systems

MDPI

Article

Designating Regional Elements System in a Critical Infrastructure System in the Context of the Czech Republic

Petr Novotny [1,*] and Michaela Janosikova [2]

[1] Faculty of Safety Engineering, VSB—Technical University of Ostrava, Lumirova 630/13, 700 30 Ostrava-Vyskovice, Czech Republic
[2] Faculty of Security Engineering, University of Zilina, 1. Maja 32, 01026 Zilina, Slovakia; michaela.janosikova@fbi.uniza.sk
* Correspondence: novotny.petr@vsb.cz; Tel.: +420-597-322-834

Received: 18 March 2020; Accepted: 17 April 2020; Published: 22 April 2020

Abstract: Critical infrastructure is a complex system whose disruption or failure results in significant impacts on state interests, i.e., territorial security, economy, and the basic needs of the population. The current European Critical Infrastructure Protection Model does not allow the direct identification of critical elements at the regional level. Based on this, the paper brings a proposal for a unified system of critical infrastructure design based on a bottom-up approach. It is a progressive approach, utilizing contemporary trends in the application of science-based knowledge to critical infrastructure. A holistic view of this issue allows us to take into account the needs and preferences of the population, the preferences of the stakeholders and the local conditions of the region under consideration. The novelty of this approach is seen, in particular, in the identification of regional critical infrastructure elements through an integral assessment of these elements' failure impact, not only on the dependent subsectors, but also on the population (population equivalent) in the assessed region. The final part of the paper presents a case study demonstrating the practical application of the proposed system to the road infrastructure in the Pardubice Region of the Czech Republic.

Keywords: critical infrastructure system; regional elements; designation; progressive approach

1. Introduction

The provision of a continuous supply of commodities and services through an infrastructure system is the basic requirement for sustaining and developing state economies (not only in the European Union) and for maintaining the required level of security and welfare in society [1]. The functionality of these infrastructures and the provision of a continual supply of products and services are constantly exposed to the impacts of natural and anthropogenic threats [2]. The extent of the unacceptable impact depends mainly on the severity of the failure, its cause (the nature of the threat) and the importance (criticality) of the affected element or sector. This impact is often expressed by economic loss, the number of people affected, the size of the affected area and other similar factors [3]. By exceeding the socially defined limit values of unacceptable impact (sectoral and cross-sectional criteria), these infrastructures are referred to as critical and together they form the so-called critical infrastructure system [4].

That is why considerable attention has increasingly been dedicated to selected vital and critical infrastructures [5], including methods of risk analysis [6], critical elements evaluation [7] and its protection [8], and impact assessment of their failure [9]. The focus is now exclusively devoted to

critical infrastructure elements[1] at the European and national levels [10], while the regional level is largely neglected. Different criteria may be used in subdividing national territory into regions. These are normally divided into normative and analytical criteria [11]. For the purposes of this article, a normative criterion, expressed as "normative regions are the expression of political will; their limits are fixed according to the tasks allocated to the territorial communities, according to the sizes of population necessary to carry out these tasks efficiently and economically, and according to historical, cultural and other factors" is chosen. In the context of this criterion, NUTS 3 territories are considered as regions in this article.

Some elements that do not meet the criteria for the European or national level may be critical for the region as their disruption or failure would have a significant impact on the regional population [12]. In contrast, elements in the region that are of national/European relevance are already identified as elements of national/European critical infrastructure (e.g., nuclear power plants). For this reason, it is necessary to continually analyse not only elements at the European and national level, but also at the regional level, and to identify critical elements based on the results of the analysis. These elements must then be subject to comprehensive security measures to strengthen their resilience [13].

An analysis of existing approaches to identifying regional critical infrastructure worldwide is also a solid basis for the subsequent development of a system of identifying a regional critical infrastructure that would be universally applicable not only in the Czech Republic but also generally in European countries. The selection of countries was based on two criteria. The first is the practical application of a systemic approach based on the consideration of cross-sectoral dependencies in the infrastructure system. The second criterion of the selection of approach is to allow at least the identification of key elements at the regional level. Based on the results of the intersection of these two criteria, a total of three European countries (i.e., Switzerland, the Netherlands, and the United Kingdom) and one outside Europe (i.e., New Zealand) of the 18 countries analysed were selected.

The first system examined was the approach to identifying regional critical infrastructure in Switzerland [14,15], which closely focused on a bottom-up approach. Here, as a basis for the identification, three types of data were applied [16]: a quantitative approach, a qualitative approach, and an assessment of the potential to cause damage. On the other hand, the approach in the Netherlands was first based on political decisions [17,18] and only later focused more on the scientific approach [19]. This is a combination of the bottom-up and top-down approach, i.e., top-level requirements combined with local-level requirements. The United Kingdom has the third relevant approach to identifying regional critical infrastructure. This is a very traditional "top-down" approach based on the close cooperation of the public and private sectors [20–22]. Its peculiar feature is the possibility of identifying so-called "Infrastructure Assets" [23–25]. These are specific objects or elements (security networks, elements of cultural heritage, etc.).

The most recently analysed system is the non-European approach to identifying regional critical infrastructure in New Zealand. This approach was analysed to compare the established system in New Zealand with traditional approaches in Europe. This is a bottom-up approach, which, as the only one of the analysed approaches, uses the assessment of the object's significance for the region [26,27]. At the same time, this approach assesses the consequences of the failure of the infrastructure function on society as well as the economic consequences. The system also allows the inclusion of so-called "assets" [26], i.e., key elements or elements of cultural heritage, or "infrastructure hotspots" [28], places which accumulate interest infrastructures or key elements.

As a part of an analysis of approaches to identifying regional critical infrastructure in selected countries, basic information for developing the proposal has been identified. In general, it has been found that the level of a comprehensive perception of critical infrastructure protection is higher in

[1] Critical Infrastructure Element is in particular understood as the construction, the equipment, the facility or public infrastructure identified by cross-cutting and sectoral criteria [4].

these countries than in the Czech Republic. From the point of view of identifying the elements at the regional level, it was found that Switzerland has an approach based on detailed process analyses using a set of different criteria [16]. On the other hand, the Netherlands places the primary emphasis on the so-called vital products and services that make up the core of the infrastructure system[2] [29]. Secondary emphasis is then placed on products and services that support this important part of the system. Element identification in the United Kingdom is based on a traditional top-down approach. This approach relies on the National Risk Register [23], the outcomes of which are the basis for risk assessment and the identification of critical infrastructure elements at the regional level. The latest approach used in New Zealand allows the projection of vital infrastructure priorities into territorial systems [27] and the direct identification of their key elements.

Considering the facts above, there is currently no uniform approach in the European Union countries for identifying critical infrastructure elements at the regional level. As a result, most European Union states lack the system of identifying and subsequently protecting regionally significant elements. The results of the analysis of selected countries indicate that the analysed approaches provide a suitable basis for developing a unified approach that would be applicable not only in EU countries. At the same time, it is important to point out that existing approaches to identifying critical infrastructure elements at the national level cannot be used at the regional level as they do not allow for the variability of national criteria and the possibility of regional element analysis. Another reason is the need to accept sectoral criteria[3], which are inappropriate for the regional level as they have been set at the national level of distinction. The last major obstacle to the use of these approaches for identifying regional critical infrastructure elements is that they are oriented solely to impact assessment in the critical infrastructure system and do not take into account the impacts on the population of the region under assessment.

Based on the above, the paper aims to develop a simple and effective tool for identifying critical regional infrastructure elements and analysis of suitable techniques and tools that will be the main methodological apparatus of this proposed tool. Implementing this approach in practice would not only contribute to improving the continuity of service delivery [30], but it will also strengthen the preparedness of the authorities responsible for preparing the territory for crisis situations; and improve the security of the area as a whole. The identification of critical infrastructure components is an initial step in protecting critical infrastructure. The follow-up steps are the analysis of the resilience of elements of these infrastructures [13], risk analysis [31,32], and the last step is the implementation of adequate measures to increase safety [33,34]. The practical application of the proposed approach is demonstrated at the end of the paper in the form of a case study.

2. Methodology: Techniques and Tools of Infrastructure Analysis at the Regional Level

This part of the paper focuses on the selection of techniques and tools suitable for infrastructure analysis at the regional level. Attention is particularly paid to such techniques and tools that are publicly available, user-friendly and well-known (although not too specific) and suitable for analysing the critical infrastructure system in the context of the regional analysis. Firstly, the issue of identifying regional critical infrastructure is set into an appropriate framework for critical infrastructure analysis. As a suitable framework, the classification for critical infrastructure analysis by Ghorbani and Bagheri [35] appears to be appropriate, as it uses the classification elaborated in Rinaldi et al. [36]. This classification enables us to carry out the analysis at the necessary width while taking into account the specific dimensions of the critical infrastructure. This part also states techniques and tools that appear to be

---

[2] In this context, vital elements are perceived as synonymous with critical infrastructure elements.

[3] Sectoral criteria mean technical or operational values to determine the critical infrastructure element in the various sectors, i.e. energy, water, food and agriculture, health, transport, communication and information systems, the financial market and currency, emergency services and public administration.

most applicable and suitable in the framework of the analysis of techniques and tools for the design of a system of regional critical infrastructure elements.

The area of critical infrastructure should be viewed as a complex adaptive system, which can be aptly described as a 'socio-technical system' [37,38]. Various aspects of the legitimacy of such system categorization can be analysed and described from different perspectives. The classification of perspectives may prove beneficial and practical in terms of infrastructure analysis. It will certainly be useful to divide the issue of critical infrastructure into five dimensions [35]: system analysis, behavior analysis, knowledge discovery, visualization and knowledge sharing. Based on this classification, a lot of valuable information about the entire system can be obtained. Moreover, this framework corresponds with the defined characteristics of infrastructure interdependencies according to Rinaldi et al. [36]. See Figure 1 below for a representation of said critical infrastructure framework.

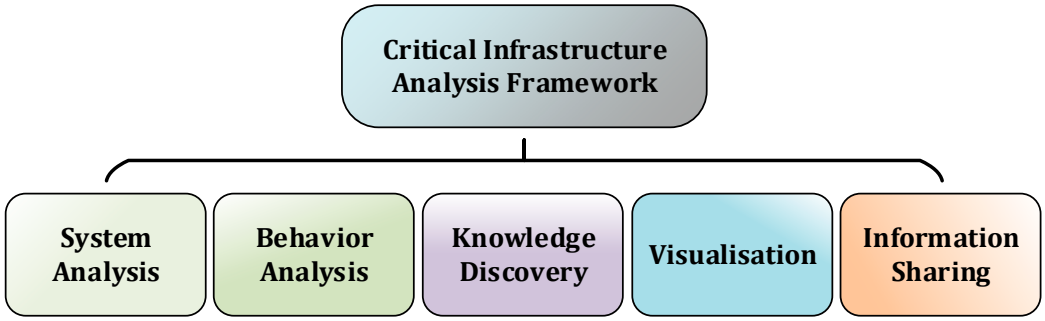

Figure 1. Selected framework for critical infrastructure analysis (taken and modified from [35]).

The first dimension concerns system analysis. The analysis is required to better understand how the infrastructure is organized and to identify its basic components. The applied risk analysis models help determine the types of threats, risks, and vulnerabilities that compromise the proper functioning of the infrastructure. These may include infrastructure profiling [39] based on the correct understanding of infrastructure organization; the IRAM model [40] designed to identify, model, assess and control significant risks threatening the infrastructure system; hybrid system modelling [41] derived from a mathematical methodology for complex system modelling and simulation, and other useful techniques and tools (for more details see [35], see other examples specified in [42,43]). This area also includes Risk Management, which will be addressed separately.

With its focus on behavior analysis, the second dimension can provide a good deal of information based on action sequence monitoring (simulations). The outcome may then include information on infrastructure behaviour within itself as well as concerning the whole system. Furthermore, it is possible to obtain useful information on the functioning of a specific element within the given infrastructure. Examples of applicable techniques and tools include Monte Carlo Simulation [44], the Scenario Building set of tools [45] designed to create alternative scenarios, the Cascade tool [46] presenting scenarios of functioning and interacting components, and the CARVER2 method [47]. Other effective tools include TRAGIS[4] [48], designed exclusively for transportation network simulation, various multi-agent systems [49] facilitating the general understanding of exceedingly complex systems, and numerous other techniques and tools. The final representative of this dimension is the Input-Output Model of Wassilly Leontief, which will also be discussed in a separate section.

Knowledge discovery as part of the third dimension in the aforementioned framework stems from the fact that human mechanisms may not always be capable of detecting all dependencies and behavioural patterns [35]. Even though the results of long-term observation may be equally

[4] TRAGIS—Transportation Routing Analysis Geographic Information System. For more information visit: https://webtragis.ornl.gov.

reliable, the use of simulation tools significantly reduces the time required for such observation. Knowledge discovery may be further supplemented based on the outcomes of different hypothesis testing or analytical studies. Of particular interest are the Hypothesis Testing model [50], based on specific assumptions about the behaviour of structures under certain conditions, and the Bayesian network model [51], derived from probability theory, where probabilistic relationships are formed between individual phenomena. Additional effective methods include Exploratory Data Analysis [52], focused on the systematic identification of hidden dependencies.

Visualisation constitutes a significant component of the framework and, as such, represents the fourth dimension. While the preceding dimensions offer a range of options, they may not always be able to reveal all properties, dependencies, and behavioural patterns. They are, above all, monitoring tools, ensuring that all relevant information has been revealed and no omission has occurred. Therefore, visualisation facilitates the identification of patterns in order to detect errors in the preceding phases. One of the advantages of visualisation techniques and tools is that they are readily applicable for revealing the visual structure of infrastructure and organizing it [53]. Other models worthy of note include the graph theory [54] and the widely used geographical information systems [55,56].

The last dimension of the presented framework is information sharing. Information sharing across all dimensions should facilitate the detection and possibly the management of unpredictable catastrophic scenarios. Information sharing is a prerequisite for the entire risk management system [6] and is also one of the bases for resilience building [57]. At the same time, it may provide new opportunities for improving the function of the entire system.

2.1. System Analysis

As part of 'system analysis', risk management is covered in general terms here [6,58], although these processes can also be applied to system analysis (infrastructure) or as a part of the critical infrastructure protection process [59,60]. The aim of all of the adopted procedures is to provide the data required to address specific risks and to select suitable solution alternatives. It is also necessary to define the key parameters of the examined system and to set the scope of applicability and the criteria [61].

General risk management methods are used to identify and assess the degree of risk involved in a process or event, and normally include three basic stages [62] of risk assessment, i.e., identification, analysis, and evaluation.

Risks related to critical infrastructure elements or processes can arise from many different causes or scenarios [63]. In order to properly analyse, assess and consider individual system risks, they must be allocated to the relevant system components. Correct identification of the source of risk, impact validation, and selection of the most appropriate strategy are among the key processes.

Risks can be assessed to varying degrees, using one or more techniques (for additional risk assessment methods see [35,64]). Risk management is a suitable cornerstone for developing a critical infrastructure identification system. The key steps of the risk management process are the basis that can be elaborated in more detail with the use of other appropriate tools.

2.2. Behaviour Analysis

The CARVER2 method [47] is considered to be a classic example of simulation models, with typical outputs including visualisation of potential criminal activity objectives. That is why this method essentially pertains to 'behaviour analysis'. For an explanation of input data see Table 1 below.

As this method is primarily employed in the area of physical security, there is a strong link to the potential disruption of system function by criminal activity. The CARVER2 method is also readily applicable to critical infrastructure, specifically in the pre-analysis phase, to explore all the elementary parts of the system.

Table 1. Explanation of basic areas addressed via the CARVER2 method [47].

Abbreviation	CARVER2	Description
C	Criticality	Degree of element importance for the whole system data
A	Accessibility	Enabling access to important elements with unwanted exposure
R	Recoverability	Time and effort required to restore the system functionality
V	Vulnerability	Level of unwanted exposure derived from negative manifestations
E	Effect	Extent and severity of unwanted consequences/manifestations in the system
R	Recognisability	Ability to recognize unwanted important elements in the system (and its vulnerability)

Based on the general equilibrium theory, the input-output model [65] also belongs to the wide group of techniques of 'behavior analysis'. The model is often applied to the input-output analysis, where the outputs of one economic sector make up the inputs of other sectors, and vice versa. It takes into account the sequential linkages between economic (infrastructure) system activities and has primarily been designed for sectors of the economy which can, in a sense, form critical infrastructure sectors. Specific models that are also widely applied to critical infrastructure can be developed based on general rules, e.g., [66,67].

The IIOM (Inoperability Input/Output Model) is based on the original model of Wassily Leontief. Initial sector barrier settings were incorporated into this model [35], which can allow the modelling of failures such as cascading effects [68] and multiple failures [36]. The dynamic setup of the method allows for a thorough analysis of the progress of such events. The IIOM is suitable for modelling dependencies in the following sectors [50]: energy, drinking water supply infrastructures, information and telecommunication technologies, virtual networks and information systems, the transportation sector (freeway and road networks in particular). It can also model political and regulatory dependencies. Based on the above, it is possible to use this model, for example, to assess the effects of a function failure within the entire functioning system.

2.3. Knowledge Discovery, Visualization and Information Sharing (Network Analysis)

Network analysis is a good example of interconnections between the above-mentioned dimensions (i.e., Knowledge Discovery, Visualization, and Information Sharing). Mutually interconnected functioning systems, relationships, and linkages within and without a system—all of these are viewed as a whole presenting network properties [69]. For the sake of simplicity, networks are viewed as a set of nodes (elements) and edges (links between nodes). The general rules applicable to networks are perceived to be equally pertinent to complex systems [70]. Network models designed for the demonstration of mutual linkages can also be used for local level infrastructures. Numerous approaches to tackling the vulnerability [71], risks and failure propagation within a network [72,73], as well as the general issue of network topology [31], have been put forward recently.

However, the current research direction [72,74] stems from the natural sciences and turns to the basic findings on networks. The set of the following three network properties seems to be key in determining infrastructure behaviour, as well as in selecting the approach to the system analysis [74]:

(a) Network density,
(b) Network homogeneity vs. network heterogeneity,
(c) Network symmetry.

Accordingly, the analysis should focus on the aforementioned key network properties [69,74]. The individual properties have been explained in more detail below and also illustrated in Figure 2.

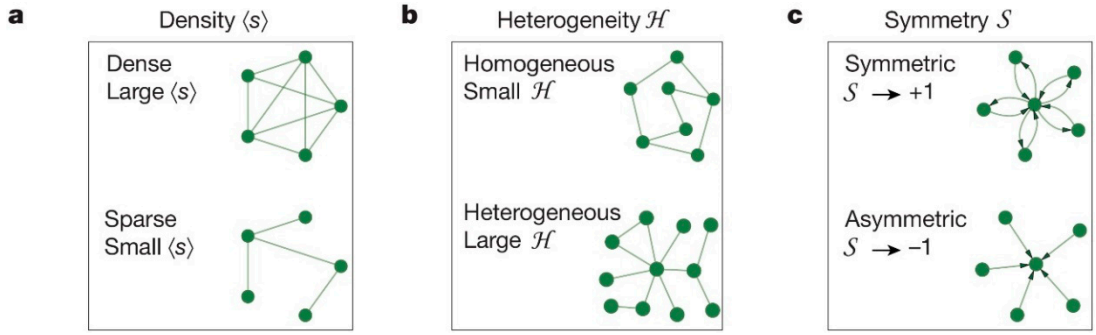

Figure 2. Properties determining network behaviour in the event of a failure (taken and modified from [68]).

An explanation of individual determinative properties [74] follows below.

Network density effects network behaviour in the event of a failure in the function of one element (node). A dense network with many linkages (edges) between nodes forms large quantities of node interconnections. If one node fails, there will be numerous other edges interlinking the remaining nodes. However, in a low-density network, with few links (edges) between its nodes, the failure of a single node can lead to the failure of the entire network.

Homogeneity vs. heterogeneity is an indication of whether there is a substantial difference between the number of nodes and the number of links between them. Homogeneity shows an identical/similar number of linkages with respect to each node, i.e., the quantities are the same. Conversely, heterogeneity suggests that the network contains nodes with both high and low numbers of linkages, i.e., there are substantial differences in the network.

Network symmetry expresses the direction of linkages (edges) between nodes. In a symmetrical network, the linkages will be mostly bidirectional. Conversely, an asymmetrical network will mostly consist of unidirectional linkages.

The assessment of the impacts of natural catastrophes on the road network [75] provides a good example of this type of analysis. Using the findings presented in Barabasi's book [69], an assessment was carried out by calculating the vulnerability of the entire network. Concrete proposals include the adoption of risk mitigation measures to reduce network vulnerability relative to the manifestation of natural disasters. The above methods can be used to assess the impact of a failure of the function of a particular element within an infrastructure of a network structure. Other methods that can be used to analyse the network structure include the critical path method [76]. This mathematical technique applies a network diagram with certain patterns.

Based on the theoretical analysis of the problem solved, the analysis of approaches in selected world countries and the analysis of techniques and approaches suitable for infrastructure analysis; the following section presents a proposal of a progressive system. Its ambition is to develop a unified approach to identifying regional elements of critical infrastructure in European countries.

The techniques and tools presented above were analysed in three basic areas (dimensions), system analysis, behaviour analysis, and network analysis. All presented techniques and tools are currently used for analysis in the critical infrastructure system. For this reason, attention was particularly paid to the applicability of these techniques and tools in the framework of the identification of critical elements at the regional level. Based on the results of the analysis, it can be concluded that for the identification of elements, it is appropriate to use the risk management framework [6,58], CARVER2 method [47], network analysis [74], critical path method [76] and Inoperability Input/Output Model [50], which are considered to be the most suitable for elemental analysis. The method of applying these methods to the proposed system is described in detail in the following section of the paper.

3. The Proposed System of Regional Critical Infrastructure Designation

The system of designating regional critical infrastructure elements can be set up in two different ways. The first approach is based on the system of designating national and European critical infrastructure elements utilizing a set of cross-cutting and sectoral criteria [4,77]. This involves a 'top-down' approach, also known as a 'conservative' model [30]. This approach has already been published and discussed at length by the authors [78]. The second approach to designating regional critical infrastructure elements is based on the 'bottom-up' assessment of elements and allows for the optional implementation of individual criteria and preferences. Furthermore, it makes it possible to designate regional critical infrastructure entities directly. The approach is labelled 'progressive' and has yet to be published.

For the above-mentioned reasons, the proposed system for the designation of regional critical infrastructure entities and elements pursues the bottom-up approach across the whole system [79]. It constitutes an approach reflecting current trends in the application of science-based findings to the area of critical infrastructure [80,81].

The designation process of the system consists of individual steps which will be explained in more detail below. Colour coding was used for convenience and to provide a clear overview of responsibilities for individual steps, the inputs, and outputs of each step and the tools and methods employed. The applied colour codes can be explained as follows:

- Yellow highlights analytical components, where these components are intended for working groups composed of experts in the field.
- Brown-green represents the decision-making component of the process, which should be undertaken exclusively by the relevant authorities.
- Light blue marks information entering the process or individual steps, or additional input information that may be required for analysis or decision-making purposes.
- Conversely, dark blue represents output information produced by a process or individual steps. The majority of output information is simultaneously used as input information for subsequent steps in the process.
- Grey identifies tools recommended for individual steps of the process or tools that may be utilized for a particular step.

White has been used as a complement only and has no bearing on the specification of responsibility. It does not affect the performance of individual steps as it only represents a kind of 'supergroup' or 'subgroup' of the steps described below. For an illustration of the entire process, including the colour coding, see Figure 3.

The nature and form of the input and output information, as well as of the utilized and recommended tools and methods, are explained in the process description that follows. The proposed process is built using a risk management framework [6,58] that enables a sequence of logical steps to form a system solution for identifying regional critical infrastructure elements. Generally, the process has been divided into four phases, with each containing one or more steps of the process. The four phases of the process are equivalent to the basic risk management framework [6], which first includes "scope and context" (equivalent to "Phase 1"), then "identification" (equivalent to "Phase 2"), "analysis" (equivalent) "Phase 3"), and last but not least, the "assessment" area (corresponding to "Phase 4"). Another essential part of the process are ongoing activities (corresponding to "Ongoing Activities") complementing the basic risk management framework, and in the areas of "communication and consultation" and "monitoring and revision".

The broad representation of participants in the proposed process has been described above generally as two main groups of participants in the process. The first is the "working group", which should include experts from the field of critical infrastructure, system analysts and experts from the critical infrastructure sectors (e.g., transport, energy, etc.). In addition, owners or infrastructure managers located in the area under consideration should also be part of this group. The second

main group is then the "relevant authorities", which should include representatives of the public administration related to the territory (e.g., Regional Authority, Security Council and the relevant Emergency Staff or security forces). The individual steps of the process are always carried out by the "working group", "relevant authorities" in a manner corresponding to the colour representation in Figure 3 ("working group" in yellow, "relevant authorities" in brown-green).

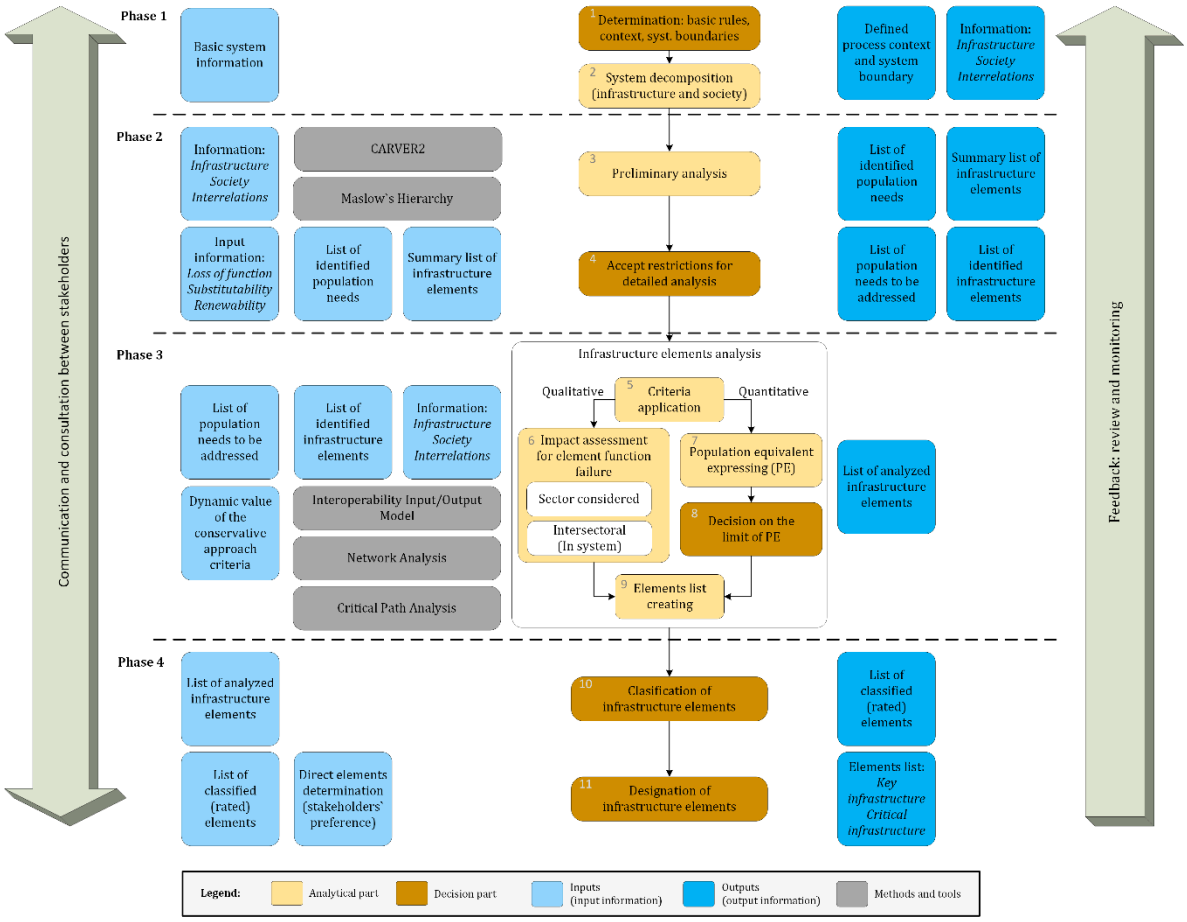

Figure 3. A proposed progressive approach to regional critical infrastructure element designation.

Other participants in the process may include non-profit organizations and interest groups using the solved infrastructure. This group of process participants can participate in ongoing process activities. The representation of the company and its interests are taken into account in the proposed process through "authority" as representatives of the local-government representing the society on the basis of their election. Representatives of local-government must comply with the legal requirements regarding confidentiality. These requirements relate to the security area (classified information, the disclosure of which could be detrimental to the security of the territory concerned). As the area of critical infrastructure is related to the security of the area, it is classified information that is not disclosed to the public. The public can only make its proposals through an elected representative of the local-government.

3.1. Phase 1: System Description

The initial phase focuses on general aspects of the designation process. While the first step consists of determining the context and boundaries of the system, the second step deals with the decomposition of the system thus established.

The determination of basic rules, the context, and boundaries of the system is the first step of the whole process (see also [6]). The basic parameters of the process must be determined in a way that

allows the requirements of stakeholders involved in the process to be factored in[5] and that does not prevent the credibility of the outcomes of the designation process from being contested. Furthermore, it is necessary to determine the parties to be involved in the performance of individual steps of the process, i.e., analytical and decision-making steps. This is followed by the establishment of system boundaries, within which the designation process is to take place [82]. The system boundaries may not always be identical. Basic rules and responsibilities for monitoring and review should be set up similarly. As it is part of decision-making, this step should be carried out by the responsible authority.

System decomposition involves its separation into infrastructure and society[6]. Infrastructure represents the means whereby the basic needs of a society are met. Criticality is thus linked to the society and relates to restrictions in the supply of services and the dependence thereon [83,84]. For a graphical representation of the system decomposition, see Figure 4 below.

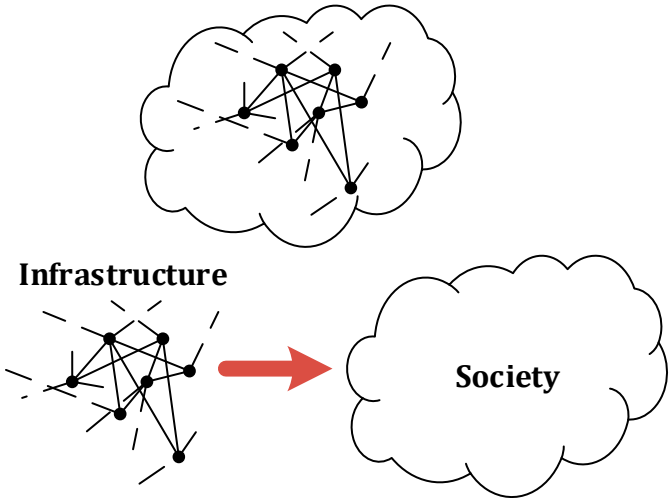

Figure 4. System decomposition into infrastructure- and society-focused components.

The basic system data represent the input information for both of these steps. By contrast, the output information yielded by the first step will be the established context of the process and the boundaries of the system. The output of the second step will consist of more detailed information about the infrastructure, the society and the linkages existing between them (interrelations).

3.2. Phase 2: Element Identification

The general focus and objective of the second phase is the creation of a list of identified infrastructure elements following specific rules and limitations. These elements are proposed by stakeholders. Similarly, to the highest level, these are institutions that, within the scope of their competence, propose individual elements for identification. The regional bodies concerned are those whose territorial scope corresponds to the region being addressed. These are the following bodies in particular: the Regional Office of the relevant region, the Regional Fire Department, the Regional Directorate of the Police of the Czech Republic, the Regional Health Emergency Service, the Regional Hygiene Station of the respective region, the Regional Veterinary Administration for the respective region, the regional office of the Czech Labor Office, and other institutions with competence in the respective region.

---

[5] These are interested parties entitled to comment on issues concerning community-wide security (see [57]) and may include various public institutions, law-enforcement agencies, called-in experts, relevant owners or operators, non-profit organizations and amateur groups.

[6] There are linkages between infrastructure and society. Simply put, commodities supplied to the society by the infrastructure flow in one direction, while infrastructure requirements flow in another direction [83]. Only the first direction has been shown here for illustrative purposes.

The preliminary analysis aims to examine all elementary system components (or elements) following specific rules. The input information consists of more detailed data on the infrastructure, the society and the linkages existing between them (interrelations). One of the tools suitable for the performance of a preliminary analysis is the CARVER2 method [47], which follows specific rules. An additional objective of this step is to identify the basic needs of the population (or society) on the understanding that these needs may vary from case to case [85,86]). Based on the completed analysis, the output of this step should include a summary list of infrastructure elements and a list of identified needs of the population concerned.

The acceptance of restrictions for detailed analysis is another step involving decision-making (at a political level). Specific restrictions can be adopted based on the established context and boundaries of the system. The purpose of introducing restrictions is to make further specifications to facilitate the subsequent analysis. The input information consists of a summary list of infrastructure elements and the list of identified needs of the population. The potential loss of function of some parts of the system, their degree of substitutability and their recovery potential should all be taken into account when deciding whether or not to adopt any restrictions. Subsequently, the lists of infrastructure elements and population needs should be reasonably reduced following the adopted restrictions. For example, a political decision to introduce restrictions on the amount of provided services could stem from the basic idea that society can function even without them [87,88]. Therefore, the output produced by this step should be a list of population needs that will be addressed and prioritized as required (existential needs should, however, invariably be given precedence—see [88,89]). Another output should be a list of identified infrastructure elements (i.e., elements selected for an in-depth analysis) reflecting the established restrictions.

3.3. Phase 3: Element Analysis

The third phase focuses on the analysis of infrastructure elements according to the set rules (see the preceding phases) using a predefined set of criteria. Its objective is to compile a list of analysed elements which is to be used as the basis for the subsequent decision-making process.

Criteria application consistent with the predefined set is based primarily on system decomposition philosophy. The criteria are then divided into quantitative and qualitative criteria, as shown in Figure 5, below.

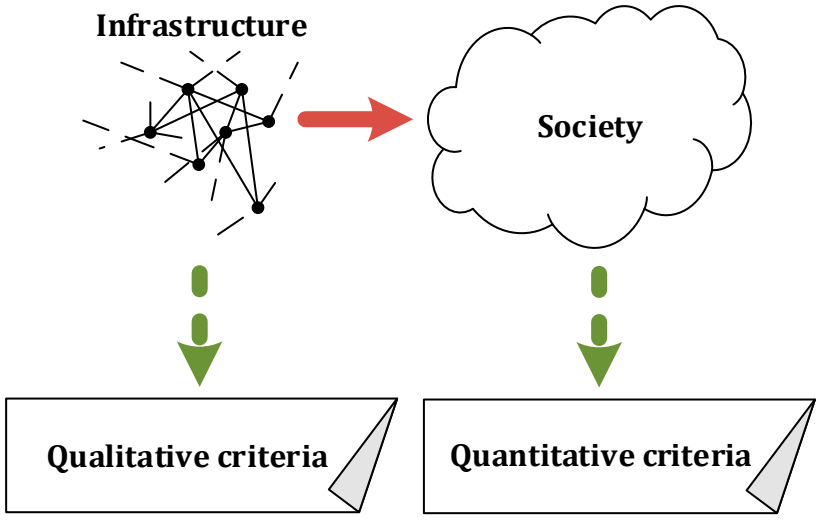

Figure 5. Decomposed system relationship with quantitative and qualitative criteria.

The quantitative criterion is directly linked to the impact of service failure on the population. Conversely, the qualitative criterion is derived from the effect of an infrastructure element failure on the entire functional unit (sector/system).

The impact assessment for element function failure involves the application of the qualitative component of the criteria. It first assesses the impact the failure of an element has on the relevant sector and then on the entire functional unit (i.e., the system as a whole). The impact of the failure of an element can be expressed qualitatively as follows:

- Consequences without a negative impact—flawless redirection of the load to another part of the system.
- Threshold loading—the system may be loaded to the near-breaking point due to the redirection.
- Overloading—the redirection may cause the remaining parts of the system to overload.

Even though the presented qualitative expression may seem rather general, it allows for an effective assessment of the impact by clearly defining the effects the element failure exerts. The input information necessary to assess the impact of a failure of a particular element should include a list of the population needs to be addressed, a list of identified infrastructure elements and information concerning the infrastructure, the society and the linkages existing between them (interrelations). For this purpose, the network analysis method [74] or the critical path method [76] should be used. The interdependencies between critical infrastructure sectors and their impact on society must also be taken into account in the context of assessing the impact of a function failure on an element [36]. For this purpose, it is appropriate to use the Inoperability Input/Output Model [50].

The expression of population equivalent 'PE' is used to define the impact a function failure has on the population. It is a quantitative expression of the size of the population that depends on the services provided by a particular element (infrastructure) and which would be adversely affected by the failure thereof. The input data are identical to the data processed in the preceding phase. Most of the information required to perform the quantification should be available by now if the above-mentioned tools are utilized. More detailed information about the infrastructure concerned will also make it possible to quantify the effects of failures in the function of infrastructure elements.

The decision on the threshold limit of PE is another step that should be carried out by the responsible authority and consists of defining an appropriate limit value for the number of people affected by a service failure. If the number of people affected by a service failure is shown to be higher than the established limit, the relevant element will be prioritized in the subsequent steps. Specific threshold limits may be set for each sector or service separately. The dynamic value of cross-cutting criteria based on the 'conservative' approach can be used as an example of input information applied to set the threshold limit (see [30]).

The output yielded by the third phase should be a list of analysed infrastructure elements. This list will essentially contain an enumeration of elements with allocated values based on both qualitative and quantitative criteria. A list such as this should provide a clear picture of the consequences that a failure in the function of a particular element can result in concerning the infrastructure and the population. Moreover, applying the interdependencies between the society and the infrastructure in combination with the proposed tools will make it possible to assess the impact on the whole system (infrastructure and society).

The application of the set of quantitative and qualitative criteria can also be seen as an application of one of the principles arising from the Council Directive [4], which focuses on the utilisation of cross-cutting and sectoral criteria. The quantitative part of the criteria, expressing the population equivalent, can be regarded as a cross-cutting criterion. Conversely, the qualitative part of the criteria, which consists of assessing the impact of the failure of an infrastructure element both on a particular sector and on the functional unit as a whole, can be treated as a sectoral criterion.

3.4. Phase 4: Element Evaluation

The final phase of the process is aimed at evaluating the elements identified and analysed in the preceding phase. Subsequently, a list of these elements can be designated as regional infrastructure. Since both steps of the fourth phase follow on from each other, they can be performed collectively.

Infrastructure element classification into specific groups is the responsibility of the relevant authorities. The input data consist of the list of analysed infrastructure elements, from which the impacts of element failure can be directly derived. The classification may include several groups; numerous professional publications can be consulted for inspiration (e.g., [90]). However, some basic rules must be established to ensure that individual elements are assigned to the appropriate category of the regional infrastructure. These rules should be clearly defined by the relevant authorities. The following scale is based on element classification into four groups, which seems to be quite adequate:

- *The special level* is represented by elements whose non-inclusion in higher-level critical infrastructure might be considered unacceptable. This may involve, for example, the failure in the function of an element with far-reaching implications for the entire region, while at the same time impacting on critical infrastructure at higher levels. Even though the probability of infrastructure failure at higher levels is generally low, it cannot be ruled out (see the Blackout in the United States and Canada: [91]). Furthermore, an element may, for example, meet the criteria for inclusion in higher-level critical infrastructure. Such elements should be re-examined and assigned to the proper level of critical infrastructure.
- *Regional critical infrastructure* comprises the second group of elements which are essential (critical) to the smooth functioning of the region. These are elements of 'vital' importance (for an equivalent thereof see [18]), forming the core of the relevant regional infrastructure. The impact of a failure in the services provided by such elements may be noticeable, but without any negative implications for the higher-level critical infrastructure. Concerning critical infrastructure and its protection, such elements should be given top (level 1) priority in terms of their protection within the region. This may include elements whose failure would be assessed as likely to result in the 'overload' of the infrastructure, in whole or in part (see the qualitative expression regarding the *Impact assessment for element function failure* above), with the impact on the number of people exceeding the set PE threshold limit, and elements providing services that are essential to the population (see [87,88]).
- *Regional key infrastructure* constitutes the third group of elements, which may include structures likely to compromise the functioning of the regional critical infrastructure under a specific set of circumstances. These are regional elements of 'non-vital' importance (for an equivalent see [18]), complementing the infrastructure function (see [19]). In terms of their protection, these elements will be given a priority lower (level 2) than 'regional critical infrastructure' elements. They may include elements whose failure would be assessed as likely to lead to the 'threshold loading' of the infrastructure, in whole or in part (see the qualitative expression regarding the *Impact assessment for element function failure* above), with the impact on the number of people exceeding the set PE threshold limit, and elements providing services that are essential to the population (see [87,88]).
- *Unclassified elements* represent a group composed of elements whose failure would lead to 'consequences without a negative impact' on either the infrastructure or the society.

However, the elements should be classified in a way that considers all associated issues and factors in element interdependencies as well as all dependencies existing between the infrastructure and the society [92]. The proposed classification scale can be adjusted to fit the requirements of the relevant authorities. The output produced by this step should be a list of classified (rated/evaluated) elements divided into the suggested categories. The list is only a proposal. The list of elements may be expanded or narrowed down based on stakeholder preferences as part of the final step of the process.

Infrastructure element designation is the final step of the presented process, wherein a final decision is made. The input data consist of the list of classified (evaluated) elements and individual stakeholder preferences. The elements proposed as part of the classification scale should be the subjects of a final discussion. The preference issue should be one of the key points on the agenda of this discussion, the outcome of which should be a consensus among the relevant authorities and stakeholders. Besides, the stakeholders may also find some elements to be essential for the functioning

of the region as a whole. Based on the consensus, the list of classified elements may be further supplemented following the above-mentioned stakeholder preferences.

The issue of the prioritisation of measures for regional infrastructure element protection could be resolved by including the relevant elements in the level 1 group. This level may be designated to indicate a direct dependency (see also [18]) between the failure of the element and the failure in the availability of a particular service within the region. Conversely, the classification of structures in the level 2 group may be understood to indicate an indirect dependency (see also [18]). The inclusion of structures in the 'unclassified' group means that under current conditions set for the designation of 'regional critical infrastructure' and 'regional key infrastructure', there are elements within the region that need to be protected primarily (and secondarily). However, the subsequent designation of elements included in this group also cannot be ruled out, depending on stakeholder preferences.

Preferences can be implemented, for example, by directly designating specific regional structures regarded by the relevant authority as highly important (or even 'critical') for maintaining the functionality of a region. Foreign experience shows (e.g., [26]) that this approach is consistently effective and is even applied to directly designating some structures or their owners (entities). Structures of high cultural importance (similar to 'Assets' specified in [26]) could also be included here. The proposed process could then be used directly to designate elements to the 'regional critical infrastructure' category or the 'regional key infrastructure' category. In terms of logic, direct inclusion of some elements in the 'special category' and the 'unclassified elements' category is not possible.

The relevant authorities should resolve to designate 'regional critical infrastructure' and 'regional key infrastructure'. The output produced by this step (and the entire process) will be a list of elements and entities included in the two aforementioned infrastructure groups.

3.5. Ongoing Activities

This part of the process is focused on ongoing activities that are carried out during the previous phases. These are activities with a high emphasis on maintaining the quality of the whole process and the quality of its outputs. The two ongoing activities below can be performed independently of each other.

Feedback: review and monitoringconstitute a fully-fledged component of the process (see [6]). Individual steps of the process can be affected retrospectively by feedback [93]. Feedback can have a positive effect in that it can be applied to enhancing the process by validating individual steps and their results, or process results. Conversely, negative feedback can counteract any irregularity (deviation) and help in the suppression thereof. The process as a whole is bound to benefit from both types of feedback.

Monitoring would be best performed for each step of the process following set rules. At the same time, an emphasis should be placed on the continuity and effectiveness of the entire process by duly correcting any irregularities. Delays in the indicators of feedback effectiveness should be viewed similarly. Feedback as part of a dynamic process may lead to some delays in the manifestation of the required changes across the process [93]. Monitoring and review should focus on the function and completeness of the presented approaches, i.e., to ensure that all elements deemed vital to maintaining infrastructure functions have been analysed [18]. For this purpose, it is advisable to put in place some sort of metrics to help evaluate individual components of the system approach. Periodic inspections and reviews of the process are crucial to maintaining the quality of the process and, as such, should be performed at regular intervals. As part of this phase [6], the whole process should be analysed to ensure its efficiency and its potential improvement by the implementation of new approaches.

Stakeholder communication and consultation is the cornerstone of the whole process. Good communication should be maintained throughout the process [6] and should include effective consultations aimed at enhancing the quality of the process itself. Care should be taken to ensure that all parties involved in the process fully understand any decisions made by the relevant authorities, and also that the authorities understand the reasons for, and the outputs of, any analytical work performed. Moreover, clear communication also facilitates the implementation of stakeholder preferences, both in the designation phase and throughout the entire process. As stakeholders show a general tendency to

view the issue primarily from their perspective, all steps of the process must be fully discussed and properly communicated. Stakeholder opinions may greatly affect the decision-making of the authorities.

Awareness of the importance of communication leading to the subsequent adoption of views held by different groups of stakeholders, as well as their direct involvement in the process, can be seen as a form of governance[7] across the process (and constitutes the application of the UNISDR [57]). In this way, communication is instrumental in building trust between partners (stakeholders) and, in general, to enhance the process and its outcomes.

The practical application of the proposed progressive approach to identifying critical infrastructure elements must also respect some of its limitations. The main limitation is the so-called territorial limitation, on the vertical level, i.e., the definition of the region. For this reason, the most appropriate solution is to regard the region as a regionally defined territorial area falling within the competence of local government. In the Czech Republic, these are mainly larger territorial units under the administration of regional authorities and smaller municipalities under municipal administration. Other important limitations include, for example, the necessary knowledge of techniques and tools for infrastructure analysis at the regional level or the need for coordinated cooperation among stakeholders.

Accepting restrictions for detailed analysis is a step whose content must be approved by stakeholders. However, the final decision depends on the responsible public institution or the responsible authority of the owner or operator of the critical infrastructure element (or their mutual consensus).

4. Case Study

An example of the practical application of the proposed system for identifying regional critical infrastructure elements is demonstrated by a case study that focuses on road infrastructure as a part of the technical infrastructure in the Pardubice Region (NUTS—CZ053), which represents the societal system. The territorial limitation of the assessed region is defined by the borders of the administrative district of the Pardubice Region. The map of the area under consideration is presented in Figure 6.

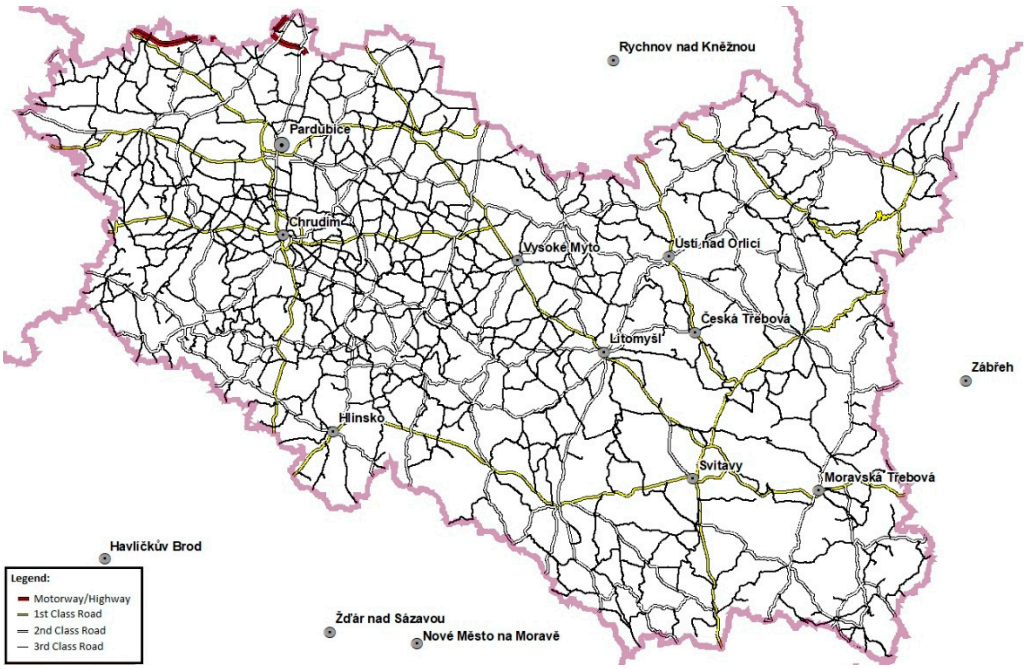

Figure 6. Road network infrastructure selected for detailed analysis (created on data provided by [94,95].

[7] For more information visit the International Risk Governance Council website at: https://www.irgc.org/risk-governance/what-is-risk-governance/.

In order to verify the proposed procedure in reality, a stakeholder team was set up containing representatives of:

1. Regional Authority of the Pardubice Region.
2. Regional Security Council of the Pardubice Region.
3. Regional Directorate of the Police (for the Pardubice Region).
4. Road Administration and Maintenance Director of the Pardubice Region.
5. Road transport expert/system analyst.
6. Critical infrastructure expert.
7. Association of Road Transport Operators.

For the purpose of carrying out the case study, Category 1-3 members represent the "relevant authorities", Category 4-6 members represent "working group", and Category 7 members represent other process participants (interest groups).

4.1. Phase 1: System Description

The assessed critical infrastructure sector is the road transport sector. The input data for this infrastructure consists of a type of road, a unique identifier (road section number), traffic intensity and interest information [96]. Based on the consensus of stakeholders, the assessment was limited to roads that allow interconnection of the region (i.e., motorways, 1st class roads, 2nd class roads, 3rd class roads)—local roads were not assessed. Concerning the accepted limitation, 500 sections of roads and 691 structures of interest (i.e., bridges, tunnels, intersections, etc.) were subjected to further assessment. This case study is based on the results of the National Transport Census [97], uniform vector transport maps [98] and available background data for GIS [94,95].

4.2. Phase 2: Element Identification

The preliminary analysis is aimed at identifying the needs of the population and compiling a comprehensive list of infrastructure elements.

In terms of applications carried out a sector with relationships being solved (road infrastructure) was supported and following the basic needs of the population [88]: (a) biological physical needs (relationship in particular to the food supply, pharmaceuticals, health); (b) the need for safety and security (mainly related to security services, electricity supply).

The basis for compiling a comprehensive list of infrastructure elements is the implementation of the Transport Census Results [97]. In this case, the traffic census replaces the preliminary analysis, which is to identify the individual sections of the road network. The assignment of certain values to these sections was performed via the CARVER2 method [47]. In this way, a total of 539 assessed sections and a total of 1055 buildings of interest within the Pardubice Region were identified. Due to the scope of the underlying data, this data are not part of this article (detailed information can be found in [97]).

The acceptance of restrictions for the detailed analysis is conducted by the responsible public institution (i.e., the Regional Authority of the Pardubice Region) or the responsible authority of the owner or operator (i.e., the Regional Authority of the Pardubice Region and the Road and Motorway Directorate of the Czech Republic). In this case, it was the consensus of both authorities. On that basis, the following restriction was adopted: For a detailed analysis, only roads allowing connection within the Pardubice region will be considered. Such roads cannot include local roads. Moreover, these are roads that are managed by the municipality, not by the regions. Based on this, the previous list of identified infrastructure elements was reduced to 500 assessed sections and 691 interest structures within the Pardubice Region.

4.3. Phase 3: Element Analysis

For the purpose of analysis, a modified critical pathway method [76] and elementary network analysis [74] were applied. Based on the application of the modified critical path method, it was possible to present the intersection of roads as nodes and sections of roads as connectors. The implementation of this application should be supplemented by basic knowledge of networks, specifically the assessment of the density and heterogeneity of the network. The following facts can be stated here:

- The solved infrastructure of the road network is rather sparse [74], in terms of density of the network of motorways and 1st class roads. Some nodes usually have only one connection, and some nodes form larger irreplaceable centres (nodes with multiple connections).
- The solved infrastructure of the road network is very dense in terms of density of the 2nd class road network [74], i.e., there are several possible connection variants between the nodes.
- The solved infrastructure of the road network in terms of the density of the 3rd class road network forms a discontinuous network and the parts of the network consist of small island (isolated) systems [69,72]. This is, however, logical, since 3rd class roads are complementary to 2nd and 1st class roads. Subsequent network analysis of 3rd class island class systems will always have the same result [72,74].

Applying the critical pathway method [76], places of high importance can be identified in the networks of different types of roads, such as a crossing of the roads of a particular class or the nodes mentioned. The list of identified elements has been supplemented by their importance in the system and one of the following options was always selected:

- Impact of the element's function failure on the entire system of the road network in the region concerned. There is no alternative route on the same type of road in the region.
- Impact of failure of the element function on a part of the system (i.e., a limit load of a part of the region) in the region concerned. For a solution, there is an alternative route on the same type of road.
- No negative effects of a failure of the system or its part in the region being solved.

An extract from the entire list of identified elements for interest buildings is presented in Table 2.

Table 2. Summary of the network analysis results for nodes/interest buildings.

Type of Road	Impact on the Entire System	Impact on a Part of a System	No Negative Impact
Motorway	3/12	0	0
1st class road	3/24	6/155	2/29
2nd class road	0	18/101	15/177
3rd class road	0	0/64	323/127

The methodology developed by the National Cooperative Highway Research Program [99] may also be used to identify elements of critical transport infrastructure. This approach is based on assessing the consequences of critical infrastructure protection in the context of threat variability and probability.

The population equivalent EP is expressed as the number of people who will not be able to use the relevant section of road primarily. Secondarily, the consequences for other parts of the population can also be deduced, for example, the loss of supply with a consequent impact on the population. However, in this case study, attention was only given to the primary consequences. The population equivalent can be determined based on the average occupancy of cars and trucks [100] and the number of vehicles passing through the 24-h section [97]. The recalculated number of inhabitants thus obtained is always related to a certain section of road. E.g., the busiest section of the motorway in the Pardubice Region reached in 2016 the value of population equivalent at 32,021 persons in 24 h.

The decision on the level of population equivalent limit was made by the responsible authority (i.e., the Regional Authority of the Pardubice Region), which decided to use the recalculated dynamic value of the affected population (proposed by authors in [30]). This value was set at the level of 6112 inhabitants of the Pardubice Region for the year 2016.

4.4. Phase 4: Element Evaluation

Since there are only some sections of the motorway in the region, the failure of these sections will always have an impact on the regional motorway system not only in the Pardubice region but also in adjacent regions. In terms of 1st class roads, these are only selected sections. The impact on the entire system is related to the structures of interest on selected sections of roads I/35 and I/43. The structures of interest on the road sections, which form connections with the nearest node in the region up to the border of the Pardubice Region will have an impact on the part of the system. On the other hand, there is no negative impact on the structures of interest on the sections between the nodes for which there are one or more alternative routes.

Similar patterns can be observed with structures of interest in the 2nd class road system, specifically with the impact of the failure of the function of a structure on a part of the system, without a negative impact on the system. No structure of interest on 2nd class roads will affect the entire system when it is disturbed. As already mentioned, 3rd class roads will in some cases function as an island system. Therefore, the damage to the interest buildings on the 3rd class road sections in the Pardubice Region may only have a partial effect or no negative impact on the 3rd class road system.

The input data for assessment of the social part of the system are mainly formed by the number of inhabitants in the municipalities, as with the increasing number of inhabitants there are growing demands for maintaining the functionality of the service supply to the population. The expression of the population equivalent was based on the results of the National Transport Census in 2016 [91]. This document indicates that the maximum equivalent number of inhabitants is reached by some sections of 1st class roads (more than motorways). The list containing the recalculated dynamic values of the affected population served as a basis for identifying the elements of the infrastructure. To protect information on potential critical infrastructure, only the general conclusions of the proposed classification can be presented:

- *Special level* comprises the elements that disable the road infrastructure for levels higher than the regional units (i.e., national level), namely motorway sections and one nationally significant building (tunnel) in the territory of the Pardubice Region. For this reason, these elements also have a significant impact on the elements of adjacent regions. The reason for this may be the fact that the motorway serves mainly for transit traffic between states and their parts. Similarly, the mentioned tunnel forms a significant obstacle to the national transit route. Routes alternative to the tunnel route are unable to provide adequate throughput for the transport capacity. A graphical representation of the special level elements in the evaluated region is presented in Figure 7. The elements of the other levels are not included in the figure due to the large amount.
- *Regional critical infrastructure* consists of elements that are non-replaceable for securing the equivalent transport capacity in the region. These are roads, which, if not in use, would make the regional transport impossible. Similarly, there are structures of interest whose rehabilitation would be very difficult. In particular, it can be a single tunnel and bridges typically located on the busiest routes and also on busy routes of larger towns in the region. It may also be the busiest crossing of the 1st class roads.
- *Regional key infrastructure*, on the other hand, is a group of elements that can be crucial to maintaining the road infrastructure function. Here, in particular, the requirements for alternative routes have been taken into account. Some sections may be exposed to a limit load and may collapse the entire infrastructure or system. These can, for example, be some elements with a partial impact on the system under consideration.

- *Unclassified elements* form an important part of all the infrastructure elements. It cannot be stated that their non-inclusion reduces their importance within the system under consideration.

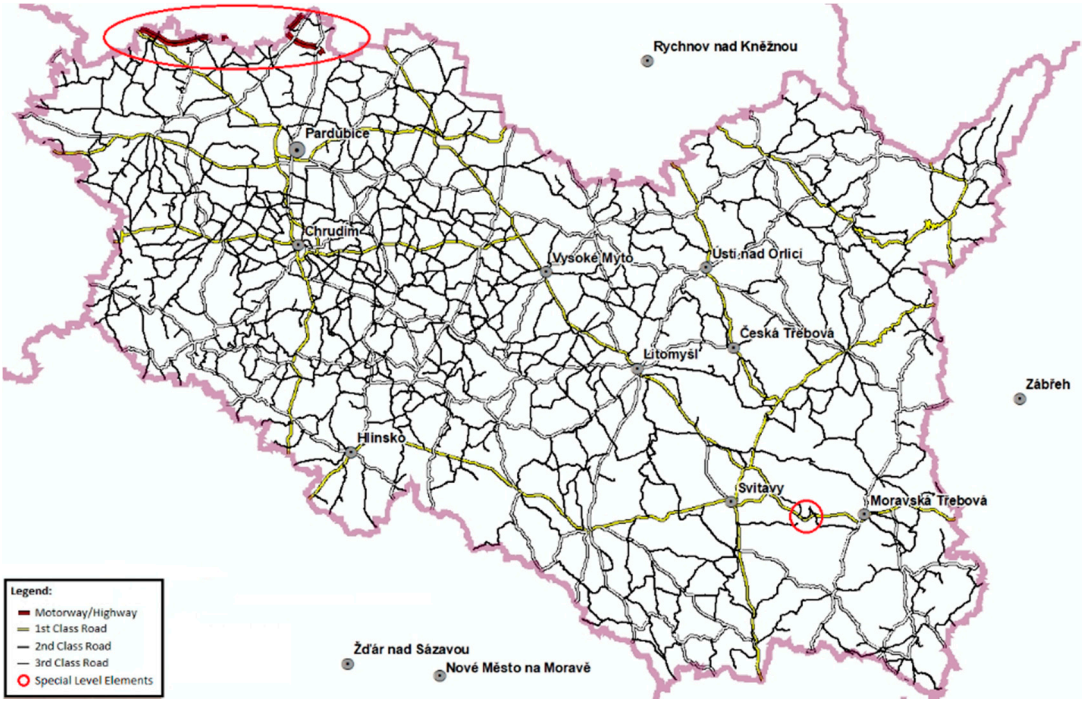

Figure 7. Graphical representation of special level elements in the evaluated region (created on data provided by [94,95]).

The element classification was conducted through holistic thinking when the importance of the element for the whole infrastructure and the system of society was considered. The preferences of stakeholders were also included in the identification process. Particularly, these were the comments of experts in the field of road transport, who specified the behaviour of the road transport system.

4.5. Ongoing Activities

Ongoing implementation of monitoring and revision activities was carried out for each phase. The reason for this was the practical prevention of errors or irregularities being introduced into the subsequent stages of the case study process. To this end, a "Monitoring Group" has been established, comprising one representative of each stakeholder in any way involved in the process (representatives from all categories 1–7). The "Monitoring Group" carried out a careful review each time the relevant phase was completed and also monitored the relevance of the input data to each step. The "Monitoring Group" then gave feedback on the conclusions of the monitoring and revision—always to those groups that were scheduled to take steps within the relevant phase.

The "Monitoring Group" also reviewed the implementation of the communication and consultations across the research team. Communication and consultation were carried out to the extent necessary to verify the feasibility of the proposed process. One of the recommendations of the "Monitoring Group" was to re-familiarize with the results of Phase 1, including "Scope and Context". The recommendation was addressed to "responsible authorities", which tended to slightly adjust the results to the needs of "responsible authorities".

5. Conclusions

The proposed system of regional critical infrastructure designation, as presented in this article, has stemmed from the necessity to come up with a systemic approach applicable to different countries at the regional level. Greater safety of regional elements is essential to ensuring the overall security of the critical infrastructure system. The presented progressive approach is based on the 'bottom-up' evaluation of elements and allows for the optional implementation of individual criteria and preferences. Furthermore, it makes it possible to designate regional critical infrastructure entities directly. Thanks to its characteristics, it can be applied to both public institutions and the private sector at the regional level. The progressive element designation process has been designed as a model presenting a basic philosophy, leaving room for further elaboration. The novelty of this approach can be particularly seen in identifying regional critical infrastructure elements through an integral assessment of these elements' failure impact, not only on the dependent subsectors, but also on the population (population equivalent) located in the assessed region.

The proposed system presents a possible managerial approach to the identification of critical infrastructure elements at the regional level. In this context, the system is intended primarily for crisis managers of local authorities. In the event of a crisis situation, it may also be an appropriate support tool for the work of the region's Security Council and the relevant Emergency Staff. Implementing this approach in practice would contribute not only to improving the continuity of service delivery of the company, but also to strengthening the preparedness of the authorities responsible for preparing the area for crises and increasing the security of the area as a whole.

From the perspective of the public sector, the primary reason for applying the presented approach to regional critical infrastructure designation is its ability to ensure the required level of regional security. Concerning the private sector, it addresses the issue of maintaining the continuity of activities that secondarily contribute to profit maximization. Finally, it can be concluded that a common understanding of the significance of the issue concerned is the social responsibility of both the public and private sectors, and is in their interests, for maintaining the function of individual regions.

Author Contributions: Conceptualization, P.N. and M.J.; methodology, P.N.; software, P.N.; validation, P.N. and M.J.; formal analysis, P.N. and M.J.; investigation, P.N. and M.J.; resources, P.N.; data curation, P.N.; writing—original draft preparation, P.N. and M.J.; writing—review and editing, P.N. and M.J.; visualization, P.N.; supervision, P.N.; project administration, P.N. and M.J.; funding acquisition, M.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Ministry of the Interior of the Czech Republic, grant number VI20192022151" and by the Internal Grant Scheme of Faculty of Security Engineering, University of Zilina, grant number IGP201903.

Acknowledgments: The article has been elaborated within the project of the Ministry of the Interior of the Czech Republic filed under VI20192022151 and entitled 'CIRFI2019: Indication of Critical Infrastructure Failure'. This work was supported by the Internal Grant Scheme of Faculty of Security Engineering, University of Zilina from the grant No. IGP201903.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Frangopol, D.M.; Soliman, M.; Dong, Y. Practical Applications of Life-cycle Considerations in Sustainable Development of Infrastructure. In Proceedings of the Conference on Sustainable Development of Critical Infrastructure, American Society of Civil Engineers, Shanghai, China, 16–18 May 2014; pp. 17–36. [CrossRef]
2. World Economic Forum. *Global Risk 2014*, 9th ed.; The World Economic Forum: Geneva, Switzerland, 2014; ISBN 978-92-95044-60-9.
3. Rehak, D.; Senovsky, P.; Hromada, M.; Lovecek, T. Complex Approach to Assessing Resilience of Critical Infrastructure Elements. *Int. J. Crit. Inf. Prot.* **2019**, *25*, 125–138. [CrossRef]

4. European Commission. *Council Directive 2008/114/ES of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection*; European Council: Brussels, Belgium, 2008.
5. European Commission. *Commission Staff Working Document "On a New Approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructure More Secure"*; European Commission: Brussels, Belgium, 2013.
6. ISO 31000:2018. *Risk Management–Principles and Guidelines*; International Organization for Standardization: Geneva, Switzerland, 2009.
7. Lukas, L.; Hromada, M. Risk Analysis in Context of Critical Infrastructure Protection. In Proceedings of the Annals of DAAAM for 2011 and 22nd International DAAAM Symposium Intelligent Manufacturing and Automation: Power of Knowledge and Creativity, Technische Universität Wien, Vienna, Austria, 23–26 November 2011; pp. 1469–1470.
8. Hromada, M.; Lukas, L. Multicriterial Evaluation of Critical Infrastructure Element Protection in Czech Republic. In Proceedings of the Conference on Advanced Software Engineering and Its Applications (ASEA) and Conference on Disaster Recovery and Business Continuity (DRBC), Jeju Island, Korea, 28 November–2 December 2012; pp. 306–309.
9. Rehak, D.; Novotny, P. Bases for Modelling the Impacts of the Critical Infrastructure Failure. *Chem. Eng. Trans.* **2016**, *53*, 91–96. [CrossRef]
10. Rehak, D.; Hromada, M.; Novotny, P. European Critical Infrastructure Risk and Safety Management: Directive Implementation in Practice. *Chem. Eng. Trans.* **2016**, *48*, 943–948. [CrossRef]
11. European Commission. *Regions in the European Union: Nomenclature of Territorial Units for Statistics NUTS 2010/EU-27*; European Commission: Brussel, Belgium, 2011.
12. Haberlin, R.J.; Haimes, Y.Y. Regional Infrastructures as Complex Systems of Systems: Shared-State Model for Regional Resilience. *J. Inf. Syst.* **2018**, *24*. [CrossRef]
13. Rehak, D.; Senovsky, P.; Slivkova, S. Resilience of Critical Infrastructure Elements and its Main Factors. *Systems* **2018**, *6*, 21. [CrossRef]
14. Swiss Federal Office for Civil Protection. *Critical Infrastructure Protection: Second Report to the Federal Council and Measures for the Period 2009–2011*; Federal Office for Civil Protection: Bern, Switzerland, 2009.
15. Swiss Federal Council. *Basic Strategy of the Federal Council-Critical Infrastructure Protection: Basis for the National Critical Infrastructure Protection Strategy*; Swiss Federal Council: Bern, Switzerland, 2009.
16. Bundesamt für Bevölkerungsschutz. *Methode zur Erstellung des SKI-Inventars, Bundesamt für Bevölkerungsschutz*; Konzeption und Koordination: Bern, Switzerland, 2010.
17. Tweede Kamer. *Eerste Voortgangsrapportage m.b.t. Actieplan Terrorismebestrijding en Veiligheid van 5 Oktober 2001 (First Progress Report w.r.t. the Action Plan Counter-terorism and Safety Dated 5 October 2001)*; Tweede Kamer der Staten-Heneraal vergaderjaar: The Hague, The Netherlands, 2001.
18. Luiijf, E.; Burger, H.; Klaver, M. *Critical Infrastructure Protection in the Netherlands: A Quick-scan*; EICAR: Copenhagen, Denmark, 2003.
19. The Hague Security Delta. *Securing Critical Infrastructures in the Netherlands: Towards a National Testbed*; The Hague Security Delta: The Hague, The Netherlands, 2015.
20. Cabinet Office. *The National Security Strategy of the United Kingdom: Security in an Independent World*; Cabinet Office: London, UK, 2008.
21. Cabinet Office. *Strategic Framework and Policy Statement: On Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*; Cabinet Office: London, UK, 2010.
22. Cabinet Office. *Keeping the Country Running: Natural Hazards and Infrastructure, Section C: Practical Guidance*; Cabinet Office: London, UK, 2011.
23. Cabinet Office. *Risk Assessment: How the Risk of Emergencies in the UK is Assessed*; Cabinet Office: London, UK, 2013.
24. Cabinet Office. *National Infrastructure Plan*; Cabinet Office: London, UK, 2013.
25. Cabinet Office. *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*; Controller of her Majesty's Stationery Office: London, UK, 2015.
26. National Emergency Management Agency. *Civil Defence Emergency Management (CDEM) Act*; The Ministry of Civil Defence and Emergency Management: Wellington, New Zealand, 2002.
27. Auckland Engineering Lifelines Group. *Auckland Engineering Lifelines Group Report: Stage 2. Version 1.1.*; Auckland Engineering Lifeline Group: Auckland, New Zealand, 2014.

28. National Emergency Management Agency. *Revised National Civil Defence Emergency Management Plan: Resilient New Zealand*; The Ministry of Civil Defence and Emergency Management: Wellington, New Zealand, 2014.
29. Pruyt, E.; Veldheer, V.; Wijnmalen, D.J.D.; Alink, F.; Dam, A.; van Horst, J.; van der Knops, J.; Bergmans, H.; Janssen, L. *National Safety and Security Programme: National Risk Analysis Method Guide*; Government of Netherlands: The Hague, The Netherlands, 2008.
30. Novotny, P.; Markuci, J.; Rehak, D. Determination of the Critical Infrastructure Elements at Regional Level. *Spektrum* **2014**, *14*, 56–59.
31. Zio, E. Challenges in the Vulnerability and Risk Analysis of Critical Infrastructures. *Reliab. Eng. Syst. Saf.* **2016**, *152*, 137–150. [CrossRef]
32. Bernatik, A.; Senovsky, P.; Senovsky, M.; Rehak, D. Territorial Risk Analysis and Mapping. *Chem. Eng. Trans.* **2013**, *31*, 79–84. [CrossRef]
33. Siser, A.; Maris, L.; Rehak, D.; Pellowski, W. The Use of Expert Judgement as the Method to Obtain Delay Time Values of Passive Barriers in the Context of the Physical Protection System. In Proceedings of the 52nd Annual IEEE International Carnahan Conference on Security Technology (ICCST), Montréal, QC, Canada, 22–25 October 2018; pp. 126–130.
34. Slivkova, S.; Rehak, D.; Nesporova, V.; Dopaterova, M. Correlation of Core Areas Determining the Resilience of Critical Infrastructure. In Proceedings of the 12th International Scientific Conference on Sustainable, Modern and Safe Transport (TRANSCOM 2017), High Tatras, Slovakia, 31 May–2 June 2017; pp. 812–817. [CrossRef]
35. Ghorbani, A.A.; Bagheri, E. The State of the Art in Critical Infrastructure Protection: A Framework for Convergence. *Int. J. Crit. Inf.* **2008**, *4*, 215–244. [CrossRef]
36. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Syst.* **2001**, *21*, 11–25. [CrossRef]
37. Rinaldi, S.M. Modelling and Simulating Critical Infrastructures and Their Interdependencies. In Proceedings of the 37th Annual Hawaii International Conference on System Science, IEEE Computer Society, Big Island, HI, USA, 5–8 January 2004.
38. Dunn, M. The Socio-political Dimensions of Critical Information Infrastructure Protection (CIIP). *Int. J. Crit. Inf.* **2005**, *1*, 258–268. [CrossRef]
39. Bagheri, E.; Ghorbani, A.A. UML-CI: A reference model for profiling critical infrastructure systems. *Inf. Syst. Front.* **2010**, *12*, 115–139. [CrossRef]
40. Ezell, B.C.; Farr, J.V.; Wiese, I. Infrastructure Risk Analysis Model. *J. Inf. Syst.* **2000**, *6*, 114–117. [CrossRef]
41. Witsenhausen, H.S. A Class of Hybrid-state Continuous-time Dynamic Systems. *IEEE Trans. Autom. Control* **1966**, *11*, 161–167. [CrossRef]
42. Ristvej, J.; Holla, K.; Simak, L.; Titko, M.; Zagorecki, A. Modelling, Simulation and Information Systems as a Tool to Support Decision-Making Process in Crisis Management. In Proceedings of the Modelling and Simulation 2013-European Simulation and Modelling Conference, Lancaster, UK, 23–25 October 2013.
43. Zagorecki, A.T.; Johnson, D.; Ristvej, J. Data Mining and Machine Learning in the Context of Disaster and Crisis Management. *Int. J. Emergy Man.* **2013**, *9*, 351–365. [CrossRef]
44. Rubinstein, R.Y.; Kroese, D.P. *Simulation and the Monte Carlo Method*; John Wiley and Sons: New York, NY, USA, 2011.
45. Zhang, G.; Bose, A. Scenario Building for Operator Training Simulators Using a Transient Stability Program. *IEEE Trans. Power Syst.* **1989**, *4*, 1542–1549. [CrossRef]
46. Newman, D.E.; Nkei, B.; Carreras, B.A.; Dobson, I.; Lynch, V.E.; Gradney, P. Risk Assessment in Complex Interacting Infrastructure Systems. In Proceedings of the 38th Annual Hawaii International Conference on System Sciences, IEEE Computer Society, Big Island, HI, USA, 3–6 January 2005.
47. *CARVER2*; National Infrastructure Institute–Center for Infrastructure Expertise: Portsmouth, UK, 2011.
48. Lima, A.; Stojanovic, R.; Papagiannaki, D.; Rodriguez, P.; Gonzales, M.C. Understanding Individual Routing Behaviour. *J. R. Soc. Int.* **2016**, *13*. [CrossRef] [PubMed]
49. Zlotkin, G.; Rosenschein, J.S. Cooperation and Conflict Resolution via Negotiation Among Autonomous Agents in Noncooperative Domains. *IEEE Trans. Syst. Man Cybern* **1991**, *21*, 1317–1324. [CrossRef]
50. Yusta, J.M.; Correa, G.; Lacal-Arántegui, R. Methodologies and Applications for Critical Infrastructure Protection: State-of-the-art. *Energy Policy* **2011**, *39*, 6100–6119. [CrossRef]

51. Ben-Gal, I. *Encyclopedia of Statistics in Quality and Reliability, Bayesian Networks*; John Wiley and Sons: New York, NY, USA, 2008.
52. Tukey, J.W. *Exploratory Data Analysis*; Addison-Wesley: Boston, MA, USA, 1977.
53. Wang, X.F.; Chen, G. Complex Networks: Small-world, Scale-free and Beyond. *IEEE Circuits Syst. Mag.* **2003**, *3*, 6–20. [CrossRef]
54. Cenek, E.W. Review of Modern Graph Theory by Béla Bollobás. *ACM SIGACT News* **2000**, *31*, 15–18. [CrossRef]
55. Wolthusen, S.D. GIS-based Command and Control Infrastructure for Critical Infrastructure Protection. In Proceedings of the 1st IEEE International Workshop on Critical Infrastructure Protection (IEEE), Darmstadt, Germany, 3–4 November 2005; pp. 40–47.
56. Ristvej, J.; Sokolova, L.; Strakacova, J.; Ondrejka, R.; Lacinak, M. Experiences with Implementation of Information Systems within Preparation to Deal with Crisis Situations in Terms of Crisis Management and Building Resilience in the Slovak Republic. In Proceedings of the International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, 23–26 October 2017. [CrossRef]
57. UNISRD. *Sendai Framework for Disaster Risk Reduction 2015–2030*; United Nations International Strategy for Disaster Reduction: Geneva, Switzerland, 2015.
58. IEC 31010:2019. *Risk Management–Risk Assessment Techniques*; International Organization for Standardization: Geneva, Switzerland, 2009.
59. Luskova, M.; Dvorak, T. Applying Risk Management Process in Critical Infrastructure Protection. *Interdiscip. Descr. Complex Syst. INDECS* **2019**, *17*, 7–12. [CrossRef]
60. Bialas, A. Risk Management in Critical Infrastructure—Foundation for Its Sustainable Work. *Sustainability* **2016**, *8*, 240. [CrossRef]
61. Lovecek, T.; Ristvej, J. Quantitative Assessment Parameters of the Protection Level of National Strategic Sites in the EU. *WIT Trans. Inf. Commun. Technol.* **2010**, *43*, 69–80. [CrossRef]
62. Boehm, B.W.; DeMarco, T. Software Risk Management. *IEEE Softw.* **1997**, *14*, 17–19. [CrossRef]
63. Zanicka Holla, K.; Ristvej, J.; Simak, L. Systematic Method of Risk Assessment in Industrial Processes. *WIT Trans. Inf. Commun. Technol.* **2010**, *43*, 115–126. [CrossRef]
64. Aagedal, J.O.; Braber, F.; Dimitrakos, T.; Gran, B.A.; Raptis, D.; Stolen, K. Model-based Risk Assessment to Improve Enterprise Security. In Proceedings of the 6th International Enterprise Distributed Object Computing Conference (EDOC), IEEE Computer Society, Lausanne, Switzerland, 15–18 December 2003. [CrossRef]
65. Leontief, W.W. *Input-Output Economics*; Oxford University Press: New York, NY, USA, 1986.
66. Setola, R.; De Porcellinis, S.; Sforna, M. Critical Infrastructure Dependency Assessment Using the Input–output Inoperability Model. *Int. J. Crit. Inf. Prot.* **2009**, *2*, 170–178. [CrossRef]
67. Jiwei, L.; Kang, T.; Kong, R.T.L.; Soon, S.M. Modelling Critical Infrastructure Network Interdependencies and Failure. *Int. J. Crit. Inf.* **2019**, *15*, 1–23. [CrossRef]
68. Rehak, D.; Senovsky, P.; Hromada, M.; Lovecek, T.; Novotny, P. Cascading Impact Assessment in a Critical Infrastructure System. *Int. J. Crit. Inf. Prot.* **2018**, *22*, 125–138. [CrossRef]
69. Barabasi, A.L. *Linked: The New Science of Networks*; Perseus Books Group: New York, NY, USA, 2002.
70. Holden, R.; Val, D.; Burkhard, R.; Nodwel, S.C. A Network Flow Model for Interdependent Infrastructures at the Local Scale. *Saf. Sci.* **2013**, *53*, 51–60. [CrossRef]
71. Johansson, J.; Hassel, H.; Cedergren, A. Vulnerability Analysis of Interdependent Critical Infrastructures: Case Study of the Swedish Railway System. *Int. J. Crit. Inf.* **2011**, *7*, 289–316. [CrossRef]
72. Setola, R.; Rosato, V.; Kyriakides, E.; Rome, E. *Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach*; Springer: Basel, Switzerland, 2017.
73. Gao, J.; Barzel, B.; Barabasi, A.L. Universal Resilience Patterns in Complex Networks. *Nature* **2016**, *530*, 307–312. [CrossRef] [PubMed]
74. Blokus, A.; Dziula, P. Safety Analysis of Interdependent Critical Infrastructure Networks. *Int. J. Mar. Navig. Saf. Sea Transp.* **2019**, *13*, 781–787. [CrossRef]
75. Bil, M.; Sedonik, J.; Kubecek, J.; Vodak, R.; Biova, M.; Andrasik, R. Road Networks Segments at Risk–Vulnerability Analysis and Natural Hazards Assessment. *Sci. Popul. Prot.* **2014**, *6*, 37–54.
76. Chanas, S.; Zielinski, P. Critical Path Analysis in the Network with Fuzzy Activity Times. *Fuzzy Sets Syst.* **2001**, *122*, 195–204. [CrossRef]

77. Collection of Laws of the Czech Republic. Act No. 240/2000 Coll., on Crisis Management and on Amendments to Certain Acts, as Amended. 2000. Available online: https://ec.europa.eu/echo/sites/echo-site/files/240_2000_crisis_management_act.pdf (accessed on 18 March 2020).
78. Novotny, P.; Rostek, P. Perspective of Cross-Cutting Criteria as a Major Instrument to Determination of Critical Infrastructure in the Czech Republic. In Proceedings of the 9th International Doctoral Seminar, The University of Zielona Gora, Zielona Gora, Poland, 19–21 May 2014; pp. 141–148.
79. Taquechel, E.F.; Lewis, T.G. How to Quantify Deterrence and Reduce Critical Infrastructure Risk. *Homel. Secur. Aff.* **2012**, *8*, 12.
80. Brown, K.A. *Critical Path: A Brief History of Critical Infrastructure Protection in the United States*; Spectrum Publishing Group: Washington, DC, USA, 2006.
81. Fotr, J.; Vacik, E.; Soucek, I.; Spacek, M.; Hajek, S. *Strategy Creation and Strategic Planning: Theory and Practice*; Grada Publishing: Prague, Czech Republic, 2012.
82. Hundt, C.; Sternberg, R. Explaining New Firm Creation in Europe from a Spatial and Time Perspective: A Multilevel Analysis Based upon Data of Individuals, Regions and Countries. *Pap. Reg. Sci.* **2014**, *95*, 223–257. [CrossRef]
83. Brown, C.; Milke, M.; Seville, E. *Discussion Paper: Should Waste Management Be Considered a Lifeline in New Zealand?* Resilient Organisations: Christchurch, New Zealand, 2010.
84. Egan, M.J. Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like Systems. *J. Conting. Crisis Manag.* **2007**, *15*, 4–17. [CrossRef]
85. Rostov, W.W. *The Process of Economic Growth*; Oxford University Press: London, UK, 1960.
86. Rosenfeld, P.; Culbertson, A.; Magnusson, P. *Human Needs: A Literature Review and Cognitive Life Span Model*; Navy Personnel Research and Development Center: San Diego, CA, USA, 1992.
87. Maslow, A.H. A Theory of Human Motivation. *Psychol. Rev.* **1943**, *50*, 370. [CrossRef]
88. Rakowski, N. *Maslow's Hierarchy of Needs Model–the Difference of the Chinese and the Western Pyramid on the Example of Purchasing Luxurious Products*; GRIN Academic Publishing: Munich, Germany, 2008.
89. Nesporova, V.; Dopaterova, M.; Slivkova, S.; Novotny, P.; Rehak, D. Approaches to Critical Elements Evaluation in the Territory on the Basis of Human Basic Needs. In Proceedings of the 25th International Conference on the Fire Protection, Association of Fire and Safety Engineering, Ostrava, Czech Republic, 5–7 October 2016; pp. 311–314.
90. Senovsky, M.; Adamec, V.; Senovsky, P. *Critical Infrastructure Protection*; Association of Fire and Safety Engineering: Ostrava, Czech Republic, 2007.
91. *Interim Report on the August 14, 2003: Blackout Report*; Independent System Operator (NYISO): New York, NY, USA, 2004.
92. Meijers, E.J.; Burger, M.J.; Hoogerbrugge, M.M. Borrowing Size in Networks of Cities: City Size, Network Connectivity and Metropolitan Functions in Europe. *Pap. Reg. Sci.* **2015**, *95*, 181–198. [CrossRef]
93. Ramprasad, A. On the Definition of Feedback. *Behav. Sci.* **1983**, *28*, 4–13. [CrossRef]
94. *Czech Office for Surveying, Mapping and Cadastre*; Czech Office for Surveying: Prague, Czech Republic, 2016.
95. *The Geographic Base Data of the Czech Republic*; Administration of Cadastre of Real Estate: Prague, Czech Republic, 2017.
96. Dvorak, Z.; Svetenkova, E.; Rehak, D.; Cekerevac, Z. Assessment of Critical Infrastructure Elements in Transport, 10th International Scientific Conference Transbaltica 2017: Transportation Science and Technology. *Procedia Eng.* **2017**, *187*, 548–555. [CrossRef]
97. Ministry of Transport of the Czech Republic. *Results of the National Census on the Motorway and Road Networks of the Czech Republic 2016*; Ministry of Transport of the Czech Republic: Prague, Czech Republic, 2017.
98. Transport Research Centre. *Single Transport Vector Map*; Transport Research Centre: Brno, Czech Republic, 2017.
99. Costing Asset Protection: An All-Hazards Guide for Transportation Agencies (CAPTA). *National Academies of Sciences, Engineering, and Medicine*; The National Academies Press: Washington, DC, USA, 2009. [CrossRef]
100. *Finding the Average Occupancy Rate and Purpose of Vehicle Ways on Selected Road and Motorway Networks of the Czech Republic in 2005 and 2006*; SBP Consult: Prague, Czech Republic, 2006.