ARCHIVES OF ELECTRICAL ENGINEERING VOL. 68(2), pp. 411–426 (2019)

DOI 10.24425/aee.2019.128277

The risk of large blackout failures in power systems

Krzysztof Sroka, Daria Złotecka

Institute of Electric Power Engineering, Poznań University of Technology
Piotrowo 3a, 60-965 Poznań, Poland
e-mail: {krzysztof.sroka/daria.zlotecka}@put.poznan.pl

(Received: 14.11.2018, revised: 12.02.2019)

Abstract: The paper concerns the assessment of blackout hazards in the power systems. On the basis of statistical data from more than one hundred failures in power systems that affected the world in the last fifty years, the analysis was carried out regarding the number of people affected by a blackout, power losses in the system, duration of a failure and its direct causes. The paper also describes the methodology of risk analysis and vulnerability analysis of the extraordinary events occurrence in electrical power systems resulting in failures. The structure of risk analysis was based on the bow tie model, identifying threats, unwanted events, barriers and consequences of a system failure. Moreover, particular attention was drawn to the impact of the power reserve deficit in the Polish Power System in the coming years on the increase in the risk of a blackout failure.

Key words: blackout, power deficit, power system, risk assessment, extraordinary events

1. Introduction

The loss of the continuity of the power system or its major part is the most serious disruption of the technical infrastructure of the country with unpredictable social and economic consequences. Reliability of the power system is understood as the ability of the system to supply electricity to the points of its receipt, maintaining the accepted standards and the required quantity. Besides the sufficiency of the system, its safety is relevant.

Power system security is defined as the ability of the power system to withstand sudden accidents, such as short-circuits or unforeseen loss of system components, including operational limitations and the ability of the system to avoid uncontrolled separation of the synchronous area as a result of a power system failure. Therefore, power system security is the state of the power system in which the risk resulting from all threats, both identified and hidden, is at an acceptable level. The operation of the power system, in addition to technical objects, also includes people and the environment, hence risk analysis and risk assessment is a complex and multi-faceted problem. In the recognition of hazards it is necessary to take into account the failures of technical facilities, human errors and the impact of the environment in which natural phenomena are distinguished, as well as bystanders' act of sabotage and technical objects in the vicinity of the operating system. The incorrect state of power system elements caused by the unwanted events requires the barriers implementation, which allow performing actions that break such a chain of adverse phenomena [1].

Effective security management based on a thorough risk analysis implemented in the power system is an integral part of its management and allows for the continuity of ongoing energy supply processes. The risk refers to the adverse events, i.e. those that have negative consequences, usually referred to as catastrophe, failure, etc.

Despite the fact that power is usually balanced in the power system and it is operated in accordance with the criterion n–1, history shows that blackout catastrophes still occur in various places around the world [2–8]. Catastrophic failures that lead to extensive power outages have serious consequences for the functioning of societies and there is a need to provide tools and methods to analyse such events, their causes and effects [9]. The study of the reliability of the power system in this issue is based on the experience resulting from previously occurring power system failures and the related power outages, and above all, the causes and consequences that disruptions in the energy supply have caused for people.

A catastrophic failure of a power system called a blackout is a wide-area or total voltage break in the power system when [8, 10]:

- a large quantity of population and wide geographical coverage is affected by a power outage, which is accompanied by large economic costs and societal impacts,
- the operation of part or all of the Transmission System is terminated,
- cross-border exchanges are inhibited,
- disposition proceeds according to National Power Disposition and Territorial Power Disposition, instead of current operating guidelines.

The majority of blackouts was caused by cascading failure. The cascading failure is a series outage initiated by one component failure in a power system which leads to over-current, voltage drop or frequency drop causing tripping in the cascade, however the cascading failures do not necessarily cause blackouts [11, 12]. Both cascading failures and blackouts were analysed in literature in the context of risk assessment and vulnerability analysis. The risk of the cascading failures according to [13] depends mainly on the cumulative index of the line overload risk, transformer overload risk, low voltage risk, lost load risk and voltage instability risk. In [1] the risk of the cascading failures in a model of a power transmission grid was analysed based on complex network theory in order to find the effective measures to maintain the reliability of the power system. The lines with a high risk coefficient were set as the initial event of the cascading failure, where the risk coefficient considered the betweenness, load rate and variable probability of electrical breakdown outages. An improved complex network theory model for power system risk was proposed in [14] where risk assessment considered both topological and electrical characteristics. In comparison with the existing complex network theory model, the improved model adopt some key characteristics such as power flow, voltage and frequency violation in order to take into account buses, substations and generators failures as cascading outage triggers. The dependence of power system load on a blackout using probabilistic methods is presented in the paper [15] where the CASCADE model, hidden failure model and ORNL-PSerc-Alaska (OPA) model were analysed. In the CASCADE model, the authors modelled random power flows by identical transmission lines, as a result of which the findings of blackout size distribution were obtained depending on the number of lines and the probability of its occurrence in a given time interval. The hidden failure model was used for additional analysis of hidden failures occurring in the case of incorrect activation of protection automation in lines adjacent to the switched off line. The blackout approach in the context of dynamic systems and their self-organised criticality was modelled using the OPA model with many critical points both on the transmission side and the generation. The improved OPA model [16] was developed in blackout risk context. In comparison to the former OPA model, the improved OPA model took into consideration the effects of dispatching, automation, communication relay protection, operation mode and planning which allowed more accurate analysis of blackouts in a large-scale power system. Load-dependent cascading outages were also considered using a Markov-Based Cascading Outage Searching Method [17] where the effect of the operational conditions and influence of the outage sequences on cascading outage probability were presented.

Due to the fact that extreme weather conditions increase significantly the risk of power system failure, numerous research works present risk estimation models considering severe weather hazards. In [18] the authors developed a two-stage hybrid risk estimation model, leveraging algorithmic data-mining technique basing on historical major power outages, climatological observations, electricity consumption patterns, socio-economic data and land-use data for the U.S. power system. An example model of a 220 kV electric power tower and pole damage probability under gusty wind hazard was calculated in [19] considering maximum gust, design wind, an electric power tower and pole operating life and micro-topographic information.

Information and communication systems are the relevant elements of a power system, hence it is important to obtain a high level of its resiliency especially in the face of the threat of a blackout. In [20] the authors presented the risk of different planning programs for an information system consisted of a monitor server, exchanger, intelligent electronic device and the communication line. Presented calculation results of overload risk and voltage violation risk for a star, ring and bus topology information system showed that the information system in the ring topology was characterised by the lowest risk factors, which can be used to help operators and planners to power a system monitor.

The planning of operation of modern power systems is changing significantly due to new mechanisms of the electricity market. In the past, the power system operator was responsible for the entire electricity supply process, from generation to distribution. Currently, the electricity market and its dispersion of electricity generation sources further complicates safety aspects. One of the important issues is the threat related to the risk of maintaining the power balance in the power system and, consequently, reducing the safety margins.

The article presents the results of the analysis of a significant number of power system failures that occurred in the world and presents the methods of hazard identification, linking possible adverse events with the consequences considered in the risk and vulnerability analysis.

2. Examples of the large power system failures

Catastrophic failures are a phenomenon affecting power systems all over the world. The inevitability of power system failures results from the diversity of their causes, which include: atmospheric conditions, technical reasons and a human factor. The following phenomena, usually weather conditions, cause cascading outages of power system fragments due to exceeding the frequency and voltage acceptable limits, most often resulting from settings of protections, leading to the development of extensive system failures.

Basing on the collected data, the authors have identified 138 failures in the power systems that affected the world in 1965–2017 [2–8]. For the purpose of the analysis, data on the number of people affected by the failure, the power loss in the system, the duration of the failure and its immediate causes were collected. The largest number of power system failures affected North America, especially the US system (45 failures) and the Canadian system (7 failures), due to the territorial extension and relatively frequent exposure to extreme weather conditions.

The severity of system failures that occurred in power systems around the world can be considered due to a number of criteria. Record blackout failures are listed below:

- due to the number of people deprived of electricity:
  - 670 million, India, 31 July 2012,
  - 230 million, India, 2 January 2001,
  - 150 million, Bangladesh, 1 November 2014,
  - 140 million, Pakistan, 26 January 2015,
- due to the duration:
  - a month, Zanzibar, 20 May 2008 and 10 December 2009,
  - from a few hours to a few weeks, Russia, 25 May 2005,
  - 3 weeks, China, 25 January 2008,
- due to the power deficit in a power system:
  - 61.8 GW, USA/Canada, 14 August 2003,
  - 48 GW, India, 31 July 2012,
  - 32.2 GW, Turkey, 31 March 2015.

The reasons initiating power system failures have been generalized to atmospheric phenomena, technical reasons and human factors. Based on the collected data [2–8], the percentage distribution of power system failures causes on individual continents was calculated, which is presented in Table 1. The development of the above-mentioned causes of failures together with their consequences for power systems are presented in detail in Chapter 3 in the context of risk analysis.

Table 1. Causes of blackouts in power systems on individual continents

Continent/ blackout causes	**Atmospheric phenomena**	**Technical causes**	**Human factors**	**Undefined causes/ lack of data**
Africa	34%	33%	33%	0%
Asia	24%	44%	12%	20%
Australia and Oceania	62%	15%	8%	15%
Europe	33%	37%	27%	3%
North America	74%	11%	9%	6%
South America	45%	44%	11%	0%

Based on the collected data, a clear tendency to a blackout occurred in summer months and in winter months can be noticed. The reason for such dependence is the intensification of extreme atmospheric conditions, such as high temperatures, gusty winds, cyclones or derecho, while winter conditions are often caused by snowstorms and accumulation of hard rime on power lines, leading to serious mechanical damage, and in extreme cases to an avalanche of shutdowns. Seasonal dependence of causes of the power system failure occurrence on the north hemisphere is presented in Fig. 1.

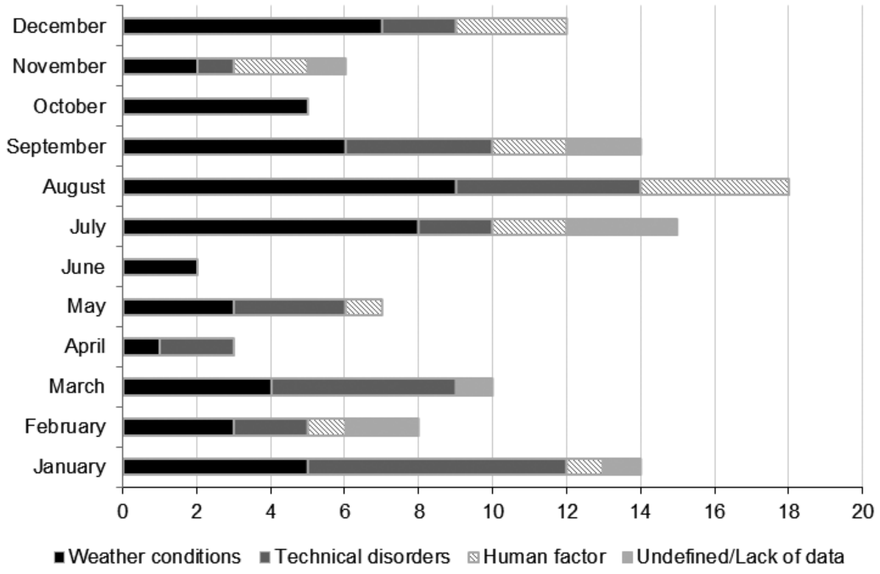

Fig. 1. Seasonal dependence of causes of the occurrence of failure on the north hemisphere

The review of historical blackouts allow one to draw conclusions that limiting the risk of a power system failure is possible both in the planning and operation phases. It can be implemented by [2, 3, 4, 6, 8]:

- maintaining adequate power surpluses in power plants and a sufficiently high level of power reserves,
- providing a diversified power generation structure,
- limiting the concentration of power in power plants,
- installation of high-class power equipment and monitoring systems,
- removing current threats, for example, by inspection and trimming of the vegetation environment around the transmission facilities,
- redundancy and reliability of remote control and communication devices,
- building connections with neighbouring systems and maintaining transmission capacity reserves on them,
- preparing effective defence and restorations plans, verified by system experiments,
- statistical data gathering in order to predict a possible power outage,

- keeping adequate awareness about a system situation by system operators and control centres, by implementation of software redundancy, a backup system and disturbance monitoring systems,
- providing qualified service,
- system operator training.

3. Review of risk analysis methods

In literature, blackout failures in power systems are analysed in the context of probability distribution and the possibility of implementation of statistical distributions. In paper [11] the authors specified two types of failure causes in power systems, dividing them into deterministic and probabilistic causes. The factors influencing the formation of power system failures were in turn divided into primary causes and causes of cascading failures as the effects of primary causes. The primary causes of blackouts, related to probabilistic failures include, among others, such phenomena as:

- short-circuit to trees due to increased slack of power lines,
- line fault,
- phase-to-ground fault,
- primary protective relay failure,
- damage of the power line due to strong wind,
- lightning discharge,
- hidden failures,
- cascading damage of the power line.

The causes of failures growing in a cascade, leading to the blackout (here above referred to as cascading failures) were divided into:

- deterministic factors – related to system operation limitations and their physical equations, they depend strictly on the system configuration, load pattern, capacities of edges and operation limits, resulting in violations of the physical operating constraints, which include:
  - frequency decrease,
  - voltage decrease,
  - overloads in the power system,
- probabilistic factors – factors overlapping deterministic factors, leading to the development of power system failures, such as:
  - failure of the tap-changing mechanism,
  - failure of communication systems,
  - failure of backup devices,
  - omissions of system operators,
  - additional atmospheric events.

This division was used to create a model of cascade development of a system failure, taking into account the time until the next primary cause. The intention of the authors of the work [11] was to prove that the blackout phenomenon can be analysed in accordance with the statistical distribution. For the assumptions, there was demonstrated a disproportional distribution of the cumulative probability of blackout occurrence, which was verified on a mathematical model of the system, consisting of 24 power stations using the Monte Carlo method.

The development of the paper [11] is presented in the article [21], where the concept of predicting the possibility of a blackout in power systems was presented with the nonlinear system model. It was assumed that in the analysis of the blackout probability, it is necessary to take into account such phenomena as transient angular instability, frequency and voltage instability or damage to devices and protections included in the power infrastructure. The modelling of factors initiating a blackout, addressed in paper [11], involved the occurrence of phenomena independently of each other with a constant value, hence the time between events took the exponential distribution. These factors include:

- changes in the system power balance (generation-load imbalance),
- voltage instability,
- frequency instability,
- branch overloads,
- hidden failures.

Thus, it was shown that the blackout in the system is a set of gamma distributions, that is, it has a continuous probability distribution.

The probability distribution function is given by Formula (1):

$$P(X^b \leq x) = \sum_{i=1}^{I_0} p_i P\left(X_i^b \leq x\right) \tag{1}$$

and the probability density function is given by Formula (2):

$$f(x) = \sum_{i=0}^{I_0} p_i f_{k_i,\theta_i}(x), \quad x \geq 0, \tag{2}$$

where: k_i is the shape parameter, θ_i is the scale parameter, I_0 is the maximum time of primary causes, X_b is the system infallibility, which takes values X_{bi} with probability p_i, where i takes values within $1 \leq I \leq I_0$, and the sum of particular probabilities takes value (3):

$$\sum_{i=0}^{I_0} p_i = 1. \tag{3}$$

Moreover, in work [21] two groups of cascading failure prediction were categorised into:

- short-term prediction (in real time) – related to a single failure event,
- long-term prediction (off-line) – related to the statistical approach based on the probability distribution, however, from the engineering point of view, it is necessary to include additional phenomena that may be associated with the growing threat, such as weather phenomena, changes in the load of generation units or other random events.

As a safety measure related to the so-called adverse events, i.e. those resulting in losses, damages, negative effects, usually referred to as an accident, disaster, breakdown, etc., in science the concept of risk is applied. The definition of risk is assumed in the form of a numerical "combination", most often in a form of a product of the probability (possibilities) of occurrence of losses and their size.

Formally, the risk is a measure expressed in numerical terms, binding the possibility of an unwanted event and the amount of losses resulting from this event. Since the sequence of successive events leading to a failure is mostly random, it is also necessary to consider probable scenarios of such a chain of events. Therefore, it should be assumed that the threat triggered by the initiating event, depending on various scenarios, will cause various losses, and as a consequence it will be characterized with a risk covering all potential consequences.

The concept of risk was defined by Stanley Kaplan and B. John Garrick (1981) [22, 23] as answers to three questions:

1. What can go wrong?
2. How likely is it that it is going to fail?
3. If it goes wrong, what are the consequences?

The answer to the first question is the failure scenario, marked by S_i. The answer to the second question is the probability p_i of a given scenario. The answer to the third question is the result in the form of consequences Y_i generated by the sequence of events described by the scenario. Therefore, the risk is presented by Kaplan and Garrick as a set of three (4):

$$\{S_i,\ p_i,\ Y_i\}, \tag{4}$$

where: $I = 1, 2, \ldots, N$ is the number of given scenario.

Each scenario is presented in the form of a chain of events (5):

$$S_i = \{F_{i1},\ F_{i2},\ F_{i3}\}. \tag{5}$$

This form of the scenario results from the fault tree analysis and similar methods used in safety engineering. Each scenario presents a characteristic combination of events. If the event F_{i1} occurs with the probability $p_i(1)$ and all subsequent events in the chain occur with the probability $p_i(k|k{-}1)$, then the probability of occurrence of the scenario consisting of k events is given by Formula (6):

$$p_1 = p_i(1) \cdot p_i(2\,|\,1),\ \ldots,\ p_i(k|\,k{-}1). \tag{6}$$

The probability of the scenario is the same as the likelihood of consequences. Therefore, the last two elements of the three p_i and Y_i determine the probability distribution of consequences (7):

$$P_Y = \{Y_i,\ p_i\}. \tag{7}$$

This is the essence of the Probabilistic Risk Assessment (PRA) formulated by Kaplan and Garrick.

Numerous risk analysis methods described in the literature are based on experience, statistics or expert knowledge. This article analyses risk assessment methods based on ISO/IEC 31010 Risk Management – Risk Assessment Techniques discussed in [24].

Depending on the stage of the risk management process, different types of methods may be implemented. The risk analysis requires many different researches, including the following aspects [9]:

- identification of threats and unwanted events – including identification of unwanted events and related threats and barriers, so far the experience has shown that the identification of extraordinary events is one of the most difficult parts of the risk analysis and vulnerability analysis,

- causal analysis – a description of the causes and probability of their occurrence; it is used to find causes leading to identified unwanted events,
- consequence analysis – classification of effects that occur after the unwanted event,
- risk assessment and vulnerability analysis – the process in which:
  - a risk hierarchy is established,
  - an acceptable level of risk is determined,
  - the risk value is estimated,
  - particular probabilities are estimated.

At this stage of the analysis it is also important to assess the existing barriers – whether they are sufficient and appropriate, and if not, whether new barriers are needed.

The risk analysis methods used in particular stages of this analysis, which can be used in the case of a power system are presented in Table 2.

Table 2. Risk analysis methods used in individual stages of risk analysis [9, 24]

Identification of threats and unwanted events	Expert interview
	Bow-tie model
	Probabilistic safety analysis
	Contingency analysis
	Graph theory
Causal analysis	Fault analysis
	Fault tree analysis (FTA)
	Analysis of the types and effects of possible errors (FMEA)
	Expert judgement
Consequence analysis	Event tree analysis (ETA)
	Power flow analysis
	Monte Carlo simulation
	Graph theory
	Discrete event simulation (DES)
	Expert judgement
Risk assessment and sensitivity assessment	Cost benefit
	Risk matrix
	Multi criteria decision analysis

From the viewpoint of power system failures, the method allowing to develop the structure of causes and effects of undesired events as the basis for risk and vulnerability analysis may be the bow tie model. The bow tie model is a simple, schematic way of describing and analysing the paths of event development from cause to consequence. It focuses on the barriers between the causes and the event and the event and its consequences [24].

The main adverse events for the power system are its failures and consequences in the form of extensive outage or complete loss of power. It is shown on the bow tie model with the main categories of threats, taking into account natural threats, technical and operational reasons, human errors and intentional actions such as a terrorist attack or sabotage. The threat can lead to a power system failure through a chain of events, while a failure can lead to minor or serious consequences as a set of subsequent events. Therefore, a number of barriers to avoid threats and undesirable events or reduce their effects are applied. The system is more vulnerable if the barriers are weak or cause malfunctions. An example of the bow tie method used for the blackout phenomenon is shown in Fig. 2.

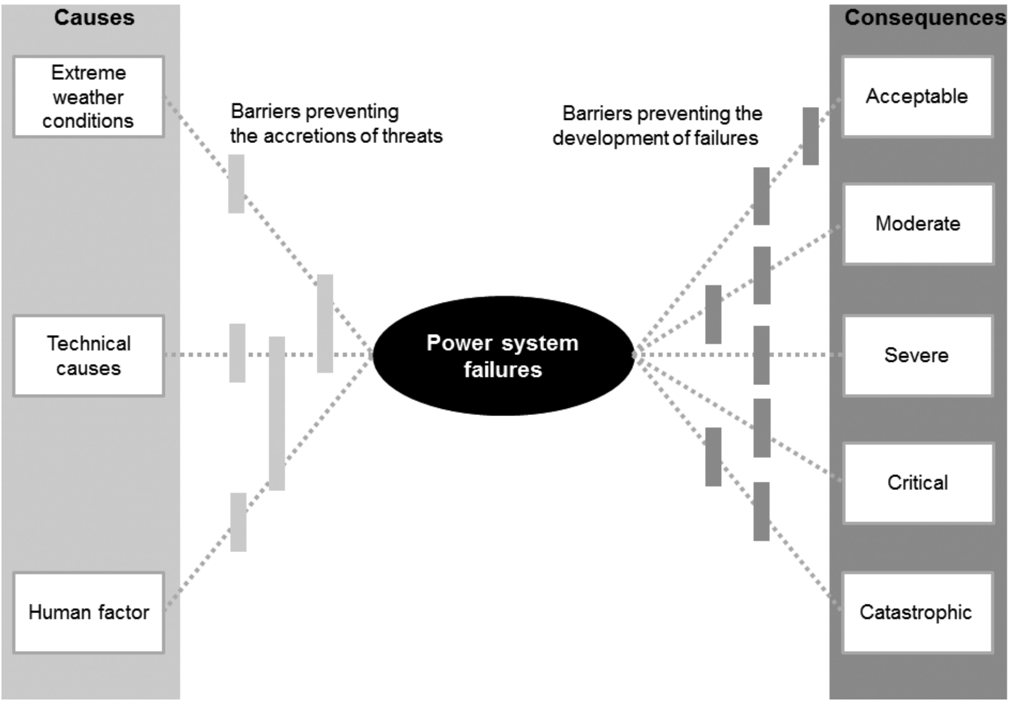

Fig. 2. An example of bow-tie model for the power system failures

Risk assessment requires preparation of an exhaustive list of:

- threats or sources of potential catastrophic disaster,
- possible consequences,
- barriers to limit or eliminate side effects.

The classification of the consequences of power system failures can be made from the point of view of their extent, i.e. the number of people affected by the failure in relation to the total population and the severity of the failure suffered in "system-minutes" according to Formula (8) [4]:

$$D = \frac{\text{undelivered energy due to failure [MWh]}}{\text{base of power [MW]}} \cdot 60. \tag{8}$$

The base of power in the denominator of Formula (8) is the peak load in the power system.

Due to the severity of the failure, five hazard levels can be classified as a consequence of the failure [4]. A list of potential lists for the power system is presented in Table 3.

Table 3. Risk analysis methods used in individual stages of risk analysis [9, 24]

Threats	Barriers	Consequences
– extreme weather conditions: – extremely low or high temperatures, – strong wind, – storms, – forest fires which threaten the network infrastructure, – technical factors: – equipment failures, – lack of adequate reserves of capacity or production capacity, – unreliability of IT, telecommunications, control or monitoring systems, – no or limited possibilities of using emergency assistance from neighbouring systems, – human factors: – operator errors or omissions and operational negligence, – vandalism, – terrorism, – inefficient cooperation between operators.	– maintaining the excess power required by the TSO, – reduction of demand for TSO command, – emergency load shedding, – effective plans for the defence and restitution of power system, – island operation of generation sources – operator import on cross-border connections, – staff training, – reliably communication systems between operators, – effective operator procedures.	– acceptable $D < 1$, – moderate $1 < D < 10$, – severe $10 < D < 100$, – critical $100 < D < 1000$, – catastrophic $D > 1000$.

4. Deficit of power reserves as a risk of power system failure

In the National Power System (NPS) historically catastrophic failures took place:

- in July 1972, covering the range of Lower Silesia,
- in February 1987 in the north-east of Poland, as a result of severe frosts and technical defects,
- in June 26, 2006 in the central-northern part of the country,
- in April 2008 near Szczecin, which was caused by the wet snow precipitation, which accumulation on the power lines led to their damage.

Currently, the greatest threat of power system failures in the NPS is connected with the risk of significant power deficits in the coming years.

Due to planned changes in the generation sector as a result of the Best Available Techniques (BAT) conclusions that tighten emission standards, the document “Forecast of peak demand for power in 2016–2035” prepared by TSO in the System Development Department [25] assumes two scenarios of the impact of the BAT conclusions on the power sector: the modernisation scenario and the BAT withdrawal scenario.

The modernization scenario assumes the adjustment of generating units to the restrictive emission standards contained in the BAT conclusions. The “Forecast ...” for this variant assumes favourable market conditions in terms of modernisation of facilities. In contrast, the BAT withdrawal scenario foresees a shortening of the operational lifetime of the generating units due to the inability to undertake activities aimed at modernization of the flue gas purification systems in order to adapt the installations to the emission standards contained in the BAT conclusions. The cumulative volume of withdrawals of installed capacity according to the above-mentioned scenarios is included in Table 4. These amounts take into account the currently built generating units and those for which the tendering procedure for the implementation of the investment has been resolved.

Table 4. Cumulative power withdrawals for the modernization scenario and the BAT withdrawal scenario [25]

Cumulative power withdrawal for Centrally Dispatched Generating Units [MW]	**Until 2020**	**Until 2025**	**Until 2030**	**Until 2035**
Modernisation scenario	2 985	3 210	5 668	13 930
Withdrawal scenario	6 617	9 928	17 321	20 920

According to the “Forecast . . . ”, for the modernization scenario, while meeting the timeliness of executed investments, sufficient power surplus in the National Power System will be maintained by 2021. The shortage of the required power surplus in the system will begin to appear already in 2022, growing up to 2030, which forecasts the situation of dependence of the covered demand on cross-border exchange, because domestic remedies will become insufficient, which significantly reduces the country’s energy security.

In the BAT withdrawal scenario, the power surplus required by the TSO will only be provided by the end of 2019. Due to the decommissioning of a significant number of generating units, the power reserve deficit in the system growing since 2021 will lead to inadequacy generation of national generating units in relation to the demand.

Based on the above-mentioned forecasts, it can be concluded that from the point of view of the NPS’s operational safety, the decreasing power reserve, constituting hitherto a barrier due to the risk of a system failure, begins to turn into a threat that significantly increases the probability of a blackout, especially in peak demand conditions. The situation related to the implementations of new environmental requirements and the consequent increase in the power deficit in the power system intensify the risk of power system failure, which may be additionally overlapped with extraordinary atmospheric, technical or human factors.

Fig. 3 presents scenarios for the development of a blackout in the power system using risk analysis methods including the combination of the fault tree and the event tree. The main reason for the events is the risk resulting from the expected power deficit in one of the above forecasts in the National Power System. On the basis of the block diagram shown, there are many scenarios that require analysis of the probability of their occurrence.

In the following years, the large scale of renewable energy integration into a power system may be expected. Both wind and solar power generation is characterised by random and fluctuant output, depending on weather conditions, such as wind speed and solar irradiation. From the energy security perspective, this specificity of power generation influences uncontrolled power flows. Wind turbine generation conditions are within the wind velocity range of 3–25 m/s, up to

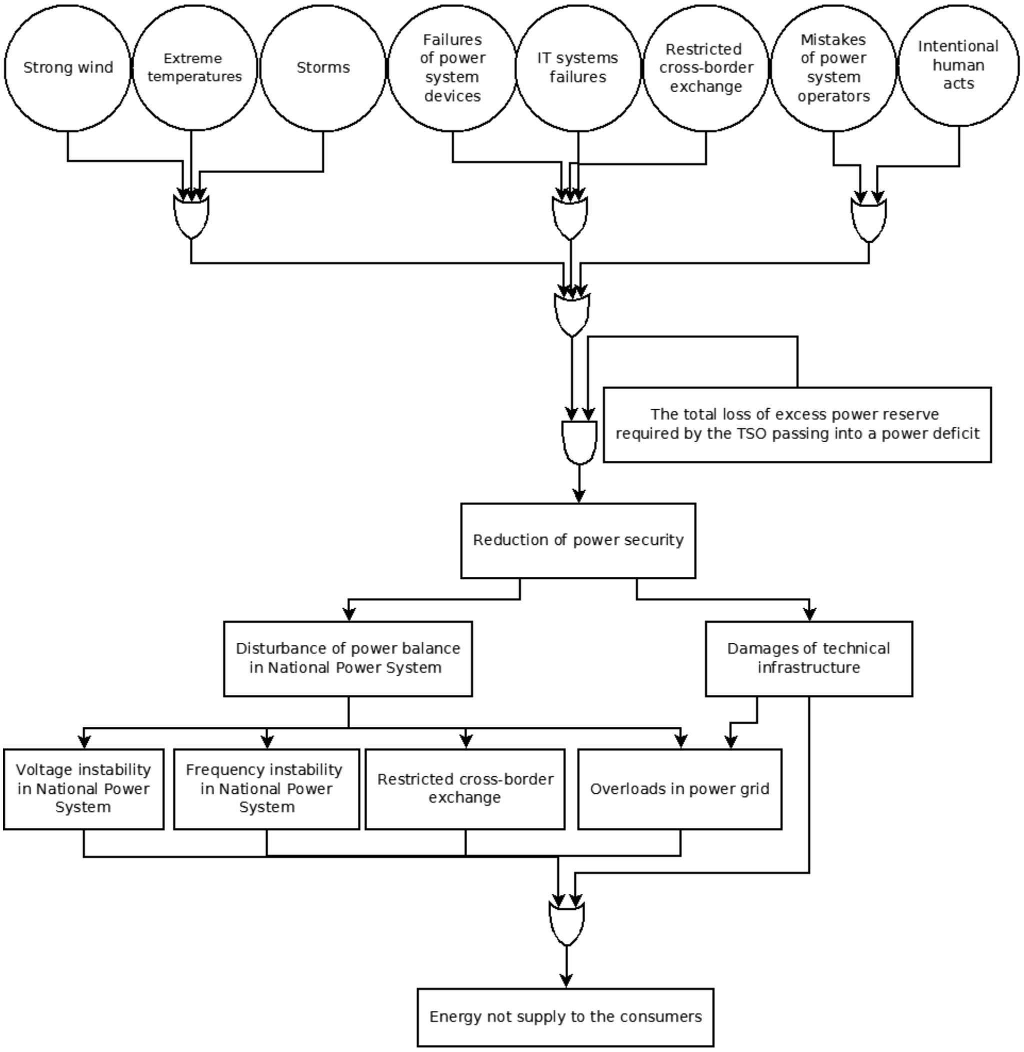

Fig. 3. Logic scheme for connecting the error tree and event tree for the power system

30 m/s [26]. The output of power generated by wind farms depends strictly on the wind speed, the changes of which cause fluctuations in power and voltage in the system nodes and may cause overloading of the network infrastructure [27]. A particular threat to the power system operation safety is connected with large wind farms in the conditions of reduced power demand in the system, because due to the obligation to ensure power balance in the power system, it may be necessary to limit the generation of power in conventional power plants being Centrally Dispatched Generating Units (CDGU), which significantly disturbs the operating conditions of generating units, especially in the case of their cold restart, which is a long-term process. The presented situation took place in the Polish Power System during the period of 23–25 December 2017.

On 23 December 2017, the amount of power generated in wind farms reached 5.344.34 MW, which was nearly 90% of the capacity installed in wind farms in the Polish Power System. The relatively low level of power demand in the system on December 25, 2017 overlapped with a record wind generation reaching 38% of the total power generated in the power system at that time, which led to a radical reduction of power generated by CDGU to 34% of the total generation in the National Power System [28]. On the other hand, in spite of the fact that wind farms have a positive impact on voltage stability, the negative effect on power system stability by virtual inertia decreasing is observed [29]. Moreover, in the conditions of high wind speed, wind turbines are disconnected from the power system. Immediate power shortage due to disconnection may cause dynamic frequency changes and influence reactive power balance and changes in virtual inertia in the power system [30]. In order to eliminate or reduce the above negative systemic effect, wind farm regulation algorithms should be improved, the effect of which would be bringing the dynamics of wind turbines closer to the dynamics of classical generating units [29]. In order to eliminate the above-mentioned challenges connected with increasing renewable power integration in the power system in the following years, there is a necessity of energy storage, which reduces the problem of uncontrolled power flows and improves power system stability. Moreover, the energy storage system has a positive influence on the power balance in the condition of changing power demand.

The issue of the adequate balance between generated power and load demand in future can be improved by proper electricity market operation and smart grid development. Electricity demand management and distributed generation management stand an opportunity for power system security improvement. The formation of dynamic tariffs will be related to the price elasticity of demand in relation to the price for electricity. This mechanism encourages the consumers to participate in the energy market in an active and conscious way leading to tightening the balance between supply and demand, especially in the condition of the rapid growth of micro-sources. The optimisation of power consumption (and possible integration of micro generation with a power system in the case of prosumers) will be possible by smart metering implementation. Therefore, smart grid development would lead to increasing off-peak load and cutting peak load by smoothening the daily curve of the power demand and may influence the dynamic development of well-managed distributed generation [31]. The above-mentioned features of smart grids, especially more predictable load demand profiles, are connected with lowering the risk of a blackout in the power system. Furthermore, in future TSO's investment plans for the power system structure it is necessary to avoid the concentration of power in power plants.

5. Conclusions

The paper describes the methodology of risk and sensitivity analysis for the power system. The power system operator (TSO) must take into account the possibility of undesirable events to achieve its intended purpose. In order to minimize or eliminate hazards, a proper risk assessment must be undertaken and the necessary preventive measures determined.

The methods that may be applicable in individual stages of risk analysis, which are presented in the paper, are methodological tools that enable detection of potential events and prevention of their occurrence. The current approach to risk assessment is based primarily on expert knowledge and experience about existing threats. Predicting the occurrence of specific events allows minimizing the negative effects and also enables more efficient management of the power system.

However, previous experience in the operation of power systems shows that identifying threats, causes and unwanted extraordinary events is one of the most difficult parts of risk and sensitivity analysis.

The authors intend to continue further work under the presented issues focusing on the methodology of dealing with extraordinary events in risk and sensitivity analysis.

References

[1] Yanbing J., Ruiqiong L., Xiaoqing H., Peng W., *Risk Assessment of Cascading Failures in Power Grid Based on Complex Network Theory*, 2018 International Conference on Control, Automation, Robotics & Vision, Phuket, Thailand, pp. 1–6 (2016).

[2] Złotecka D., Sroka K., *The characteristics and main causes of power system failures basing on the analysis of previous blackouts in the world*, 2018 International Interdisciplinary PhD Workshop IIPhDW, Świnoujście, Poland, pp. 257–262 (2018).

[3] Atputharajah A., Saha T., *Power System Blackouts – Literature review*, Fourth International Conference on Industrial and Information Systems, ICIIS 2009, 28 – 31 December 2009, Sri Lanka, pp. 460–465 (2009).

[4] Veloza O., Santamaria F., *Analysis of major blackouts from 2003 to 2015: Classification of incidents and review of main causes*, Electricity Journal 26, pp. 42–49 (2016).

[5] List of major power outages, https://en.wikipedia.org/wiki/List_of_major_power_outages, accessed November 2017.

[6] Zeng B., Shaojie O., Jinhua Z., Hui S., Geng W., Ming Z., *An analysis of previous blackouts in the world: Lessons for China's power industry*, Renewable and Sustainable Energy Reviews 42, pp. 1151–1163 (2015).

[7] Woliński K., *Power system failures in Europe* (in Polish), Wiadomości Elektrotechniczne, Rok LXXII, no. 3, pp. 3–4 (2004).

[8] Project SESAME: *Securing the European Electricity Supply against Malicious and Accidental Threats. D1.1. Analysis of historic outages*, https://www.sesame-project.eu/publications/deliverables/d1-1-report-on-the-analysis-of-historic-outages/at_download/file, accessed June 2018.

[9] Gjerde O., Kjølle G.H., Detlefsen N.K., Brønmo G., *Risk and Vulnerability Analysis of Power Systems Including Extraordinary Events*, Proceedings of IEEE PES Trondheim PowerTech, Trondheim, Norway (2011).

[10] Entso-e Continental Europe Operation Handbook, *Policy 5: Emergency Operations v 3.1*, https://docstore.entsoe.eu/publications/system-operations-reports/operation-handbook/Pages/default.aspx, accessed June 2018.

[11] Gou B., Zheng H., Wu W., Yu X., *Probability Distribution of Power System Blackouts*, Proceedings of IEEE PES General Meeting, pp. 1–8 (2007).

[12] Yu X., Singh C., *A Practical Approach for Integrated Power System Vulnerability Analysis Protection Failures*, IEEE Transactions on Power Systems, vol. 19, no. 4, pp. 1811–1820 (2004).

[13] Yan J., Ji Y., *Risk Assessment of Six Indicators in Power System Operation*, 2010 Asia-Pacific Power and Energy Engineering Conference, pp. 1–4 (2010).

[14] Wang Z., Hill D., Chen G., Dong Z.Y., *Power system cascading risk assessment based on complex network theory*, Physica A 482, pp. 532–543 (2017).

[15] Dobson I., Chen J., Thorp J.S., Carreras B.A., Newman D.E., *Examining criticality of blackouts in power system models with cascading events*, Proceedings of the 35th Hawaii International Conference on System Sciences (2002).

[16] Mei S., He F., Zhang X., Wu S., Wang G., *An Improved OPA Model and Blackout Risk Assessment*, IEEE Transactions on Power Systems, vol. 24, no. 2, pp. 814–823 (2009).

[17] Cheng L., Liu M., Dent C., *A Markov-Based Cascading Outage Searching Method Considering Load-Dependent Outages*, 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), pp. 1–6 (2018).

[18] Mukherjee S., Nateghi R., Hastak M., *A multi-hazard approach to assess severe weather-induces major power outage risks in the U.S.*, Reliability Engineering and System Safety 175, pp. 283–305 (2018).

[19] Yu S., Wu H., Geng H., Yu J., Mao S., Hou H., Mao Z., *Study on Risk Assessment of the Electric Power Tower and Pole Damage in Power System Under Typhoon Disaster*, The 4th International Workshop on Wireless Technology Innovations in Smart Grid, Procedia Computer Science 130, pp. 1164–1169 (2018).

[20] Zhao T., Lu D., Wang D., Zeng Y., Liu Y., *A Risk Assessment Approach for Power System Based on a Comprehensive Fault Probabilistic Model*, 2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT), Changsha, China, pp. 574–577 (2015).

[21] Gou B., Wu W., *WiP Abstract: Possibility of Power System Blackout Prediction*, ACM/IEEE International Conference on Cyber-Physical Systems ICCPS (2013).

[22] Kaplan, S., Garrick, B.J., *On the quantitative definition of risk*, Risk Analysis 1, vol. 1, pp. 11–27 (1981).

[23] Wal K.D., *The Kaplan and Garrick Definition of Risk and its Application to Managerial Decision Problems*, Dudley Knox Library, Monterey (2011).

[24] Wróblewski J. (ed.), *Risk assessment – review of methods*, Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego, Państwowy Instytut Badawczy (in Polish), Józefów (2018).

[25] *Forecast of peak demand for power in 2016-2035*, https://www.pse.pl/-/prognoza-pokrycia-zapotrzebowania-szczytowego-na-moc-w-latach-2016-2035 (in Polish), accessed June 2018.

[26] Malska W., *Analysis of the Impact of Wind Speed for Power Generation on the Example of Wind Farm*, Przegląd Elektrotechniczny (in Polish), vol. 93, no. 4, pp. 54–57 (2017).

[27] Paska J., *Wind power plants in electric power system and their load carrying capability*, Przegląd Elektrotechniczny, vol. 85, no. 12, pp. 224–230 (2009).

[28] www.pse.pl/dane-systemowe, accessed May 2018.

[29] Lubośny Z., *The Impact of Renewable Energy Generation Sources on the Operational Safety of the National Power System*, XVII Seminar "Automation in Power Engineering" (in Polish), Gliwice, Energotest sp. z o.o., pp.1–16 (2014).

[30] Yuxin Z., Xuemin Z., Shengwei M., Deming X., Shuai W., Rui S., *Blackout Risk Analysis and Control of Power System Integrated with Wind Farm*, 2016 Chinese Control and Decision Conference (CCDC), Yinchuan, China, pp. 876–882 (2016).

[31] Kielerz A., *Smart Grid and Sustainable Electricity Systems with Power Production Increase from Various Energy Sources*, XXIX Conference on Issues of Energy Resources and Energy in The National Economy, Zakopane, Poland, pp. 111–119 (2015).