Scientific Papers of
the Department of Electrical Power Engineering of
the Wrocław University of Technology

PRESENT PROBLEMS OF POWER SYSTEM CONTROL

7

Wrocław 2016

Department of Electrical Power Engineering
Wrocław University of Science and Technology
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland
phone: +48 71 320 35 41
www: http://www.weny.pwr.edu.pl/instytuty,52.dhtml; http://www.psc.pwr.edu.pl
e-mail: wydz.elektryczny@pwr.edu.pl

OFICYNA WYDAWNICZA POLITECHNIKI WROCŁAWSKIEJ
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław
http://www.oficyna.pwr.edu.pl
e-mail: oficwyd@pwr.edu.pl
zamawianie.ksiazek@pwr.edu.pl

ISSN 2084-2201

Print and binding: beta-druk, www.betadruk.pl

smart power grid, digital security, risk analysis, hazard valuation, cyber-physical security.

Robert CZECHOWSKI*

CYBERSECURITY RISK ANALYSIS AND THREAT ASSESSMENT WITHIN SMART ELECTRICAL POWER DISTRIBUTION GRIDS

Development of electrical power systems and their integration with an increasing number of smart automation devices compel to undertake a new approach to the issue of the system's security. Reliability of an electrical power system and high service availability are the essential characteristics of efficient strategic electricity customers, i.e.: large industrial facilities, railway transport, medical service providers and life-saving institutions. The time of manual or automatic system recovery after a failure, which increases its security, is not without significance, either. The article discusses the issues of risk assessment and management, including the overall process of analysis and assessment of threat probability in electrical power systems.

1. INTRODUCTION

The beginning of the XXI century marked rapid development of digital technology in critical systems, which gave them brand new significance to efficient and secure functioning of a country. Systems with extensive structure and range of their functionality, such as: fuel distribution, drinking water supply, mass media and communication, and especially electricity suppliers, currently constitute the most important branches of economy, and disruption of their operation might put a country or its citizens at risk of serious consequences. During the last twenty years, protection of these systems has become very important due to increasingly complicated infrastructure and new threats. These systems also pose a challenge for their designers.

Potential system failures (regardless of the system's current technological level) directly determine the system's efficiency, but also indirectly – scope of the impact

*Wrocław University of Science and Technology, Department of Electrical Power Engineering, Wybrzeże Wyspiańskiego 27, 50-370 Wroclaw, Poland, e-mail: robert.czechowski@pwr.edu.pl

which influences bodies using the system's services. Making strategic decisions on designing, managing and developing an electrical power system can significantly influence a country's functioning and development perspectives in the future, and especially be of importance for its security and international position, as well as its economic and defensive potential. Moreover, political turmoil, conflicts and international crises occurring in certain regions can directly impact a country's energy security. Another possible cause of a crisis constitutes actions rooted in sabotage, and threats originating from third parties, like acts of terrorism.

Supply of electrical energy by use of a smart grid is increasingly often tied to digital information flow, allowing for both continuous monitoring of the demand, and control of the grid itself. In effect, it will directly translate into its increased efficiency. Such solutions allow for flexibly shaping the demand and adjusting the supply to daily requirement. Combined with utilization of energy-efficient devices, smart solutions and fully automated technological processes, it will increase energetic efficiency of the entire system. To a certain degree, these solutions will also limit potential risks related to failures or intentional attacks. Recently, more methods and technical measures have appeared to aid in system operation optimization and minimizing potential effects of disrupted system operation. They include such actions as: risk analysis and threat assessment, created for the needs of centralized management. In order to effectively utilize the aforementioned methods, it is essential to sweep the supervised system and identify threats whose removal requires nonstandard procedures and resources. It is worth mentioning that risk (lat.: *Risico*) is a possibility to make profit or sustain losses as a result of a certain action, and threat assessment means evaluation of a given threat's impact based on its origin, duration, effects and determination of resources necessary to neutralize it. Among the many definitions, the most adequate one, in the context of an electrical power system, is operational risk which constitutes possible adverse effects of computer system errors or organizational errors.

Risk estimation and threat assessment methods allow to notice and take preventative action, as well as determine the degree of security improvement in an electrical power system as a result of the undesirable situation. On one hand, the decision maker has to consider purely technical solutions, on the other – consequences resulting from possible discredit of the system and lost trust for a given operator.

2. STRATEGY

The general security strategy for smart grids assumes both common and specific needs for individual infrastructure parts, i.e.: security of information, data bases and technological process visualization. The main tasks of cybersecurity strategies are making employees aware of potential threats and taking action in order to prevent

them. Nevertheless, a strategy to react, mitigate the effects of a failure or cyberattacks, and make a full system recovery should be developed in case of a cyberattack against an electrical power system.

Implementation of a security strategy requires determination and implementation of a specific threat assessment process dedicated to assure cybersecurity of an entire smart electrical grid. The associated risk concerns probability of an undesirable incident or event, as well as related consequences. Organizational risk can encompass many kinds of risk (e.g.: risk related to investment, budget, strategy management, legal responsibility, automation digital security, inventory and information systems). The most common causes of increase and emergence of risk are:

- human errors – losses sustained due to human mistakes inside the company or mistakes of external employees (e.g. customer extortion),
- process errors – losses reflecting potential weaknesses in procedures,
- poor work organization – risk resulting from e.g. changes implemented into management or communication methods,
- technological errors – equipment failures, software errors, network outages or failures of other kinds of technology, as well as loopholes in security measures of IT systems,
- external causes – legal proceedings or natural disasters.

Risk assessment process in a smart grid is based on existing ways and methods of risk assessment devised by the private and public sectors, and it encompasses identification of consequences, vulnerability to attacks and threats. In order to assess risk in relation to a smart grid, their protection has to be flexible and include coexistence of all components of the system, as smart grids encompass systems from sectors of IT, telecommunication and energy. Risk assessment process concerns all three sectors and their interaction with smart grids and smart metering. All in all, priority goals of IT system security measures include confidentiality, as well as integrity and accessibility. In industrial control systems, including power systems, accessibility takes priority over all security measures, then comes integrity, and then confidentiality. The goal of risk management process is also indication of so-called strategic goals – determining what actions should be taken in order minimize the possibility of a threat or its consequences. Fig. 1 shows exemplary components and course of action, which can be as follows:

- threat analysis – indication of where threats can be found, description of their scenarios,
- prevention – determination of a strategic goal, undertaking ventures necessary to achieve the strategic goal, and the necessary forces and resources,
- preparation – determining where locally, regionally and nationally implemented programs are indicated, whose goal is increased security,
- response – determination of response principles, as well as response priorities in case of threats,

– historical data analysis – analysis of crisis events that have taken place in the past (according to the following parameters: date or time interval; place/area of appearance; short description; consequences of the loss),
– conclusion analysis – analysis of conclusions derived during the preceding events related to the analyzed case.

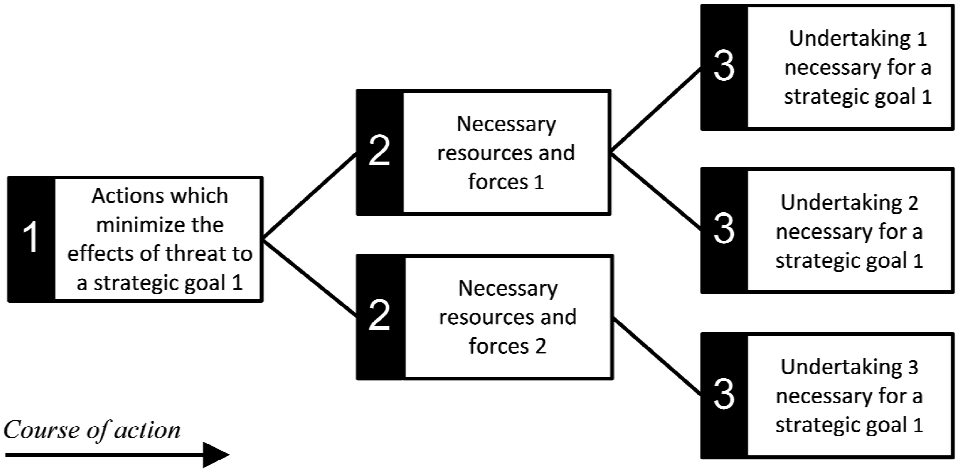

Fig. 1. Chart of threat analysis and estimation process' organization.
Legend: 1 – analysis and plan of action, 2 – determination of forces and resources for a strategic goal, 3 – realization of the strategic goal.

Awareness of borne risk is definitely very important in decision-making on the financial market. Sometimes, however, it is worth taking risks, as it often turns out that greater risk leads to potentially greater profit (sadly, also greater possible loss). The possibility to make above-average profit is enough of a temptation for some financial institutions to decide to take the risk, exposing themselves to possible losses. In line with the act on crisis management [1], these goals have been ordered according to their importance and the ones that take priority from the perspective of national security have been indicated. For all strategic goals, the indicated elements are strength and resources necessary to achieve them, as well as ordered undertakings which must be realized in order for a strategic goal to be achieved.

3. RISK ANALYSIS AND ASSESSMENT

In analysis of consequences for critical infrastructure, it is determined – if and how a given scenario influences the functionality of a given critical infrastructure and if there is a potential threat to the system. In line with the act on crisis management [1], critical infrastructure is understood as a system and interrelated functional objects that constitute it, including construction objects, telecommunication equipment, telecommunication installations and other services crucial for the security of

a country and its citizens. The constituents also aim at ensuring proper functionality of public administration bodies, as well as institutions and businesses. Still, each critical infrastructure is very important from the perspective of security of a country's operation, especially: mass media service providers, water and energy fuel suppliers – the most important of them are electrical power systems. Such a strong and high position of electrical power systems is caused by virtually every branch of economy being reliant on the supply of electricity. From this point of view, the infrastructure of creation and distribution of electricity encompasses nearly all systems, from communications systems, teleinformation networks, financial markets, healthcare and rescue, to logistics systems (Fig. 2).

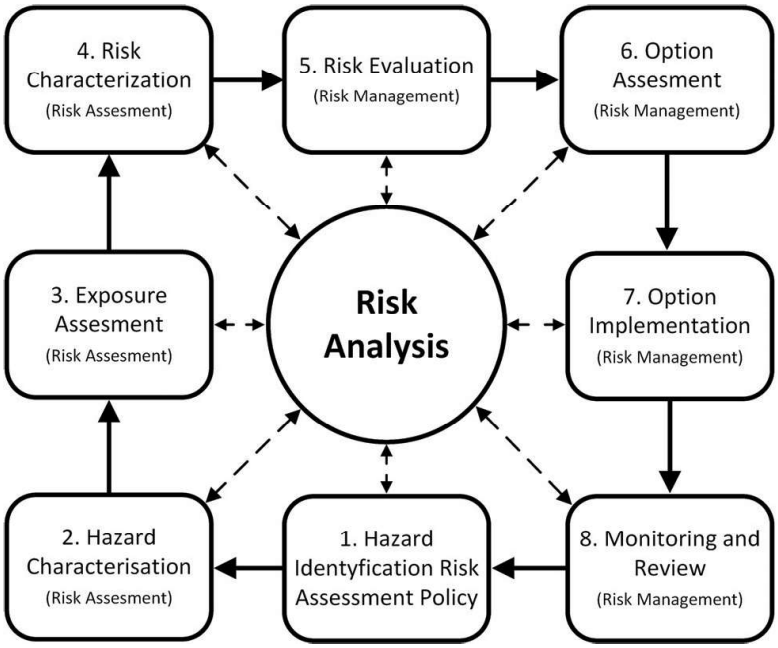

Fig. 2. Diagram of risk analysis process.
Diagram of communication between participants and agents

Risk analysis process is also a pre-determined course of action which is described in directives or internal documents of a given company. The analysis procedure can be written, graphical or tabular, based on which a given scenario has been developed. It is also recommended to include a map indicating the area and reach of a potential threat, separate for each scenario [2]. From the formal perspective, the document should include all important information that may influence the final assessment and outcome of risk estimation. Detailed risk analysis should be divided into individual analytical, decision-making and implementation stages. The most important constituents of risk analysis and estimation, although not the only ones, are entry parameters (stage 1) which include:

- threat monitoring, warning and alarm system,
- threat characteristics and assessment of its occurrence risk,

- risk map and threat map,
- list of tasks and responsibilities of crisis management participants in the form of security grid,
- list of strengths and resources available for use in crisis situations,
- crisis response procedures determining the course of action in crisis situations,
- plan of communication and power organization in case of cascade failure,
- principles and procedure of damage assessment and documentation,
- procedures of initiating energy reserves,
- principles of informing the population of threats and course of action in case of threats [3].

After the probability and consequences have been determined, it is possible to indicate the risk value (stage 2). Risk value for each scenario is indicated on the risk matrix showing the dependence between probability and consequences (Fig. 3). Visualization is not only helpful in quick classification of a given event, it also allows for reading the distribution of most critical situations in relation to their probability.

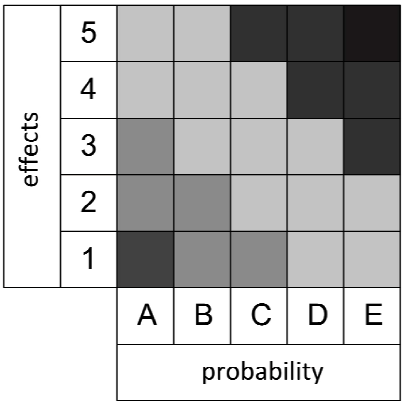

Fig. 3. Risk values have been color-marked:
from minimal (A1) do extreme (E5)

Another stage is a process of risk acceptance (stage 3) within category 4:

- accepted risk (A) – no additional security measures are required, current solutions and their assigned forces and resources are accepted, standard monitoring actions are undertaken,
- tolerated risk (acceptable) (B) – assessment should be made of other solutions or possibilities to implement small organizational, legal or functional changes which will contribute to security improvement,
- conditionally tolerated risk (C, D) – additional security measures should be implemented within a certain period and the utilized solutions should be improved,
- unacceptable risk (E) – immediate action should be taken to assure and improve security, and to implement additional or new solutions.

In the final stage, justification of risk acceptance level should be made (stage 4). Occurrence frequency is often based on historical data and shared experience with bodies undertaking similar activities. Government crisis response documents are often the source of risk estimation concept [3]. Potential threats can be classified as follows:

- very rare (1) – the event might occur only in exceptional circumstances,
- rare (2) – it is not expected for the event to happen, prior occurrence of the threats has not been documented in similar organizations or reports made after an incident. There is little chance, reason or other circumstances for the event to happen,
- possible (3) – might happen in a certain time and conditions, rarely by accident, events are sometimes documented entirely or most often partly. There is some chance, reason for the event to happen,
- probable (4) – there is a probability that the event will take place in specific circumstances, such events are systematically documented, and information on them is provided. There is a specific reason or cause for which the event takes place,
- very probable (5) – the event is expected to happen, it will take place in most circumstances, and such events are well documented [4].

Risk analysis and estimation is a very complicated process which requires not only synthetic knowledge of its creation methodology, but also practical industry knowledge both appropriate and required by a given system. The greatest problem for designing an analytical model aimed at helping with decision-making is estimation of potential threats' impact and preparation of adequate solutions, taking priorities, means and system recovery time into account.

4. CYBERATTACKS AND ELECTRICAL POWER GRID FAILURES

Presently, cybernetic threats we deal with in today's world are characterized by high precision and sophistication. In terms of extensive electrical power systems, it means that critical systems must be systematically monitored and analyzed in case of threats, also in the form of an intentional attack. Large-area electrical power grid failures caused by destructive actions of third parties is the worst possible scenario. Such an attack may target the entire energy sector – power plants, thermal power plants, transmission and distribution networks, even low-voltage networks. High vulnerability of a system to damage and attacks might cause very spectacular and costly failures which include:

- large-area electrical power grid failures – network failures cause by weather factors in large concentrations (natural disasters), causing serious disruptions in electricity supply throughout larger areas.

- widespread long-term system blackouts – dysfunction of the electrical power system of a country or its significant portion – disappearance of energy supply ability to a large number of consumers in sufficiently long time or weather conditions.
- power deficit – limitations in electricity supply and consumption caused by a shortage of production capacity in state system power plants or resulting from limited transfer capabilities [4].

The contemporary grids' problems detailed above are events most often caused by spontaneous damage of elements in an electrical power grid and system, related to impact of weather factors – causing local disruptions in electricity supply. In recent years, however, a brand new threat, related to actions of third parties, has emerged – cybernetic attacks – they are some of the most effective and most bothersome (as far as damage goes) actions striking against an electrical power system's operation security and its related cooperative bodies, and electricity consumers. Cyberterrorism is becoming an increasingly common method, as the only things necessary to undertake cyberattack-related actions are a computer and World Wide Web connection. It is worth mentioning that the cyberspace has no control barriers, but the attacker's experience plays a significant role, as they not only need ICT and programming knowledge, but also industry knowledge specific for the attacked system. Attack targets may vary vastly – from an operator's system management center, to transmission and distribution networks, to low voltage networks – electricity meter grids and smart home gateways controlling local automation and receptions. The probability of discovering loopholes in a seemingly secured electrical power system is relatively high. This is evidenced by media reports on subsequent large-area failures (or attacks), such as: Pakistan (26 January 2015) [5], Kuwait (11 February 2015) [6], the Netherlands (27 March 2015) [7], Turkey (March 31, 2015) [8], USA, Washington, Spokane County (November 17, 2015 [9]), Crimea (21 November 2015) [10].

Poland is not currently among countries targeted by terrorist attacks. However, because of the country's international activities, like participation in Afghanistan operations, policy of cooperation with the USA, the risk of a terrorist attacks against strategic objects, including critical systems, cannot be completely ignored. The common causes of failures include the human factor (ignorance, disregard for regulations, bribery, frustration, ideology), system and data modification, organizational and technical errors, sabotage, damage or theft of transmission elements, which might lead, among others, to:

- disruptions in functionality of hydro-technical infrastructure devices,
- disruptions in communication infrastructure: urban, rail and air,
- disruptions in functionality of communications systems and teleinformation systems: limitation or complete loss of radio and phone communications, threats to proper functionality of an IT system,
- hindered information flow and no access to data necessary for security and public order services to work,

- suspension of border checks of passengers, transports,
- failure of a banking system and non-cash transactions,
- no functionality of central accounting systems,
- lack of or limited telecommunications or mail services.

Cybernetic security of electrical power systems covers all issues related to automation and communication, which influence functionality of the tools governing these systems. It also includes tasks of prevention, mitigation of consequences, as well as facing other cybernetic terrorist events.

5. CONCLUSIONS

The considerable degree of complexity of electrical power systems, which has become especially apparent in the recent years, inclines to take a brand new look on security of electrical power systems. Except for procedures described in a security policy, decision-making should be also supported by decision models of risk analysis and estimation. These models are a valuable tool for making decisions in situations with uncertain or difficult to predict results. Risk estimation process allows the decision-maker to make a final decision based on historical data, current status, expected profit or possibility of potential losses. Based on analysis of many cases, a system designer or a person responsible for the security of an existing system can determine and estimate risk accompanying normal operation of an electrical power system. It requires the decision-maker to constantly monitor the system and be ready to devise emergency plans and quick response in case of threats to the project's success. If there are no formal courses of action prepared for potential decisions, an attempt should be made to prepare a formal document based on historical data, containing a description of action for e.g. when risk is acceptable and when it should be reduced. Decisions should be made along with the entire team responsible for risk management in the company, especially with people responsible for management of the entire organization, not just the security segment. Risk estimation models dedicated for electrical power systems are the second (after the security policy) most important element constituting security of the system's operation. Risk estimation involves convincing our consciousness to make more accurate decisions regarding the state of system security, and then undertaking certain preventative actions, all the while having the organization's main goal in mind, which is most commonly maximizing profit and minimizing losses. As a result of risk analysis, we can conclude what threatens the security of our system and what the consequences of these hazards coming to life may be. The described methods also allow to decide what to do with identified and classified risk. It should be remembered, however, that effective risk management requires adequate analytical knowledge, time and often significant financial resources.

This paper was realized within NCBR project: ERA-NET, No1/SMARTGRIDS/2014, acronym SALVAGE. "Cyber-Physical Security for the Low-Voltage Grids".

REFERENCES

[1] Dz.U. 2007 nr 89 poz. 590, *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, Tekst ujednolicony: D20070590Lj.pdf, 2007.

[2] UNDERBRINK A., *Risk Analysis in Distribution and Transmission Networks*, ABB AG, Mannheim, Germany, 9th International Conference on Probabilistic Methods Applied to Power Systems KTH, Stockholm, Sweden, 2006.

[3] Rządowe Centrum Bezpieczeństwa, *Ocena ryzyka na potrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego*, Warszawa 2013.

[4] Rządowe Centrum Bezpieczeństwa, *Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego*, Warszawa, 2010,

[5] Sky News, *Militant Attack Plunges Pakistan Into Darkness*, http://news.sky.com/story/1414477/militant-attack-plunges-pakistaninto-darkness (access date: 22.03.2016), 2015.

[6] Mail Online Wires, *Most of Kuwait hit by Power Blackout*, http://www.dailymail.co.uk/wires/afp/article-2949576/Most-Kuwaithit-power-blackout.html, (access date: 22.03.2016), 2015.

[7] ESCRITT T., Reuters, *UPDATE 5-Power returns to Amsterdam after outage hits a million homes*, http://uk.reuters.com/article/dutch-poweroutages-idUKL6N0WT1DI20150327, (access date: 22.03.2016), 2015.

[8] RT Question More, *Turkey struck by biggest power cut in 15 years, investigation underway*, https://www.rt.com/news/245529-massivepower-outage-turkey/, (access date: 22.03.2016), 2015.

[9] FOX News Weather Center, *Tens of thousands shivering without power in Washington City*, http://www.foxnews.com/weather/2015/11/24/tens-thousands-shiveringwithout-power-in-washington-city/, (access date: 22.03.2016), 2015.

[10] RT Question more, State of emergency, *Blackout in Russias Crimea after transmission towers in Ukraine blown up*, https://www.rt.com/news/323012-crimea-blackout-lines-blown-up/, (access date: 22.03.2016), 2015.