cut supply, and install anti-personnel mines all around towers to make it more difficult to restore supply. For example, in August 2012, electric supply was cut for 17 days when 8 electric towers were

destroyed²³. This led to losses about 4 million US\$ and big disturbances to economy and life of 190 000 inhabitants in the zone. 5 people were killed and 6 injured by anti-personnel mines.

Once more, guerrilla attacked 4 towers on Tuesday 1st October 2013 and 3 more on Wednesday 2nd October 2013²⁴, and installed handicraft mines around towers to hinder reparation works. From then, the guerrilla kept attacking towers until 23rd October 2013, what led to more than 24 towers fallen this month. As consequence, zone suffered continuous energy cuts, and economic losses amounted to about 400,000 € per day. Citizens suffered lack of water, which had to be brought using storage tanks. As another example of effects, fishers had to throw or give away fish because they were not able to use fridges.



Source: Radio Santa Fe. Website: www.radiosantafe.com

Figure 7. Civil workers repairing a tumbled electric tower in Tumaco (Colombia).

6.2.3 Control centres

Control centre gathers all relevant information which is collected by the SCADA and other applications that are connected to the power system. Apart from collecting information on the system, it allows operators to take actions to modify it, for example it is possible to put new transformers or other equipment into operation, or modify the topology.

There are 3 different threats that can affect the control center:

²³ Colombia.com. “Se restablece la luz en Tumaco tras 16 días de atentados”. 25th August 2012. <http://www.colombia.com/actualidad/nacionales/sdi/44811/se-restablece-la-luz-en-tumaco-tras-16-dias-de-atentados>

²⁴ Radio Cadena Social. “Reportan millonarias pérdidas diarias por falta de servicio de energía en Tumaco”. 21st October 2013. <http://www.rcnradio.com/noticias/atentado-deja-nuevamente-sin-energia-tumaco-96135>

- ✓ Alarm without destruction: there is alarm, and it is necessary to evacuate the control centre, but finally no damage is produced in equipment.
- ✓ Alarm with destruction: Attack destroys totally or partially equipment of the control centre.
- ✓ Cyber-attacks: They can produce damage to the control centre or not, but always involve a loss of control of the system.

These threats are studied deeply hereinafter:

- (i) Alarm without destruction: It is the easiest to be carried out. The attacker has to send a credible communication to authority making it believe that real or false attack will be produced in the control centre. People in will be evacuated, so there will be a loss of control over the system until real or fictitious threat is eliminated, and security of people is guaranteed.

Sometimes, the attacker takes advantage of lack of personnel and control on assets, carrying out other attacks which cannot be counteracted. Thus, final damage can be considerably bigger.

This attack can be easily avoided if a back-up control centre is created. To do this, only communication channel and a remote operator are needed.

- (ii) Alarm with destruction: Physical attack on the control centre can make it unavailable. The attacker can choose to destroy physical infrastructure of the control centre or some essential equipment that is out of the centre, like communication antennas or fiber optic cables.

Regarding attacks on the control centre, normally it is well protected, and computers are duplicated and allocated in different rooms, so this kind of attack is not easy. On the other hand, antennas and communication systems (radio, microwave or laser) are normally visible and easy to access.

Damage to these systems leads to loss of control on the network, as almost all substations are unattended and companies have no enough personnel to manually operate all substations. Therefore, there will be lack of control and operation capacity until the system is repaired.

Damages can be even bigger if the attacker comes from the company inside. In this case, he/she will know which the more vulnerable facilities are, and where extent of damage can be bigger.

Solution for this can be installing backup systems, but they are expensive, and must be continuously connected to all substations, and kept updated. This implies that all substations need independent computer and communication system.

- (iii) Cyber-attacks: These attacks on computer systems, especially SCADA, take partial or total control on them. Even when these systems are well protected with firewalls, there are some holes in security system, such as:

- a. Back doors or connection facilities: They are used to maintain the system out of office hours. They are protected by passwords and other security systems, but they are not as secure as main system.
- b. Remote Information: The need for connection between technical or management personnel is very high, to transmit or receive information. This lead to a big number of systems in remote offices and other places connected to the main system. Some of these systems can be more vulnerable.

Cyber-attack can destroy software or databases, or control the system.

7 POLISH CASE STUDY

7.1 *Description of the cyber attack case and effects on power plants and electric grid of capital city Warsaw*

Polish case study concern hypothetical serious disturbance on substations on Warsaw Network Node, resulting in a cascading loss of power supply in entire Warsaw city. For purposes of Polish case studies analysis the Warsaw blackout could have taken place on 21st of September 2012, starting at 10 a.m and ending at 4 p.m.

Substations are very vulnerable to attack, as was presented in 6.2.1 and risks of successful cyber-attacks are large.

Carrying out successful attack on indicated substations is possible when the attacker gain access to them resulting in possibility of execution of malicious code, issue invalid command or damage ICT systems gathered there. According to communication scheme of ICT systems can be met by:

- ✓ Attacking local or remote directly from the public or indirectly by the central SCADA system,
- ✓ Independent attacking local ICT systems on many substations,
- ✓ Attacking local ICT system layers on one substation,

Simulation scenarios for these attacks were to check whether there are vulnerabilities possible to use in attacks on individual layers ICT systems and that function of detection methods of reconnaissance and attack propagation, which would allow early detection of incident.

Effects are dependent on what type of device has been compromised (for example, whether it is security or CCTV camera) and level of expertise in the field of electricity. It should be noted, however, that they do not fall beyond a power station where incident took place, and in event of attack on system which is not component of control substation (SE), there will be no other consequences for National Power System than possible data theft. The transmission and distribution network, as well as generation are prepared for occurrence of such accidents, procedures for their disposal exist and are used;

Main factors that can affect propagation of attack are:

- ✓ Use of devices from a single manufacturer for a number of power facilities;
- ✓ Realization of servicing and maintenance on multiple objects by one and the same group of contractors (employees or external service providers);
- ✓ Lack of security monitoring tools to substation and communication between them.

In accordance with the existing communication system, the attacks on the local system or remotely from a central public or SCADA system, as well as on local ICT in many stations allow an attacker through an external supplier infected system for install malicious software, such as logic bomb. External technician, moving between power facilities, will transfer infection to many objects, which can lead to achieve widespread effects of attack.

In the case of a existence of third factor, an attacker who obtains a remote or local access to layers can freely seek vulnerabilities allowing him to communicate with the central ICS Scada or mini SCADA systems at other substations.

In addition, analysed fact that each of these attacks can potentially be performed by a person who normally has access to targeted infrastructure (such as disappointed employee).

7.1.1 Description of the method to simulate attacks

To simulate attacks and determine whether it is possible that they impact on the transmission system operation , the following assumptions were adopted:

- ✓ it was assumed that if vulnerability existed, it was used by the method of attack,
- ✓ it was assumed that the attacker has enough time and expertise to carry out reconnaissance and search susceptibility, unless within logic level have been implemented appropriate countermeasure and security monitoring.

In order to identify a list of countermeasures, implementation of which could result in detection and interruption, or in minimization of the consequences of attacks, according to above scenarios, a table was prepared, specifying for each countermeasure:

- maturity of resulting force in the EU and Polish law,
- impact of countermeasure to minimize likelihood of remote attack,
- impact of countermeasure to minimize likelihood of local attack,
- impact of countermeasure in increasing probability of detection of the attack reconnaissance phase,
- impact of countermeasure in minimizing or shortening the duration of incident.

We identified and analysed 250 countermeasures recommended to implementation for minimum security level of ICT infrastructure.

We have identified:

- ✓ a set of 54 countermeasures, which act to block feasibility of remote attack by unauthorized persons (remote attack means that it was realized from different system than attacked),
- ✓ a set of 78 countermeasures, which act to block possible local attack (with physical access to the console of a system or its products) either by staff or by unauthorized persons,
- ✓ a set of 40 countermeasures, which interact to allow hazard identification stage reconnaissance and preventing its escalation,
- ✓ a set of 39 countermeasures, which interacts to shorten downtime of systems that have been successfully attacked.

We concluded that the feasibility of each described scenario of attack (aimed to disrupt work of several objects of national power system) is demonstrated. At the same time it should be emphasized that estimation is not subjected likelihood of attack scenario, because it is assumed that assessed probability of success is expressed by the attack itself, when the attacker chooses to carry out any attack.

According to authors, mere fact of presence of viable scenarios of attacks should not be over-inflated as existence of high level of risk. Due to high level of implementation on Polish power system objects of physical and environmental protection measures, and high level of implementation of countermeasures in the Central Scada system and business systems, office and DMZ, carrying out attacks using the described scenario is possible only by attackers with very high qualifications and large funds. Today however, organization of physical attack would be cheaper and more effective, with equally low probability of remaining undetected as cyber-attack.

7.2 Energy generation and distribution system in Warsaw

Warsaw is a capital and the biggest Polish city, to over 38 million citizens of Poland, situated in the central part of Poland in Mazowieckie voivodship. Warsaw currently constitutes one borough (in Polish: gmina), also as city with a county (in Polish: powiat) status, with rights of county with 18 districts. City population amounts to 1.714 mln citizens living in area of about 517 sq. km. Warsaw metropolitan area has over 3.3 million people and includes 20 satellite towns. Density of population is 3315 people / 1 sq. km.


Electricity to Warsaw agglomeration is supplied mainly from 5 public power plants and 2 Warsaw cogeneration plants: Żerań and Siekierki owned by PGNiG Termika.

The main public power sources of power supply are:

- 7.1.1. Koźienice Power Plant through a 400 kV line Koźienice-Miłosna and double track line Koźienice-Mory i Koźienice-Piaseczno-Mory;
- 7.1.2. Belchatów Power Plant by 400 kV Rogowiec-Mościska-Miłosna line and 220 kV Rogowiec-Janów-Mory line;
- 7.1.3. Pątnów Power Plant by 220 kV Pątnów to Warsaw Network Node (in Polish: Warszawski Węzeł Elektroenergetyczny²⁵).
- 7.1.4. Konin Power Plant - by 220 kV line Konin-Mory,
- 7.1.5. Ostrołęka Power Plant - by 220 kV line Ostrołęka-Miłosna.

Warsaw cogeneration plants produce in total 3.7 TWh of electricity and ca. 12 TWh of heat per year:

²⁵ Warszawski Węzeł Elektroenergetyczny - Warsaw Network Node are formed from one track 400 kV line from Koźienice – Miłosna and Rogowiec – Mościska, double track line with voltage 400 kV from Miłosna – Mościska/Płock and double track line with voltage 220 kV from Koźienice – Mory/ Piaseczno and also one track line with voltage 220 kV from Janów – Mory, Sochaczew – Mory, Podolszyce – Mory oraz Ostrołęka – Miłosna, as well as a substations: Miłosna - 400/220/110 kV, Mościska - 400/110 kV, Mory - 220/110 kV, Towarowa - 220/110 kV, and Piaseczno - 220/110 kV. (Figure 8)

<p>CHP Żerań has thermal capacity equal to 1 580 MW and electrical capacity to 386 MW, CHP Siekierki has thermal capacity equal to 2 078.2 MW and the electrical capacity to 622 MW.</p>	
---	--

Peak power demand reached 1464 MW in winter 2012. During the winter time Warsaw cogeneration plants Siekierki and Żerań are covering ca. 55% of Warsaw power demand.

Primary energy sources for Warsaw is mainly hard and brown coal and biomass.

The RWE Operator is Distribution System Operator in Warsaw, and PGE Operator in one district - Wesoła.

Length of power line in Warsaw are presented in Table 5.

Table 5. Power lines of the distribution network in the Warsaw area in 2012.

Line type	Length of line	
220 kV power line of high voltage	overhead	8 km
110 kV power lines of high voltage	overhead cable lines	391 km (per one track) 76 km
15 kV power lines of medium voltage	overhead cable lines	299 km 6732 km
0,4 kV power lines of low voltage	overhead cable lines	1339 km (without connections) 5146 km (without connections)

Source: RWE

Type and a number of station are presented in Table 6.

Table 6. Power station in Warsaw area in 2012.

Type of station	Number of stations
400 kV	2 PSE SA owner
220 kV	1 PSE SA owner
110 kV	3 PGNiG Termika owner
220 kV	1 (RWE owner)
110 kV	36 (RWE owner)
15 kV	5998 (RWE owner)

Source: PSE Operator and RWE Distribution Operator

The most important substations for the security of power supply in Warsaw agglomeration are :

- Substations owned by PSE SA
 - Miłosna (400/220/110 kV),
 - Mory (220/110 kV) ,
 - Mościska (400/110 kV)
- Substations 100 kV owned by PGNiG Termika
 - Siekierki
 - Kawęczyn
 - Żerań

There are also important substations belong to RWE, such as: the GPZ Towarowa with autotransformer 220 kV/110 kV/15 kV, with capacity 160 MVA, as well as node substations: Gdańska, Południowa and Wschodnia. Main weakness of power supply system security is lack of double-track 400 kV line closing the ring around Warsaw. In Warsaw network are working 74 transformers of 115 kV/16, 5 kV with rated power of 63 MVA, 40 MVA, 31.5 MVA, 25 MVA, 16 MVA.

The latest failures of electrical system in Warsaw took place in October and December 2012 and was respectively due to heavy snowing and transformer short circuit on Migdałowa substation (RWE). In the southern part of Warsaw, the districts of Ursynów, Natolin, Służew and Powsin were out of electricity from 7 a.m even to 6 p.m in several streets. Also, in June 2009 emergency shutdown of one transformer affected eastern districts: Saska Kępa and Gołław.

In August 2008, primary cause of failure was emergency shutdown of block nr 9 in CHP Siekierki. Although the function of inactive block took 3 other blocks, there was overload of several stations in southern part of Warsaw. Warsaw did not get feed from other sources and 5 substations remained without voltage. The southern districts of Stegny, Ochota, Ursynów, Imielin, Służewiec, and Konstancin stayed without electricity for about 30 minutes. In November 2006, disruption of Towarowa substation (RWE) deprived 60% of Warsaw residents of electricity supply by 302 minutes. The cause of failure was short circuit in the Towarowa transformer station. This came during technical works on this station. It was probably due to an

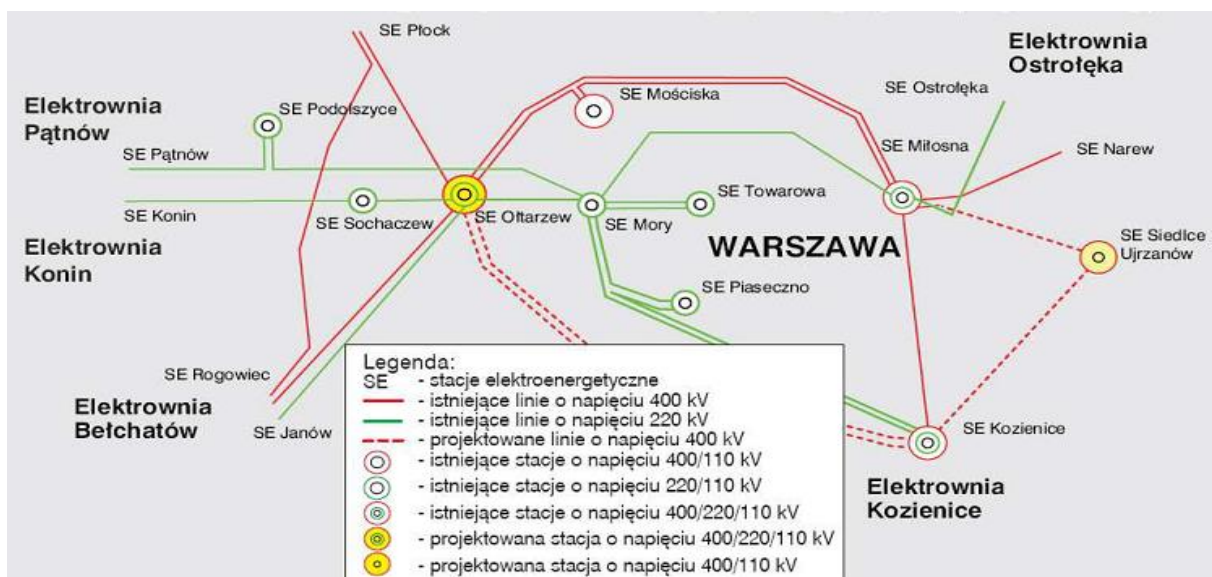
operation mistake, consisting in leaving an earthing switch on a busbar 110kV in running tests. At the time of trial protection devices were turned off, and the busbar protection was missed. Prolonged duration of short circuit has led to exclusion of 3 other stations. Deprived of electricity left several large districts of Warsaw downtown, Mokotów, Ursynów, Ochota, Żoliborz and Wola.

In November 2004, cause of failure was short circuit on 110 kV busbar systems of Południowa substation (RWE) due to rupture and break ceramic insulators VKLF 75/16 type.

As result of short circuit on the busbar all lines extending from the substation have been excluded, including south lines connecting CHP Siekierki, causing asynchronous switching generators in CHP Siekierki. As result of non-synchronous dynamic switching, automation of turbine caused the turbine sets off from work. Power supply shuts off line extending from the busbar 110 kV Siekierki, and outages were expanded.

Left part of Warsaw, in several large districts such as Mokotów, Ursynów, Ochota, Wilanów, Włochy, was deprived of electricity for period of 129 minutes. Also the airport, trams and underground stopped functioning. Such effects of this fault resulted from negligence of technical solutions of Południowa substation. Consequences of failure would have been much greater if turbine sets had been damaged. This technical flaws had already been removed in 2006, as part of modernization of Południowa substation and modernization of automatic system protection structures in CHP Siekierki.²⁶

Main electric sources and lines in Warsaw and elements of planned 400 kV construction of ring around Warsaw (dashed red line) is shown in Figure 8.



Source: Miasto Stołeczne Warszawa, Biuro Infrastruktury.

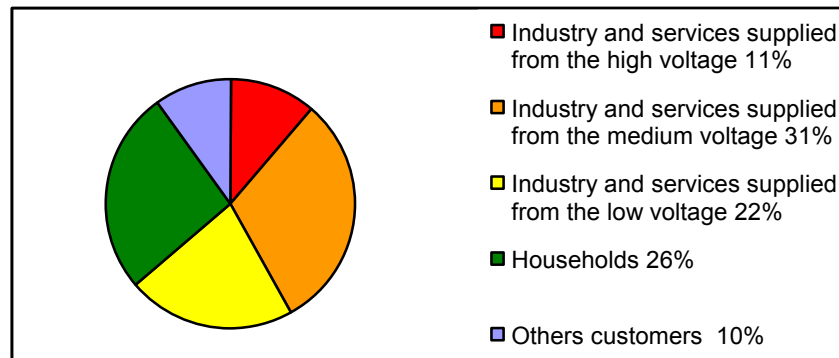
Figure 8. High voltage grid with planned investment related to Warsaw agglomeration

²⁶ H. Dytry, M. Niedźwiedzik, W. Szweicer, S. Wróblewska, Analiza i optymalizacja EAZ sieci wielkomiejskich 110 kV. Instytut Energetyki 2008.

7.3 Specification and statistical data of Warsaw electricity customer groups.

In 2012 electricity consumption in Warsaw reached 7404 GWh. Electricity consumption in household was amounted to 1735,4 GWh, ie. ca. 1014 kWh per capita.²⁷

The Figure 9 presents the structure of electricity consumption in Warsaw.



Source: Agencja Rynku Energii, UM Warszawa.

Figure 9. Structure of electricity consumption in Warsaw

The impact on customers of energy not supplied during an interruption depends on many factors, such as types of interrupted customers, load demand at time of outage, duration, time of the year and of the day, as well as day of week (working day, weekend).

Different customers types could be more exposed to electric interruptions effects and incur higher costs at different times of the year due to seasonal nature of their activities and needs. Some industries in some season or months are more active than in other. Costs of interruption in households primarily depend on whether someone is at home during outages and also some use more energy for heating or cooling in winter or summer time.

Commonly disruption of an electric system may be classified as direct socio-economic and indirect impacts. Direct economic impact resulting from sudden cut of supply includes: lost production, idle but paid-for resources, spoilage of raw materials or food, and equipment damage, direct costs associated with human health and safety, as well as, utility costs associated with interruption.

Direct social impact includes: inconvenience due to lack of electricity at home, lack of transportations, personal injury etc.

Indirect impacts for examples are: civil disobedience and looting during extended blackout, failure of industrial safety device in entities, necessitating neighbouring residential evacuation, etc.²⁸

²⁷ www.um.warszawa.pl, Statistical Yearbook of Warsaw.

²⁸ R. Billington (chair); Methods to consider customer interruption costs in power system analysis. Task Force 38.06.01, CIGRE 2001.

Basically, electricity customers can be divided into following groups: residential, industrial, commercial and services. Warsaw is a home city to over 50 corporate operations hubs and 31% of office stock in Central Europe. There are 831 000 household and 355 083 registered enterprises (December 2012)²⁹.

Number of entities registered in the Warsaw, in 2012 year by sectors are following³⁰ :

- industry - 25 955,
- construction - 28 738,
- trade; repair of motor vehicles - 84 456,
- transportation and storage - 21 412,
- accommodation and catering - 9 034,
- information and communication - 24160,
- financial and insurance activities - 14009,
- real estate activities - 19 659,
- professional, scientific and technical activities - 57 940,
- administrative and support service activities - 13 915,
- education - 11 35,
- human health and social work activities - 15 122,
- arts, entertainment and recreation - 5 550,
- other service activities - 21 773,
- agriculture, forestry and fishing - 1 216,
- public administration and defence; compulsory social security - 363.

Gross domestic product (GDP) in 2011 reached 204 086 million PLN (ca. 51 025 million Euro) ie. 119 828 PLN (ca. 29 957 Euro) per capita, and reflected final result of activity of all entities of Warsaw economy.

Gross domestic product is equal to sum of gross value added generated by all national institutional units, increased by taxes on products and decreased by subsidies on products.

Gross value added measures newly generated value as result of production activity of national institutional units. Gross value added is difference between gross output and intermediate consumption, and is presented at basic prices.

Gross Value Added in 2011 amounted to 179 279 million PLN, in this :

- industry - 15 001 million PLN,
- construction - 10 666 million PLN,
- trade and services (repair of motor vehicles; transportation and storage; accommodation and gastronomy, information and communication) - 70 100 million PLN,

²⁹ Miasto Stołeczne Warszawa, Biuro Infrastruktury

³⁰ Entity of the national economy – legal person, organizational unit without legal personality and natural person conducting economic activity. In REGON register a term entity of the 1 economy is understood as a legal unit. Legal personality is not a criterion, which determines whether the entity is a legal unit.

- financial and insurance services; real estate activities - 35 814 million PLN,
- other services - 47 698 million PLN.

7.3.1 7.4 Daily load profile for Warsaw city.

In order to evaluate the socio-economic impact of Warsaw blackout, it is necessary to define daily load profile in unperturbed day and in case of blackout.

For purposes of our studies it can be assumed, as example time: 21st September, Friday 10 a.m. – 16 p.m., which will result in hypothetical break in power supply in Warsaw agglomeration. Hypothetical attack for Warsaw substations and electricity interruption in Warsaw for purposes of Polish case studies lasting for 6 hours, affected on different customer group and have different consequences on them.

In order to estimate load profile for Warsaw, available data for Poland are extrapolated by means of consumption.

Yearly consumption in Poland in 2012 - 148415 GWh

Yearly consumption in Warsaw in 2012 - 7404 GWh.

Therefore, load profile for Warsaw is reduced by a factor 0,049887, equal to ratio 7404/148415. Hourly load profile, on 21st September 2012, with 96 values of the day is presented on Figure 10.

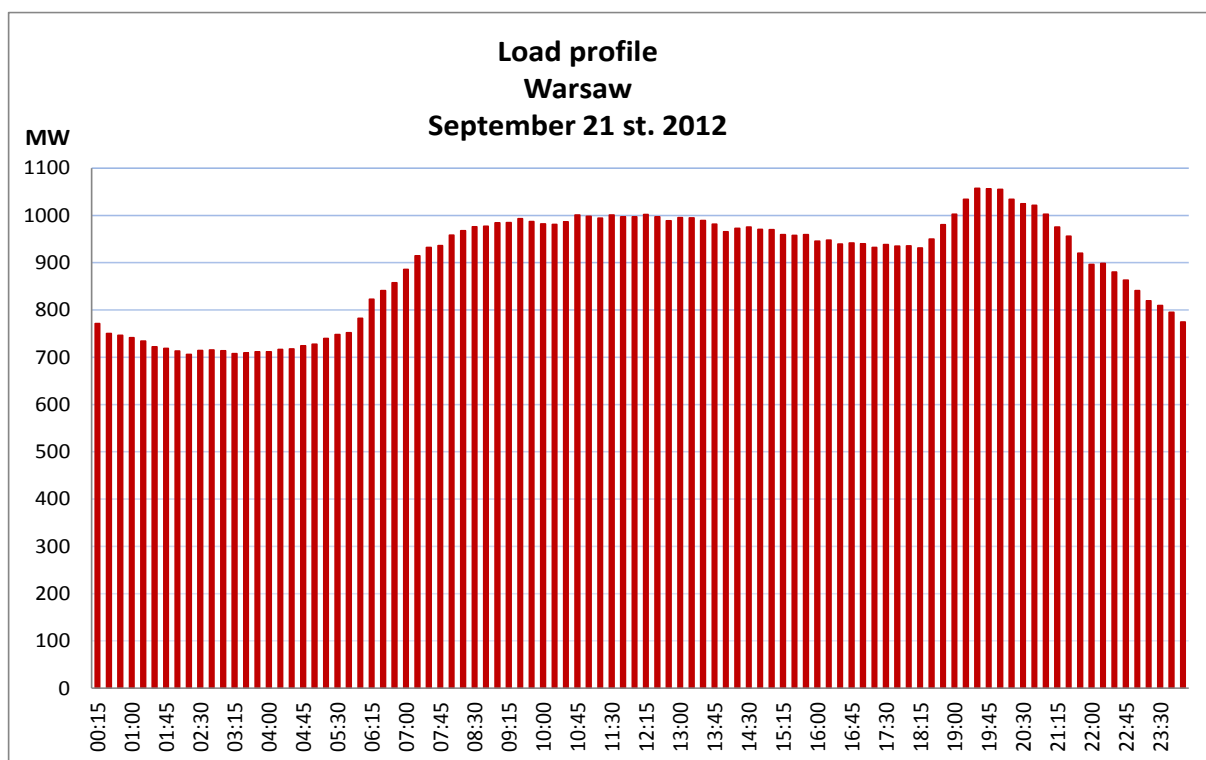


Figure 10. Load profile for Warsaw on September 21st, 2012 [MW]

Daytime load is always maintained above 705 MW, reached minimum at 2.30 am with value 705.6 MW and maximum above 1057.5 MW at 7.30 p.m. during evening peak.

Taking into account ratio between annual consumption in Warsaw and in Poland, structure of energy consumption in Poland, as well as number of working days consumption load profiles for 21st September for main categories of users: industry, agriculture, services (commerce and public services) and residential, have been estimated.

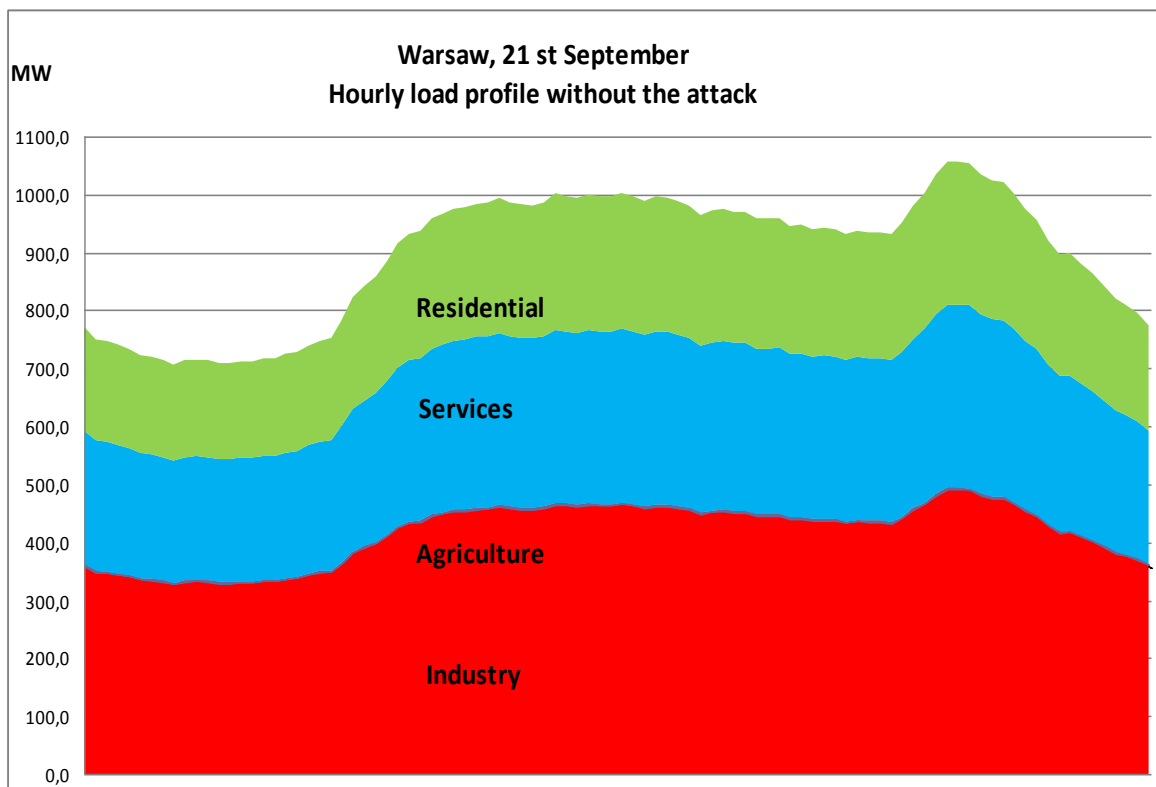


Figure 11. Hourly load profile without the attack.

The next the total energy consumption before attack and during attack for: industry, agriculture, services and residential were calculated.

Total electricity not supplied due to blackout (between 10 a.m. to 4 p.m.) equal to ca. 5904 MWh.

Electricity was not delivered to the following customers:

- industry and service – 4521 MWh,
- households – 1371 MWh,
- agriculture – 12 MWh.

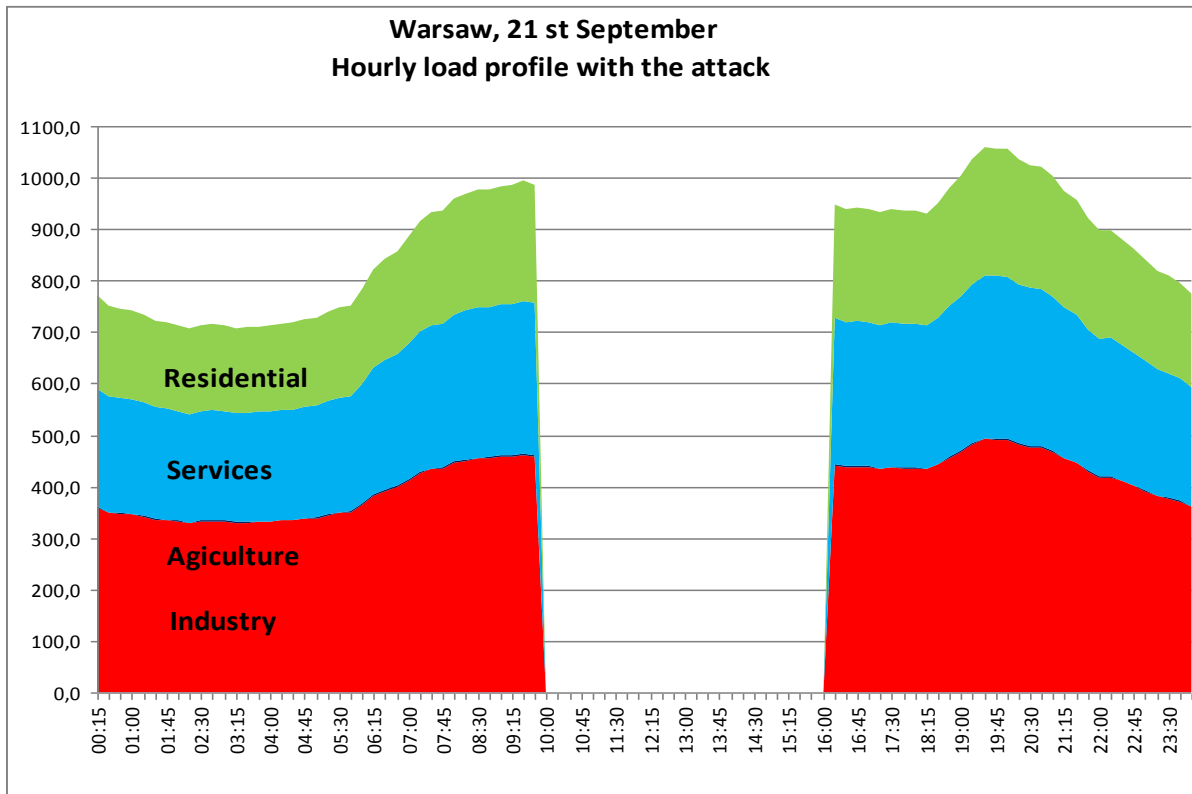


Figure 12. Hourly load profile with the attack.

In summary, effects of blackouts were summarized and presented in Table 7., which shows energy levels (MWh) consumed on 21st September, 2012 for different categories of users without and with blackout.

Table 7. Energy consumption (MWh) without and with black-out for different user categories.

Category	Unperturbed situation MWh	With blackout MWh	Difference MWh	% in the day
Agriculture	33	21	12	36,3
Industries	10052	7232	2820	28,05
Services	6070	4369	1701	28,02
Residential	4755	3384	1371	28,8
TOTAL	20910	15006	5904	28,2

7.4 Standard implementation

For the Polish case study analysis the following security standards: the ISO /IEC 27000- Information Security Management Systems series of standards, the NIST SP-800-53 - Information Security, Recommended Security Controls for Federal Information System and Organizations, and the IEC 62351 - Power system management and associated data exchanges, have been identified as particularly relevant.

Selection of these standards was dictated by comparison of ISO standards (used by TSO in Europe) and NIST standards (U.S. standard used by the United Kingdom TSO), as well as by confronting countermeasures described in these standards of attack scenarios in order to determine their impact on minimizing risks.

Choice of countermeasures should be preceded by the analysis of operation of the transmission system properly built and designed for methods of dealing with failures. The transmission system, as mentioned, is designed to maintain continuity of supply according to N-1 criterion. Further consequence of such networking is that only coincidence of many failures is able to significantly disturb its operation as a whole.

This strategy should be adapted to design of ICT security at substations. Key importance should be attributed to countermeasures that affect limitation of spread of cyber incident, and with respect to a single object, minimizing impact on duration of disruption.

This strategy must be matched to the status of transmission facility, where a distinction should be made among at least three types of power stations, which are particularly important:

- substations supplying urban agglomerations,
- substations discharging capacity of power plants,
- substations of international trade.

Polish case study focuses on failure of substations around urban area, however, for each of the other 2 categories of objects there are also scenarios of events that can cause serious disturbance with transmission even when failure will involve a single object.

The first case refers to situations such as overlap between work planned at many power plants resulting in their exclusion, working on other power plants with very little available power (in summer of 2013 recorded such situations in the national power system where power supply fell below required minimum) and failure at a station connected directly with the power plant. Loss of power in system, which may occur at such time, could not be quickly compensated by other blocks, and existing transmission lines will not be able to send energy to all receiving stations 400/220/110 kV.

National power system, in such situation, would be at risk at least of asynchronously dividing islands and areas excluded from power.

The second case, which refers to substations of international trade, is observed on Polish-German border, and concerns sudden shutdown of international exchange station when it is transmitted by large amount of energy in transit from north to south Germany. This situation, in particular, may threaten stability of the German transmission system, but like any large perturbation will result in entire system connected to the ENTSO-E.

These failures may occur as result of ordinary mishap or malfunction of equipment, but it is necessary in first place, as supplementary design of transmission and generation system, to eliminate single points of failure there, as not meeting N-1 criterion.

Polish case concerned by power disturbances for capital city of Warsaw. It would be reasonable to build such countermeasures which would mainly impact on:

- maximum handicap of attack propagation, carried out on levels such as organizational (diversification of service providers), network transmission (heterogeneous structure of devices all of which are built facilities which supply agglomeration) and operation of ICT systems on stations (removing vulnerabilities, hardening, separation, white listing, firewalls),
- maximizing probability of attack detection during reconnaissance phase, implemented through construction of intersystem communication nodes and inter-control points (which will automatically detect malicious attempts to communicate), construction of honey pot traps type and construction of systems for automatic analysis and correlation of events,
- minimizing duration of single failure.

Building based on above assumptions will result in a security strategy that should significant reduce number of potential cyber attackers to very limited group of experts, whose knowledge, budget and time allow to break any security in a manner transparent to monitoring systems (in practice, high probability of being detected at first error committed during attack, should effectively discourage vast majority of attackers to implement attacks, as other methods of their performance - by physical attack, may be as effective).

7.4.1 Cost of standards implementation



ICT systems for power facilities significantly differ from those employed in IT companies (see Table 8), and differences are not due to use of technology but to the methods of their implementation. The difference, which has the greatest impact on security, is use particular technology for period many times longer than originally anticipated for (consider, for example, the fact that operating system Microsoft Windows XP, commonly used for construction of IEDs and automation sector office, at power stations will have to work even for dozen consecutive years). Even the most safety-conscious providers of equipment and IT systems will not be able to remove vulnerabilities in products they offer, as manufacturers will not use subcomponents of this support.

Therefore, solution may be more common than originally anticipated, making replacement of equipment (unfortunately automation belongs to one of the most expensive endowments power stations, and its exchange is accompanied by high workload of specialists from deployments, and large expenditures of time needed to dismantle old equipment, installation and programming of new one and then testing them prior to entry into service), or construction or modernization of existing power facilities, to their logical architecture to support monitoring of their safety and protecting building, next to them, of dedicated IT security solutions. Another reason for complications associated with implementation of IT security for substations are different needs in terms of continuity, certainty of time parameters of devices and reliability of communications sent by them.

In contrast, to business systems for power facilities is not possible to obtain breaks execution of operational service (after all this change, it should be tested in whole logic of an object, and therefore actual lack of test environments in which these tests could be carried out earlier, this will result in along pause) because they are associated with interruptions in providing or receiving energy.

Installed countermeasures cannot introduce delays in transmission of signals (e.g. packet Goose in accordance with IEC 61850) and shall not generate an increased process protection time, which would result in delay in sending a packet. Filtering at network level cannot cause changes in sequence of packets or modify their contents or drop packets, which could cause misrepresentation of transmission.

Table 8. ITC for power system

	Energy Control Systems 	Office IT 
Anti-virus / mobile code	Uncommon / hard to deploy	Common / widely used
Component Lifetime	10-30 years	3-5 years
Outsourcing	Rarely used	Common
Application of patches	Use case specific	Regular / scheduled
Real time requirement	Critical due to safety	Delays accepted
Security testing / audit	Rarely (operational networks)	Scheduled and mandated
Physical Security	Very much varying	High
Security Awareness	Increasing	High
Confidentiality (Data)	Low – Medium	High
Integrity (Data)	High	Medium
Availability / Reliability	24 x 365 x ...	Medium, delays accepted
Non-Repudiation	High	Medium

Sources: IEC/TR 62351-10

Therefore, when developing proposals for list of recommended standards, it is necessary to take into account not only their costs, but also an estimation of the difficulties of their implementation, which result from need to maintain required quality parameters IED work on substations (the higher degree of difficulty, the less likelihood of success in their implementation).

The analysis of costs of implementing various countermeasures takes into account cost of TSOs not having any security, as well as reference to costs that will be necessary to pay for necessary supplements in Poland.

In Polish case analysis, the following assumptions were adopted:

- Countermeasures are calculated for 100 substations;
- Information Industrial Control Systems (ICS Systems), Office Systems (MMS office) in primary and in backup data centre counted 100 servers;
- Implementing of the security standards refers to the acquisition and installation of hardware and software;
- Maintaining of the security standards refers to the annual cost of the implemented countermeasures, that is software licences, warranties, upgrading and personnel;
- The costs of 1 man-hour for an expert worker is € 20;
- Redundant Internet nodes count for a total of 40 servers;
- The Polish transmission system operator (PSE) employs at present 2,000 employees.

Analysis was performed for the following cases:

- ✓ implementation and maintenance of countermeasures affecting minimize remote attack,
- ✓ implementation and maintenance of countermeasures to minimize influence of local attack,
- ✓ implement and maintain countermeasures to prevent propagation and escalation attack,
- ✓ implement and maintain countermeasures shortening duration of effects of cyber attack.

Total implementation costs were calculated for each security countermeasure separately, without taking into account relationship with other countermeasures.

In Polish case study the costs were calculated in terms of what should be borne if no security standards had been implemented yet (costs starting from 0), and costs that should be borne starting from current situation in order to manage higher supplementary security (Delta costs).

The total cost for implementing (initial investment) and maintaining (annual management) in Poland the security standards encompassing the listed countermeasures in the case of “Cost starting from 0”. That is € 26,016,000 for implementing and 5,016,280 for maintaining.

The total cost of implementation of additional countermeasures not yet existing in transmission system is € 7,486,000 and the additional annual cost for maintaining the implemented countermeasures is € 2,457,200.

The most recommended way to increase level of security is comprehensive implementation of countermeasures in all listed groups.

Table 9: Total cost of the implementation all countermeasures by a TSO (€)

Group of countermeasures	Substations		Information control systems		Office systems	
	Implementing	Maintaining	Implementing	Maintaining	Implementing	Maintaining
Antivirus protection	16,000	40,000	2,000	150	30,000	4,000
Backup infrastructure	200,000	100,000	200,000	20,000	600,000	35,000
Data loss prevention	270,000	350,000	4,000	2,690	11,900	36,000
SCADA protocols validation	3,000,000	300,000	50,000	5000		
Firewalls and IPS Protection	1,500,000	350,000	20,000	12,000	90,000	28,000
Integrity of communication	135,000	40,000	50,000	1,200	100,000	5,000
Physical access control	1,600,000	800,000	4,000	2,000	28,000	7,000
Change of existing system configuration	45,000	60,000	67,200	80,000	183,000	160,000
LAN segmentation	820,000	20,000	8,000	10,000	13,000	10,000
Maintenance work	0	280,000	3,000	80,000	133,900	200,000
Procedures	12,000	3,000	15,000	5,000	60,000	5,000
Redundancy	0	0	3,000,000	300,000	5,400,000	1,100,000
Remote and external access-centralized system	0	20,000	20,000	7,000	55,000	18,000
Communication confidentiality (substation and centralized system)	100,000	40,000	20,000	7,000	55,000	18,000
Security events monitoring, managing and reporting	100,000	30,000	120,000	28,000	280,000	20,000
Physical, environment	7,080,000	300,000	40,000	7,000	201,000	9,240
Vulnerability management	240,000	50,000	10,000	1,000	24,000	10,000
TOTAL	15,118,000	2,783,000	3,633,200	568,040	7,264,800	1,665,240

Source: own calculations.

8 POLISH CASE STUDY – BENEFIT ANALYSIS.

8.1 Evaluating cost of blackouts

Blackout cost evaluation is a complex issue. Main difficulty relies to fact that, although markets for electricity exists, markets for interruptions do not, therefore it is not possible to rely on market prices to estimate economic value of electric supply continuity.

Nevertheless, in economic literature several methods have been developed to infer cost of electricity interruptions. De Nooij et al. (2007) provide a taxonomy.

- *Stated preferences methods*, based on surveys. Interviewed people are asked to state value for blackouts, either in terms of amount they would pay to avoid or reduce interruption (willingness to pay - WTP) or in terms of amount they would like to receive as compensation for increase in interruptions (willingness to accept – WTA). They can also be asked to choose among given combinations of interruption characteristics and monetary values. This method is useful since it relies on preference directly elicited from interviewees. The main drawback is related to fact that this approach can be prone to different types of bias of cognitive source; in particular, way question are asked plays major role (see for instance Beenstock et al., 1998; Carlsson and Martinsson, 2008).
- *Production function approach*, which estimates damages from interruptions in terms of lost production (non-households) or lost leisure time (households). Damage is proportionally related to energy lost, since underlying assumption is that no productive activity is possible in absence of electricity (in the same vein, leisure time cannot be enjoyed in case of electricity interruptions). The main advantage is that the application is straightforward, once macro-economic data on production and energy consumption are publicly available. Main drawbacks rely on the fact that result is an approximation of total damage (some authors identify this category as *proxy methods*), as it ignores factors such as restarting times, damages to equipment or non-complete energy dependence. Nevertheless, the literature agrees in recognizing that these approaches provide good estimate of the order of magnitude of the global damage. More advanced applications, requiring broader sets of information, rely on input-output matrices to consider interdependence across different sectors or on methods assigning positive cost for load disconnected in addition to cost for energy non-supplied. For recent examples of application of this approach, see De Nooij et al. (2007); Leahy and Tol (2011); Linares and Rey (2013).
- *Revealed preference methods*, based on market behaviour. This methods infer value of supply security by observing some particular choices of electricity users, such as purchase of backup facilities or use of interruptible contract (Caves et al., 1992). This approach has the appealing feature of relying on real market choices. On the other hand, these choice options are available for few users categories (mainly large users), while no information would be provided with respect to the other segments.
- *Case studies*. Common feature of this set of approaches is presence of real blackout. Consequences of blackout can be listed and monetized, or surveys can be carried out immediately after the event (Serra and Fierro, 1997). Main desirable property of this method is that it allows to evaluate

consequences of a real event. However, the possibility of generalizing or extending evaluation to other events is very limited.

Finally, the different approaches are not mutually exclusive: Reichl et al. (2013) employ the stated preference approach for households and a production function approach enriched with information collected through firms' survey for the productive sectors.

After a careful evaluation of the *pros and cons* of the available methods, we have chosen to employ a mixed strategy based on the former two methodologies, because they can be more easily generalised and then adapted to hypothetical blackout scenarios involving all the users' types. We will rely on stated preference (surveys) for households, since we believe that this method better captures the main source of damage for families, which is likely to be of psychological rather than of material origin. On the other hand, the very low response rate registered by the previous studies relying on firms surveys led us to prefer a production function approach based on local macro-level data of production (value added) and electricity consumption, which can be retrieved from public statistics.

8.2 Damage for non-households

As stated in the previous subsection, we have decided to rely on a "production function" approach to evaluate damage for non-residential users.

This approach presents the important advantage of being of straightforward application, once necessary macro-economic information are available.

The approach, in its more recent applications, estimates damage by sector relying on constant measure of Value Of Lost Load (VOLL) computed for each sector as a ratio

$$VOLL_i = \frac{VA_i}{EC_i}$$

Where $VOLL_i$ is the value of lost load for sector i , VA_i is the annual value added and EC_i is the annual energy consumption, both referred to the same sector.

Unfortunately, with reference to Warsaw city, data on energy consumption of different sectors are not available. This implies that the sector-specific VOLL measures cannot be estimated at local level. A possible solution could be to rely on national-level data, but careful evaluations showed that VOLL levels computed with this approach relevantly underestimated damage for Warsaw, due to the concentration of high value-added activities in the capital city.

To overcome this issues, we have decided to employ a single average VOLL measure to be applied to total energy non-delivered to non-households.

$$VOLL = \frac{Total VA}{Total EC}$$

The method based on production function implies a linear relationship between lost production (expressed in terms of value added) and energy non supplied. It constitutes a proxy of the actual damage that would occur in case of interruption since it relies on several assumption and simplifications (see De Nooij et al. 2007 and Billinton et al. 2001):

- 1) It ignores potential costs related to damaged equipment, which are more likely in some sectors than in others, and which are probably not directly linked to quantity of energy non delivered.
- 2) It assumes that the damage corresponds to lost value added, i.e. value of production net of external purchases. Indeed, it is in general reasonable to assume that when production is stopped, firms do not employ (i.e. save) material and services (including energy). Nevertheless, in some processes, also some external input can be lost. For instance, this is the case of perishable raw materials, or energy, in productions processes where temperature must be kept high or low and interruption implies re-heating or re-cooling operations.
- 3) It ignores re-starting times, which can be very relevant in some industries.
- 4) It does not consider that some kinds of activities can be carried on even in absence of electricity. Their weight largely depends on type of production.

Drawbacks described in points 1) to 3) would imply underestimation of total damage, while the issue described in point 4) would lead to overestimation; these effects are likely to compensate each other. Globally, as pointed out in De Nooij et al. (2007), and Billinton et al. (2001), the model can be considered a valid method to provide reliable evaluation of the order of magnitude of total damage, for general policy evaluations, main aim of this study, although it could not be sufficiently reliable for accurate sector-specific considerations.

Total damage can be computed by multiplying the VOLL by total energy non delivered.

Data on value added are available in the “Warsaw Statistic Yearbook”, and the most recent refer to the year 2011. Therefore, value added amounts have been adjusted for inflation to the first quarter of the year 2014³¹.

We would like to point out that available data do not allow to exclude the energy sector from evaluation. However, we believe that this approximation does not represent relevant distortion of results.

Average VOLL computed for the entire productive system of Warsaw is 31.60 PLN/kWh (7.58 €/kWh). For comparison purposes, we can for instance see that this value is consistent with finding of De Nooij et al. (2007) for the Netherlands (7.59 €/kWh) but higher than results of Linares and Rey (2013) for Spain (5.56 €/kWh)³².

As a refinement, we will try to modify our evaluation to account for the fact that some of considered industries manage activities which are not strictly dependent on electricity supply (see Linares and Rey, 2013). Construction is example of such industries. Also for financial services, although strictly dependent on information systems mainly electricity-based, we can assume that main output (i.e. financial rents on investments) is not lost in case of blackout.

³¹ Consumers price index is employed.

³² In current values for the first quarter 2014.

Finally, we are not considering agricultural activities (which are as well only marginally depending from electricity) since their weight is negligible with respect to the city total value added. Therefore, we have chosen to provide also a “prudential” version of total damage, by reducing average VOLL by the percentage of value added related to construction and financial services, getting an “adjusted VOLL” of 23.41 PLN/kWh. This value can be interpreted as a “minimal” one, since damage for sectors with evident low electricity dependence has been set to zero, while additional cost component are still not considered. Therefore, it can reasonably be taken as very close to the lower bound of possible damage.

Finally, we propose a third evaluation applying electricity dependence shares used in Linares and Rey (2013) (L&R 2013). Shares should reflect weight of processes for which electricity is necessary input. Authors, however, define employed shares as a “best guess” of the actual part of value added lost in case of blackout, since no empirical support is available at the moment. The proposed VOLL is therefore weighted by share of value added produced by each sector and by electricity dependence coefficient proposed in L&R 2013. This approach lead to an average VOLL of 24.79 PLN/kWh.

Table 10. reports contributions of different sectors to total Value Added produced in Warsaw in 2011, as well as electricity dependence coefficients proposed in L&R, 2013.

Table 10. Shares of value added by sector and electricity dependence coefficients.

Sector	Share of value added	Share of electricity dependence (L&R 2013)
Industry	0.084	0.9
Construction	0.059	0.4
Trade and services	0.391	0.8
Financial, insurance and real estate	0.200	0.8
Other services	0.266	0.8

The approach based on “average” value added lead to total damage results of about 143 millions PLN (34 millions €), while the two “prudential” approaches lead to similar results: 106 million PLN (25 millions €) and 112 millions PLN (27 millions €) respectively.

Table 11 summarizes these findings.

Table 11. Blackout damage for non-households.

Specification	VOLL (PLN/kWh)	Energy non- supplied (MWh)	Damage (PLN thousands)	Damage (€ thousand ³³)
"Average" damage evaluation	31.6	4521	142,852.61	34,257.22
"Prudential" damage evaluation	23.41	4521	105,828.47	25,378.53
"Prudential" damage evaluation with energy dependence shares	24.79	4521	112,066.97	26,874.57

8.3 Damage for the electricity sector

We want to provide specific evaluation for the electricity sector in terms of value of non-supplied energy to final customers.

For generators, lost revenues can be expressed in terms of energy not sold evaluated at market price of a day of an event.

We will employ for this purpose actual hourly market prices registered for September 21th, 2012 (source: Polish Power Exchange), which will be multiplied by non-delivered energy in each hour of blackout (unfortunately, available data do not allow to net out the sector auto-consumption).

Table 12. shows the following results:

Table 12. Damage for producers in Warsaw, on 21th of September 2012

Time	Price (PLN/MWh)	Energy lost (MWh)	Lost revenues (PLN)	Lost revenues (€) ³⁴
10.00	199.54	988	197,061	47,718
11.00	202.14	997	201,619	48,822
12.00	198.85	996	198,109	47,972
13.00	190.35	990	188,494	45,644
14.00	188.5	971	183,048	44,325
15.00	186.19	962	179,040	43,354
	TOTAL	5904	1,147,372	277,834

³³ Exchange rate of March 31st, 2014

³⁴ Exchange rate of September 21st, 2012

In order to achieve damage evaluation homogenous to the one proposed in previous paragraph, in terms of value added, we net out, from total revenue lost, the corresponding cost of coal (the main external input), evaluated in 184,541 €.

$277,834 - 184,541 = € 93,293$ VA lost for generators (in current value for 2012).

For homogeneity with other parts of the analysis, we would like to express this value adjusted for inflation to the first quarter 2014.

We got a value of VA lost for generator equal to 95,010³⁵.

For the whole electricity chain (remuneration of generators is therefore included), it is possible to approximate total damage using value of different component of price (price for medium residential users in the second semester 2013 is employed), retrieved from EUROSTAT.

Since the first stage of the production chain (generation) is included, we provided damage computation for the entire sector net of cost of non-employed fuel mentioned above.

Table 13. Damage for the whole sector³⁶

	Value of the price component (€/MWh)	Energy non-supplied (MWh)	Total damage (€)
Energy and supply	58.6	5904	345,986
Network costs	53.5	5904	315,875
Tax & levies	31.6	5904	186,573
Total			848,434
Net damage			661,153

8.4 Damage for households

For households we have adopted a stated preference method based on customer surveys. Approach relies on a choice experiment, where choice questions were set in terms of willingness to accept (WTA) blackouts of certain durations, provided that supplier would have compensated households with a bill discount. The respondent was simply asked to state whether or not he would have accepted given interruptions (with discount).

A total of 28 scenarios (i.e. combination of duration and discount) were constructed, since we have hypothesized:

³⁵ The consumer price index has been employed.

³⁶ In current prices for second semester 2013.

- 4 duration levels: 1 minute, 2, 4 and 6 hours.
- 7 discount levels: 1, 7, 13, 19, 25, 31, 37 euros.

In order to not impose an excessive effort on respondents, only 7 randomly chosen scenarios were presented to each one of them.

In literature the most common approaches rely on willingness to pay (WTP) in order to avoid blackouts. In general, WTP and WTA differ relevantly, with the latter exceeding the former by several times. This is due to so-called “endowment effect”, which is psychological tendency for an average person to ask higher compensation to give away something he owns with respect to the amount he would pay to purchase the same good or service.

Therefore we expect *a priori* higher results than in studies relying on WTP.

Nevertheless, we have chosen a WTA approach because, after careful evaluation, we believe it is more respondent to the need of evaluating a single blackout (rather than more general scenarios describing supply security in terms of interruption frequency and other characteristics). WTP approach would in this case be not completely suitable, since users’ opinion (this is especially true for residential users) is that continuity is necessary characteristics of service. Interruption could represent sort of “pathological” disservice, and it is very likely that many respondents would be willing to pay no additional money to avoid it, or that the WTP expressed would understate actual value they assign to interruption.

Interviews have been mainly carried out by means of online questionnaires (integrated with face-to-face interviews to cover customer segments not easily reachable through internet and paper-based questionnaires) starting from March 2014. The same questionnaire has been distributed in Italy and in Poland (with monetary values expressed in local currency) in order to have a sample covering residential users of both countries involved in case studies developed through ESSENCE.

We have collected a total of about 500 questionnaires in Italy and 120 in Poland, of which about the 80% was complete and could be employed for the estimates.

In order to evaluate the households inconvenience in case of electricity interruption, let us assume that the utility of family i with respect to the alternative j is defined as

$$U_{ij} = V_{ij} + \varepsilon_{ij}$$

Where ε_{ij} is a stochastic component, while V_{ij} is a deterministic component that depends on respondent and interruption characteristics and on a set of unknown parameters to be estimated; it is the term we are interested in.

For each choice option, we do not know V , but we know whether the respondent has chosen ($y=1$) or not ($y=0$) the blackout alternative.

To conduct the estimates, we have followed approach described in Bennet e Blamey (2001), that would require to apply the Mc Fadden (1974) conditional logit model. However, when choice includes only two alternatives, model can be estimated as a common binary logit model, where interruption attributes (duration and discount) appear as difference between two options (see Schultz et al., 2013). Since alternative “no

blackout” has both duration and discount set at zero, the variables values correspond simply to attribute levels. Moreover, since we want to estimate a model without the constant term³⁷, we should keep in mind that respondent characteristics can be introduced only if interacted with (i.e. multiplied by) blackout attributes.

General formulation of the model that will allow to estimate V as a function of a set of variables and of related parameters is the following:

$$PR(y = 1|x) = G(V) = G(x\beta)$$

Where $PR(y = 1|x)$ represents probability of choosing interruption scenario (with respect to the “no-blackout” option), which is function of a set of unknown parameters β , to be estimated, given a set of blackout and respondents characteristics x , through functional form G , representing the logit model:

$$G(x\beta) = \exp(x\beta)/(1 + \exp(x\beta))$$

Finally, the empirical functional form of $x\beta$ that we want to test is the following:

$$\begin{aligned} x\beta = & \beta_{DUR} * dur + \beta_{2DUR} * dur^2 + \beta_{DISC} * disc + \sum_{i=1}^n \beta_{ziDUR} * dur * z_i \\ & + \sum_{i=1}^n \beta_{ziDISC} * disc * z_i + \beta_{PDUR} * dur * d_{pol} + \beta_{P2DUR} * dur^2 * d_{pol} + \beta_{PDISC} * disc * d_{pol} \\ & + \sum_{i=1}^n \beta_{PziDUR} * dur * z_i * d_{pol} + \sum_{i=1}^n \beta_{PziDISC} * disc * z_i * d_{pol} \end{aligned}$$

Where

- dur is the duration variable in hours. It also appears squared.
- $disc$ is the discount variable expressed in euros (converted for Polish respondents).
- d_{pol} is a dummy (binary) variable equal to 1 when the respondent is Polish

Moreover, the “z” variables are:

- d_{age18_24} : dummy variable equal to 1 when the respondent is between 18 and 24 years old;
- d_{age25_44} : dummy variable equal to 1 when the respondent is between 25 and 44 years old;
- d_{age45_69} : dummy variable equal to 1 when the respondent is between 45_69 years old;

³⁷ In such a model, the constant term would capture the average respondent attitude towards the blackout scenario that cannot be explained by the attributes (duration and discount), or, to say it differently, the same attitude when duration and discount are set at zero. Since duration=0 implies absence of interruption, and, in any case, we believe that the attributes provide a full descriptions of our (purely hypothetical) scenarios, we have decided to estimate a model without the constant term.

- *d_age70*: dummy variable equal to 1 when the respondent is older than 70;
- *d_female*: dummy variable equal to 1 when the respondent is a woman;
- *d_income_hlevel*: dummy variable equal to 1 if the respondent has declared that the economic level of the household is medium-high or high;
- *d_educated*: dummy variable equal to 1 if the respondent has an high school certification or more;
- *d_countryside*: dummy variable equal to 1 if the household lives in the countryside, i.e. not in a city, in a town or in a village.
- *mec*: monthly electricity cost. It is average monthly expenditure of household for electricity bill, expressed in euros (converted for Polish respondents). This value has been normalized for Italian and Polish respondents on respective sample median of the variable, to account for difference in energy cost in two countries.

Basically, we assume that probability of choosing given blackout scenario (and therefore associated utility for respondent) is function of blackout characteristics, of the respondent and household characteristics and of country of residence.

The base case is tailored on an Italian respondent, while variables interacted with *d_pol* are aimed to measure whether it exists significant shift in parameters when respondent is Polish.

To say it differently, we want to allow possibility that the same variables impact differently on choices of Italian and Polish respondents.

In order to keep only significant variables (since later parameters will be employed for simulation purposes), a (backward) stepwise procedure has been implemented starting from the full model (model with all described variable and interactions), and gradually eliminating non-significant variables, with critical significance level corresponding to p-value of 0.1³⁸.

Moreover, we employed clustered robust standard errors to account for potential correlation among observations (i.e. choices) coming from the same respondent.

Estimates of the logit model provide the following results.

³⁸ The p-value represents the probability of making an error in rejecting the “null hypothesis” that the estimated coefficient is equal to zero (in this case the variable would have no impact on the choice probability). The lower the p-value, the lower the likelihood that the data are consistent with the null hypothesis, and the higher the support to the “alternative hypothesis” of an actual impact of the variable on the choice outcome. A p-value smaller than 0.1 is in general considered as acceptable; a p-value smaller than 0.05 represents a good significance level, while a p-value smaller than 0.01 is considered highly significant.

Table 14. Logit estimates

Variable	Coefficient	Coefficient value	p-value
<i>dur</i>	β_{DUR}	-0.6246	0.000
<i>dur</i> ²	β_{2DUR}	0.0432	0.000
<i>disc</i>	β_{DISC}	0.0582	0.000
<i>dur*d_countryside</i>	$\beta_{DUR_COUNTRY}$	-0.2080	0.009
<i>dur*d_age18_24</i>	β_{DUR_AGE18}	-0.1669	0.035
<i>dur*mec</i>	β_{DUR_MEC}	-0.0525	0.005
<i>dur*d_pol</i>	β_{PDUR}	-0.1902	0.003
<i>dur*d_age25_44*d_pol</i>	β_{PDUR_AGE25}	0.1863	0.015
<i>disc*d_countryside</i>	$\beta_{DISC_COUNTRY}$	0.0407	0.001
<i>disc*d_age18_24</i>	β_{DISC_AGE18}	0.04	0.002

Results show, as expected, that higher duration reduces probability of accepting blackout scenarios, although this effect slow-down for long duration levels. Also the discount term has expected sign, since higher discounts increase probability of accepting proposed scenario.

People living in countryside are more sensitive to duration, but appreciate more discount. In general, and our data support this point, respondents living in countryside have higher acceptance rate, therefore blackout is perceived as less annoying, probably because these individuals are more used to such events, and this fact would lead to greater appreciation of the offered discount, for a given duration. However, as duration gets longer, in rural environment “solutions” to cope with absence of electricity (e.g. eating out when cooking is impossible, or finding alternative ways to spend leisure time) are much less readily available. This could be reason explaining higher sensitivity to longer interruptions.

The same holds for respondents between 18 and 24 years old, which are as well more sensitive to duration effect (probably since they are more dependent on electricity-consuming activities), but appreciate more discount.

Respondents with higher monthly bill are more sensitive to duration: a reason could be that affording higher electricity costs makes these consumers more exigent with respect to the quality of service.

Finally, Polish respondents’ attitude with respect to proposed discount does not differ significantly from Italians’ one: indeed, all related variables have been dropped in stepwise procedure since they were not significant. On the other hand, Polish people are more sensitive to duration, as shown by negative and significant interaction. However, Polish respondents between 25 and 44 years old suffer duration effect significantly less.

Estimated parameters can be employed to predict utility lost with interruption in absence of discount (V_{nd}), i.e. decrease in utility due to the mere presence of blackout of certain duration. To be expressed in monetary value, V_{nd} must be divided by marginal utility of discount parameter.

Since the model includes interactions with the discount term, monetary value of lost utility is computed as:

$$\text{Monetary value of lost utility} = V_{nd} / (\beta_{DISC} + \beta_{DISC_COUNTRY} * d_{countryside} + \beta_{DISC_AGE18} * d_{age18_24})$$

We have simulated three possible value of damage for Polish households (i.e. by setting $d_{pol}=1$):

- Maximum damage, occurring for a family not living in countryside, with head of the household non belonging to age range included between 25 and 44 years³⁹, with high electricity bill.
- Minimum damage, occurring for a family living in the countryside, with head of the household aged 25-44, paying low electricity bill.
- An average case reflecting a “typical family”: not living in countryside, with a head of household aged more than 44 and energy monthly cost set at sample median (€ 26.45).

We get the results described in Table 15.

Table 15. Damage for households.

Damage	Maximum case	Minimum case	Average case
Damage per household for 6 hours interruption in €	73.46	35.31	62.65
Total damage in € Millions	61.05	29.34	52.06
Average damage per family in €/h	12.24	5.89	10.44
Average damage per person in €/h ⁴⁰	4.37	2.10	3.73

In relation to the Polish case study, a damage for non-households take a value of 25-35 € millions, while for households the range is between 30 and 61 € millions. If we consider the characteristics of the average residential consumer, we get a total cost of about 52 € millions. For the electric operators the damage is about 0.7 € millions.

In conclusion, estimated damage for households is higher by far than for non-households. Damage for the electricity sector (not taking into account the damage to reputation) is a very small fraction of total estimated damage.

³⁹ Simulation on the age range 18-24 cannot be implemented since the age class, poorly represented in the Polish sample, disappeared after the outliers detection procedure.

⁴⁰ Computed assuming an average Polish household of 2.8 members.

Presented analysis shows that from a mere economic viewpoint electric companies should not increase their security levels, as the annual costs of those countermeasures is much greater than their direct cost of a single blackout. However the total cost of an event for the society as a whole is by far greater than the annual cost of the said countermeasures. Therefore it is of interest for the community to take actions to raise the security level and ultimately reduce global risk.

The whole European Electric System is interconnected. An event on the electricity grid in one of the EU countries may have repercussions onto many others. Therefore it is up to public authorities require the overall adoption of current security standards and countermeasures to the companies operating in the electric system of the European Union.

9 REFERENCES

- Act of 10 April.1997 – The Energy Law (Journal of Laws of 2003 No.153, with later changes).
- Ordinance of Ministry of Economy from 4.05.2007 about detailed terms of operation of power system (Journal of Laws of 2007 No.93, Item 623).
- Analiza procesu wdrażania “Polityki energetycznej m.st. Warszawy do 2020 r.” wykonanie za 2011 r. Biuro Infrastruktury Urzędu Miasta Warszawy, Warszawa 2012 r. (Eng. Analysis of the implementation of the "Energy Policy till 2020 of the City of Warsaw . "execution for 2011. City of Warsaw, Infrastructure Department, Warsaw 2012.)
- Analiza procesu wdrażania “Polityki energetycznej m.st. Warszawy do 2020 r.” wykonanie za 2012 r. Biuro Infrastruktury Urzędu Miasta Warszawy, Warszawa 2013 r. (Eng. Analysis of the implementation of the "Energy Policy till 2020 of the City of Warsaw . "execution for 2012. City of Warsaw, Infrastructure Department, Warsaw 2013.)
- Beenstock, M., Goldin, E., Haitovsky, Y. (1998). Response bias in a conjoint analysis of power outages. *Energy Economics*, 20, pp. 135-156.
- Bennet, J., Blamey, R. (2001). The choice modelling approach to environmental valuation. Edward Elgar Publishing.
- Billinton, R., Abilgaard, H., Alabbas, A.M., Allan, R.N., Arnborg, S., Bogoi, C., Bozic, Z., Goncalves, L.F.M., Dialynas, E., Holen, E.A.T., Logan, D., Manning, T., Neves De Mesquita, E., Schmitt, O., Shirani, A.R., Simpson, B., Yinbiao, S. (2001). Methods to consider custode interruption costs in power system analysis: task force. Cigrè .
- Carlsson, F., Martinsson, P. (2008). Does it Matter When a Power Outage Occurs? A Choice Experiment Study on the Willingness to Pay to avoid Power Outages . *Energy Economics*, 30, pp.1232-1245.
- Caves, D.W., Herriges, J.A., Windle, R.J, (1992). The cost of electric power interruption in the industrial sector: estimates derived from interruptible service programs. *Land Economics*, 68, 1, pp.49-61.
- De Nooij, M., Koopmans, C., Bijvoet, C. (2007). The value of supply security. The cost of power interruptions: economic input for damage reduction and investment in networks. *Energy Economics*, 29, pp.277-295.
- Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC.
- Directive 2005/89/EC of the European Parliament and of the Council of 18 January 2006 concerning measures to safeguard security of electricity supply and infrastructure investment OJ L 33, 4.2.2006,
- Directive of the European Parliament and of the Council 2010/75/EU of 24 November 2010 on industrial emissions (integrated pollution prevention and control), OJ L 133/17.
- Dołęga W., ”The role of energy enterprises performing licensed business activity consisting in transmission electricity in view of past law regulations in aspect of energy security”, *Elektroenergetyka: współczesność i rozwój*, no. 1/2009.

- Energy Regulatory Office Report from 2010-2012 <http://www.ure.gov.pl>
- ETSO (European Transmission System Operators) <http://www.etsonet.org>
- Instruction of Transmission System Operation and Maintenance, PSE 2006.
- Leahy, E., Tol, R.S.J. (2011). An estimate of the value of lost load in Ireland. *Energy policy*, 39, pp.1514-1520.
- Linares, P., Rey, L. (2013). The cost of electricity interruptions in Spain. Are we sending the right signals? *Energy Policy*, 61, pp.751-760.
- McFadden, D. L. (1974). Conditional logit analysis of qualitative choice behavior. In *Frontiers in Econometrics*, ed. P. Zarembka, 105-142. New York: Academic Press.
- Miasto Stołeczne Warszawa, Biuro Infrastruktury, www.um.warszawa.pl
- Ministry of Economy: Sprawozdanie z wyników monitorowania bezpieczeństwa dostaw energii elektrycznej, Ministerstwo Gospodarki Warszawa 2013.
- Ordinance of Ministry of Economy from 2.07.2007 about detailed principles of tariffs calculations and accounts for electricity trade (Journal of Laws of 2007 No.128, Item 895).
- Power systems management and associated information exchange – Data and communications security . Technical Specification International Electrotechnical Commission, IEC Ts 62351-1, 2007.
- Plan działań na rzecz zrównoważonego zużycia energii dla Warszawy w perspektywie do 2020 roku. Warszawa, 2011.
- PSE Annual Reports 2010- 2012.
- PSE Operator SA development plan. PSE SA, Warszawa, 2010
- Reichl, J., Schmidthaler, M., Schneider, F. (2013). The value of supply security: the cost of power outages to Austrian households, firms and the public sector. *Energy Economics*, 36, pp.256-261.
- Reichl, J., Schmidthaler, M., Schneider, F. (2013). Power outage cost evaluation: reasoning, methods and application. *Journal of scientific research & reports*, 2 (1), pp. 249-276.
- Schultz, N., Breustedt, G., Latacz-Lohmann, U. (2014). Assessing farmers' willingness to accept "greening": Insights from a discrete choice experiment in Germany. *Journal of agricultural economics*, 65,1, pp. 26-48.
- Serra, P., Fierro, G. (1997). Outage cost in Chilean Industry. *Energy Economics*, 19, pp. 417-434.
- Statistical Yearbook of Warsaw, Statistical Office in Warsaw 2013. ISSN 1425–9486
- Statystyka elektroenergetyki polskiej. Agencja Rynku Energii SA, Warszawa 2013 r.
- Transmission Grid Use and Operation Manual. General Part. Version 1.2. PSE- Operator Limited Company. Warsaw 2006.
- Tomaszewski M., Ruszczak B. Analysis of frequency of occurrence of weather conditions favouring wet snow adhesion and accretion on overhead power lines in Poland. Elsevier, 2013.
- UCTE (Union for the Co-ordination of Transmission of Electricity) <http://www.ucte.org>
- .