Electrical Power and Energy Systems 136 (2022) 107700

Contents lists available at ScienceDirect

International Journal of Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Dynamic robustness modelling of electricity critical infrastructure elements as a part of energy security

David Rehak [a,*], Martin Hromada [b], Vendula Onderkova [a], Neil Walker [c], Clemente Fuggini [d]

[a] VSB – Technical Unversity of Ostrava, Faculty of Safety Engineering, Lumirova 13, 700 30 Ostrava – Vyskovice, Czech Republic
[b] Tomas Bata University in Zlin, Faculty of Applied Informatics, Nad Stranemi 4511, 760 05 Zlin, Czech Republic
[c] International Association of Critical Infrastructure Protection Professionals, 200 Ware Road, Hoddesdon Herts EN11 9EY, United Kingdom
[d] Rina Consulting S.p.A., Via Gran S. Bernardo Palazzo R, 20089 Rozzano, Italy

ARTICLE INFO

Keywords:
Electricity critical infrastructure
Resilience
Robustness assessment
Dynamic modelling
Disruptive event
Dynamic Robustness Modelling (DRM) method

ABSTRACT

The key components of an Electricity Critical Infrastructure (ECI) are the elements of system required to permanently provide services with a certain performance level. In the case of disruptive events effects on these elements, the key security factor is their robustness, which is an important determinant of element resilience. Current methods can already assess the static level of element resilience but are as yet unable to creating dynamic models of resilience decrease due to disruptive events. In this context, dynamic security assessment is an important area for determining energy supply security. Based on this observation, the authors of the article created a method for Dynamic Robustness Modelling (DRM) which allows ECI element robustness dynamic modelling which can be clearly considered as a new concept of robust, secure and resilient of ECI. This stochastic method uses integral calculus and analysis of dynamic robustness in elements in the context of a predicted disruptive event scenario. The method quantifies the negative effect of predicted disruptive events and the subsequent decrease in the level of robustness due to this effect at the expected time of exposure. Practical use of the method is illustrated through a case study that models a decrease in the level of robustness of an electricity transformer station during an intentional man-made attack.

1. Introduction

Critical infrastructure (CI) is an irreplaceable source of vital services in large urban agglomerations. The Council of the European Union [1] defines critical infrastructure as *"an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions"*. A similar understanding of critical infrastructure is also given in the National Infrastructure Protection Plan of 2013 [2] by the U.S. Department of Homeland Security, which defines critical infrastructure as *"systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"*.

The hierarchy of critical infrastructure consists of three levels that form the vertical structure of the system [3]: (1) system level, (2) sector level, and (3) elementary level. Critical infrastructure is classified into the system level according to functional specifics. The system level covers two areas, namely technical infrastructure (e.g. energy, transport) and socio-economic infrastructure (e.g. health, emergency services). The sectoral level consists of individual sectors (e.g. energy) and subsectors (e.g. electricity) of critical infrastructure. The elementary level consists of individual elements (e.g. power plants, transformers) that form the basic building blocks of the system hierarchy in those sectors. The overview of specific critical entities in the field of electricity is given in the Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities [4].

The most important technical sector of the critical infrastructure system, which is called uniquely critical on the basis of Presidential Policy Directive / PPD-21 [5] and Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities [4], is energy. This unique criticality is especially evident in the electricity sub-sector, on the supply of which all other critical infrastructure sectors are depend [6]. The importance of the energy sector is also

* Corresponding author.
E-mail address: david.rehak@vsb.cz (D. Rehak).

https://doi.org/10.1016/j.ijepes.2021.107700
Received 4 June 2021; Received in revised form 23 September 2021; Accepted 11 October 2021
Available online 1 November 2021

evident in critical infrastructure systems on other continents, such as Asia [7] or Australia [8]. For this reason, it is necessary to pay attention not only to the development of energy technologies, but also to energy security [9,10].

In the context of pervasive security issues, electricity critical infrastructure (ECI) elements are continuously exposed to the adverse effects of naturogenic and anthropogenic threats [11–13]. Ensuring a high level of robustness in these elements against the adverse effects of disruptive events is therefore essential. Robustness is an important determining factor in resilience, which in the context of critical infrastructure, resilience is defined as *"the ability to reduce the magnitude and/or duration of disruptive events; the effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event"* [14]. The European Commission has recently proposed a new directive to enhance the resilience of critical infrastructure and create an all-hazards framework to support Member States in ensuring that critical entities are able to prevent, resist, absorb and recover from disruptive incidents, both natural and man-made [4]. Critical entities would be required to carry out risk assessments of their own, take appropriate technical and organisational measures in order to boost resilience, and report disruptive incidents to national authorities.

At present, resilience in critical infrastructure elements can be measured statically [15]. This method provides information about the level of resilience in an element at the time before a disruptive event occurs. However, when a disruptive event affects a critical infrastructure element, the informative value of resilience is lost since its resilience level has already started declining [16]. Static resilience, therefore, does not let us analyse dynamic resilience at the time of a disruptive event [17] and predict the critical point of failure in critical infrastructure element performance. The starting point for this statement is the Critical Infrastructure Resilience Final Report and Recommendations [14] which works with the term Absorptive Capacity that is defined as *"the ability of the system to endure and disruption without significant deviation from normal operating performance"*. The absorption process is dynamic (takes place over time), as a result of which the absorption capacity of the element is gradually depleted. In contrast, at a time when there is no absorption capacity, the level of resilience is constant or static. Based on this, the terms static and dynamic resilience are used only in relation to the method of assessing resilience.

Static resilience in a critical infrastructure system can be assessed using a number of specific methods. The most suitable of these methods are especially: Resilience Assessment in Electricity Critical Infrastructure from the Point of View of Converged Security [18], A Performance-based Tabular Approach for Joint Systematic Improvement of Risk Control and Resilience Applied to Telecommunication Grid, Gas Network, and Ultrasound Localization System [19], Assessing and Strengthening Organisational Resilience – ASOR Method [20], Critical Infrastructure Elements Resilience Assessment – CIERA Method [21], Availability-based Engineering Resilience Metrics and Corresponding Evaluation Methodology [22], Resilience Capacities Assessment for Critical Infrastructure Disruption: The READ Framework [23], A Quantitative Method for Assessing Resilience of Interdependent Infrastructures [24], Guidelines for Critical Infrastructure Resilience Evaluation [25], Measuring Critical Infrastructure Resilience: Possible Indicators [26], and Resilience Measurement Index – RMI [27].

Some publications have investigated dynamic modelling in critical infrastructure systems in a different context. For example, Dynamic Functional Modelling of Vulnerability and Interoperability of Critical Infrastructures [28], Review on Modelling and Simulation of Interdependent Critical Infrastructure Systems [29], A System Dynamics Framework for Modelling Critical Infrastructure Resilience [30], Dynamic Interdependency Models for Cybersecurity of Critical Infrastructures [31], Resilience Assessment for Interdependent Urban Infrastructure Systems Using Dynamic Network Flow Models [32], and A Functional Index Model for Dynamically Evaluating China's Energy Security [33]. None of these studies, however, explored methods to predict the decline in resilience in critical infrastructure elements due to the effects of a disruptive event.

Based on the above, no suitable method for dynamic modelling of resilience, respectively robustness, in critical infrastructure elements is currently described. The authors of the article therefore created Dynamic Robustness Modelling (DRM) method, which is presented in more detail in the following sections. This stochastic method applies mathematical methods, specifically integral calculus, and analysis of dynamic robustness in elements in the context of a predicted disruptive event scenario.

The ambition of the author's team is to expand the perception and understanding of the basic philosophical level of resilience and include the aspect of time-changing attributes entering the process of assessing (modelling) robustness. Another aspect of novelty is to some extent the elementary level of robustness assessment resulting from the bottom-up approach, where robustness is tied to a specific element of critical infrastructure and is not limited by the perspective of cross-sectoral failure, within which it is fundamentally impossible to distinguish between static and dynamic resilience.

The mentioned statement is primarily reflected by the orientation of the case study to the application of the DRM method on the transformer station, which pragmatically expresses and can be considered as an elementary approach and level of assessment. However, the DRM method presented in the next part of the text can be used as a starting point and basis for higher levels of assessment, and thus for critical infrastructure subsector or sector robustness assessment, assuming the use of another mathematical superstructure. This fact can therefore be accepted as a bottom-up approach, as evidenced, inter alia, by the document Analysis of Critical Infrastructure Dependencies and Interdependencies [34], which deals with the definition of Bottom-up and Top-down Approaches. For better comprehensibility, the application of the DRM method was demonstrated only at the elementary level of a selected critical infrastructure element.

2. Methods of modeling dynamic systems

Dynamic systems are the opposite of static systems. The state of a dynamic system evolves over time through input signals, external disruption and natural developments [35]. Dynamic modelling of these systems is used to describe and predict the interactions over time of these systems with several factors of a given phenomenon [36]. These dynamic models can be either deterministic or stochastic. A deterministic model is one in which the values for the dependent variables of the system are completely determined by the parameters of the model. In contrast, stochastic, or probabilistic, models introduce randomness in such a way that the outcomes of the model can be viewed as probability distributions rather than unique values [37].

Currently, graphical-analytical methods (e.g. network analysis), statistical methods (e.g. Bayesian kernel, statistical hypothesis testing) and mathematical methods (e.g. topology, integral calculus, the Euler's method, and pairwise comparison) are used to model dynamic systems. The section below describes these methods and the advantages and disadvantages of their use in dynamic robustness modelling of elements in electricity critical infrastructure.

Graphical-analytical methods are a combination of graphical and analytical methods. Graphical methods are especially suitable for illustrating and presenting typical statistical data through the use of graphs [38]. Analytical methods examine selected facts and are therefore limited in time and task. Specifically, network analysis allows detailed relationships between the components of an issue to be resolved [39]. This method can be used to determine the relationship between a disruptive event and the robustness in a critical infrastructure element.

For example, Murray et al. [40] used network analysis to create an optimization method for use with telecommunications flows. Using network analysis, Eusgeld et al. [41] analysed critical infrastructure

vulnerabilities and assessed the capture potential and detailed dynamics of scenarios that affect the most vulnerable parts of critical infrastructure. Ongkowijoyo and Doloi [42] introduced a new method called Fuzzy Critical Risk Analysis (FCRA), which integrates an existing risk analysis of the impact of the spread of risk with a new analysis. The disadvantage of graphical-analytical methods is their complexity, which results from a detailed analysis of entire networks and the expressions of interdependence between individual elements.

Bayesian statistics is the most frequently used method applied to critical infrastructure [43]. This method is typical for modelling parameters that are mostly unknown values and only estimated from measured data. This area of statistics is based on predicting, sorting and managing dynamic systems with a degree of uncertainty. The estimate is calculated using Bayes' theorem [44].

One example of the use of Bayesian statistics is given in an article which explored the issue of optimizing and managing resilience in critical infrastructure [45]. Similarly, Baroud and Barker [46] expanded the model with a data analysis and created a Bayesian kernel model for modelling the level of importance of resilience-based network components. Since quantifying resilience is a vital part of infrastructure risk analysis, Baroud and Barker [47] applied the Beta Bayesian kernel model to estimate resilience metrics used to analyse the recovery process of disrupted critical infrastructure systems. In her dissertation, Baroud [48] developed a new Bayesian kernel model to predict the frequency of failure. This model was subsequently applied to modelling important measures based on the resilience of the critical infrastructure system.

Statistical methods applied to critical infrastructure also include interdependence and regression or correlation according to the type of dependence, which may be unilateral or mutual [49]. Mackenzie and Barker [50] discuss and give an example of regression in quantifying critical infrastructure resilience using a dynamic I/O model to map Oklahoma's production losses due to a power outage. Statistical methods primarily aim to obtain statistical data that are important in dynamic modelling of systems, but they do not allow these systems to be defined.

Graphical-analytical and statistical methods also do not reveal the correlation between a disruptive event and resilience in a critical infrastructure element as they develop over time. Mathematics, which is a science of structure, order and relationship, is suitable for solving this problem. Mathematical methods apply logical reasoning and quantitative calculations and can express a degree of abstraction [51]. Studying this group of methods is therefore appropriate. Selecting the most suitable method for calculating hazard levels and determining the level of robustness in a critical infrastructure element is imperative. Given the above facts, mathematical elements and some form of abstraction are necessary in order to create the individual steps of the dynamic modelling process.

From mathematical methods, four methods were studied in more detail, which seem to be suitable for dynamic modelling of electric power critical infrastructure element robustness. Specifically, these are Topology [52], Integral calculus [53], Euler's method [54] and Pairwise comparison [55]. The essence of choosing a suitable method is the requirement to obtain a numerical value from three or more variables with respect to their development over time. Based on this requirement, it is not possible to use the pairwise comparison method, because it is based on the creation of variants and subjective ordering of criteria for the selection of the most suitable variant. Topology is a general interpretation for defining the concept of space and deals with shapes and spaces. The disadvantage of topology is that it does not take distances into account. In connection with the solved problem, it is specifically the duration of the adverse event with respect to the development over time. Also, Euler's method works with only two variables and is based on the equation for changing position and velocity. This method is only used to approximate the function using differential equations.

The last potentially suitable method is the integral calculus, which is used to find areas, volumes and lengths of curves. This method allows the integration of multiple variable factors in a specific calculation. When the hazard level of a disruptive event is calculated, an integral can incorporate the duration, intensity and progress of the disruptive event simultaneously. This step represents a relevant starting point for dynamic modelling robustness of element in electricity critical infrastructure.

3. Factors in dynamic robustness modelling of electricity critical infrastructure elements

After applying the above definition of modelling a dynamic system in critical infrastructure [36], we can conclude that the basic components of dynamic modelling of robustness in electricity critical infrastructure elements are the level of static resilience of a CI element, the character of a disruptive event (i.e. type and forecast scenario of its development) and time.

It is important to consider all the factors that positively and negatively affect robustness in electricity critical infrastructure elements for dynamic modelling. In this context, two factors determine the level of robustness in electricity critical infrastructure elements: (1) factors determining robustness (i.e. robustness components) and (2) factors adversely affecting robustness (i.e. components constituting the hazards of a disruptive event).

3.1. Factors determining robustness in electricity critical infrastructure elements

The first group consists of factors that determine robustness in electricity critical infrastructure elements. The document Critical Infrastructure Resilience Final Report and Recommendations [14] defines robustness as one of the three basic components determining the resilience of critical infrastructure elements. Robustness is the ability of an element to absorb the effects of a disruptive event that is already in progress. These effects can be absorbed through early detection and adequate response, conceivably by activating the redundant capacity of the element.

Other determinants of resilience are recoverability and adaptability [21]. Recoverability is the ability of an element to restore its activity to its original (required) level of service once the disruptive event has ended. It should be noted that recoverability especially is limited by the availability of financial, material and human resources. Adaptability is the ability of a critical infrastructure entity (i.e. an organization) to prepare an element for the recurrence of a disruptive event. Adaptability represents the dynamic (long-term active) ability of an organization to adapt to a changing situation.

The term resilience and the structures and functions of the above-mentioned resilience factors were first defined by Holling [56] in connection with resistance and stabilization in ecological systems (later also socio-ecological systems). Interestingly, the term resistance itself is not included in the National Infrastructure Advisory Council's definition [14]. The document only describes robustness, recoverability, and adaptability, which are repressive factors (i.e. performing their function only at the time of a disruptive event). By contrast, resistance can be understood as the ability of an element to prevent the occurrence of a disruptive event, which is an important preventive factor [57]. According to this, viewing resistance as a fourth and very important component of resilience in critical infrastructure elements is appropriate. Resilience is determined mainly by the preparedness and physical resistance of an element to a crisis. However, in the context of this article, resistance and its determinants will continue to be seen as part of robustness.

Fig. 1 shows a graphical presentation of the robustness of critical infrastructure element in the context of a disruptive event's effect on the performance of this element.

When an element is subject to the effects of a disruptive event, the absorption capacity of the element is spread over two phases [58]. In the

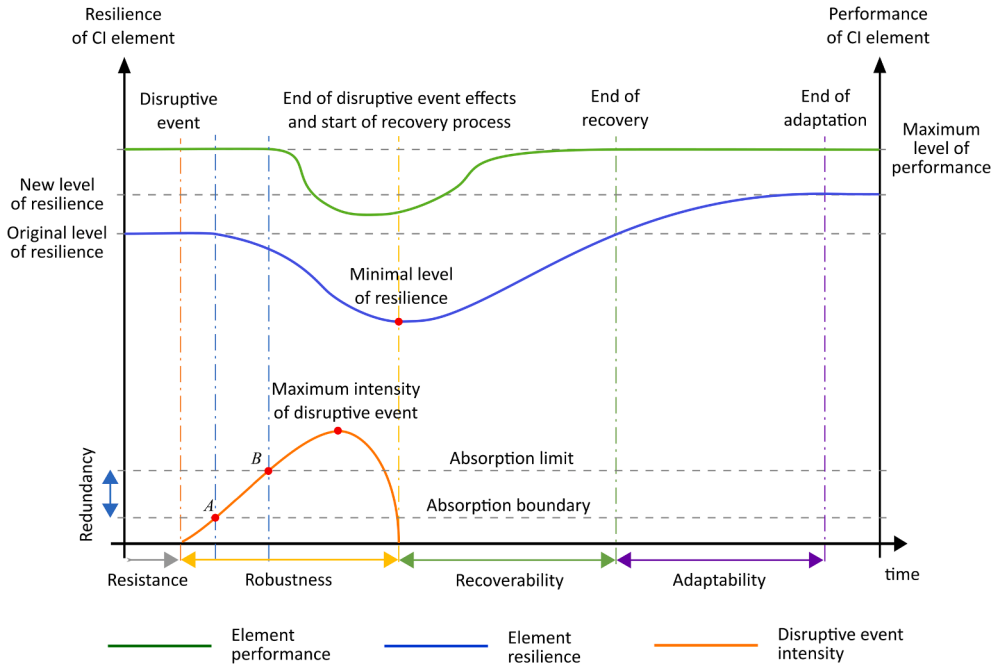


Fig. 1. Expressing the robustness of a critical infrastructure element in the context of an disruptive event (modified according to [58]).

first phase, the system can absorb the effect of a disruptive event without involving redundant capacity, up to the element's ability to fully absorb the effect of the disruptive event (point A on Fig. 1). In the second phase of absorption, the redundant capacity available to the element is engaged. As a result, robustness begins to decrease, however the element can still provide the full power required. At this point, there is still room to detect a disruptive event and respond to its effects. If an element's redundant capacity is exhausted, such as its ability to absorb the effect of a disruptive event (point B on Fig. 1), only then do the adverse effects of the event begin to manifest as a decline in functionality. The nature of the decline is determined by the element's ability to defend itself against the effects of the event. If this ability exists, the reduction in power provided by the element may be gradual, but if the intensity of the disruptive event overcomes these abilities, the reduction in power is usually steep or even instantaneous.

Based on the above, it can be stated that the robustness of the elements of the electricity critical infrastructure is determined by the following factors [58]:

- Crisis preparedness (set of measures to increase the preparedness of a critical infrastructure element for disruptive events);
- Detection capability (probability and / or time of disruptive event detection);
- Responsiveness (probability and / or time of intervention leading to the elimination of the causes of the disruptive event or the minimization of its consequences);
- Redundancy (ability to immediately substitute the power of the disturbed part of the element or strengthen its capacity);
- Physical resistance (structural characteristics of buildings or technologies used and implemented security measures, i.e. a set of organizational and regime measures and technical means to increase the security of a critical infrastructure element against disruptive events).

At the same time, however, it is necessary to realize that robustness is one of the three determinants of the electricity critical infrastructure elements resilience (the other two are recoverability and adaptability) [14,59,60]. For this reason, the above-mentioned factors determining the elements robustness are at the same time partial factors determining the elements resilience, but only in the phase of prevention and immediate reaction, i.e. at the time of the adverse event.

3.2. *Factors determining the hazards of a disruptive event*

The factors that determine robustness in an element are counterbalanced by the factors that disrupt this robustness. In this case, these are the components that constitute the hazards of a disruptive event. These factors are defined as the escalation, exposure, de-escalation, and intensity of the disruptive event [16,61,62]. Escalation is the initial phase of a disruptive event and is determined by the escalation function and the level of intensity achieved in the final part of the phase. Exposure is the duration of a disruptive event delimited by the escalation and de-escalation phases. This stage can be divided into any number of substages depending on the variation in intensity level of the disruptive event. This assertion is based on Bayesian statistics, which uses probability in relation to unknown past factors and estimation of resistances [47]. De-escalation is the final phase of a disruptive event and is determined by the de-escalation function and the initial intensity level in the initial phase. The final variable determining hazard level in a disruptive event is intensity. The intensity of a disruptive event is a common factor during escalation, exposure and de-escalation. This factor describes the degree of a disruptive event's destructiveness and its ability to adversely effect on a critical infrastructure element. The intensity of a disruptive event may vary considerably over the duration of its effect.

A graph of the correlation between factors determining the hazard of an adverse effect is shown in Fig. 2.

The default factor that determines the effect of a disruptive event on robustness in a critical infrastructure element is escalation. The level of escalation of a disruptive event is determined by the escalation function and the level of its intensity at time t_1 (Fig. 2). The different types of escalation functions can be classified into five levels according to the effect on the critical infrastructure element. A value of 1 represents the escalation function with the least effect. A value of 5 represents the greatest effect. Examples of measurable items that determine the type of escalation function of a disruptive event are presented in Fig. 3.

Power escalation is the escalation of the disruptive event with the lowest impact. This is due to the fact that the increase in the intensity of

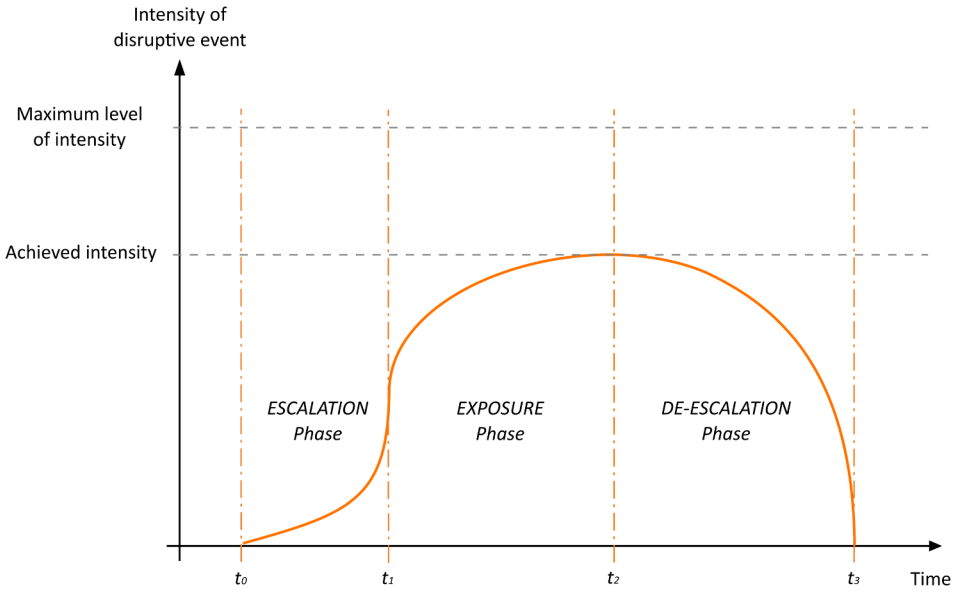


Fig. 2. Factors determining the hazards of a disruptive event.

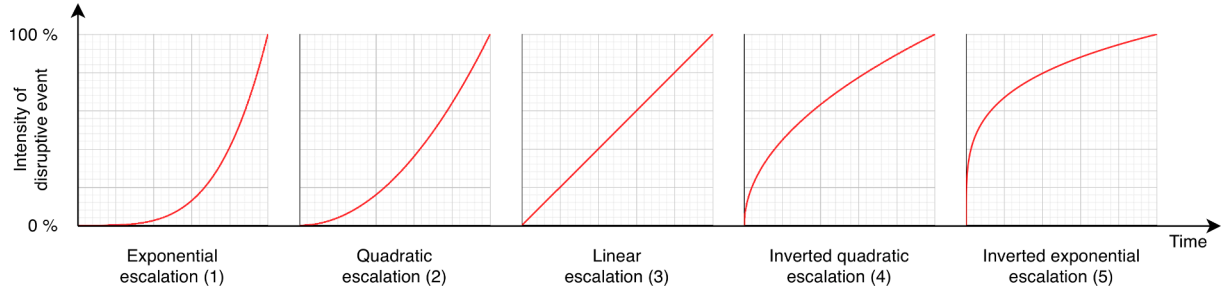


Fig. 3. Measurable items determining the type of escalation function of a disruptive event.

this disruptive event is gradual and allows for early detection and subsequent adoption of security measures. In contrast, inverse power escalation represents a very rapid (almost instantaneous) increase in the intensity of a disruptive event. As a result, it is not possible to detect this event in time and its effects can be very high. Examples of selected disruptive events and associated escalation function are presented in Table 1.

The second factor that determines the effect of a disruptive event on critical infrastructure element robustness is exposure. Exposure to the disruptive event can be divided into any number of sub-phases according to the intensity of the disruptive event (Fig. 2). The level of exposure in each sub-phase is determined by the intensity of the event.

The third factor that determines the effect of a disruptive event on robustness in a critical infrastructure element de-escalation of the event. The level of de-escalation is determined by the de-escalation function and the initial level of its intensity at time t_2 (Fig. 2). The different types of de-escalation functions can be classified into five levels according to the effect on the critical infrastructure element. A value of 1 represents the de-escalation function with the least effect. A value of 5 represents the greatest effect. Examples of measurable items that determine the type of de-escalation function of a disruptive event are presented in Fig. 4.

As in the case of escalation, in this case as well, the power de-escalation represents a gradual decrease in the intensity of the disruptive event, which enables the timely commencement of liquidation work and the recovery process. In contrast, inverse power de-escalation represents a very rapid (almost instantaneous) decrease in the intensity of a disruptive event. As a result, it is not possible to start the immediate restoration of the element, which increases the impact caused. Examples of the type of de-escalation function of selected disruptive events is presented in Table 2.

The final factor that determines the effect of a disruptive event on critical infrastructure element robustness is the event's intensity. The level of intensity is determined by the degree of the event's destructiveness and ability to adversely effect on the element. The intensity of all types of disruptive events can be classified into five levels according to these criteria. A value of 1 represents the escalation function with the least effect. A value of 5 represents the greatest effect. An example of the classification of measurable items that determine the intensity of a selected disruptive event is presented in Table 3.

The above example shows that measurable items are defined only for those disruptive events which have the potential to disrupt the robustness of critical infrastructure elements. Winds below 62 km/h on the

Table 1
Examples of disruptive events for individual escalation functions.

Disruptive event	Type of escalation function
Physical attack on any critical infrastructure element	Inverted exponential escalation
DDoS attack on SCADA systems in electricity distribution network dispatching systems	Inverted quadratic escalation
Escalation of traffic intensity on a highway	Linear escalation
Over-pressurization in a gas pipeline	Quadratic escalation
Impact of wind or storms on electricity transmission or distribution systems	Exponential escalation

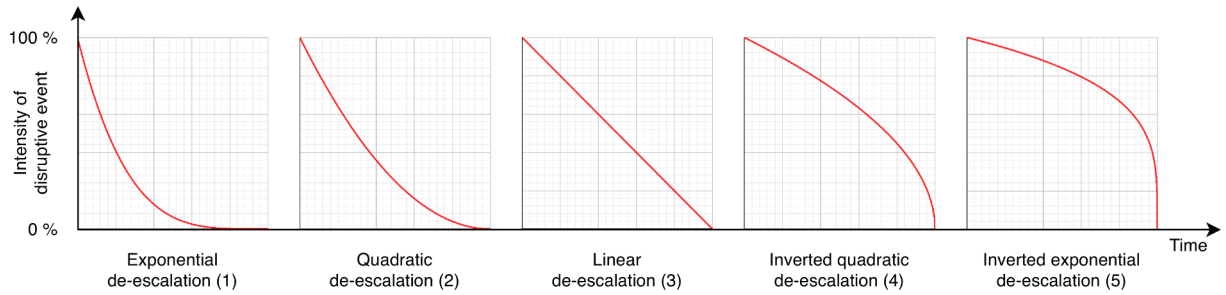


Fig. 4. Measurable items determining the type of de-escalation function of a disruptive event.

Table 2
Examples of disruptive events for individual de-escalation functions.

Disruptive event	Type of escalation function
Physical attack on any critical infrastructure element	Inverted exponential de-escalation
DDoS attack on SCADA systems in electricity distribution network dispatching systems	Inverted quadratic de-escalation
Effects of flooding on an electricity distribution network	Linear de-escalation
Effects on transportation infrastructure due to rapid landslides or other shifts in land	Quadratic de-escalation
Effects on electrical energy transmission or distribution networks due to earthquake	Exponential de-escalation

Beaufort scale for extreme wind effects, therefore, were not included in the measurable items [63].

Finally, we should highlight that the point evaluation scale used to assess the levels of escalation, de-escalation and intensity of a disruptive event is based on Linear Aggregation [64]. In this principle, the difference between individual point values is directly proportional. In practice, an increase from 1 to 2, for example, is the same as an increase from 4 to 5. The increase is thus 20%.

4. Method for dynamic robustness modelling of electricity critical infrastructure elements

The Dynamic Robustness Modelling (DRM) method proposed in the article was created by the authors in order to address the need for dynamic modelling of robustness in electricity critical infrastructure elements. This stochastic method uses integral calculus and analysis of dynamic robustness in elements in the context of a predicted disruptive event scenario. This method quantifies the adverse effect of predicted disruptive events and the subsequent effect of this impact on the decrease in robustness at the expected time of exposure. The method can predict critical point of failure in performance in electricity critical infrastructure elements and identify weaknesses that contribute to insufficient protection and subsequent failure of performance.

4.1. Dynamic robustness modelling framework

The starting point for the DRM method was defining a framework for dynamic robustness modelling (Fig. 5). This framework defines the areas necessary for the modelling process and subsequent analysis. These areas are: (1) assessed electricity critical infrastructure elements, (2) assessed disruptive events, (3) determining factors, and (4) methodology. All the above areas represent an important and necessary part of dynamic robustness modelling of critical infrastructure elements.

In order to apply DRM method effectively, the electricity critical infrastructure elements that the method is suitable for must be clearly defined. In the context of the problem, these are all technical elements of generation, transmission and distribution of electricity critical infrastructure, such as generation with a total installed electrical capacity of at least 500 MW, transmission system lines of at least 110 kV, transformer stations and technical dispatching.

Similarly, the disruptive events that dynamic robustness is modelled against should also be defined. The authors therefore based their selection on the typology of PERIL events [65] and the data available for these large-scale events. From these events, the authors selected and modified groups of events where the threat primarily affected infrastructure. According to this classification, disruptive events of a naturogenic (geological and meteorological), technogenic (process-technological and cascading) and anthropogenic character (personnel, cybernetic and physical) were identified.

Another essential area of the dynamic robustness modelling framework is the factors that contribute to the robustness of electricity critical infrastructure elements. Specifically, there are two types of factors [58]: (1) factors determining and limiting robustness (i.e. components determining a robustness) and (2) factors affecting robustness (i.e. components determining a disruptive event). The individual factors have been described in detail in the previous section of the article.

The final, important area in correctly modelling dynamic robustness is a suitably selected methodology. In the context of the proposed dynamic robustness modelling procedure (see below), the methodology is divided into three closely related parts. The first part defines the scenario of disruptive events. Specific methods such as Event Tree Analysis – ETA [66] and Fault Tree Analysis – FTA [67] can be applied in this area. The second part of the methodology analyses the static robustness of a critical infrastructure element using one of the following three methods: (1) Critical Infrastructure Elements Resilience Assessment – CIERA [21], (2) Resilience Measurement Index – RMI [27], and (3) Guidelines for Critical Infrastructure Resilience Evaluation [25]. However, the authors recommend the CIERA method which best suits the conditions of integration into the DRM method with the structure of the classification of variables and the method of point assessment. For other

Table 3
Example of classification of measurable items that determine the intensity of selected disruptive events.

Threat category	Threat group	Disruptive event	Measurable items
Naturogenic threats	Meteorological threats	Extreme wind events	**5:** Hurricane (over 118 km/h, destructive effects) **4:** Powerful windstorm (103–117 km/h, very rare, causing severe damage to housing, forests) **3:** Strong wind (89–102 km/h, rarely occurs inland, blows over trees, causes more extensive damage **2:** Windstorm (75–88 km/h, wind causes minor damage to structures (knocks over chimneys, tears off roof tiles) **1:** Storm winds (62–74 km/h, wind breaks branches, walking against the wind is almost impossible)

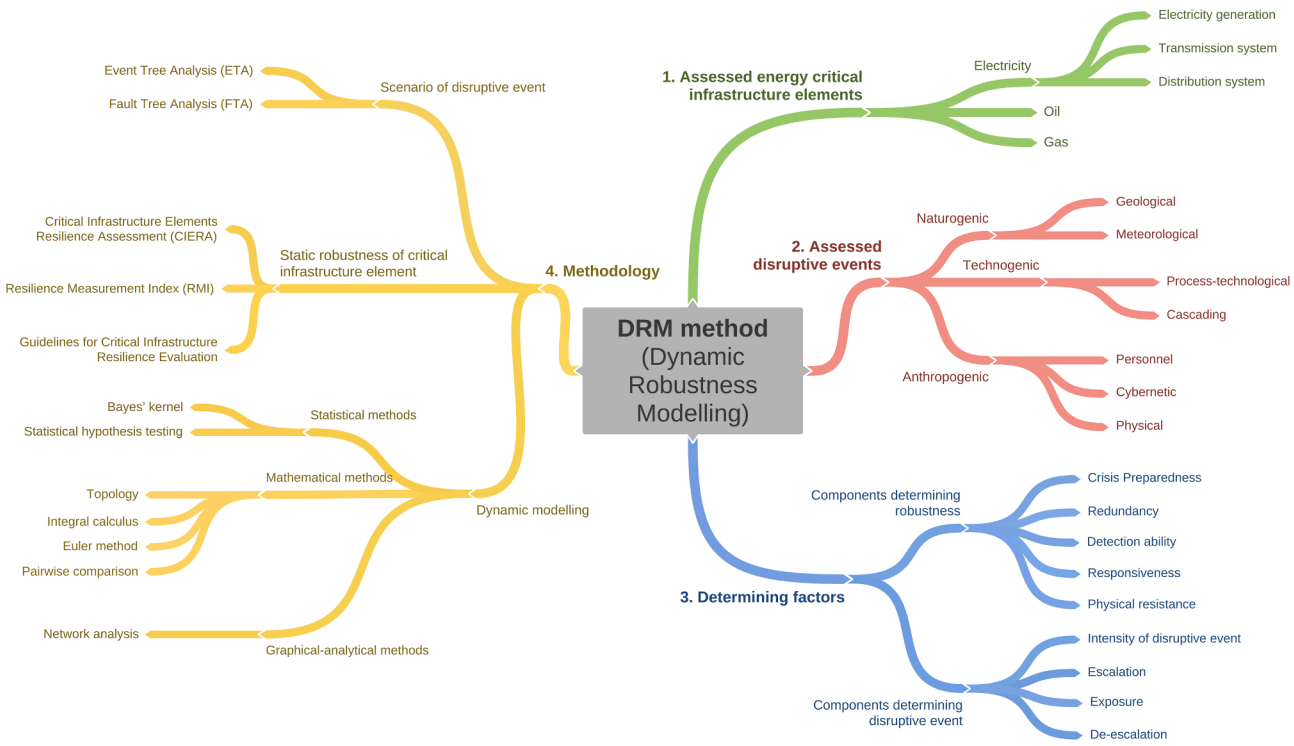


Fig. 5. Framework for dynamic robustness modelling of electricity critical infrastructure elements.

methods, the resulting values would have to be converted to the corresponding point scale suitable for the DRM method. The final part of the methodology applies dynamic modelling. In this context, relevant statistical methods (i.e. Bayes' kernel, statistical hypothesis testing), mathematical methods (i.e. topology, integral calculus, Euler method and pairwise comparison) and graphical-analytical methods (i.e. network analysis) are applied.

4.2. Dynamic robustness modelling procedure

Based on the initial conditions and conditions established by the framework, a procedure for dynamic robustness modelling in electricity critical infrastructure elements can be defined. This procedure includes seven interconnected steps (Fig. 6), which provide assessors with a clear guide in determining the robustness of an element under the effects of a disruptive event. The results of the analysis indicate the dynamically changing robustness level of the evaluated element and allow an estimation of the element's ability to resist the effect of a disruptive event and whether its performance will fail (i.e. predict the critical point of failure).

Step 1: Selecting the electricity critical infrastructure element and a disruptive event

The first step in the proposed procedure is selecting a specific electricity critical infrastructure element which will have its dynamic robustness modelled. This selection is limited to technical elements of production, transmission and distribution of electricity critical infrastructure for which the level of static robustness can be determined (see dynamic robustness modelling framework). A specific disruptive event that the selected element will be evaluated against is then selected. For this event, a scenario of the effect on the selected electricity critical

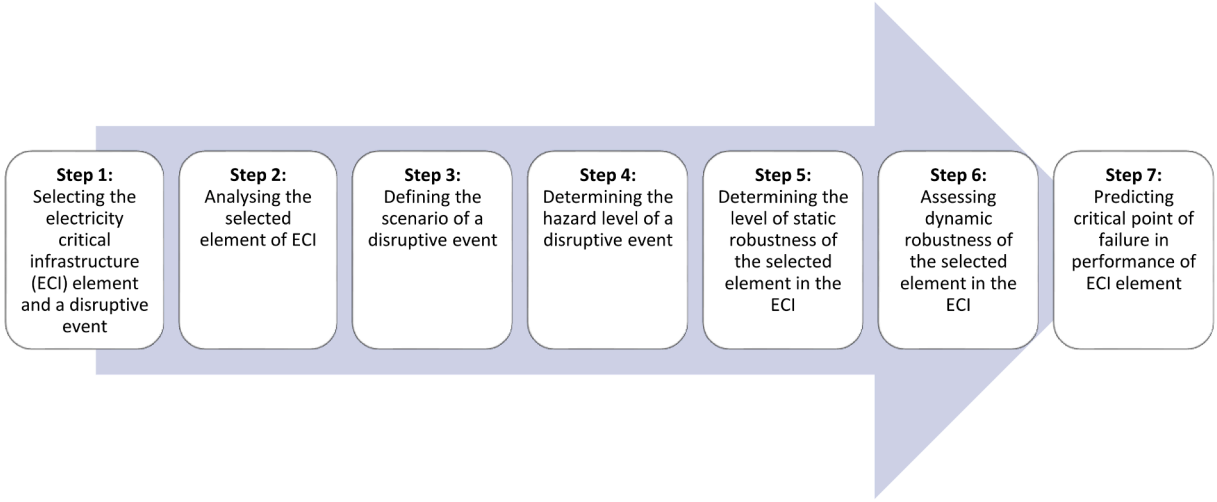


Fig. 6. Procedure for dynamic robustness modelling of electricity critical infrastructure elements.

infrastructure element is defined. Due to the need to unify the methodology for calculating static robustness, the disruptive event should be categorized according to the CIERA method [21] into one of the following groups of threats: geological, meteorological, process technology, cascading, personnel, cyber and physical.

Step 2: Analysing the selected element of electricity critical infrastructure

The second step is analysing the element, classifying the element according to the electricity critical infrastructure, describing the element's structural and performance parameters, and identifying the data concerning the factors which determine the robustness of the element. The classification of an element results from its performance parameters, on the basis of which it can be assessed whether it meets any of the relevant sectoral criteria. Performance parameters specify the technological structure of the element and describe the performance of key technologies. By contrast, structural parameters specify the topological structure of the element, i.e. whether it is a point, linear, or surface element. The final part of the second step identifies the data concerning factors which determine level of element robustness. Analysis of the selected element should be performed in accordance with the CIERA method [21].

Step 3: Defining the scenario of a disruptive event

The third step is defining the scenario of a disruptive event and its development over time. This is a necessary starting point for dynamic robustness modelling. The course of a disruptive event is classified according to three key phases: escalation, exposure and de-escalation. The first phase defines the course of the escalation function and its intensity at time t_1. This is followed by the exposure phase, where the assessor must determine the course of the disruptive event until it de-escalates. During the exposure phase, the intensity of the disruptive event may increase, decrease or remain constant. If the intensity during this stage is variable, the interval determining the duration of the exposure phase may be divided into several parts. This assertion is based on Bayesian statistics, which uses probability in relation to unknown past factors and estimation of resistances [47]. The final phase defines the course of the de-escalation function and its intensity at time t_2. Since each phase continues for a certain amount of time, its duration must also be defined. The ETA [66] or FTA [67] methods are suitable for defining scenarios.

Step 4: Determining the hazard level of a disruptive event

Once the scenario of a predicted disruptive event has been defined, the level of hazard can be determined. To calculate this level, the type of the specific function for each phase and the intensity of the disruptive event at each point in time must be known, i.e. t_0 to t_3 (Fig. 2). The level of hazard of a disruptive event can then be determined using integral calculus [53]. This calculation consists of two steps: (a) selecting the functions that determine the scenario of a disruptive event, and (b) including the intensity of the disruptive event in the calculation.

(a) Selecting the functions that determine the scenario of a disruptive event

H(t) is the mathematical notation for the calculation describing the overall hazard of a disruptive event. In general, if the continuous functions *f(t)* which determine the individual phases of the disruptive event (i.e. escalation, exposure, de-escalation) at time t for $t \in \langle t_0; t_n \rangle$ are known, then the overall hazard level of the disruptive event for a given time interval can be calculated according to the integral (Eq. (1)):

$$H(t) = \int_{t_0}^{t_n} f(t)dt \tag{1}$$

where $H(t)$ = hazard level of disruptive event over time t; $f(t)$ = continuous function determining the course of the disruptive event over time t.

This interval can be divided into several parts and used to calculate the hazard levels of individual phases as a sum of partial integrals, as follows (Eq. (2)):

$$H(t) = \int_{t_0}^{t_1} f_{Es}(t)dt + \int_{t_1}^{t_2} f_{Ex}(t)dt + \int_{t_2}^{t_3} f_{De}(t)dt \tag{2}$$

where $H(t)$ = hazard level of disruptive event over time t; $f_{Es}(t)$ = continuous function determining the course of escalation; $f_{Ex}(t)$ = continuous function determining the course of exposure; $f_{De}(t)$ = continuous function determining the course of de-escalation.

Time t is considered a generic unit of time, regardless of whether a minute, hour, day, week, month, or year. For the purposes of the calculation, time is divided equally according to the duration of the given phase. The sum of these proportions must equal 1. For example, if the escalation phase continues for three units of time, then a proportion of 0.3 applies. For an exposure period of four units of time, 0.4 applies. In this case, the remaining duration of the de-escalation phase is 0.3.

The first part of Eq. (2) represents the escalation phase (*Es*). A specific function can be used in this equation as a measurable item according to the progress of a disruptive event over the time interval $\langle t_0; t_1 \rangle$. Specific types of functions $f_{Es}(t)^x$ interpreted in Fig. 3 are shown in Fig. 7 together with their mathematical notations.

The second part of Eq. (2) is used to calculate the exposure (*Ex*) to a disruptive event in the time interval $\langle t_1; t_2 \rangle$. In this phase, the effect of a disruptive event could suggest that the development of a function may be constant but also unstable. To calculate a constant function, Eq. (3) is applied. However, if the function does not have a constant character at this stage, the equations for escalation (Fig. 3) or de-escalation (Fig. 4) can be used for the calculation. To simplify the calculation of a disruptive event's hazard level, the course of the exposure phase can be divided into any number of time intervals.

$$f(t) = \int_{t_1}^{t_2} cdt = c\int_{t_1}^{t_2} 1dt \tag{3}$$

where $f(t)$ = continuous function determining the course of the disruptive event over time t; c = constant.

The third part of Eq. (2) for calculating the total intensity of a disruptive event is the de-escalation (*De*) phase in the time interval $\langle t_2; t_3 \rangle$. Specific types of functions $f_{De}(t)^x$ interpreted in Fig. 4 are shown in Fig. 8 together with their mathematical notations.

When the functions that determine the selected disruptive event scenario are selected, the intensity of the disruptive event can then be considered. Intensity will vary from phase to phase (Fig. 2). Intensity does not always therefore reach 100%, as illustrated in Figs. 3 and 4.

(b) Applying intensity in the calculation of hazards for a disruptive event

Determining the intensity level is based on the predefined values of measurable items in a disruptive event (e.g. extreme wind phenomena in Table 3). However, to determine the hazard level of a disruptive event, these point values must be converted into percentages with linearly increasing character. A point value of 1 therefore represents 20% of the intensity of a disruptive event's effect on a critical infrastructure element. Similarly, a point value of 2, 3, 4, and 5 represent 40%, 60%, 80%, and 100% intensity, respectively.

As a disruptive event progresses, its intensity will vary. In the escalation phase, intensity increases, being zero at t_0 and reaching a level in the interval $\langle 0; 1 \rangle$ at t_1, where 0 represents 0% of the disruptive event's effect on the selected element and 1 represents 100%. In the exposure phase, the level of the disruptive event may remain constant, decrease or increase. If the intensity varies (i.e. achieves more than one function), dividing the exposure phase into any number of time intervals is recommended. The de-escalation phase has a decreasing character over time, where time t_2 is the same level as at the end of the escalation phase at time t_3, and time t_3 is again at zero intensity.

The intensity of the disruptive event during the continuous function may thus reach different levels, which are always related to specific times (i.e. t_0 to t_n) that bound the evaluated intervals. Thus, at the beginning of the action (i.e. at time t_0), the intensity of the disruptive

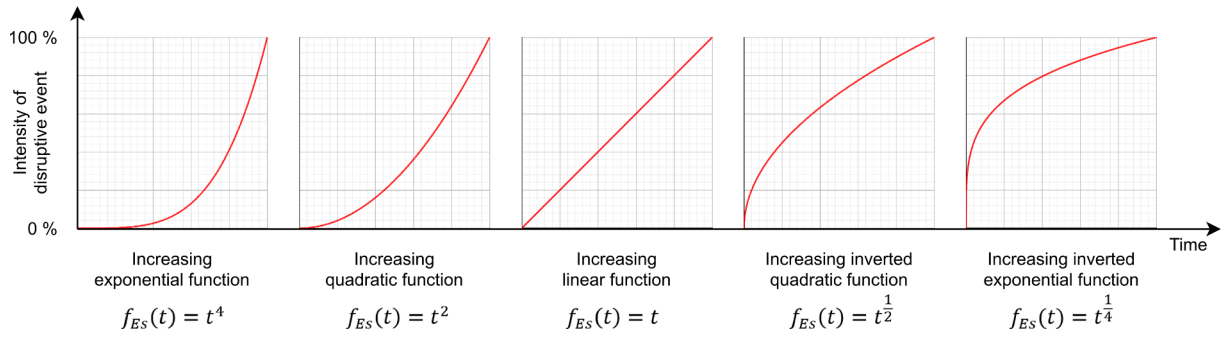


Fig. 7. Prescribed functions for calculating individual types of escalation of disruptive events.

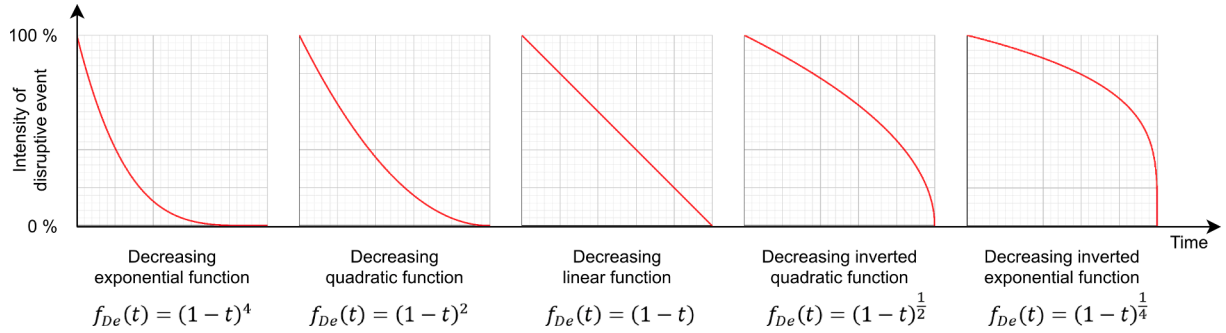


Fig. 8. Prescribed functions for calculating individual types of de-escalation of disruptive events.

event I_0 is at 0%. Similarly, at the end of the effect (i.e. at time t_3), the intensity of the disruptive event I_3 is again 0%. At times t_1 and t_2, intensities I_1 and I_2 may reach any level in the interval $\langle 0;1 \rangle$. According to this, general equations for calculating the increasing, constant, and decreasing intensity levels can be defined (Eqs. (4)–(6)).

The escalation phase with increasing character in a disruptive event is calculated according to Eq. (4):

$$H_{Es}(t) = \int_{t_0}^{t_1} \int_{0}^{\frac{I_1 - I_0}{(t_1 - t_0)^x} * f_{Es}(t)} dIdt \tag{4}$$

The exposure phase with a constant character in a disruptive event ($I_1 = I_2$) is calculated according to Eq. (5):

$$H_{Ex}(t) = \int_{t_1}^{t_2} I_1 dt \tag{5}$$

The de-escalation phase with a decreasing character in a disruptive event is calculated according to Eq. (6):

$$H_{De}(t) = \int_{t_2}^{t_3} \int_{0}^{\frac{t_3 - I_2}{(t_3 - t_2)^x} * f_{De}(t)} dIdt \tag{6}$$

where $H_{Es}(t)$ = hazard level of disruptive event in the escalation phase (i.e. t_0 to t_1); $H_{Ex}(t)$ = hazard level of disruptive event in the exposure phase (i.e. t_1 to t_2); $H_{De}(t)$ = hazard level of disruptive event in the de-escalation phase (i.e. t_2 to t_3); $\langle t_{n-1}; t_n \rangle$ = interval bounding the time period of the disruptive event phase; $\langle I_{n-1}; I_n \rangle$ = interval bounding the intensity of the disruptive event phase; x = exponent depending on the type of function $f(t)$.

To calculate the escalation phase with increasing character in the function that determines the disruptive event according to the type of function in Eq. (4), the corresponding equations given in Fig. 7 are applied. The time variables t_0, t_1 and the intensity level I_1 of the disruptive event, based on Table 3, must also be input. The de–escalation phase is calculated in the same manner. To calculate the decreasing character of the function, the equations from Fig. 8 are applied to Eq. (6)

The exposure phase can apply three calculations according to whether intensity is constant (Eq. (5)) or variable. If the course of the function in this phase is variable, then Eq. (4) is applied for an increasing character (I_n, I_{n+m}) and Eq. (6) is applied for a decreasing character (I_n, I_{n-m}), to which a range between zero intensity I_0 and the lower boundary of the assessed intensity I_n in the given time interval must be added (Eq. (7)):

$$\int_{t_n}^{t_{n+1}} \int_{I_0}^{I_n} 1 dIdt \tag{7}$$

The hazard level of the disruptive event (Eqs. (4)–(6)) in the relevant equations is determined by finding the values of time and level of intensity, together with the function determining the course of the given disruptive effect over time, and the level of intensity, together with the function determining the course of the given disruptive effect.

Step 5: Determining the level of static robustness of the selected element in the electricity critical infrastructure

After analysing the selected element, the level of its static robustness can be determined. For this step, the CIERA method [21] is best applied. The CIERA method assesses not only the comprehensive level of resilience in the element but also the level of robustness in its individual components, i.e. robustness, recoverability and adaptability. Using the CIERA method, resistance is assessed in terms of robustness, represented by two variables, namely the element's crisis preparedness and its physical resistance. At this stage of the procedure, each measurable item is scored and then the percentage level of static robustness in the electricity critical infrastructure element is calculated.

Step 6: Assessing dynamic robustness of the selected element in the electricity critical infrastructure

Once the disruptive event hazard and static robustness level of the selected critical infrastructure element have been determined, the final step is assessing the dynamic robustness. In this step, the assessor studies the course of decrease in the element's robustness according to the effect of the disruptive event (i.e. its function and intensity). In general, escalation increases intensity over time, and the progress may be rapid or gradual. Robustness decreases as a result of an increase in the

disruptive event's intensity. The exposure phase can take several forms and remain constant, increase or decrease. The rate of decrease in the element's robustness may also vary. In the de-escalation phase, the decrease in robustness is again more gradual until the disruptive event's intensity reaches zero, when the robustness level stagnates and can then begin to recover (i.e. in the element recovery phase) and strengthen (i.e. in the element adaptability phase).

Dynamic robustness can be expressed with a curve that links the levels of individual values of static robustness R_0 through R_n over time. Its function is derived from the disruptive event function. For example, an exponential increase in the intensity of a disruptive event that is initially slow and subsequently steep will result in an exponential decrease in the robustness of the element, which is also initially slow and subsequently steep.

The values of the new level of robustness R_{n+1} are calculated from one phase *ph* (i.e. escalation, exposure and de–escalation) of the disruptive event using direct proportions and percentages according to the development over time. Therefore, to calculate a new level of robustness R_{n+1}, the initial value of robustness R_n must be known. This value has a certain level, which is always considered 100% level at a given stage. Consequently, the result calculated in step 5 should be applied, namely the determined hazard level of the disruptive event $H_{ph}(t)$, which represents a reduction of 100% of the robustness level in this phase due to the disruptive event ($100\text{-}H_{ph}(t)$). The robustness level at the end of each phase is calculated according to Eq. (8):

$$R_{n+1} = R_n \bullet \frac{\left(100 - H_{ph}(t)\right)}{100} \tag{8}$$

From the robustness level calculations of each phase of the disruptive event, the assessor can derive a suitable number of values that follow a decreasing sequence. The values obtained from dynamic robustness modelling can then be summarized (Table 4).

The resulting robustness values can then be expressed on a curve that simply shows the level of expected development of dynamic robustness in the disruptive event.

In this context, it should be noted that the DRM method works with time t only as a quantity that to some extent considers the ratio and relationship between the various phases of the adverse event, which is acceptable for predicting the critical point of element failure. Thus, this quantity does not consider the actual duration of the adverse event and therefore cannot be used as an indicator for the level of static robustness assessment, in particular the detection and response capabilities. In such a case, it is more appropriate to use specific methods for mathematical modelling of the critical infrastructure elements physical protection system (e.g. Kampova et al. [68] and Zou et al. [69]). For example, in the case of an element against the effects of physical threats robustness assessment, these methods work with the so-called breakthrough resistance of mechanical barrier systems and the range time of the intervention unit with a relevant degree of standard deviation.

Step 7: Predicting critical point of failure in performance of electricity critical infrastructure element

The final step in the process of dynamic modelling of robustness in electricity critical infrastructure element is predicting the critical point of failure in in performance of element. This condition occurs when the disruptive event hazard reaches a level greater than the robustness level of the element at a given time, assuming an increasing disruptive event hazard function. At this point, robustness is so low that it can longer protect the critical infrastructure element and performance fails as a result of further disruptive event.

Predicting the critical point of failure in performance is achieved by summing the resulting modelled values of dynamic robustness. The example presented above (Table 4) shows that the hazard of a disruptive event reached 40% in the exposure phase. In the same phase, the element's robustness decreased to 32%. In the following phase (i.e. de-escalation), the hazard of the disruptive event reduced to a level of 20%, with the element's robustness at the end of the phase dropping to 26%. If the disruptive event had continued its exposure, for example, with an additional increase of 10%, the element's robustness in the de-escalation phase would have fallen to 16% and not been able to sufficiently protect the element, resulting in immediate failure of performance. In this case, the critical point of failure in performance of a critical infrastructure element was time t_2.

The following practical step of the application of the DRM method, which, however, is no longer the subject of the presented procedure, is the pragmatic formulation of measures in the context of the creation and subsequent implementation of the strategy and the aspect of corrections. The created repair strategy is also perceived by the author's team as an important aspect of increasing the resilience of a selected group of elements, where resilience is formed by attributes of robustness, recoverability and adaptability. Given the necessary sustainability of this approach, after the implementation of the strategy can be expected to restart the continuous and cyclical process of dynamic modelling of robustness, taking into account the positive effect of the group of measures.

Table 4
Example of the sum of resulting values of dynamic robustness modelling over time according to the effect phase of a disruptive event.

Effect phase of disruptive event	Time	Disruptive event hazard level	Robustness level	Δ Robustness
Escalation	$t_0 = 0$ $t_1 = 0.3$	$H_{Es} = 20\%$	$R_0 = 68\%$ $R_1 = 54\%$	$\Delta R_{Es} = 14\%$
Exposure	$t_1 = 0.3$ $t_2 = 0.7$	$H_{Ex} = 40\%$	$R_1 = 54\%$ $R_2 = 32\%$	$\Delta R_{Ex} = 22\%$
De-escalation	$t_2 = 0.7$ $t_3 = 1$	$H_{De} = 20\%$	$R_2 = 32\%$ $R_3 = 26\%$	$\Delta R_{De} = 6\%$

5. Case study of DRM method application

The DRM method has already been successfully tested on selected critical infrastructure entities in the Czech Republic and Slovakia. The most important of these are the Transmission System Operator of the Czech Republic and Central Slovak Power Distribution Company. The following text presents a practical application of the DRM method on a selected critical infrastructure element. For security reasons, the basic information (i.e. name, location, and structural and performance parameters) about this element is anonymised, however, all parameters necessary for the validation of the assessment process are presented in the text.

Step 1: A specific electricity critical infrastructure element was first selected for dynamic robustness modelling, along with a specific disruptive event to evaluate the selected element against. The selected element is a 400 kV transformer station, designated in accordance with the Council Directive of the European Union [1] and national criteria of the Czech Republic [70] as an element of European Critical Infrastructure[1]. The selected disruptive event on this transformer station was an intentional man-made attack using explosives.

Step 2: The element was then analysed, providing a classification of the element according to the electricity critical infrastructure, a description of the element's structural and performance parameters, and identification of the data concerning factors which determine the

[1] European critical infrastructure (ECI) means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure.

robustness of the element. The transformer station was classified according to the energy sector and electricity supply subsector, i.e. a transmission system with an electric system of a voltage of at least 110 kV. Structural parameters: 400 kV transformer station, point topological structure [21], element redundancy according to the principle of N-1 criterion[2] [71]. Performance Parameters: the transformer station consists of seven key technologies: bus bars and branching, circuit breakers, disconnectors and ground switches, instrument voltage transformers, instrument current transformers, transformers, and compensating chokes. The element is protected by technical protection systems, physical security and routine measures according to the internal standards of the operator [72–74].

Step 3: The next step defined the scenario of the selected disruptive event and its progress over time. This was achieved using Event Tree Analysis – ETA method [66]. The disruptive event scenario is presented in Fig. 9.

Step 4: The hazard level was then determined. This was calculated using integral calculus [53] and consisted of two sub-steps: (a) hazard calculation according to the type of function, and (b) applying the variable intensity of the disruptive event in the calculation.

Step 4a: The type of specific function for each phase and the intensity of the disruptive event at each time (i.e. t_0 to t_3) was analysed and subsequently determined. Due to the character of the disruptive event (i.e. an intentional man-made attack using improvised explosive device), an inverted exponential function (see Table 1) was assumed in the escalation phase (i.e. t_0 to t_1). The exposure phase (i.e. t_1 to t_2) was not defined for this type of attack and an inverted exponential function (see Table 2) was therefore assumed in the de-escalation phase (i.e. t_2 to t_3). A graph of this disruptive event according to the function type is presented in Fig. 10.

Step 4b: The intensity of the attack can be applied in the calculation according to the definition of the type of functions that determine the course of an intentional man-made attack. This intensity has a variable character. At t_0 and t_3, intensity is zero, while at t_1 (and t_2), it is derived from the scenario of the given disruptive event (Fig. 9). In this case, an intentional man-made attack was expected, which would result in a partial reduction in transformer functionality due to the destruction of an extra high voltage line. Based on this scenario, the intensity of the attack was set at level 4, or 80% (Table 5).

The hazard values of the disruptive event at each stage, i.e. escalation, exposure, and de-escalation were calculated next. The values from above, i.e. the formula for the selected function type (see Fig. 11) and the intensity (see Table 5) of the disruptive event, were first applied in Eq. (4) to calculate the escalation phase. The result was then applied in Eq. (9):

$$H(t)_{Es} = \int_0^{0.5} \int_0^{\frac{0.8}{(0.5-0)^{\frac{1}{4}}} \bullet t^{\frac{1}{4}}} dIdt \tag{9}$$

At an intensity of 80%, the effect of the attack on the transformer station resulted in a level of 32% in the disruptive event in the escalation phase.

Although the exposure phase had a duration of zero, it could still be verified by inputting values into the equation for a constant character (Eq. (5)) since it fulfilled the condition of $I_1 = I_2$. The result is was as follows Eq. (10):

$$H(t) = \int_{0.5}^{0.5} 0.8dt$$

$$H(t) = \int_{0.5}^{0.5} 0.8dt = 0.8[t]_{0.5}^{0.5} = 0 \tag{10}$$

The final phase de-escalation phase was calculated according Eq. (6), resulting in Eq. (11):

$$H(t) = \int_{0.5}^{1} \int_0^{\frac{-0.8}{(1-0.5)^{\frac{1}{4}}} \bullet (1-t)^{\frac{1}{4}}} dIdt$$

$$H(t) = \int_{0.5}^{1} \frac{-0.8}{(0.5)^{\frac{1}{4}}} \bullet (1-t)^{\frac{1}{4}} dt = -0.9514 \bullet \int_{0.5}^{1} (1-t)^{\frac{1}{4}} dt$$

$$= -0.9514 \bullet \left[\frac{(1-t)^{\frac{5}{4}}}{\frac{5}{4}} \right]_{0.5}^{1} = 0.32 \tag{11}$$

At an intensity of 80%, the effect of the attack on the transformer station resulted in a level of 32% in the disruptive event in the de-escalation phase.

Step 5: Building on the analysis of the transformer station, the level of its static robustness could be determined. For this step, the CIERA method [21] was applied. The CIERA method assesses not only the comprehensive level of resilience in the element but also the level of its individual components, i.e. robustness, recoverability and adaptability. The results of the assessing the element robustness are presented in Fig. 11.

Step 6: Once the static robustness level of the electricity critical infrastructure element and the hazard level of the disruptive event were determined, the dynamic robustness of the transformer station could then be assessed according to the function and intensity of the attack. This step assesses the decrease in element robustness for each phase of the disruptive event. The robustness level occurring at the end of each phase was calculated according to Eq. (8). A summary of the values obtained from dynamic robustness modelling is presented in Table 6.

Because the process of dynamic robustness modelling is mathematically demanding, the authors created the *DRM Tool* application for users. The essence of this application is the comprehensive integration of the complete Dynamic Robustness Modelling Procedure (see Section 4.2) into a user-friendly and easy-to-use environment. The tool is a software application which automatically calculates the resulting values for dynamic robustness modelling of an element after the input data (i.e. static robustness of the electricity critical infrastructure element and disruptive event scenario) is entered. This *DRM Tool* also allows the exposure phase to be omitted (as in the case study presented above) or extended over multiple time intervals. The resulting values of the case study using the *DRM Tool* are presented in Fig. 12.

The *DRM Tool* can also chart the development of dynamic robustness

$$H(t)_{Es} = \int_0^{0.5} \int_0^{\frac{0.8}{(0.5)^{\frac{1}{4}}} \bullet t^{\frac{1}{4}}} dIdt = \int_0^{0.5} [I]_0^{\frac{0.8}{(0.5)^{\frac{1}{4}}} \bullet t^{\frac{1}{4}}} dt = \int_0^{0.5} \left[0.95 \bullet t^{\frac{1}{4}} \right] dt = 0.95 \int_0^{0.5} t^{\frac{1}{4}} dt = 0.95 \bullet \left[\frac{t^{\frac{5}{4}}}{\frac{5}{4}} \right]_0^{0.5} = 0.32$$

[2] The N-1 criterion states that a system that is able to withstand at all times an unexpected failure or outage of a single system component, has an acceptable reliability level. This implies that some simultaneous failures could lead to local or widespread electricity interruptions.

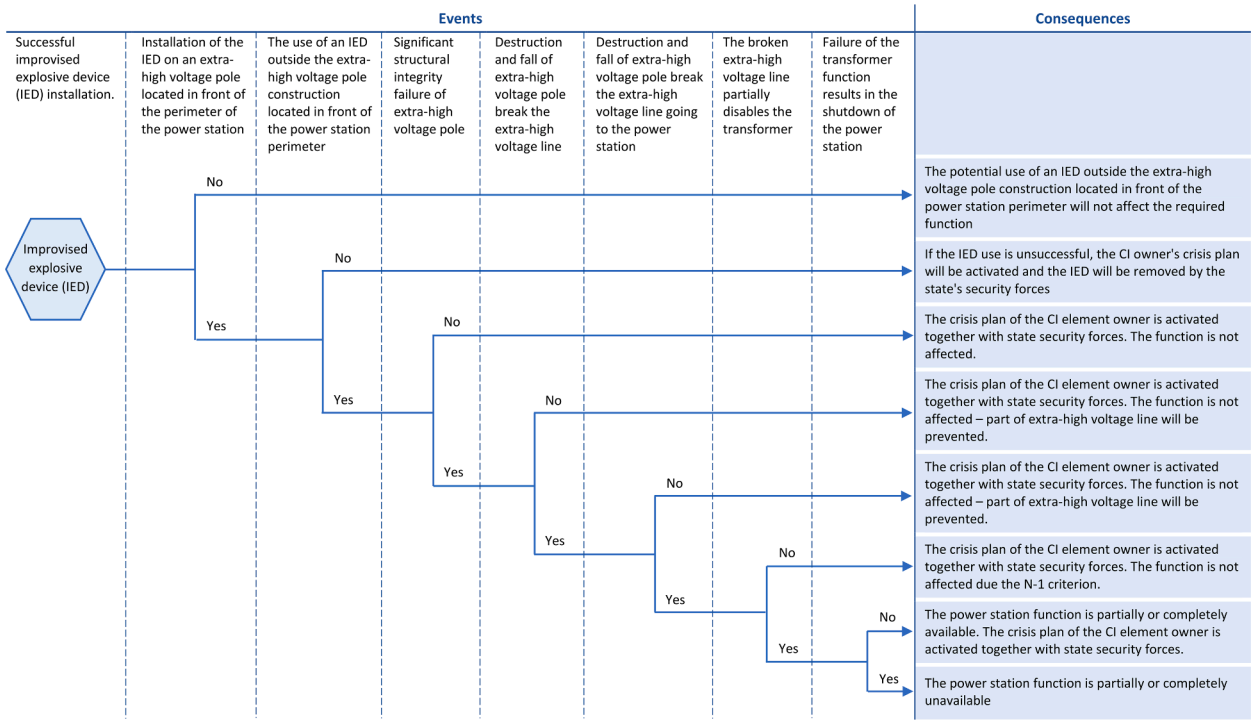


Fig. 9. Scenario of the selected disruptive event defined using the ETA method.

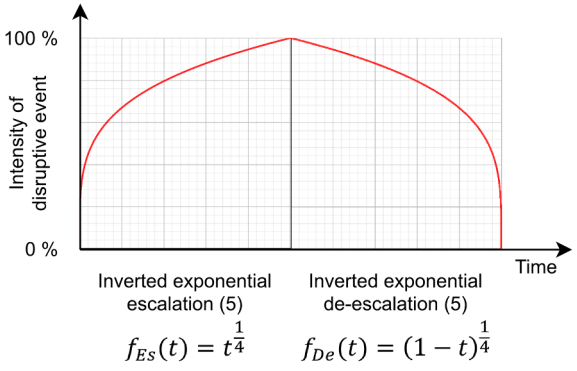


Fig. 10. Graph expressing the selected disruptive event according to the type of function.

Table 5
Measurable items determining the intensity of an intentional man-made attack on a transformer substation.

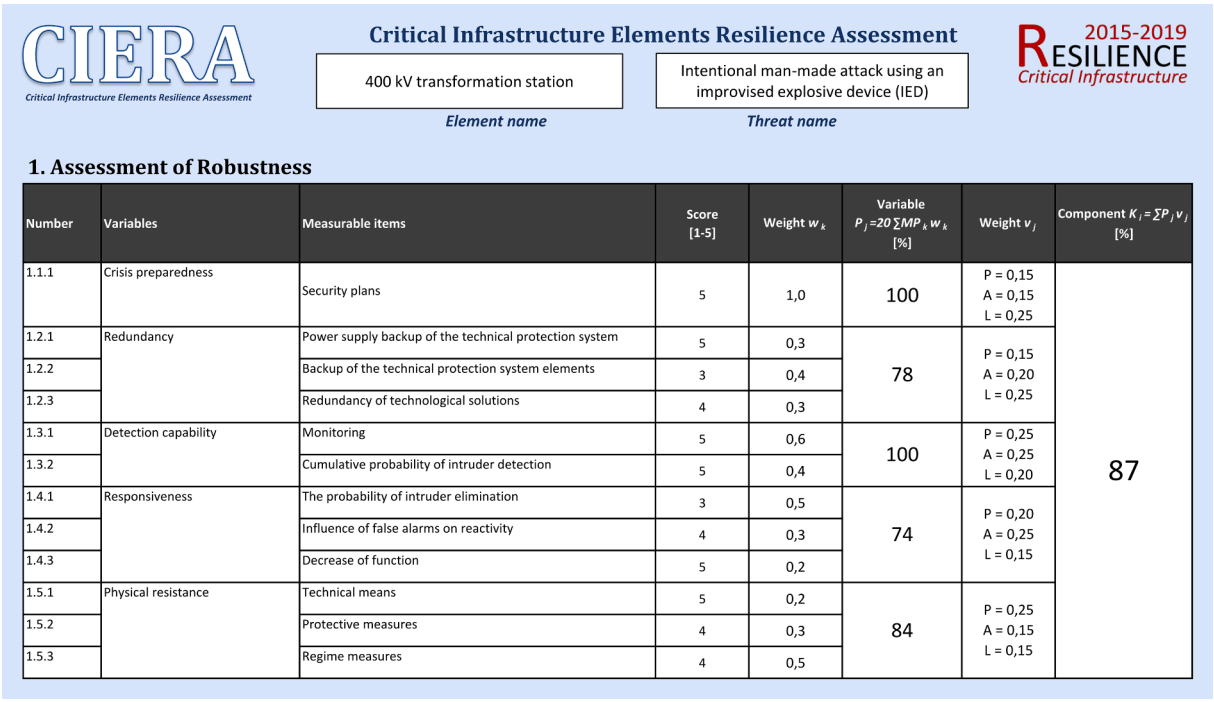
Description of measurable items in attack intensity	Point values	Percentages
Complete restriction of functionality in a critical infrastructure element (i.e. 100% restriction of functionality)	5	100%
*Complete shutdown of key technology and partial restriction of functionality in a critical infrastructure element (*i.e. *50% restriction of functionality)*	4	80%
Complete shutdown of key technology without restriction of functionality in a critical infrastructure element	3	60%
Partial shutdown of key technology without restriction of functionality in a critical infrastructure element	2	40%
Disruption of key technology without restriction of functionality in a critical infrastructure element	1	20%

and its relationship to a disruptive event, although it is only output as a simple line graph. A graph of the results of the case study using the *DRM Tool* is presented in Fig. 13.

Step 7: The final step in modelling dynamic robustness in the transformer station was predicting its critical point of failure in performance. This condition occurs when the disruptive event hazard reaches a level greater than the robustness level of the element at a given time, assuming an increasing disruptive event hazard function. At this point, the absorption capacity of the robustness is exhausted and the element is no longer able to withstand the effects of the disruptive event. Fig. 13 shows that at its peak (i.e. at time $t_1 = t_2$), the hazard level of the intentional man-made attack reached a level of 32%. In the same phase, the transformer station's robustness decreased from 87% to 59%. At the end of the subsequent phase (i.e. de-escalation), the hazard level of the disruptive event dropped to zero, and the transformer station achieved a stable robustness level of 40% at the end of the phase.

From the results, we can state that the critical point of failure in performance of the transformer station would not be reached and that it would continue supplying electricity. The factor contributing to this positive state was the transformer station's high level of robustness, especially its crisis preparedness (100%), redundancy (78%) and physical resistance (84%).

Due to the fact that the selected critical infrastructure element has the point element character, it is possible to state a significant share of physical security in the overall degree of robustness. In this context, it is therefore possible to consider the increased importance of the basic functions of the physical protection system (i.e. detection, delay and response) and thus the need to design and configure the system with respect to its effectiveness. For these purposes, it is recommended to implement selected specific modelling tools (e.g. SAVI / ASSESS; Sprut (ISTA, Russia); Vega-2; SFZ Analyzer; SAPE; Assessment of Terrorist Attack in a Network of Objects) into the design configuration or modification process, and the physical protection system effectiveness [75]. The results of this implementation can then be used to significantly robustness increase of a power critical infrastructure selected element.



1. Assessment of Robustness

Number	Variables	Measurable items	Score [1-5]	Weight w_k	Variable $P_j=20\sum MP_k w_k$ [%]	Weight v_j	Component $K_j=\sum P_j v_j$ [%]
1.1.1	Crisis preparedness	Security plans	5	1,0	100	P = 0,15 A = 0,15 L = 0,25	87
1.2.1	Redundancy	Power supply backup of the technical protection system	5	0,3	78	P = 0,15 A = 0,20 L = 0,25	
1.2.2		Backup of the technical protection system elements	3	0,4			
1.2.3		Redundancy of technological solutions	4	0,3			
1.3.1	Detection capability	Monitoring	5	0,6	100	P = 0,25 A = 0,25 L = 0,20	
1.3.2		Cumulative probability of intruder detection	5	0,4			
1.4.1	Responsiveness	The probability of intruder elimination	3	0,5	74	P = 0,20 A = 0,25 L = 0,15	
1.4.2		Influence of false alarms on reactivity	4	0,3			
1.4.3		Decrease of function	5	0,2			
1.5.1	Physical resistance	Technical means	5	0,2	84	P = 0,25 A = 0,15 L = 0,15	
1.5.2		Protective measures	4	0,3			
1.5.3		Regime measures	4	0,5			

Fig. 11. Assessment of element robustness in an intentional man-made attack using CIERA method.

Table 6
Resulting values of dynamic robustness modelling of the transformer station according to the effects of the disruptive event.

Phase of effect of disruptive event	Time	Hazard level of disruptive event	Robustness level	Δ Robustness
Escalation	$t_0 = 0$ $t_1 = 0.5$	$H_{Es} = 32\%$	$R_0 = 87\%$ $R_1 = 59\%$	$\Delta R_{Es} = 28\%$
Exposure	$t_1 = 0.5$ $t_2 = 0.5$	$H_{Ex} = 0\%$	$R_1 = 59\%$ $R_2 = 59\%$	$\Delta R_{Ex} = 0\%$
De-escalation	$t_2 = 0.5$ $t_3 = 1$	$H_{De} = 32\%$	$R_2 = 59\%$ $R_3 = 40\%$	$\Delta R_{De} = 19\%$

6. Conclusion

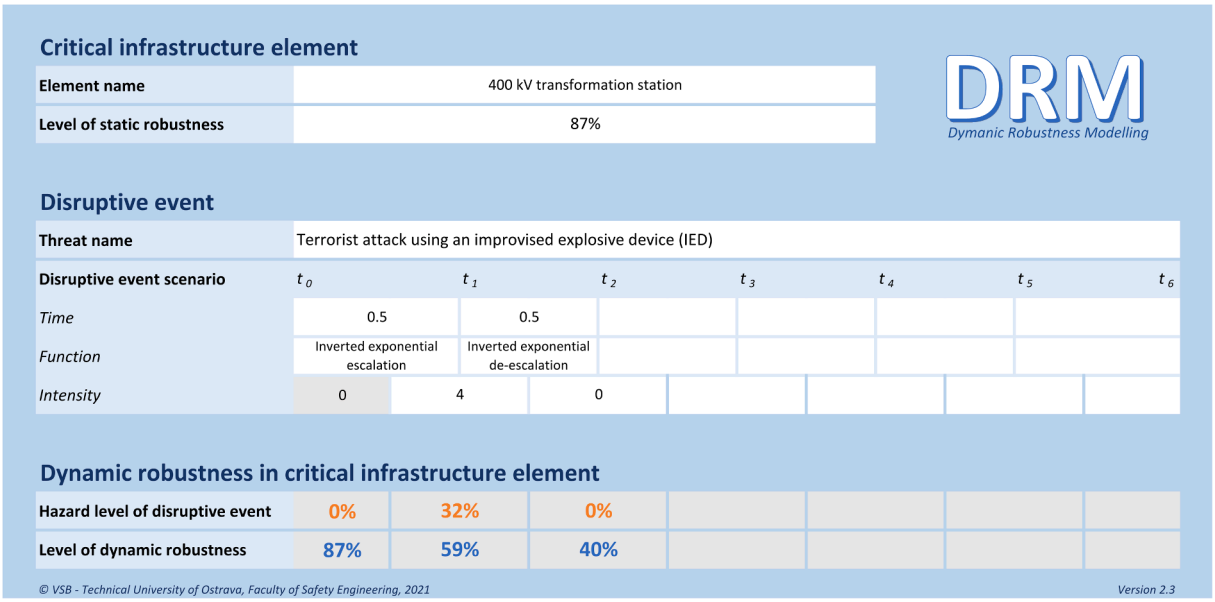
The article presented a stochastic DRM (dynamic robustness modelling) method. The method uses integral calculus and analysis of dynamic robustness in elements in the context of a predicted disruptive event scenario. The method quantifies the negative effect of predicted disruptive events and the subsequent decrease in robustness due to this effect at the expected time of exposure. The method can predict critical point of failure in performance in electricity critical infrastructure elements and identify weaknesses that contribute to insufficient protection and subsequent failure of performance.

The DRM method is primarily designed to assess dynamic robustness of technical elements of generation, transmission and distribution of electricity critical infrastructure, such as plants with a total installed electrical capacity of at least 500 MW, transmission system lines of at least 110 kV, transformer stations and technical dispatching. However, the assessment principle can also be applied in dynamic modelling of the robustness of other elements of the energy sector, such as oil and gas elements. The resulting information can be used as a guide for management—weaknesses can be identified and subsequently removed, thereby strengthening robustness, which is a crucial factor in the security of a critical infrastructure system. The DRM method has already been successfully applied to several critical infrastructure entities in the Czech Republic and the Slovak Republic, such as the Transmission System Operator of the Czech Republic and Central Slovak Power Distribution Company.

The article presented a practical demonstration of the DRM method in a case study. The selected element was an electricity transmission system's transformer station, designated in accordance with the Council Directive of the European Union and national criteria of the Czech Republic as an element of European Critical Infrastructure. The selected disruptive event on this transformer station was an intentional man-made attack using explosives. The analysis showed that the robustness of the transformer station after the attack dropped from its default of 87% to 40%, however no critical point of failure in performance was achieved and the station remained functional. The factor contributing to this positive state was the transformer station's high level of robustness, especially its crisis preparedness, redundancy, and physical resistance. However, the transformer station had specific weaknesses: the backup of the technical protection system, the reparability of the assets key technology, and long-term time horizon of repairing or replacing key technology.

The DRM method was created in order to fill the current research gap in the field of critical infrastructure protection. The main motivation was the fact that current approaches focus mainly on the critical infrastructure elements static resilience assessment in the context of the entire network resilience. For this reason, they do not allow the prediction of a dynamic decrease in the critical infrastructure individual elements resilience depending on the effect of the adverse event. The DRM method thus brings a completely new perspective on assessing the robustness of electricity critical infrastructure elements at the elementary level. The assessed robustness is thus tied to a specific critical infrastructure element and is not limited by the perspective of intersectoral failure, within which it is in principle impossible to distinguish between static and dynamic resilience.

At the same time, however, it must be stated that the proposed DRM method is limited by certain facts in its application. Primarily, it should be noted that the DRM method is a preliminary predictive tool whose ambition is not to provide exact information but a general overview of the expected decrease in robustness at the time of the disruptive event. The assessment results serve the user for basic orientation, i.e. the identification of weak points and predicting the critical point of failure in performance of the element. The use of the CIERA method, which is based on the subjective user assessment, can be considered as a



Critical infrastructure element

Element name	400 kV transformation station
Level of static robustness	87%

DRM
Dymanic Robustness Modelling

Disruptive event

Threat name	Terrorist attack using an improvised explosive device (IED)						
Disruptive event scenario	t_0	t_1	t_2	t_3	t_4	t_5	t_6
Time	0.5	0.5					
Function	Inverted exponential escalation	Inverted exponential de-escalation					
Intensity	0	4	0				

Dynamic robustness in critical infrastructure element

Hazard level of disruptive event	0%	32%	0%				
Level of dynamic robustness	87%	59%	40%				

 Version 2.3

Fig. 12. Resulting case study values from the DRM Tool.

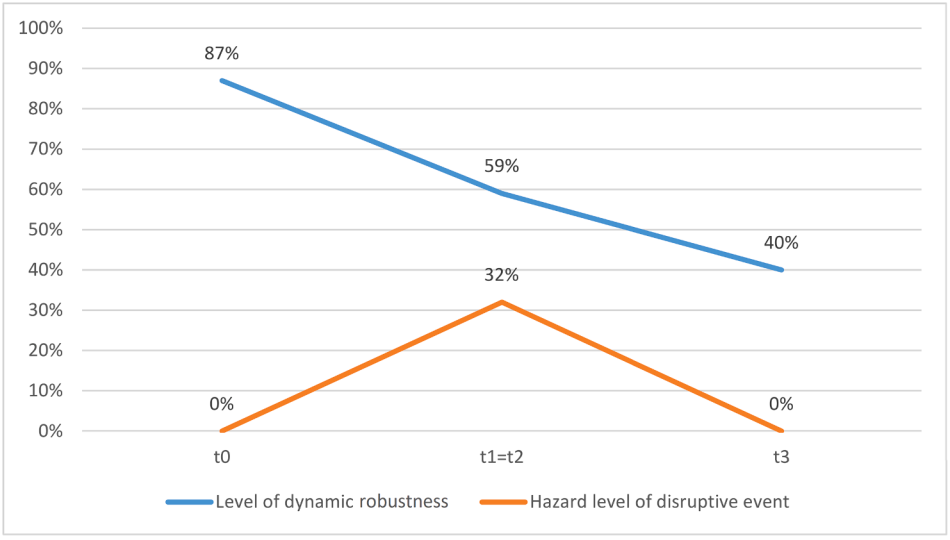


Fig. 13. Graph of the development of the dynamic robustness of a transformer station subject to an intentional man-made attack.

secondary limitation. Based on these facts, the DRM method can be considered as a simplified model providing initial information that is the basis for further user decisions. Despite these limitations, an important aspect of the novelty and benefits of the DRM method is the convergence of currently available best practices and integral calculus. The practical aspect of the application of the methodology is positively reflected at least in the V4+ area, despite considering the national specifics of the critical infrastructure protection environment.

Further development of the DRM method can be seen mainly in its extension by other components of resilience, i.e. recoverability and adaptability. This convergent approach would thus allow complex dynamic modelling of resilience as a whole. As a result, the method would allow the quantification of the negative impacts of predicted adverse events and the identification of weaknesses also in the phase of element recovery and adaptation. This extension of the DRM method would thus provide more comprehensive information important for the integrated electricity critical infrastructure element protection.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was supported by the Ministry of the Interior of the Czech Republic [grant number VI20192022151] and by VSB - Technical University of Ostrava [grant number SP2021/28].

References

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Brussels: Council of the European Union; 2008.
[2] National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience. Washington, DC: U.S. Department of Homeland Security; 2013.

[3] Rehak D, Markuci J, Hromada M, Barcova K. Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system. Int J Crit Infrastruct Prot 2016;14:3–17. https://doi.org/10.1016/j.ijcip.2016.06.002.

[4] Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities (COM/2020/829 final). Brussels: Council of the European Union; 2020.

[5] Presidential Policy Directive – Critical infrastructure security and resilience (PPD-21). Washington, DC: The White House; 2013.

[6] Vichova K, Hromada M. Power outage in the hospitals. In: Proceedings of the International Conference on Intelligent Medicine and Image Processing (IMIP '19); 2019, p. 15-20. https://doi.org/10.1145/3332340.3332345.

[7] Han F, Zio E. A multi-perspective framework of analysis of critical infrastructures with respect to supply service, controllability and topology. Int J Crit Infrastruct Prot 2019;24:1–13. https://doi.org/10.1016/j.ijcip.2018.10.009.

[8] Security of Critical Infrastructure Act 2018, No. 29 of 11 April 2018. Canberra: Australian Government; 2018.

[9] Winzer Ch. Conceptualizing energy security. Energy Policy 2012;46:36–48. https://doi.org/10.1016/j.enpol.2012.02.067.

[10] Cherp A, Jewell J. The concept of energy security: Beyond the four As. Energy Policy 2014;75:415–21. https://doi.org/10.1016/j.enpol.2014.09.005.

[11] Mikellidou CV, Shakou LM, Boustras G, Dimopoulos Ch. Energy critical infrastructures at risk from climate change: a state of the art review. Saf Sci 2018; 110:110–20. https://doi.org/10.1016/j.ssci.2017.12.022.

[12] Ward DM. The effect of weather on grid systems and the reliability of electricity supply. Clim Change 2013;121:103–13. https://doi.org/10.1007/s10584-013-0916-z.

[13] National Research Council. Terrorism and the Electric Power Delivery System. Washington, DC: The National Academies Press; 2012. https://doi.org/10.17226/12050.

[14] National Infrastructure Advisory Council. Critical Infrastructure Resilience Final Report and Recommendations. Washington, DC: U.S. Department of Homeland Security; 2009.

[15] Simonovic SP, Arunkumar R. Comparison of static and dynamic resilience for a multipurpose reservoir operation. Water Resour Res 2016;52:8630–49. https://doi.org/10.1002/2016WR019551.

[16] Rehak D, Onderkova V, Brabcova V. Determinants of Dynamic Modelling of the Critical Infrastructure Elements Resilience. In: M. Beer, E. Zio, editors. *Hannover: European Safety and Reliability Conference (ESREL 2019)*. European Safety and Reliability Association; 2019. https://doi.org/10.3850/978-981-11-2724-3_0070-cd.

[17] Park J, Seager TP, Rao PSC, Convertino M, Linkov I. Integrating risk and resilience approaches to catastrophe management in engineering systems. Risk Anal 2013;33: 356–67. https://doi.org/10.1111/j.1539-6924.2012.01885.x.

[18] Hromada M, Rehak D, Lukas L. Resilience assessment in electricity critical infrastructure from the point of view of converged security. Energies 2021;14: 1624. https://doi.org/10.3390/en14061624.

[19] Haring I, Fehling-Kaschek M, Miller N, et al. A performance-based tabular approach for joint systematic improvement of risk control and resilience applied to telecommunication grid, gas network, and ultrasound localization system. Environ Syst Decisions 2021;41:286–329. https://doi.org/10.1007/s10669-021-09811-5.

[20] Rehak D. Assessing and strengthening organisational resilience in a critical infrastructure system: case study of the Slovak republic. Saf Sci 2020;123:104573. https://doi.org/10.1016/j.ssci.2019.104573.

[21] Rehak D, Senovsky P, Hromada M, Lovecek T. Complex approach to assessing resilience of critical infrastructure elements. Int J Crit Infrastruct Prot 2019;25: 125–38. https://doi.org/10.1016/j.ijcip.2019.03.003.

[22] Cai B, Xie M, Liu Y, Liu Y, Feng Q. Availability-based engineering resilience metric and its corresponding evaluation methodology. Reliab Eng Syst Saf 2018;172: 216–24. https://doi.org/10.1016/j.ress.2017.12.021.

[23] Kozine I, Petrenj B, Trucco P. Resilience capacities assessment for critical infrastructures disruption: The READ framework. Int J Crit Infrastruct 2018;14: 199–220. https://doi.org/10.1504/IJCIS.2018.10015604.

[24] Nan C, Sansavini G. A quantitative method for assessing resilience of interdependent infrastructures. Reliab Eng Syst Saf 2017;157:35–53. https://doi.org/10.1016/j.ress.2016.08.013.

[25] Bertocchi G, Bologna S, Carducci G, Carrozzi L, Cavallini S, Lazari A, et al. Guidelines for Critical Infrastructure Resilience Evaluation. Rome: Italian Association of Critical Infrastructures' Experts; 2016.

[26] Prior T. Measuring Critical Infrastructure Resilience: Possible Indicators (Risk and Resilience Report 9). Zurich: Eidgenössische Technische Hochschule; 2015.

[27] Petit F, Bassett G, Black R, Buehring W, Collins M, Dickinson D, et al. Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience. Lemont, IL: Argonne National Laboratory; 2013.

[28] Trucco P, Cagno E, De Ambroggi M. Dynamic functional modelling of vulnerability and interoperability of critical infrastructures. Reliab Eng Syst Saf 2012;105: 51–63. https://doi.org/10.1016/j.ress.2011.12.003.

[29] Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. Reliab Eng Syst Saf 2014;121:43–60. https://doi.org/10.1016/j.ress.2013.06.040.

[30] Cavallini S, d'Alessandro C, Volpe M, Armenia S, Carlini C, Brein E, et al. A System Dynamics Framework for Modeling Critical Infrastructure Resilience. In: Butts J, Shenoi S, editors. Critical Infrastructure Protection VIII. Berlin: Springer; 2014. p. 141–54.

[31] Canzani E. Dynamic Interdependency Models for Cybersecurity of Critical Infrastructures. [Dissertation]. Munich: Bundeswehr University Munich; 2017.

[32] Goldbeck N, Angeloudis P, Ochieng WY. Resilience assessment for interdependent urban infrastructure systems using dynamic network flow models. Reliab Eng Syst Saf 2019;188:62–79. https://doi.org/10.1016/j.ress.2019.03.007.

[33] Wang D, Tian S, Fang L, Xu Y. A functional index model for dynamically evaluating China's energy security. Energy Policy 2020;147:111706. https://doi.org/10.1016/j.enpol.2020.111706.

[34] Petit F, Verner D, Brannegan D, Buehring W, Dickinson D, Guziel K, et al. Analysis of Critical Infrastructure Dependencies and Interdependencies. Lemont, IL: Argonne National Laboratory; 2015.

[35] Ducard G. Modeling and Analysis of Dynamic Systems. Zurich: Institute for Dynamic Systems and Control; 2017.

[36] Irwin M, Wang Z. Dynamic Systems Modeling. In: Matthes J, Davis ChS, Potter RF, editors. The International Encyclopedia of Communication Research Methods. Hoboken, NJ: Wiley; 2017. https://doi.org/10.1002/9781118901731.iecrm0074.

[37] Rey SJ. Mathematical Models in Geography. In: Wright JD, editor. International Encyclopedia of the Social & Behavioral Sciences. Amsterdam: Elsevier; 2015. p. 785–90. https://doi.org/10.1016/B978-0-08-097086-8.72033-2.

[38] ITRC. Graphical Methods. Washington, DC: Interstate Technology and Regulatory Council; 2013.

[39] Chiesi AM. Network analysis. In: Wright JD. Editors. *International Encyclopedia of the Social & Behavioral Sciences*. Amsterdam: Elsevier; 2015. p. 518-523. https://doi.org/10.1016/B978-0-08-097086-8.73055-8.

[40] Murray AT, Matisziw TC, Grubesic TH. Critical network infrastructure analysis: interdiction and system flow. J Geogr Syst 2007;9:103–17. https://doi.org/10.1007/s10109-006-0039-4.

[41] Eusgeld I, Kröger W, Sansavini G, Schläpfer M, Zio E. The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. Reliab Eng Syst Saf 2009;94:954–63. https://doi.org/10.1016/j.ress.2008.10.011.

[42] Ongkowijoyo C, Doloi H. Determining critical infrastructure risks using social network analysis. Int J Disaster Resilience Built Environ 2017;8:5–26. https://doi.org/10.1108/IJDRBE-05-2016-0016.

[43] Peter ML. Bayesian statistics: an introduction. Hoboken, NJ: Wiley; 2012.

[44] Murphy KP. Dynamic Bayesian networks: representation, inference and learning. Berkeley, CA: University of California; 2002.

[45] Eldosouky AR, Saad W, Mandayam N. Resilient critical infrastructure: bayesian network analysis and contract-based optimization. Ithaca, NY: Cornell University; 2017.

[46] Baroud H, Barker KA. Bayesian kernel approach to modeling resilience-based network component importance. Reliab Eng Syst Saf 2018;170:10–9. https://doi.org/10.1016/j.ress.2017.09.022.

[47] Baroud H, Barker K. Bayesian kernel methods for critical infrastructure resilience modeling. In: M. Beer, S. Au, J.W. Hall, editors. *Vulnerability, Uncertainty, and Risk*. Reston, VA: American Society of Civil Engineers; 2014, p. 987-694. https://doi.org/10.1061/9780784413609.070.

[48] Baroud H. Bayesian Kernel Methods for the Risk Analysis and Resilience Modeling of Critical Infrastructure Systems, [Dissertation]. Norman, OK: University of Oklahoma; 2015.

[49] Utne IB, Hassel H, Johansson J. A Brief Overview of Some Methods and Approaches for Investigating Interdependencies in Critical Infrastructures. In: Hokstad P, Utne IB, Vatn J, editors. Risk and Interdependencies in Critical Infrastructures. London: Springer; 2012. p. 1–11. https://doi.org/10.1007/978-1-4471-4661-2_1.

[50] Mackenzie CA, Barker K. Empirical data and regression analysis for estimation of infrastructure resilience with application to electric power outages. J Infrastruct Syst 2013;19:25–35. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000103.

[51] Dasgupta B. Applied mathematical methods. London: Pearson; 2006.

[52] Kahn DW. Topology: An introduction to the point-set and algebraic areas. New York, NY: Dover Publications; 1995.

[53] Patil DP. Riemann integration. Resonance 2006;11:61–80. https://doi.org/10.1007/BF02834475.

[54] Ascher UM, Petzold LR. Computer methods for ordinary differential equations and differential-algebraic equations. Philadelphia, PA: Society for Industrial and Applied Mathematics; 1998.

[55] Saaty TL. The analytic hierarchy process, planning, priority setting, and resource allocation. New York, NY: McGraw-Hill; 1980.

[56] Holling CS. Resilience and stability of ecological systems. Annu Rev Ecol Syst 1973; 4:1–23. https://doi.org/10.1146/annurev.es.04.110173.000245.

[57] Sugden AM. Resistance and resilience. Science 2001;293:1731. https://doi.org/10.1126/science.293.5536.1731b.

[58] Rehak D, Senovsky P, Slivkova S. Resilience of critical infrastructure elements and its main factors. Systems 2018;6:21. https://doi.org/10.3390/systems6020021.

[59] Carlson JL, et al. Resilience: Theory and Application. Lemont, IL: Argonne National Laboratory; 2012. https://doi.org/10.2172/1044521.

[60] Béné C, Wood RG, Newsham A, Davies M. Resilience: New Utopia or New Tyranny? Reflection about the Potentials and Limits of the Concept of Resilience in Relation to Vulnerability Reduction Programmes. IDS Working Papers 405 (2012) 1-61. https://doi.org/10.1111/j.2040-0209.2012.00405.x.

[61] Bühne S, Halmans G, Pohl K. Modelling dependencies between variation points in use case diagrams. In: Workshop on Requirements Engineering - Foundation for Software Quality (REFSQ '03). Klagenfurt:Velden; 2003. p. 59-69.

[62] Jeong H. Understanding conflict and conflict analysis. London: SAGE Publications; 2008.

[63] Royal Meteorological Society. The Beaufort Scale: How is wind speed measured?, https://www.rmets.org/resource/beaufort-scale; 2018 [accessed 9 May 2021].

[64] Nasibova RA, Nasibov EN. Linear aggregation with weighted ranking. Autom Control Comput Sci 2010;44:96. https://doi.org/10.3103/S0146411610020057.

[65] IRDR. Peril classification and hazard glossary. Beijing: Integrated Research on Disaster Risk IPO 2014.
[66] IEC. 62502, Analysis Techniques for Dependability – Event Tree Analysis (ETA). Geneva: International Electrotechnical Commission 2010.
[67] IEC. 61025, Fault Tree Analysis (FTA). Geneva: International Electrotechnical Commission 2006.
[68] Kampova K, Lovecek T, Rehak D. Quantitative approach to physical protection systems assessment of critical infrastructure elements: use case in the Slovak Republic. Int J Crit Infrastruct Prot 2020;30:100376. https://doi.org/10.1016/j.ijcip.2020.100376.
[69] Zou B, Yang M, Guo J, Benjamin ER, Wu W. A heuristic approach for the evaluation of physical protection system effectiveness. Ann Nucl Energy 2017;105:302–10. https://doi.org/10.1016/j.anucene.2017.03.029.
[70] Government Decree 432/2010 of 22 December 2010 on criteria for determination of the critical infrastructure element. Prague: Government of the Czech Republic; 2010.
[71] Ovaere M. Electricity Transmission Reliability Management. IAEE Energy Forum, http://www.iaee.org/en/publications/newsletterdl.aspx?id=326; 2016 [accessed 14 April 2021].
[72] Methodology to Ensure of Critical Infrastructure Protection in the Area of Electricity Generation, Transmission and Distribution. Prague: Deloitte Advisory; 2017.
[73] Lovecek T, Velas A, Durovec M. Level of Protection of Critical Infrastructure in the Slovak Republic. In: Majernik M, Daneshjo N, Bosak M, editors. Production Management and Engineering Sciences. London: Taylor & Francis Group; 2016. p. 163–8.
[74] Hromada M, Lukas L. Multicriterial Evaluation of Critical Infrastructure Element Protection in Czech Republic. In: Proceedings of International Conferences on Computer Applications for Software Engineering, Disaster Recovery, and Business Continuity. Korea: Jeju Island; 2012, p. 361-368.
[75] Lovecek T, Strakova L, Kampova K. Modeling and simulation as tools to increase the protection of critical infrastructure and the sustainability of the provision of essential needs of citizens. Sustainability 2021;13:5898. https://doi.org/10.3390/su13115898.