sustainability

MDPI

Article

Strengthening the Sustainability of Energy Critical Entities Through a Business Continuity Management System

David Rehak [1,*], Martin Hromada [2], Simona Jemelkova [1], Lenka Brumarova [1] and Ivo Haring [3]

[1] Faculty of Safety Engineering, VSB—Technical University of Ostrava, 70030 Ostrava, Czech Republic
[2] Faculty of Applied Informatics, Tomas Bata University in Zlin, 76005 Zlin, Czech Republic
[3] Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, EMI, 79104 Freiburg, Germany
* Correspondence: david.rehak@vsb.cz; Tel.: +420-597-322-816

Abstract: Energy supply is currently considered a key area that is essential for the functioning of the entire society, remaining one of the most fundamental sectors of critical infrastructure worldwide. However, the functionality of energy systems is threatened by a number of threats from various areas, such as natural influences, technological threats, terrorism, and even state-supported organized attacks. For this reason, there is an active effort by all interested parties to achieve a sufficient resilience and sustainability level of these systems. Currently, various tools are used for this purpose, the essence of which is to ensure the preparedness of energy systems. Primarily, basic dependable systems aspects are applied according to the planning documentation and according to the N-1 principle from the transmission system code. These tools are functional and very proven in practice. However, the sprawling threat landscape and the COVID-19 pandemic have shown that the use of individual, separate tools may not comprehensively cover the entire area of preparedness, especially for unexpected events or expected events of unexpected dimensions. To address this challenge, the article takes up the professional abstract recommendation of ensuring the preparedness of the entire system comprehensively, i.e., by involving all possible tools, knowledge, and resources that the critical entity has. It proposes and tailors a Business Continuity Management System (BCMS) for the energy domain. The approach covers the entire management system of the organization, in which it establishes, implements, operates, monitors, reviews, maintains, and improves the continuity of activities in terms of key energy system functions. The aim is to ensure the sustainability of the functionality of the given systems within acceptable ranges. The article presents the targeted BCMS targets, building blocks, and representative implementation methods and tools. It is argued that the proposal is ready for application in the specific area of energy critical entities and systems by providing examples of partial implementation.

Keywords: energy; energy critical entity; sustainability; business continuity; BCMS; critical infrastructure protection; tailoring and implementation

Academic Editors: Bowen Zhou and Firoz Alam

Received: 12 February 2025
Revised: 12 March 2025
Accepted: 18 March 2025
Published: 20 March 2025

Citation: Rehak, D.; Hromada, M.; Jemelkova, S.; Brumarova, L.; Haring, I. Strengthening the Sustainability of Energy Critical Entities Through a Business Continuity Management System. *Sustainability* **2025**, *17*, 2766. https://doi.org/10.3390/su17062766

1. Introduction

Energy is one of the most important industries that is essential for the functioning of society. For this reason, the European Directive was adopted in 2008 [1], on the basis of which selected energy systems were identified as critical infrastructure elements. It was subsequently necessary to ensure a sufficient resilience level for these elements, i.e., "*the ability to reduce the magnitude and/or duration of disruptive events*" [2]. In the long term, however, it is necessary to ensure not only the required resilience level for critical energy

systems, but also their sustainability. For this reason, energy sustainability is one of the priority objectives of the European Union [3].

The energy organizational–technical systems under consideration are public or private entities that own or operate critical infrastructures according to the Directive [4] in the energy domain. Similar definitions can be found worldwide [5]. A sufficient resilience level of energy critical entities is one of the important prerequisites for the long-term sustainability of critical energy systems [6].

The sustainability of critical energy systems is currently philosophically based on general approaches to sustainability. In principle, the three pillars of sustainability are reflected in the organization's context, i.e., social, economic, and environmental [7]. Within these three pillars, effective technologies and practices, such as smart grids, energy-efficient buildings, and industrial processes, are being implemented to support the sustainability of critical energy systems [8].

Sustainability is understood in the sense that key energy system performance functions or key performance indicators [9] are also provided in case of adverse events stemming from different domains, including in particular the properties and capabilities of the energy systems to protect the environment and climate [10] and related assessments and preparedness [11], even if sustainability is increasingly used in the sense of being resilient [12,13].

In the context of the specifics of critical energy systems, their sustainability is also strengthened through the application of the classical N-1 Criterion principle [14], which ensures the redundancy of the energy infrastructure. This criterion ensures that a system that is able to withstand an unexpected failure of one component of the system at any time has an acceptable reliability level. The sustainability of critical energy systems is also appropriately ensured through emergency preparedness [15], or short-term resilience [16]. Specifically, this involves the implementation of procedures from crisis plans, emergency plans, and critical entities' crisis preparedness plans.

In parallel with these measures, management approaches can also be used to support the sustainability of critical energy systems, but they are more oriented towards the energy critical entities' resilience. The core management approach of a general nature is the risk analysis and management-generic ISO 31000 family, including recommended methods [17–19]. By managing risks, critical entities minimize the likelihood of the disruption or failure of critical energy systems, thereby supporting their sustainability. This approach is often reinforced by the implementation of related domain-specific management systems, such as quality management [20], environmental management [21], organizational resilience [22], crisis management [23], or business continuity management [24].

The generic concept of risk as advocated by Kaplan and Garrick [25] and Schoppe et al. [26] and implemented in the ISO 31000 framework standards [27] has been often challenged [28] but has greatly advanced and evolved [29,30], notably including the clarification of terminology [31] and refinement of the definition of risk [32] and its ontological–epistemological nature [33], and is by now a proven tool for increasingly domain-specific practitioners in risk management [34].

ISO 31000 has a flexible applicability as a working framework for improving critical energy infrastructure protection by adopting its five-step scheme, for instance, by using lightweight semi-quantification [35] and nested tabular approaches [36], as well as the energy sector-specific adaptations of ISO 31000, e.g., to gas networks [37], electricity grids [38], the oil industry [39], offshore wind energy production [40], and to photovoltaic, biogas, and hydro power generation [41]. Therefore, the generic risk analysis and management standard ISO 31000 is well suited as an abstract framework for the sustainability management objectives of critical infrastructure energy systems. The above reviewed examples of the specific risk analysis and management applications of ISO 31000 are primarily intended for

the effective and safe management of organizations' socio-technical systems and businesses regarding civil security and safety threats. However, this strongly hints that ISO 31000 can also address, either in addition to or jointly, the risks on the sustainability objectives of energy systems within similar adaptations of ISO 31000.

A more detailed analysis shows that risk management is mainly applied within the framework of energy system security [42,43]. However, risk management in the context of energy critical entities is given significantly less attention. Most approaches have long been oriented generally at the level of organization risk management [44–46]. In this context, the most appropriate management approach is the Business Continuity Management System [24], which allows for increased organizational resilience to disruptive incidents, reduced financial losses, and improved reputation and credibility with customers. It is also worth mentioning that there are other approaches in the field of business management, but they are more oriented towards strengthening the market potential of energy entities through technological innovations [47–50]. Based on these facts, the aim of this article is to present the possibilities of using a BCMS to strengthen the energy critical entities' sustainability.

The current work aims to go beyond sample applications of facets of continuity management and the BCMS to the energy sector. For instance, in Kohl [51], BCMS approaches are reviewed from a general perspective only but are not applied to critical infrastructure sectors. Kosmowski et al. [52] focus on cyber security and safety continuity management in the energy sector. An application of a management system for business continuity for the oil sector is given in Golebiewski and Kosmowski [53] and for energy supply at a community level in Brattgard [54].

After the motivation of the application of the BCMS concept to ensure sustainability in a broad sense for energy systems in Section 1, Section 2 further investigates the domain of applications and further facets and gaps of the BCMS approach to be considered. Based on this, Section 3 presents a structured BCMS approach tailored to the energy sector to ensure the sustainability of its functions, services, and key properties, culminating in an implementation process proposed. Section 4 critically summarizes the approach and proposes further steps.

2. Materials and Methods

The essence of this part of the article is to define two key thematic areas on which the achievement of the article's goal is based. For this reason, first, the definitions of critical energy systems and energy critical entities that own or operate these systems are given. Subsequently, the definition of a Business Continuity Management System is given, which can be used to strengthen the sustainability of energy critical entities.

2.1. Definition of Energy Critical Entities

Critical energy systems are energy systems that have been designated as critical infrastructure. They are therefore facilities that are significant for the provision of essential services. An essential service in this context means "*a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment*" [4]. Within the European Union, critical energy systems are classified into five subsectors, i.e., electricity, district heating and cooling, oil, gas, and hydrogen.

Since 2022, owners and operators of the above-mentioned critical energy systems have been designated as critical entities. When determining energy critical entities, the results of the risk assessment must be taken into account and the following criteria (C) must be applied [4]:

(C1) the energy entity provides one or more essential services;

(C2) the energy entity operates in the territory of a European Member State and its critical infrastructure is located there;
(C3) the incident would significantly disrupt the provision of one or more essential services of the energy entity or of another critical entity that is dependent on the supply of those essential services.

2.1.1. Categories of Energy Critical Entities

Based on the results of the risk assessment and the application of the above criteria, energy critical entities are currently being gradually identified within the EU Member States. These entities are classified into five categories (CECs) in the context of the above subsectors:

(CEC1) The first category is energy critical entities falling within the electricity subsector. Specifically, these are electricity companies, distribution system operators, transmission system operators, and producers [55].
(CEC2) The second category is energy critical entities falling into the district heating and cooling subsector. These entities include operators of heat and cooling production facilities and operators of their distribution facilities [56].
(CEC3) The third category consists of energy critical entities falling within the oil subsector. In this case, these are oil pipeline operators, operators of oil extraction, refining and processing facilities, operators of storage and transmission facilities, and central stock managers within the meaning of the Council Directive [57].
(CEC4) The fourth category is energy critical entities falling into the gas subsector. Specifically, these are distribution system operators, transmission system operators, storage system operators, LNG facility operators, gas companies, and operators of natural gas refining and processing facilities [58].
(CEC5) The fifth category is energy critical entities falling into the hydrogen subsector. In this case, these are operators of hydrogen production, storage, and transportation [4].

2.1.2. Basic Tools and Measures for Energy Critical Entities

In accordance with the Directive [4], designated critical entities must adopt appropriate and proportionate technical, security, and organizational measures to ensure their resilience. This resilience is subsequently defined as the "*ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident*"; see, e.g., for similar definitions [59]; for more abstract definitions, see, e.g., Mentges et al. [60]. It is now possible to measure the energy critical entities' resilience level and identify weaknesses based on the results [9,61].

In the case of energy critical entities, publications are already available presenting tools suitable for strengthening the resilience of these weak points [6]. One of the important groups of these tools is the category of process tools, which include, for example, Integrated Management Systems [62] or Business Continuity Management Systems [24]. A significant benefit of this group of tools, especially BCMS, is that they can be used not only in the short term, but also in the context of ensuring the long-term sustainability of energy critical entities [63,64].

2.2. Definition of Business Continuity Management System

To successfully manage an unexpected event or crisis, effective preparation of the entire entity is always necessary. Since it is impossible to know in advance the exact nature of the event or crisis (timing, place of occurrence, speed of development, or more detailed specifications), it is necessary to keep all responsible persons and necessary resources in a state of readiness for action at all times [65]. Ultimately, however, this always assumes

that all necessary organizational, personnel, material, and infrastructural prerequisites are prepared, in operation, and constantly maintained so that it is possible to act optimally and to be structured, if necessary, even in the long term [66]. The unexpected dimensions of a crisis often also require a number of other abilities and skills, such as improvisation, flexibility, creativity, adaptability, and decisiveness [67].

2.2.1. Background of Business Continuity Management System

The crisis preparedness of an organization, including an energy critical entity, is mostly understood as an internal matter, especially in relation to addressing internal organizational risks [67]. In the context of current requirements and the security situation, however, there is a need to perceive the entity's crisis preparedness in a more comprehensive way, namely, as a set of organizational, methodological, and material–technical measures, most often carried out by the entity's management in accordance with applicable legal standards, the entity's crisis plan, and the current state of the entity's crisis environment [68].

The importance of implementing risk management and business continuity is an often-mentioned element of organizational governance. The Sendai Framework [69] declares that entities need to integrate disaster risk management, including business continuity, into business processes through disaster risk-informed investments. Tools supporting Territorial Risk Analysis and Mapping play a significant role in this area, for example [70].

Nowadays, every organization is exposed to risks from both the internal environment (e.g., personnel or process risks) and the external environment (e.g., natural disasters or cyber-attacks). In order to respond to these risks correctly and effectively, it is necessary to have an effective risk management system in place [71]. The Business Continuity Management System is one of the latest risk management frameworks that enables organizations to improve their resilience to effectively cope with identified risks [72]. The comprehensive implementation of risk management and continuity management throughout the entire company structure helps to effectively respond to crises and thus ensures the smooth operation and competitiveness of the company [73].

The high rate of negative incidents occurring worldwide encourages organizations and entities to design and implement their own customized business continuity management system, in many cases based on BCMS [74]. According to Sahebjamnia et al. [75], the goal is always to prepare for any potential disruption to the provided function. Through the implementation of a BCMS, an organization or entity will obtain appropriate Business Continuity Plans (BCP) that will enable it to respond effectively and efficiently to potential incidents or crisis situations [76].

2.2.2. Perception and Grasping of Business Continuity Management System

A Business Continuity Management System is that part of the overall management system of an organization or entity that establishes, implements, operates, monitors, reviews, maintains, and improves the continuity of activities [24]. It is an organization's Business Continuity Management System that includes the organizational structure, policies, planning activities, responsibilities, practices, procedures, processes, and resources to achieve the organization's stated objectives. Business continuity is understood as the strategic and tactical capability of an organization in terms of preparing for and responding to incidents and disruptions to restore operations to a predetermined level.

Business continuity management (BCM) forms part of supply chain risk management and is an important competitive factor for companies by ensuring the smooth functioning of critical business processes in the event of a failure [72]. BCM refers to a set of principles, policies, and tools to support organizations in maintaining their critical business processes [77]. This is a systemic procedure aimed at guaranteeing the continuous functioning

of the entity in the event of unforeseen disruptions or crises [78]. BCM is a strategic process that seeks to identify and assess potential risks, formulate comprehensive plans to mitigate these risks, and maintain the smooth functioning and operational efficiency of an entity during periods of disruption [79]. BCM practices enable organizations to remain resilient and robust [80]. BCM increases the organization's resilience, as it can help maintain the entity's essential services and also ensures planned resumption of operations if necessary and in a degraded mode [81].

Interest in business continuity is growing. This is evidenced by the upward trend in research publications on the topic of continuity. This fact is demonstrated, for example, in an article by Sadeghi [82]. The global COVID-19 pandemic has provided practical evidence of the need for a system that ensures business continuity even during extraordinary negative incidents. It has caused unprecedented disruption to communities and organizations around the world [83,84]. In addition, the COVID-19 pandemic has affected the readiness of organizations regarding the maturity of organizations' available BCMS operations [85].

Organizations realize that without business continuity plans, the consequences can lead to the loss of profit at best and, at worst, complete business closure [84,86]. The study of Fani and Subriadi [87] shows that organizations with a Business Continuity Plan have a better chance of ensuring business continuity. However, each organization has different methods and approaches to creating a BCP.

Another concept that can motivate managers to implement a BCM in their organizations is asset management [88]. The main objective of this standard is to prepare an organization for effective asset management. However, a key topic that remains unexplored in the field of asset management is how an organization manages its assets during incidents. It is in this regard that incident response planning, risk management, and business continuity plans can help an organization in an effective and efficient manner [89].

From the research conducted, it can be deduced that it is possible to work with a BCMS in a way that makes it helpful in any industry or corporate environment [90]. The relevancy of a BCMS to counter the negative impacts of various disruptions also applies to the energy sector [91]. Johnstone and Kivimaa [92] point to the need and willingness to embrace disruptions regarding innovations in the energy sector. These linkages concern both the technology itself and the organizational aspects from the perspective of corporate governance. However, in the present article, we continue to show that disruption management for energy systems by tailoring the BCMS approach is promising for the energy sector. The result is a positive push for effective industrial policy and continuity, which can better manage and help manage unexpected incidents.

3. Results

The following text presents the implementation of the Business Continuity Management System to the critical entity environment in the energy sector. The implementation process and the management of the continuity of the energy critical entity itself are specified in more detail. Strategies for the continuity and recovery of processes and strategies for securing key resources are supplemented. A basic manual for creating a Business Continuity Plan is also outlined. The conceptual framework for the implementation of a BCMS into an energy critical entity environment is presented in Figure 1.

A description of the individual phases of BCMS implementation into the environment of an energy critical entity is provided in the following text.

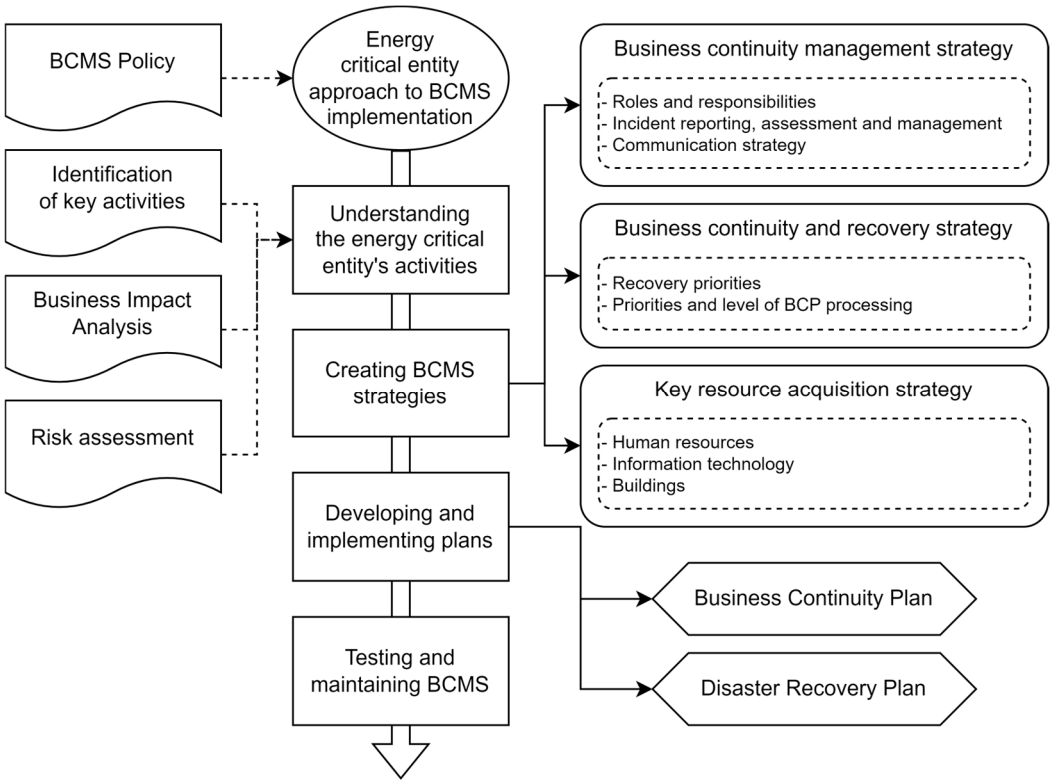

Figure 1. Conceptual framework for implementation of a Business Continuity Management System.

3.1. Energy Critical Entity Approach to BCMS Implementation

The business continuity management system is always implemented within the energy critical entity environment based on a management decision, as also confirmed by Johnstone and Kivimaa [92]. The BCMS is based on the BCMS Policy document. The BCMS Policy provides a framework for setting the entity's business continuity objectives and includes a commitment to meet the relevant requirements. The energy critical entity implements and operates the BCMS in accordance with the recommendations of the standard [24] and includes four basic phases, which are based on the principle of the Deming cycle [93]:

(P1) Understanding the energy critical entity's activities;
(P2) Creating BCMS strategies;
(P3) Developing and implementing plans;
(P4) Testing and maintaining BCMS.

To establish, implement, operate, monitor, maintain, and improve the BCMS, the energy critical entity uses a process approach, again according to ISO 22301 [24]. A continuous improvement approach is applied to all phases of the BCMS.

3.1.1. Understanding the Energy Critical Entity's Activities

Within the analytical activities of this phase, key process domains, processes, and activities are identified that enable the energy critical entity to meet business objectives. At the same time, the impacts of the disruption/interruption of individual processes on the entity and their development over time are assessed. With regard to the magnitude of the impacts, priorities for the restoration of disrupted processes are determined. The correct setting of objectives and restoration priorities is very beneficial for the entity [82].

This phase of BCMS implementation also includes identifying threats that may cause process disruptions. Where effective and beneficial, appropriate measures are implemented to cover the identified threats. To ensure the effective analysis of the impact of an energy critical entity disruption over time, it is appropriate to use the Business Impact Analysis [94].

Another essential activity is risk assessment. This step is a fundamental to gain an overview of which risks are a priority for a given organizational unit [95,96]. Both internal and external risks are assessed. The basic risk assessment may be followed by the determination of various scenarios of anticipated incidents.

The outputs and evaluation of this phase are subject to regular annual review. At the same time, any significant change in the organization of an energy critical entity, e.g., the introduction of a new service or the launch of a new application, must be accompanied by a review of the outputs of this BCMS phase.

3.1.2. Creating BCMS Strategies

The outputs from the analysis phase, i.e., understanding the energy critical entity's activities, are important for creating effective BCMS strategies. The strategies set the entity's approach to implementing and operating the established BCMS, setting roles and responsibilities, securing the necessary resources, setting up communication about the incident, etc.

3.1.3. Developing and Implementing Plans

In the event of an incident, business continuity plans are developed to support the provision of activities within individual process domains or within the organizational units of an energy critical entity.

Plans are developed as a priority for process domains where the greatest impacts in the event of a disruption of activities were identified during the analytical work. The BCP must ensure that in the event of an incident, the activities of the organizational unit are restored within the RTO (i.e., Recovery Time Objective), which is determined within the framework of the Business Impact Analysis (BIA). The RTO represents the time frame for restoring disrupted activities to a specified minimum acceptable level [97]. Each BCP also lists the key applications that support the processes and activities being performed. Well-established processes strongly focus on restoring key products or services [98,99], similar to keeping systemic performance functions within acceptable limits in case of resilience engineering for critical infrastructures; see, e.g., Haring et al. [9].

Another planning document used to quickly restore the system to normal operation is the Disaster Recovery Plan (DRP). It focuses on restoring the functionality of the system after a disaster.

3.1.4. Testing and Maintaining BCMS

Regular tests of plans, which applies to both BCP and DRP, are held periodically at set intervals. Specific dates are determined for the organizational unit by its guarantor. Plans must also be updated whenever significant changes occur within the energy critical entity that may affect the recovery procedures. In addition to regular tests of plans, a review of contact information in individual plans (telephone directories, supplier contacts, service departments, etc.) must be performed at least once every 6 months.

The scope and complexity of the planned tests must increase over time. Planned testing (applicable to both the BCP and DRP testing of individual applications) is classified into three levels:

(T1) The simplest type of test is a plan completeness check, which includes a theoretical review of the completeness of the information contained in the plans.

(T2) The second level of test is a theoretical walkthrough of the plan, i.e., a plan completeness check extended by a theoretical review of specific recovery procedures, and verification of knowledge of the roles of individual team members and their mutual communication.

(T3) The last level is simulation tests, i.e., the practice and verification of individual procedures and team interactions according to pre-prepared scenarios [100–102].

The updating process is not limited to the plans themselves, but also includes regular reviews of strategies, considering the periodic repetition of impact analysis and risk assessment. Given the constantly evolving environment, it is also appropriate to consider some possible elements of BCM improvement [72].

3.2. Business Continuity Management Strategy

The purpose of business continuity management strategies (BCMS strategies) is to identify the requirements and needs for ensuring the continuity and recovery of energy critical entity processes in the event of their disruption or interruption. In the event of incidents, the key functions of the energy critical entity will be maintained, or they will be restored to the required level and at the times identified in the BIA.

Strategies approved by management are subsequently developed into plans and procedures for ensuring continuity and processes recovery. The strategies also include decisions on taking measures to address identified risks that may interrupt or limit the activities of an energy critical entity. In practice, individual adjustments and different approaches to the details of BCP processing are common [87].

3.2.1. Initial Assumptions

The business continuity management strategies of an energy critical entity are based on ensuring the continuity and key process recovery domains and processes within the RTO times as determined in the BIA and approved by the entity's management.

The performance of processes within the main process domains depends on the functioning of other (supporting) process domains and on the key resources provision, such as employees, information and communication technologies, and buildings. The requirements for continuity and supporting processes recovery are based on the requirements for securing resources for the main processes.

Therefore, in order for the approved strategies to be implemented, the energy critical entity employees must participate in the preparation of appropriate plans and, in the event of an incident, in the implementation of the recovery procedures described in the appropriate plans. Appropriate resources, i.e., human, material, technical, information, and financial, must also be provided [65]. The continuity management strategy is approved by the energy critical entity's management [68].

3.2.2. Roles and Responsibilities

The energy critical entity's Chief Executive Officer (CEO) has primary responsibility for establishing, implementing, operating, monitoring, maintaining, and improving the BCMS and overall incident preparedness [68]. To ensure an effective and efficient BCMS, additional tasks are assigned to individual persons. These tasks relate to all levels of entity management, i.e., from BMC managers, through guarantors of given sections, through specific resolvers, to individual employees. The tasks are primarily focused on preparation, documentation processing, training, testing, management, and established cooperation in resolving the incident.

A Crisis Team is established in the company to resolve incidents. The usual composition of the team includes a team leader, his or her deputy, a BCP coordinator, and other members of the crisis team, e.g., representatives of information technology, building management, and physical security. To ensure the effectiveness of crisis teams [103], their structure can be classified into three management levels, which are described in more detail

in Figure 2, which can be seen as confirmation of best practices for the energy sector; see, e.g., Hiles [104].

Management levels	Description
Bronze (operational) level	Crisis team at the organizational unit level of the energy critical entity, which ensures the first response to the incident, i.e. assessment and reporting. It also implements the first steps to ensure business continuity, the first steps to recover, informing higher management and basic communication and coordination.
Silver (tactical) level	Crisis management at the energy critical entity CEO level. This group comes into play in cases of larger-scale incidents. Crisis management is provided here by the CEO in cooperation with the BCM manager. Recovery activities are managed and coordinated in accordance with BCP procedures. The group is also a communication channel between the bronze and gold levels.
Gold (strategic) level	Top management of the energy critical entity (deputies, CEO). This group is activated in the case of the most serious incidents. It determines the priorities for resolution and provides additional necessary resources, beyond the competences of the silver level.

Figure 2. Classification of crisis teams for energy systems by management level.

3.2.3. Incident Reporting, Assessment, and Management

Each employee reports all incidents to their superior. Reporting is performed up to the level corresponding to the Crisis Team Leader for the organizational unit. The Crisis Team Leader performs an initial assessment. Based on the classification of the incident into the appropriate level (see Figure 3), he or she activates the relevant part of the BCP. The Crisis Team Leader primarily protects the health and lives of employees and proceeds in accordance with the rules of fire protection, OHS, and the local evacuation plan. Subsequently, the Crisis Team Leader manages the restoration of processes according to the developed BCP.

Incident levels	Event type / Impact
1	Shorter outages of key energy systems (usually hours to units of days), limited operation of the building / workplace (usually hours to units of days), absence of employees (usually approx. 30% of employees).
2	Outages of key energy systems (usually units of days), limited operation of the building / workplace (usually units of days), absence of employees (usually approx. 60% of employees).
3	Outages of key energy systems (usually units of days to weeks), limited operation of the building / workplace (usually weeks), absence of employees (usually approx. 80-90% of employees).
4	Failure of all key energy systems, destruction of the headquarters building, virus epidemics with an impact on the entire entity, resulting in the outage of the entire organizational unit, long-term outages of key applications, etc.

Figure 3. Classification of energy critical entity incidents by event/impact type.

The type of event may be different for different organizational units and may indicate a different level of incident. For example, in some cases, an incident of a key system failure will be indicated in the order of hours, in other processes in the order of days. Defining incidents and indication levels should be performed individually in each BCP according to the results of the BIA [94].

3.2.4. Communication Strategy

A communication strategy serves to establish procedures, methods, and ways/channels for sharing information between internal and external stakeholders during an incident [105]. Reporting and providing information to all interested parties (i.e., owners, employees, regulators, IRS units, family members, etc.) about an incident is governed by established procedures that need to be included in an internal order.

The company's spokesperson is responsible for communication with the public and the media. Apart from the spokesperson, no one else is allowed to communicate with the media or to provide information about the situation—employees always refer to the company's spokesperson.

3.3. Business Continuity and Recovery Strategy

The continuity and recovery strategy for process domains and processes results from the requirements for their recovery, determined within the framework of the BIA. As a result of an incident, multiple processes can be disrupted simultaneously; it is therefore important to set priorities for their recovery already at the planning stage [106].

3.3.1. Recovery Priorities

Priorities for ensuring the processes recovery and activities are set in the BCP created at the level of the organizational unit or process domain. Specific BCPs determine the priority of individual activities, especially in cases of critical employee absence or outages of key applications [86].

The parameter that determines the requirement for the speed of process recovery in the event of an interruption is the Recovery Time Objective (RTO). This is the time period in which it is possible and effective to restore the functionality of an interrupted process (by activities performed within the process domain or organizational unit). When setting the RTO of processes, the maximum acceptable process downtime is considered.

3.3.2. Priorities and Level of BCP Processing

BCPs are processed as a priority for the most critical process domains. At various levels of detail, BCPs must be processed at the level of all process domains/organizational units.

For process domains with low recovery priority (1 week or more), the BCP can be processed to a minimum extent—composition of the crisis team, incident reporting, communication strategy, contact details. Priorities for maintaining/restoring activities are determined by the Crisis Team only at the moment of the incident.

3.4. Key Resource Acquisition Strategy

Internal and external resources are used to ensure continuity and key processes recovery. To meet the requirements for process availability in the event of an incident, it is necessary to ensure the availability of human, informational, technical, material, and financial resources [107]. Proper allocation of these resources is also essential [108].

Specific resource requirements that are important for ensuring process continuity and recovery are identified in the BIA. In the vast majority of processes, the most important resources from the perspective of process operation and continuity are operational applications and employees.

3.4.1. Human Resources

Employees, their skills, and their expertise are the most valuable asset of an energy critical entity. The staffing requirements for processes within individual process domains are mapped in detail within the framework of the BIA reviews and are kept up to date.

Detailed information on the requirements for human resources (standard and minimum numbers), important for ensuring the continuity and recovery of activities, is provided in the BCP. In the case of incidents with an impact on human resources (e.g., epidemics, mass accidents, or building fires), the BCP sets the priorities and level of performance of activities within the process domain or organizational unit [109].

The BCP also includes options for employees to work from home, or their willingness to temporarily relocate to an alternative location. The requirements for employees in resolv-

ing and eliminating the consequences of incidents are specified in the BCP or determined by crisis team leaders.

3.4.2. Information Technology

The dependence of energy critical entities on information technology and operational applications (ICT/OCT) is very significant [110]. In the vast majority of process domains, the failure of key applications of ICT/OCT will cause a disruption/interruption of activities. The disruption of activities in key applications is not limited to just one organizational unit but can affect a large part of the energy critical entity's functioning.

The options for alternative methods of performing activities when key applications are unavailable are very limited, ineffective, and in many cases completely impossible. The performance of activities when applications are unavailable is described in detail in the organizational unit's BCP. In the event of an incident, the restoration of application availability is fully within the competence of the Information Technology Services Department.

3.4.3. Buildings

The entity's processes are implemented at headquarters, regional branches, or business locations, which are significant assets of process domains/organizational units. The implementation of the BCMS in combination with asset management [88] allows energy critical entities to be prepared for effective asset management during incidents. This mainly concerns ensuring the availability of assets in the appropriate quantity and quality required to manage specific incidents.

The list of buildings is kept up-to-date in a separate document. The performance of processes within individual process domains and organizational units does not have to be significantly dependent on a specific workplace. In the event of the unavailability of one of the organizational units (e.g., due to a fire), the performance of activities can be ensured in the form of working from home or a substitute organizational unit. There can be several reasons for the unavailability of organizational units, and they are mainly due to their geographical location [82].

A replacement organizational unit is usually established in another facility of the entity, often by preparing a replacement organizational unit in a matter of hours (installation of computer equipment, connectivity to IT systems, etc.). A specific option for ensuring activities in the event of the unavailability of the primary location is always specified in the BCP.

3.5. Manual for Creating BCP

The following text is a basic guide to creating the BCP and is divided into two parts, namely, Generation and Review, Updating, and Monitoring.

3.5.1. Generation

Most of the recommended parts of the BCP have already been mentioned in the text above. Creating the BCP is a lengthy process and requires the involvement of well-selected affected employees, including the entity's management [92]. The following core persons are proposed: responsible representatives of general management, financial management, technical management, and the operational management of energy systems, persons responsible for key performance functions as identified in the BCP as well as experienced practitioners and stakeholders representative of service users. It is advisable to form a group of people who will be responsible for creating the BCP. They can then cooperate/consult with other employees of the energy critical entity on individual parts of the plan.

At the beginning of the manual creation, it is appropriate to create a general structure that will respect the continuity of the individual steps (chapters) of the BCP. During the

actual creation, it is then necessary to respect these connections. The outline of the BCP is not clearly defined in advance, but in the case of energy critical entities, it is appropriate for the BCP to contain the parts presented in Figure 4.

BCP structure	Description
Title page	Contains basic identification data of the organizational unit of the energy critical entity (e.g. address, management, basic presentation of the function).
Introduction, context, and system definition	Contains a description of the organizational unit of the energy critical entity and assumptions and instructions for using the plan. System is defined in terms of internal and external boundaries.
System functions, services, and capabilities	Lists the key energy system performance or non-performance functions that should be kept within acceptable limits, e.g. percentage households not served over critical time.
Recovery priorities	This section is a summary of the basic functions of the given organizational unit, with emphasis on those priority functions that are to be ensured by the plan. This assessment is based on an understanding of the activities of the given organizational unit.
Analysis of the impacts of possible incidents	This part of the plan contains the results of the Business Impact Analysis.
Risk assessment, incident scenarios, and ranking	This step is a fundamental step to gain an overview of which risks are a priority for a given organizational unit. Both internal and external risks are assessed. The basic risk assessment may be followed by the determination of various scenarios of anticipated incidents.
Crisis teams and recovery teams	This section presents the staffing of unified crisis teams, or also teams that will be created to achieve effective recovery (recovery team). Their powers and responsibilities are also listed for individual persons, primarily with regard to further procedures.
Incident reporting and declaring crisis states	Contains a set procedure by which the entire incident is identified and monitored, from the initial reporting of the incident to determining individual states and their assessment.
Incident management	A specific procedure for individual steps leading to the management, control and management of the incident, with regard to the established powers and prepared resources.
Crisis communication	Contains basic aspects of communication between affected persons, other entities, the media, etc.
Recovery plans	They represent a summary of the basic elements to achieve recovery according to individual scenarios.
Contacts	Overview of current contacts for people affected by the plan.
Crisis team locations	Specification of the crisis team location.

Figure 4. Recommended Business Continuity Plan structure for energy critical entities.

3.5.2. Review, Updating, and Monitoring

The created BCP then needs to be assessed. The primary assessment is the suitability, adequacy, and effectiveness of the impact analysis, risk assessment, solution strategies, and, ultimately, the entire plan. The assessment is carried out using reviews, analyses, exercises, tests, incident reports, etc. The assessment is carried out at planned intervals, after an incident, after activation, or when significant changes to the plan occur. Testing is also an important part of the effort to improve the effectiveness of the plans [72].

4. Conclusions

The importance of the energy sector is undeniably very high because energy has long been the primary sector of critical infrastructure. However, even this sector is not immune to incidents that can cause the failure of the provided services. Such failures

often lead to the limitation of basic functions of society and industry. Hence, the long-term efforts of the affected energy critical entities to eliminate such negative impacts, or also the effort to quickly and effectively restore the disrupted functions, are evident. Currently, a comprehensive approach to the overall entity's resilience analysis and management to control overall risk is often used in this regard.

One of the tools that can significantly contribute to strengthening this resilience management by ensuring the continuity and business relevancy contextualization of the provided energy functions is the BCMS. It is systematically focused on the sustainability of the functionality of the given systems. This work showed that its application is also possible in the specific environment of energy critical entities. We discussed why a BCMS and business continuity in general are a possible appropriate management framing to ensure the advanced overall risk control and resilience generation of socio-technical energy entities of the transitioning energy supply sector. It was seen that the analytical–engineering core of the assessment can be defined to form risk and resilience analysis, quantification, and improvement.

The article presented the following basic aspects of the implementation of the BCMS in the environment of a critical entity in the energy sector based on exploring the application domain and the concepts, aims, and approaches summarized as the BCMS: (i) the critical energy entity's approach to implementing the BCMS, (ii) the energy critical entity's business continuity management strategy, (iii) the process continuity and recovery strategy, (iv) the key resource provision strategy, and (v) the manual for creating a Business Continuity Plan. This article showed how existing best practices can be tailored and amended for the energy sector for each of these proposed steps.

Energy BCMS plans are beneficial for various levels of energy critical entity management. Primarily, these are people in the top level of the energy critical entity's management (i.e., deputies and executive director), including the BCM manager and the security manager. Other important subjects are all responsible persons who may be affected by the continuity objectives and the Business Continuity Plan. These are mainly heads of organizational units and other key employees. The article provides all these persons with a basic overview of the key aspects for ensuring business continuity according to the BCMS.

The introduction of a Business Continuity Management System into the environment of energy critical entities can bring a number of advantages and benefits. Thanks to the BIA, the commonly used classic risk assessment is supplemented with an impact analysis from the perspective of business objectives. This way, the key elements, domains, processes, or people of the entity are better and more comprehensively identified and perceived. The strategies created will also help these entities respond better to an incident or negative event. The continuity management strategy provides clear roles and responsibilities in the event of an incident, clear procedures for reporting and managing the event, and also a uniform and effective communication style. The process recovery strategy identifies recovery priorities and recovery requirements. The key resource strategy provides a comprehensive list of necessary commodities. Last but not least, the BCP clearly and effectively summarizes all the basic aspects needed to ensure continuity goals.

The article is conceived in a general way, considering the wide variability of organizational units of energy critical entities. This general level may be perceived as a certain deficiency that may discourage responsible managers from implementing a BCMS in the environment of an energy critical entity. However, the different specifications of individual organizational units do not allow further research at this level. It is possible to apply separate research to the specific conditions of individual energy organizational units in the future. This should always be focused on a specific organizational unit and thus reflect its

unique environment and specifications. Such research will be very individual and specific. However, this research will also be based on the basic aspects presented in this article.

Author Contributions: Conceptualization, D.R. and M.H.; methodology, D.R. and M.H.; formal analysis, D.R., M.H., and I.H.; investigation, S.J. and L.B.; resources, D.R. and I.H.; data curation, M.H.; writing—original draft preparation, D.R., M.H., S.J., L.B., and I.H.; writing—review and editing, D.R., M.H., S.J., L.B., and I.H.; visualization, D.R.; supervision, M.H.; project administration, D.R.; funding acquisition, D.R. 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 VK01030014.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data and information are available in this article.

Conflicts of Interest: The authors declare no conflicts 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.

Abbreviations

The following abbreviations are used in this manuscript:

BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CEO	Chief Executive Officer
DRP	Disaster Recovery Plan
ICT/OCT	Information Technology and Operational Applications
IRS	Integrated Rescue System
LNG	Liquefied Natural Gas
OHS	Occupational Health and Safety
RTO	Recovery Time Objective

References

1. Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. Available online: https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng (accessed on 30 January 2025).
2. National Infrastructure Advisory Council. *Critical Infrastructure Resilience Final Report and Recommendations*; U.S. Department of Homeland Security: Washington, DC, USA, 2009.
3. European Union. *Investing in a Sustainable Energy Future for Europe*; Directorate-General for Communication: Brussels, Belgium, 2024.
4. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC. Available online: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng (accessed on 31 January 2025).
5. Smith, K.; Wilson, I.D. Critical Infrastructures: A Comparison of Definitions. *Int. J. Crit. Infrastruct.* **2023**, *19*, 323–339. [CrossRef]
6. Rehak, D.; Slivkova, S.; Janeckova, H.; Stuberova, D.; Hromada, M. Strengthening Resilience in the Energy Critical Infrastructure: Methodological Overview. *Energies* **2022**, *15*, 5276. [CrossRef]
7. Purvis, B.; Mao, Y.; Robinson, D. Three Pillars of Sustainability: In Search of Conceptual Origins. *Sustain. Sci.* **2019**, *14*, 681–695. [CrossRef]
8. Muniz, R.N.; da Costa Junior, C.T.; Buratto, W.G.; Nied, A.; Gonzalez, G.V. The Sustainability Concept: A Review Focusing on Energy. *Sustainability* **2023**, *15*, 14049. [CrossRef]
9. Haring, I.; Schafer, J.; Vogelbacher, G.; Fischer, K.; Riedel, W.; Faist, K. From event to performance function-based resilience analysis and improvement processes for more sustainable systems. *Int. J. Sustain. Mater. Struct. Syst.* **2021**, *5*, 90–120. [CrossRef]

10. Elkhatat, A.; Al-Muhtaseb, S. Climate Change and Energy Security: A Comparative Analysis of the Role of Energy Policies in Advancing Environmental Sustainability. *Energies* **2024**, *17*, 3179. [CrossRef]
11. Krebs, H.A.; Hagenweiler, P. *Energy Resilience and Climate Protection*; Springer Fachmedien: Wiesbaden, Germany, 2022.
12. Mohanty, A.; Ramasamy, A.K.; Verayiah, R.; Bastia, S.; Dash, S.S.; Cuce, E.; Khan, T.M.Y.; Soudagar, M.E.M. Power system resilience and strategies for a sustainable infrastructure: A review. *Alex. Eng. J.* **2024**, *105*, 261–279. [CrossRef]
13. Lotfi, R.; Kargar, B.; Hoseini, S.H.; Nazari, S.; Safavi, S.; Weber, G.W. Resilience and sustainable supply chain network design by considering renewable energy. *Int. J. Energy Res.* **2021**, *45*, 17749–17766. [CrossRef]
14. Ovaere, M.; Proost, S. Optimal Electricity Transmission Reliability: Going Beyond the N-1 Criterion. *Energy J.* **2018**, *39*, 211–234. [CrossRef]
15. Philpott, D. *Emergency Preparedness: A Safety Planning Guide for People, Property and Business Continuity*, 2nd ed.; Bernan Press: Blue Ridge Summit, PA, USA, 2016.
16. Younesi, A.; Shayeghi, H.; Wang, Z.; Siano, P.; Mehrizi-Sani, A.; Safari, A. Trends in modern power systems resilience: State-of-the-art review. *Renew. Sustain. Energy Rev.* **2022**, *162*, 112397. [CrossRef]
17. *ISO 31000*; Risk Management. International Organization for Standardization: Geneva, Switzerland, 2018.
18. *IEC 31010*; Risk Management—Risk Assessment Techniques. International Organization for Standardization: Geneva, Switzerland, 2019.
19. *ISO/TS 31050*; Risk Management—Guidelines for Managing an Emerging Risk to Enhance Resilience. International Organization for Standardization: Geneva, Switzerland, 2023.
20. *ISO 9001*; Quality Management Systems. International Organization for Standardization: Geneva, Switzerland, 2015.
21. *ISO 14001*; Environmental Management Systems. International Organization for Standardization: Geneva, Switzerland, 2015.
22. *ISO 22316*; Security and Resilience—Organizational Resilience—Principles and Attributes. International Organization for Standardization: Geneva, Switzerland, 2017.
23. *ISO 22361*; Security and Resilience—Crisis Management. International Organization for Standardization: Geneva, Switzerland, 2022.
24. *ISO 22301*; Security and Resilience—Business Continuity Management Systems. International Organization for Standardization: Geneva, Switzerland, 2019.
25. Kaplan, S.; Garrick, B.J. On The Quantitative Definition of Risk. *Risk Anal.* **1981**, *1*, 11–27. [CrossRef]
26. Schoppe, C.A.; Haring, I.; Siebold, U. Semi-formal modeling of risk management process and application to chance management and monitoring. In *Safety, Reliability and Risk Analysis: Beyond the Horizon, Proceedings of the European Safety and Reliability Conference (ESREL 2013)*; Steenbergen, R.D.J.M., van Gelder, P.H.A.J.M., Miraglia, S., Vrouwenvelder, A.C.W.M., Eds.; CRC Press: Boca Raton, FL, USA, 2013.
27. Leitch, M. ISO 31000:2009—The new international standard on risk management. *Risk Anal.* **2010**, *30*, 887–892. [CrossRef]
28. Lalonde, C.; Boiral, O. Managing risks through ISO 31000: A critical analysis. *Risk Manag.* **2012**, *14*, 272–300. [CrossRef]
29. Olechowski, A.; Oehmen, J.; Seering, W.; Ben-Daya, M. The professionalization of risk management: What role can the ISO 31000 risk management principles play? *Int. J. Proj. Manag.* **2016**, *34*, 1568–1578. [CrossRef]
30. Selvaseelan, J. Development and Introduction of the Risk-Sentience Auxiliary Framework (RSAF) as an Enabler to the ISO 31000 and ISO 31010 for High-Risk Environments. *Adm. Sci.* **2018**, *8*, 22. [CrossRef]
31. Aven, T. On the new ISO guide on risk management terminology. *Reliab. Eng. Syst. Saf.* **2011**, *96*, 719–726. [CrossRef]
32. Aven, T.; Renn, O.; Rosa, E.A. On the ontological status of the concept of risk. *Saf. Sci.* **2011**, *49*, 1074–1079. [CrossRef]
33. Ylonen, M.; Aven, T. A framework for understanding risk based on the concepts of ontology and epistemology. *J. Risk Res.* **2023**, *26*, 581–593. [CrossRef]
34. Widianti, T.; Firdaus, H.; Rakhmawati, T. Mapping the landscape: A bibliometric analysis of ISO 31000. *Int. J. Qual. Reliab. Manag.* **2024**, *41*, 1783–1810. [CrossRef]
35. Haring, I.; Ebenhoch, S.; Stolz, A. Quantifying Resilience for Resilience Engineering of Socio Technical Systems. *Eur. J. Secur. Res.* **2016**, *1*, 21–58. [CrossRef]
36. Haring, I.; Fehling-Kaschek, M.; Miller, N.; Faist, K.; Ganter, S.; Srivastava, K.; Jain, A.K.; Fischer, G.; Fischer, K.; Finger, J.; et al. A performance-based tabular approach for joint systematic improvement of risk control and resilience applied to telecommunication grid, gas network, and ultrasound localization system. *Environ. Syst. Decis.* **2021**, *41*, 286–329. [CrossRef]
37. Ganter, S.; Finger, J.; Haring, I. Gas network modelling to support pipeline hub area risk assessment study. In *Advances in Modelling to Improve Network Resilience*; European Commission: Brussels, Belgium, 2022; pp. 159–162. [CrossRef]
38. Setiawan, A.B.; Syamsudin, A.; Sasongko, A. Implementation of Secure Smart Grid as Critical Information Infrastructure in Indonesia: A Case Study in Smart Grid Electricity. In *4th International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec)*; Institute of Electrical and Electronics Engineers: New York, NY, USA, 2015; pp. 34–39. [CrossRef]
39. Sepp-Neves, A.A.; Pinardi, N.; Martins, F.; Janeiro, J.; Samaras, A.; Zodiatis, G.; De Dominicis, M. Towards a common oil spill risk assessment framework—Adapting ISO 31000 and addressing uncertainties. *J. Environ. Manag.* **2015**, *159*, 158–168. [CrossRef] [PubMed]

40. Kopke, C.; Mielniczek, J.; Roller, C.; Lange, K.; Torres, F.S.; Stolz, A. Resilience management processes in the offshore wind industry: Schematization and application to an export-cable attack. *Environ. Syst. Decis.* **2023**, *43*, 161–177. [CrossRef]
41. Ibrahim, N.A.; Alwi, S.R.W.; Manan, Z.A.; Mustaffa, A.A.; Kidam, K. Risk matrix approach of extreme temperature and precipitation for renewable energy systems in Malaysia. *Energy* **2022**, *254 Pt C*, 124471. [CrossRef]
42. Gorzen-Mitka, I.; Wieczorek-Kosmala, M. Mapping the Energy Sector from a Risk Management Research Perspective: A Bibliometric and Scientific Approach. *Energies* **2023**, *16*, 2024. [CrossRef]
43. Potemina, D.; Ryakhovskaya, A.N. Risk Management in Energy Companies. *Bus. Strateg.* **2020**, *8*, 271–274. [CrossRef]
44. Eichholz, J.; Hoffmann, N.; Schwering, A. The role of risk management orientation and the planning function of budgeting in enhancing organizational resilience and its effect on competitive advantages during times of crises. *J. Manag. Control* **2024**, *35*, 17–58. [CrossRef]
45. Bockius, H.; Gatzert, N. Organizational risk culture: A literature review on dimensions, assessment, value relevance, and improvement levers. *Eur. Manag. J.* **2024**, *42*, 539–564. [CrossRef]
46. Nyenno, I.; Selivanova, N.; Korolenko, N.; Truba, V. The energy policy risk management system model: Theories and practices. *Energy Policy J.* **2020**, *23*, 33–48. [CrossRef]
47. Ben Khaled, M.W.; Ouertani Abaoub, N. Energy Sector Evolution: Perspectives on Energy Platforms and Energy Transition. *Platforms* **2024**, *2*, 68–83. [CrossRef]
48. Gitelman, L.; Kozhevnikov, M. New Business Models in the Energy Sector in the Context of Revolutionary Transformations. *Sustainability* **2023**, *15*, 3604. [CrossRef]
49. Chasin, F.; Paukstadt, U.; Gollhardt, T.; Becker, J. Smart energy driven business model innovation: An analysis of existing business models and implications for business model change in the energy sector. *J. Clean. Prod.* **2020**, *269*, 122083. [CrossRef]
50. Hall, S.; Roelich, K. Business model innovation in electricity supply markets: The role of complex value in the United Kingdom. *Energy Policy* **2016**, *92*, 286–298. [CrossRef]
51. Kohl, H. Generic Standards for Management Systems: An Overview. In *Standards for Management Systems. Management for Professionals*; Kohl, H., Ed.; Springer: Cham, Germany, 2020; pp. 19–249. [CrossRef]
52. Kosmowski, K.T.; Piesik, E.; Piesik, J.; Sliwinski, M. Integrated Functional Safety and Cybersecurity Evaluation in a Framework for Business Continuity Management. *Energies* **2022**, *15*, 3610. [CrossRef]
53. Golebiewski, D.; Kosmowski, K. Towards a process based management system for oil port infrastructure in context of insurance. *J. Pol. Saf. Reliab. Assoc.* **2017**, *8*, 23–38.
54. Brattgard, N. *Community Continuity Management: An Exploration of the Energy Production and Use of a Fictional Stockholm Neighbourhood in a Crisis (Dissertation)*; KTH Royal Institute of Technology: Stockholm, Sweden, 2023.
55. Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on Common Rules for the Internal Market for Electricity and Amending Directive 2012/27/EU. Available online: http://data.europa.eu/eli/dir/2019/944/oj (accessed on 17 March 2025).
56. Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the Promotion of the Use of Energy from Renewable Sources. Available online: https://eur-lex.europa.eu/eli/dir/2018/2001/oj/eng (accessed on 17 March 2025).
57. Council Directive 2009/119/EC of 14 September 2009 Imposing an Obligation on Member States to Maintain Minimum Stocks of Crude Oil and/or Petroleum Products. Available online: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32009L0119 (accessed on 17 March 2025).
58. Directive (EU) 2024/1788 of the European Parliament and of the Council of 13 June 2024 on Common Rules for the Internal Markets for Renewable Gas, Natural Gas and Hydrogen, Amending Directive (EU) 2023/1791 and Repealing Directive 2009/73/EC. Available online: http://data.europa.eu/eli/dir/2024/1788/oj (accessed on 17 March 2025).
59. Thoma, K.; Scharte, B.; Hiller, D.; Leismann, T. Resilience Engineering as Part of Security Research. Definitions, Concepts and Science Approaches. *Eur. J. Secur. Res.* **2016**, *1*, 3–19. [CrossRef]
60. Mentges, A.; Halekotte, L.; Schneider, M.; Demmer, T.; Lichte, D. A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. *Int. J. Disaster Risk Reduct.* **2023**, *96*, 103893. [CrossRef]
61. Rehak, D.; Splichalova, A.; Janeckova, H.; Oulehlova, A.; Hromada, M.; Kontogeorgos, M.; Ristvej, J. Critical Entities Resilience Assessment (CERA) to Small-Scale Disasters. *Int. J. Disaster Risk Reduct.* **2024**, *111*, 104748. [CrossRef]
62. Bugdol, M.; Jedynak, P. *Integrated Management Systems*; Springer: Cham, Germany, 2015. [CrossRef]
63. Simmonds, S. Sustainability Through Business Continuity Management. 2015. Available online: https://www.linkedin.com/pulse/sustainability-through-business-continuity-management-simmonds (accessed on 6 December 2024).
64. Moskova, E.; Buganova, K. Improving Business Sustainability by Connecting Business Continuity Management and Risk Management. *WSB J. Bus. Financ.* **2023**, *57*, 38–45. [CrossRef]
65. Phelps, R. *Crisis Management: How to Develop a Powerful Program*; Chandi Media: San Francisco, CA, USA, 2018.

66. Fritzen, B.; Hummel, S.; Schmidt, J. *TB 09-01 Leitfaden Krisenmanagement für Behörden und Unternehmen*; Vfdb: Münster, Germany, 2021.
67. SIUS Consulting. Leitfaden und Tipps zum Krisenmanagement. 2025. Available online: https://www.krisenmanagement.de/leitfaden-tipps-krisenmanagement (accessed on 17 March 2025).
68. Thiessen, A. *Handbuch Krisenmanagement*; Springer Fachmedien Wiesbaden: Wiesbaden, Germany, 2014.
69. UNISDR. *Sendai Framework for Disaster Risk Reduction 2015–2030*; United Nations Office for Disaster Risk Reduction: Geneva, Switzerland, 2015.
70. Bernatik, A.; Senovsky, P.; Senovsky, M.; Rehak, D. Territorial Risk Analysis and Mapping. *Chem. Eng. Trans.* **2013**, *31*, 79–84. [CrossRef]
71. Torabi, S.A.; Giahi, R.; Sahebjamnia, N. An Enhanced Risk Assessment Framework for Business Continuity Management Systems. *Saf. Sci.* **2016**, *89*, 201–218. [CrossRef]
72. Schätter, F.; Hansen, O.; Wiens, M.; Schultmann, F. A Decision Support Methodology for a Disaster-Caused Business Continuity Management. *Decis. Support Syst.* **2019**, *118*, 10–20. [CrossRef]
73. Buganova, K.; Moskova, E.; Simickova, J. Increasing the Resilience of Transport Enterprises through the Implementation of Risk Management and Continuity Management. *Transp. Res. Procedia* **2020**, *55*, 1522–1529. [CrossRef]
74. Azadegan, A.; Parast, M.M.; Lucianetti, L.; Nishant, R.; Blackhurst, J. Supply Chain Disruptions and Business Continuity: An Empirical Assessment. *Decis. Sci.* **2020**, *51*, 38–73. [CrossRef]
75. Sahebjamnia, N.; Torabi, S.; Mansouri, S. Integrated Business Continuity and Disaster Recovery Planning: Towards Organizational Resilience. *Eur. J. Oper. Res.* **2015**, *242*, 261–273. [CrossRef]
76. Malachova, H.; Oulehlova, A. Application of Business Continuity Management System into the Crisis Management Field. *Trans. VSB—Tech. Univ. Ostrav. Saf. Eng. Ser.* **2016**, *11*, 43–50. [CrossRef]
77. Peck, H. *Resilience in the Food Chain: A Study of Business Continuity Management in the Food and Drink Industry*; Cranfield University: Bedford, UK, 2006.
78. Carracedo, P.; Puertas, R.; Marti, L. Research lines on the impact of the COVID-19 pandemic on business. A text mining analysis. *J. Bus. Res.* **2021**, *132*, 586–593. [CrossRef]
79. Ambarwati, R.; Dijaya, R.; Anshory, I. A multi-method study of risk assessment and human risk control for power plant business continuity in Indonesia. *Results Eng.* **2024**, *21*, 101863. [CrossRef]
80. Ali, Q.S.A.; Hanafiah, M.H.; Mogindol, S.H. Systematic literature review of Business Continuity Management (BCM) practices: Integrating organisational resilience and performance in Small and Medium Enterprises (SMEs) BCM framework. *Int. J. Disaster Risk Reduct.* **2023**, *99*, 104135. [CrossRef]
81. Bhamra, R.; Dani, S.; Burnard, K. Resilience: The concept, a literature review and future directions. *Int. J. Prod. Res.* **2011**, *49*, 5375–5393. [CrossRef]
82. Sadeghi, N. Continuity of small businesses when facing increased flood risk due to global climate change impacts: A systematic literature review. *Int. J. Disaster Risk Reduct.* **2022**, *82*, 103316. [CrossRef]
83. Schmid, B.; Raju, E.; Jensen, P.K.M. COVID-19 and business continuity—Learning from the private sector and humanitarian actors in Kenya. *Prog. Disaster Sci.* **2021**, *11*, 100181. [CrossRef]
84. Frikha, G.; Lamine, E.; Kamissoko, D.; Benaben, F.; Pingaud, H. Toward a Modeling Tool for Business Continuity Management. *IFAC-Pap.* **2020**, *54*, 1156–1161. [CrossRef]
85. Russo, N.; Reis, L.; Silveira, C.; Mamede, H.S. Towards a Comprehensive Framework for the Multidisciplinary Evaluation of Organizational Maturity on Business Continuity Program Management: A Systematic Literature Review. *Inf. Secur. J. Glob. Perspect.* **2024**, *33*, 54–72. [CrossRef]
86. Faertes, D. Reliability of Supply Chains and Business Continuity Management. *Procedia Comput. Sci.* **2014**, *55*, 1400–1409. [CrossRef]
87. Fani, S.V.; Subriadi, A.P. Business Continuity Plan: Examining of Multi-Usable Framework. *Procedia Comput. Sci.* **2018**, *161*, 275–282. [CrossRef]
88. *ISO 55000*; Asset Management—Vocabulary, Overview and Principles. International Organization for Standardization: Geneva, Switzerland, 2024.
89. Rabbani, M.; Soufi, H.R.; Torabi, S. Developing a two-step fuzzy cost–benefit analysis for strategies to continuity management and disaster recovery. *Saf. Sci.* **2016**, *85*, 9–22. [CrossRef]
90. Russo, N.; São Mamede, H.; Reis, L.; Silveira, C. FAMMO^{CN}—Demonstration and evaluation of a framework for the multidisciplinary assessment of organisational maturity on business continuity. *Heliyon* **2022**, *8*, e10566. [CrossRef]
91. Ketsopoulou, I.; Taylor, P.; Watson, J. Disruption and continuity in energy systems: Evidence and policy implications. *Energy Policy* **2021**, *149*, 111907. [CrossRef]
92. Johnstone, P.; Kivimaa, P. Multiple dimensions of disruption, energy transitions and industrial policy. *Energy Res. Soc. Sci.* **2018**, *37*, 260–265. [CrossRef]

93. Swamidass, P.M. Deming Cycle (PDCA). In *Encyclopedia of Production and Manufacturing Management*; Springer: Boston, MA, USA, 2000. [CrossRef]
94. *ISO 22317*; Security and Resilience—Business Continuity Management Systems—Guidelines for Business Impact Analysis. International Organization for Standardization: Geneva, Switzerland, 2021.
95. Rehak, D.; Danihelka, P.; Bernatik, A. Criteria Risk Analysis of Facilities for Electricity Generation and Transmission. In *Safety, Reliability and Risk Analysis: Beyond the Horizon (ESREL 2013)*; CRC Press: Boca Raton, FL, USA, 2014; pp. 2073–2080.
96. Rehak, D.; Senovsky, P. Preference Risk Assessment of Electric Power Critical Infrastructure. *Chem. Eng. Trans.* **2014**, *36*, 469–474. [CrossRef]
97. Broder, J.F.; Tucker, E. *Risk Analysis and the Security Survey*, 4th ed.; Butterworth-Heinemann: Oxford, UK, USA, 2012. [CrossRef]
98. Torabi, S.A.; Rezaei, S.H.; Sahebjamnia, N. A new framework for business impact analysis in business continuity management (with a case study). *Saf. Sci.* **2014**, *68*, 309–323. [CrossRef]
99. Bouloiz, H. Sustainable performance management using resilience engineering. *Int. J. Eng. Bus. Manag.* **2020**, *12*, 184797902097620. [CrossRef]
100. Lovecek, T.; Strakova, L.; Kampova, K. Modeling and Simulation as Tools to Increase the Protection of Critical Infrastructure and the Sustainability of the Provision of Essential Needs of Citizens. *Sustainability* **2021**, *13*, 5898. [CrossRef]
101. Oulehlova, A.; Malachova, H.; Kinc, P.; Navratil, J. Simulated Exercise—"Gale" Crisis Scenario. In Proceedings of the 28th International Business Information Management Association Conference—Vision 2020: Innovation Management, Development Sustainability, and Competitive Economic Growth, Seville, Spain, 9–10 November 2016; Volume I–VII, pp. 3867–3876.
102. Ristvej, J.; Zagorecki, A.; Holla, K.; Simak, L.; Titko, M. Modelling, Simulation and Information Systems as a Tool to Support Decision-Making Process in Crisis Management. In Proceedings of the European Simulation and Modelling Conference (ESM 2013), Lancaster, UK, 23–25 October 2013; pp. 71–76.
103. King, G. Crisis Management & Team Effectiveness: A Closer Examination. *J. Bus. Ethics* **2002**, *41*, 235–249. [CrossRef]
104. Hiles, A. *Business Continuity Management. Global Best Practices*, 4th ed.; Rothstein Associates: Brookfield, CT, USA, 2014.
105. Savolainen, R. Information Sharing and Knowledge Sharing as Communicative Activities. *Inf. Res.* **2017**, *22*, 9.
106. Zorn, C.R.; Shamseldin, A.Y. Post-disaster Infrastructure Restoration: A Comparison of Events for Future Planning. *Int. J. Disaster Risk Reduct.* **2015**, *13*, 158–166. [CrossRef]
107. Mohan, P.S. Disasters, Disaster Preparedness and Post Disaster Recovery: Evidence from Caribbean firms. *Int. J. Disaster Risk Reduct.* **2023**, *92*, 103731. [CrossRef]
108. Zhang, C.; Kong, J.J.; Simonovic, S.P. Restoration Resource Allocation Model for Enhancing Resilience of Interdependent Infrastructure Systems. *Saf. Sci.* **2018**, *102*, 169–177. [CrossRef]
109. Proag, V. Human Resources Management for Infrastructure. In *Infrastructure Planning and Management: An Integrated Approach*; Springer: Cham, Germany, 2021; pp. 563–593. [CrossRef]
110. Swathika, G.O.V.; Karthikeyan, A.; Karthikeyan, K.; Sanjeevikumar, P.; Thomas, S.K.; Babu, A. Critical review of SCADA and PLC in smart buildings and energy sector. *Energy Rep.* **2024**, *12*, 1518–1530. [CrossRef]