infrastructures

MDPI

Article

Framework for Operational Resilience Management of Critical Infrastructures and Organizations

Daniel Lichte [1,*], Frank Sill Torres [2] and Evelin Engler [3]

[1] Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center, 53757 Sankt Augustin, Germany
[2] Institute for the Protection of Maritime Infrastructures, German Aerospace Center, 27572 Bremerhaven, Germany; frank.silltorres@dlr.de
[3] Institute of Communication and Navigation, German Aerospace Center, 17235 Neustrelitz, Germany; evelin.engler@dlr.de
* Correspondence: daniel.lichte@dlr.de

Abstract: Progressing digitalization and networking of systems and organizations representing Critical Infrastructures opens promising new potentials and opportunities, which on the downside, are accompanied by rising complexity and increasingly opaque interdependencies. The consequently increasing lack of knowledge leads to uncertainties affecting risk assessment and decision-making in case of adverse events. This trend motivated recent discussions and developments in risk science, emphasizing the need to handle such uncertainties. Complementarily, research in the resilience domain focuses on system capabilities to handle surprising hazardous situations. Several frameworks presented in the literature aim at combining both perspectives but either lack the focus on operational management, have a rather theoretical approach, or are designed for specific applications. Based on this observation, we propose an approach that integrates resilience management into the actual operation of Critical Infrastructure Systems and Organizations by providing an operational process that coordinates the fundamental resilience capabilities of responding, monitoring, anticipation, and learning. Furthermore, we tackle the challenge of uncertainties resulting from a lack of knowledge by aligning the concepts of digital twin and resilience management. The proposed framework is extensively discussed, and required processes are presented in detail. Eventually, its applicability and potential are reviewed by means of a complex hazardous situation at a Bavarian district heating power plant.

Keywords: resilience; risk; resilience management; digital twin; uncertainties; operational framework

Citation: Lichte, D.; Torres, F.S.; Engler, E. Framework for Operational Resilience Management of Critical Infrastructures and Organizations. *Infrastructures* **2022**, *7*, 70. https://doi.org/10.3390/infrastructures7050070

Academic Editors: José Campos e Matos and David Lattanzi

Received: 19 March 2022
Accepted: 28 April 2022
Published: 6 May 2022

1. Introduction

Modern societies critically rely on the supply of a variety of goods and services, such as energy and government. Most societies agree on a similar set of these goods and services to be defined as critical for societal and economic well-being [1]. Thus, the infrastructures responsible for the provision of such goods and services are identified as Critical Infrastructures (CI). Correspondingly, such infrastructures are found in different sectors of modern societies, e.g., energy or water supply, governmental institutions, or security and defense authorities [2]. Consequently, CI cannot be assigned to a specific type of system or organization. In general, the various Critical Infrastructure Systems and Organizations (CISOs) serve to securely provide the variety of critical goods and services mentioned above [3,4].

Due to its nature, it is of utmost importance to provide solutions that enable such CISOs to deal with corresponding risks and vulnerabilities. The International Organization for Standardization (ISO) defines risk as the effect of uncertainty on goals [5]. The Society of Risk Analysis (SRA) has developed a more comprehensive definition to give more attention to the diversity of uncertainties and objectives [6,7]. Risk concepts are now

addressed in all areas of a CI, for example in commercial sector [8,9], chemical sector [10,11], public health [12,13], transportation [14–17], information technology [18,19] and water systems sector [20,21]. The examples also illustrate the great variety of risk assessment and risk management approaches developed to analyze and manage risk. Therefore, it is not surprising that in the last decade, a risk science has emerged and established, which deals with the development of ge**n**eric concepts, theories, principles, methods, frameworks, procedures, and models to enhance the understanding, assessment, modelling, controlling and management of risks [7,22–24]. This development has been even more promoted by the ongoing digitization of organizations and the increasing interconnectedness of technical and socio-technical systems. Increasing complexity and growing interdependencies lead, in addition to other things, to uncertainties in the modeling, understanding, and assessment of risks [7,11,12,23–26]. It is now undisputed that uncertainties reflect the knowledge or lack of knowledge in risk analysis. Therefore, the amount of uncertainty consequently determines the informative value of the risk assessment result that should be communicated to decision-makers. Uncertainty assessment and its consideration in risk-related decision-making are current fields of research and development becoming even more important due to the COVID-19 pandemic [23,24,26–28].

In recent decades, a complementary line of development has emerged that results from the rising interest in the concept of resilience. It focuses on practicable approaches that enable the effective handling of surprises originating from uncertainties induced by lacking knowledge about interdependencies, changes, and prospects [29–31]. Analogous to risk science, research activities were either dedicated to fundamental questions, such as the definition, characteristics, concepts, and cornerstones of resilience [30–34], or aimed at providing methods and frameworks for analyzing or managing resilience [33,35–42]. The wide variety of fields of application and perspectives in which resilience in socio-technical systems is considered has led to different definitions. For example, the European Commission defines resilience as the "ability of an individual, a household, a community, a country or a region to withstand, to adapt, and to quickly recover from stresses and shocks" [43], reflecting a rather societal view. In contrast, the International Maritime Organisation (IMO) took a more technological view on resilience and defined it as the "ability of a system to detect and compensate external and internal disturbances, malfunction and breakdowns in parts of the system", preferably without loss of functionalities and any degradation of their performance [44]. Woods proposed that the label "resilience" shall be reserved for the ability of a system to deal with disturbances and interruptions outside the range of the nominal system capabilities and nominal use conditions [45]. Hollnagel defined resilience as "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances so that it can sustain required operations under both expected and unexpected conditions" [42]. In parallel, academic discussions started on whether resilience analysis and management should be seen as an extension of risk analysis and management or as an integral part of it [29,46,47]. However, a unifying goal of risk and resilience science is to ensure the operationality and reliability of vital Critical Infrastructure Systems and Organizations (CISO) regardless of whether the focus is rather on preventing or averting adverse events and consequences. To achieve this goal effectively and effi**c**iently, the close relationship between risk and resilience strategies in their many forms must be tapped, coordinated, and exploited [29]. For this, it is also necessary to consider all aspects of the CISO whose resilience is to be consolidated or increased. Häring et al. provided a framework and principles for generic resilience management that was derived from the standardized risk management process [38]. Within this framework, they identified nine iterative steps that enable resilience quantification and development. Additionally, the authors provided a comparison of several resilience assessment methods. The authors put high emphasis on analyses and decisions during system design, while process steps during operation are unified in a single process responsible for monitoring and review. In addition, a variety of resilience frameworks have been developed in recent years that focus on either the analysis [33,35,37,41,48–50], assessment [51–53], or

management [36,40] of resilience, or a combination thereof [39]. The solution approaches are often discussed rather theoretically at the algorithm and method level [33,52] or in the application context [35–37,39,42,48–51,53–56].

Driven by Hollnagel's ability-oriented definition of the resilience concept, this paper introduces a framework for the operational management of the resilience capabilities of Critical Infrastructure Systems and Organizations (CISO). To the best of our knowledge, this is the first framework for operational resilience management that integrates the concept of digital twins and, thus, allows for the comprehensive and timely preparation and response to emerging threats.

The remainder of this work is organized as follows. Section 2 briefly presents background information on concepts and cornerstones related to resilience and specifies the requirements for operational resilience management. Section 3 introduces the proposed operational resilience management framework and its main components. The following Section 4 presents and discusses in detail the tasks within the proposed operational resilience management process. Section 5 provides application examples to illustrate the advantages of this approach, and Section 6 concludes this work.

2. Background

2.1. Challenge

Hollnagel identified four cornerstones that are essential for the resilience of a CISO [32]: The first is the ability to respond to permanent as well as sudden onset disruptions, disturbance, and changes.

The second is the ability to monitor both the system state, including technical and human components and the environmental conditions in which the system operates, in particular dynamic changes in performance demand. This enables the detection of realizing hazards and the identification of emerging threats. The third is the ability to anticipate positive as well as negative developments to protect the system's performance and to search for new opportunities. The last is the ability to learn from the past to extend or adjust the employed competence model of the CISO. However, the presence of these four abilities alone is not enough to ensure a desired level of resilience. Furthermore, it is necessary to find operationally feasible solutions for the desired capabilities and to coordinate their use, considering dependencies and interactions as well as current and future situations. The framework for operational resilience management proposed in this paper addresses this challenge and provides a process-based approach for effective handling of adverse events, unexpected developments, and other surprises.

2.2. Operational Management and Requirements

Considering a CISO at initial operation, it can be justifiably assumed that the construction and operation of the CISO correspond to the state-of-the-art and, thus, to the state of knowledge. This applies to measures implemented to minimize risks, mitigate damage, detect, and respond to changes with risk potential. It also holds true for actions designated to achieve rapid recovery of CISO functionality following the occurrence of destructive events. In summary, the ensemble of all measures represents the level of risk and resilience management supported by the CISO.

The likelihood of a failure in risk and resilience management increases in situations where the CISO enters into unanticipated states or the management itself is confronted with surprising events, e.g., known or unknown hazards or threats.

In the case of complex and interconnected CISOs, there are various reasons for the possible emergence of hazards or threats of high impact with uncertain or possibly surprising occurrences:

- CISOs tend to operate as a complex network of subsystems serving a higher purpose. Lacks of knowledge about the system behavior, e.g., evoked by undesired interactions between subsystems, can potentially lead to the emergence of unan-

ticipated incidents, which then may turn into adverse events, such as threats and damages [26–28,31,32,45–47].

- In case of emerging unanticipated incidents, situation analysis and assessment are afflicted with uncertainty resulting from insufficient information provision. Additionally, forecasting potential scenario developments is limited by epistemic uncertainties. Not only that such incidents must be detected, but decisions have to be taken under stress with incomplete or non-existing situation analysis and assessment in the early stages of a developing incident. Hence, selecting appropriate means and measures to avoid a transition from incident to adverse events becomes a decision under (severe) uncertainty. This also applies in particular to the prevention of cascading effects [11,12,20,26–28,40,45–47].
- Uncertainties at the time of decision making also exist regarding the availability and effectiveness of identified and selected measures as well as associated resources. For this reason, decisions that have already been made and their outcome must be monitored and reviewed so that they can be adjusted if necessary. This applies equally to activities aimed at mitigating risks as well as to restoration and recovery activities.

Therefore, it is not surprising that both risk and resilience research are looking for solutions that enable them to act effectively despite uncertainties in situation awareness and regarding possible development [28,45–47]. Resilience-based approaches have been developed to improve the handling of challenges originating from epistemic uncertainty caused by insufficient knowledge about current and future situation development [29,31,34]. The four resilience cornerstones specify a methodical approach for the improvement of CISO resilience in a generic manner [32]. Implementation of these four cornerstones into a CISO requires a framework that facilitates the accumulation and utilization of knowledge for the improvement of resilience capabilities and their coordinated use. Consequently, it is necessary that the four cornerstones are functionalized. This can be conducted via machine functions, human tasks, or a mixture of both in combination with control and decision activities [57,58]. In this context, a strict distinction between the complementary activities of risk and resilience management is neither considered useful nor conducive to the goal. As both aim to avoid negative consequences of adverse events, risk can be considered as the operative term for both methodologies [42].

Operationalizing resilience management requires consideration of the dynamic nature of evolving situations caused by constant changes within the CISO, its environment, and the knowledge associated with both. Scenarios are used to describe possible CISO behavior over time as a function of specific influencing factors. As a scenario unfolds over time, more information becomes available about both the scenario and the response of the CISO. Comparative analyses create new information supporting the inherently dynamic process of decision making as well as reducing initially existing knowledge gaps [28]. In summary, operational resilience management must not only coordinate the resilience capabilities of a CISO but additionally enable adaptation to developing situations, new information, and related uncertainties.

The coupling of these assumptions to the fundamental resilience cornerstones by Hollnagel [32] implies a number of general deductions regarding resilience management:

- Monitoring of developing scenarios and available knowledge requires a knowledge base that comprises available actual and historical data and information
- Prediction or Anticipation demand profound knowledge about system behavior and real-time information about the system state and its environment
- Responding to hazards or threats in a flexible and correctable way needs a dynamic informed decision support incorporating uncertainties
- Learning about the complex behavior and response of systems to hazards or threats as well as countermeasures requires the ability to feedback real system behavior and related information to the knowledge base used, e.g., modeling or analysis purposes
- The adaptation of employed models and methods to the latest knowledge requires self-controlling processes for the alignment to real-system developments

Following these deductions, Table 1 provides an initial list of requirements for operational resilience management. Here, Hollnagel's cornerstones are understood as core functionalities that have to be applied to various objects in order to fulfill one or more purposes.

Table 1. Requirements for operational resilience management based on Hollnagel's four cornerstones of resilience [32].

Cornerstone	Objects (Excerpts)	Purpose
Monitoring	■ Status and behavior of CISO ■ Environmental factors ■ Knowledge ■ Interdependencies	Providing the information needed for situation awareness and assessment of developing scenarios including indication of the quality of information. Information may be used to improve modeling.
Recognition	■ Current and emerging threats ■ CISO changes ■ Environmental changes ■ hanging criticality of interdependencies	Tools and skills for comprehensive situation awareness and assessment regarding risk potential of events and changes as essential input for operative decision making in the context of risk/resilience management.
Learning	■ CISO behavior and response to hazards and threats ■ Possibilities of controlling and management ■ Reliable recognition of hazards and threats ■ Suitable countermeasures and effectiveness ■ Administration of knowledge ■ Decision support and self-monitoring of effectiveness	Advancement of skills, means, and measures for operational resilience management based on the extension of knowledge in relation to changes of any kind.
Anticipation	■ Prediction of CISO behavior ■ Forecasting of environmental influences ■ Simulation and analysis of hazardous events ■ Simulation and assessment of means and measures for danger prevention and mitigation	Provision of skills, means, and measures to predict and assess potential scenario developments (CISO, environment, and dependencies) and to support the decision making around CISO adjustments regarding prevention and mitigation of risks as well as reduction and avoidance of negative consequences.

2.3. The Digital Twin Concept in Resilience Management

Digital Twins (DT) are usually defined as a virtual representation of physical objects across their lifecycle. The DT concept is composed of a physical object in real space and its digital counterpart, both connected via data flows. The digital representation consists not

only of data but can inherit models and algorithms or other software characterizing the properties and behavior of the real physical object [59,60]. All kinds of data gathered by sensors or other sources of information are employed for the simulation of the behavior of the real system in real-time or serve, in combination with historical data, for prediction purposes. Analysis and information fusion are then used to optimize the real system in a feedback loop. In this way, DT are nowadays used in design, simulation, monitoring, and optimization in a variety of fields. Due to their data-driven architecture and the rising capabilities in information technology, e.g., big data processing and storage, DT are especially of interest in domains of complex systems [61].

When first introduced by Grieves in 2002, the DT concept was proposed to improve product lifecycle management [60]. In the meantime, DT play an important role in the concept of Industry 4.0 [62–64]. Recently, the DT concept also emerged in different other fields [65–69]. Although DT are utilized in the context of failure prediction and predictive maintenance, application in the resilience domain is rare. An approach developed by Ivanov et al. uses a DT to manage the resilience of supply chains against disruptions [70], while Bécue et al. focused on the resilience of factories [71]. Lately, the concept has also appeared in the context of smart cities [72–75].

Surprisingly, the above-introduced properties of the DT concept substantially match the requirements for the operational resilience management derived in Section 2.2

- DT can be considered as an evergrowing knowledge base consisting of gathered data and information covering the whole lifecycle of the real object.
- DT comprise models that allow simulation and prediction of system behavior, especially of complex systems, based on actual and historical data.
- The influence of the environment on the DT behavior is captured by the real-time gathering of data and information through the sensor network. Additional models can support the integration of environmental information.
- Feedback of the behavior of the real system to the models and analysis within the DT is a basic feature of the DT concept and its flow of actual data and information from a variety of sources.

In summary, it appears rational to include the DT concept in further considerations of a framework for operational resilience management. Moreover, the need for a comprehensive knowledge base as well as tools for dynamic feedback loops and model alignment renders the DT concept an integral component. The following Section 3 specifies in detail how resilience management requirements affect the conception of a DT.

3. Resilience Management Framework

This section introduces the framework for Operational Resilience Management (ORM) and presents its two basic components—a Data and Information Base (DIB) and a resilience management process.

3.1. Thematic Classification

The aim of resilience management is to coordinate the recognition, monitoring, anticipation, and learning as core competencies of resilient Critical Infrastructure Systems and Organizations (CISO) [31]. Although Woods suggested that the label "resilience" should refer more to the management of disruptions and interruptions outside the nominal operational area [34], it is hardly useful to consider nominal and abnormal conditions separately. It is rather important that the CISO is aware of its own competencies and capabilities in terms of detection, monitoring, and anticipation. The CISO must also be able to identify both systemic and environmental situations that deviate from the valid specification of nominal conditions. For these, it is necessary to assess whether the anomaly may cause additional risks. If this question is answered in an affirmative manner, then appropriate measures must be identified to reduce the resulting risks and mitigate their negative consequences. Therefore, the framework proposed and discussed in this paper

should facilitate operation under rated conditions and the detection of and adaptation to abnormal conditions.

Learning is represented in the framework rather indirectly. The design and operation of the CISO with all its functions, methods, and measures is only possible with qualified personnel whose qualification is the result of an ongoing learning process. Learning is also part of the recognition of anomalies, the evaluation of their criticality as well as identification and evaluation of potential mitigation measures, and thus, serves to build competencies. The effectiveness of what is learned is determined to a large extent by how these competencies can be maintained, adjusted, and retrieved. For this reason, it is necessary that the framework is also designed to manage and develop competencies efficiently.

3.2. Data and Information Base

The presented requirements on the ORM framework strongly motivate the availability of a Data and Information Base (DIB) that contains knowledge of the CISO's ACTUAL and TARGET behavior, environment, and interdependencies. The TARGET behavior is defined by the performance requirements for the CISO services and the target conditions and influences assumed in the design phase. In contrast, the ACTUAL behavior is described using appropriate models parameterized with measured values.

Therefore, the CISO should be designed and operated based on state-of-the-art competence models, which cover the CISO, environmental conditions, and practicable resilience capabilities. Furthermore, the proposed framework requires that the model of the CISO is a digital representation of the reality in terms of components, functions, and processes. Compared to what was presented in Section 2.3, one can note that these requirements match the digital twin (DT) concept. Additionally, processable environmental models (EM) are needed to describe relevant environmental conditions in all their diversity and variability that can significantly affect the functionality and performance of the CISO.

In general, DT and EM are composed of descriptive and predictive models. Descriptive models ensure that the diversity of components and aspects is sufficiently depicted. These models describe the system's behavior based on historical as well as actual data and information [76]. Predictive models are able to explain changes based on causes, dependencies, and interactions. Hence, these models enable the investigation of "what will happen" and "what should be done to make or to avoid it happening" [77]. However, the consequent complexity of predictive models is significantly higher compared to descriptive models. Descriptive as well as predictive models should reflect the current state and behavior of the CISO and environment, including intrinsic interactions, through appropriate model parameterization and real-time monitoring of the model parameters (MP_{RT}). Furthermore, the nominal behavior should be characterized by nominal values for the model parameters (MP_N).

The described features of the DT concept are useful for the implementation and realization of advanced resilience capabilities. In the simplest case, the monitoring of MP_{RT} and the comparing analysis between MP_{RT} and MP_N should enable the recognition of regular as well as irregular disruptions, disturbances, and changes. A more challenging approach analyses the changes within the CISO and environment in order to anticipate the emerging risks in time. This requires constant monitoring and assessment of the observed and expected behavior of the CISO as well as its response to environmental changes. This provides the necessary lead time to decide on the appropriate use of adaptive measures and to implement them. The anticipation skills can be further improved if DT and EM are connected to a suitable simulation environment. This enables the combined consideration of systemic/organizational and environmental aspects in their complexity and in relation to the diversity of potential scenario developments. Such scenario developments are also an appropriate means to perform a predictive assessment of the effectiveness of potential decisions and adaptive measures.

Core elements of the DT and the EM are modelling methods, ideally provided as executable software, whose corresponding properties are described in the model documen-

tation (D). Furthermore, both models are parametrized by the model parameters (P). The model data of these parameters can be real-time data (RT) or nominal data (N). A DT or EM that is parametrized with RT reflects the current state of the CISO or environment. In contrast, a parametrization with N represents the intended or typical behavior. The features and model data of the DT and EM are stored in a respective data and information base (see Figure 1a,b), which enables further analysis and processing.

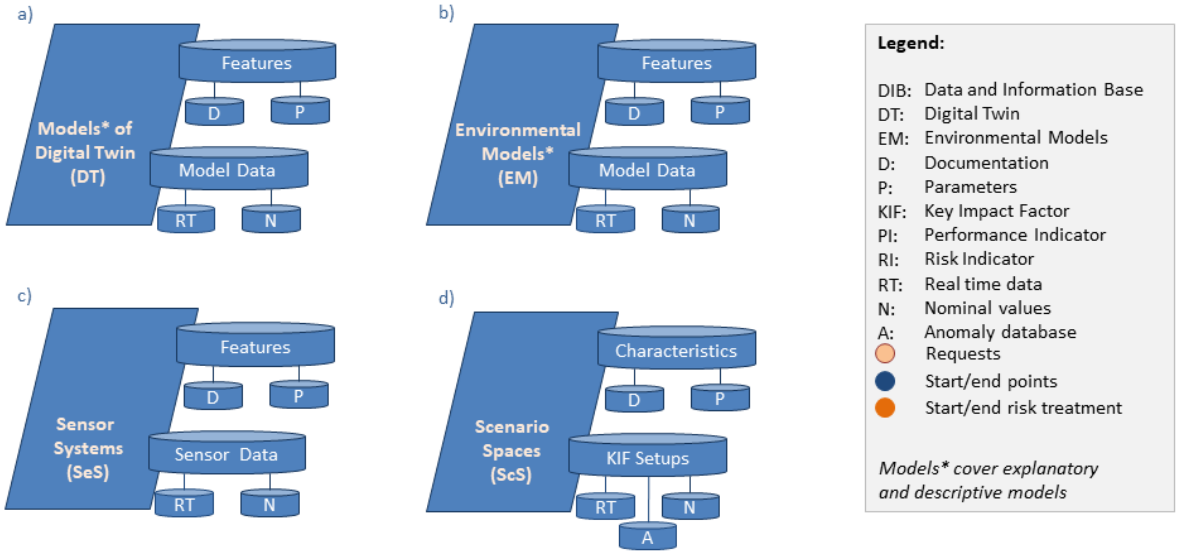

Figure 1. Data and information base (DIB) of the proposed resilience management: (**a**) the digital twin models, (**b**) environmental models, (**c**) sensor systems, and (**d**) scenario spaces.

The real-time data (RT) are gathered by the sensor systems (SeS), which are either part of the actual CISO or are operated by external service providers (Figure 1c). In this paper, a sensor system is used as a synonym for any information source that is needed to collect information about the situation-related system status or environmental conditions. The specified sensor system ultimately determines which information is applicable in order to perform monitoring, assessment, controlling, and decision-making processes within the system or organization. It is mandatory that the SeS is able to provide the required data in the desired quality and frequency in order to assure that later analysis and processing are executed on the actual state of the CISO. A SeS is characterized by its parameters (P) and the corresponding documentation. The parameters can be of a different type, e.g., configuration data, control data, or the performance data of the sensor system, and enable the evaluation of the usability of the sensor system. Similar to the DT and EM, this comprises real-time data (RT) or nominal data (N). Please note that the actually measured values and attained information of the SeS are not located together with these parameters but are stored as the RT of the DT or EM.

Morphological analysis [78] is a promising approach for scenario modelling, e.g., as applied in [79]. The resulting scenario space contains all scenarios and may be described by the available parameters (P) of DT and EM and their feasible characterizations. Analogously to a morphological space, P and their characteristics are brought into relation to each other. Thus, different combinations within the space enable a derivation of scenarios. Consequently, a scenario can be described by certain parameters (P) that should be documented (D). From these parameters, the so-called Key Impact Factors (KIF) can be derived, which enable the sufficient characterization of a scenario. That means each scenario is described by a certain setup of KIF. Again, the setups can be based on real-time data (RT), nominal data (N), or already investigated scenarios (A). The corresponding information and database (DIB) are depicted in Figure 1d.

3.3. Resilience Management Process

The purpose of this section is to provide an overview of the resilience management process at a somewhat abstract level to illustrate the main tasks and their relations (Figure 2). The subsequent Section 4 details the main tasks and describes the required functions as well as inherent interactions.

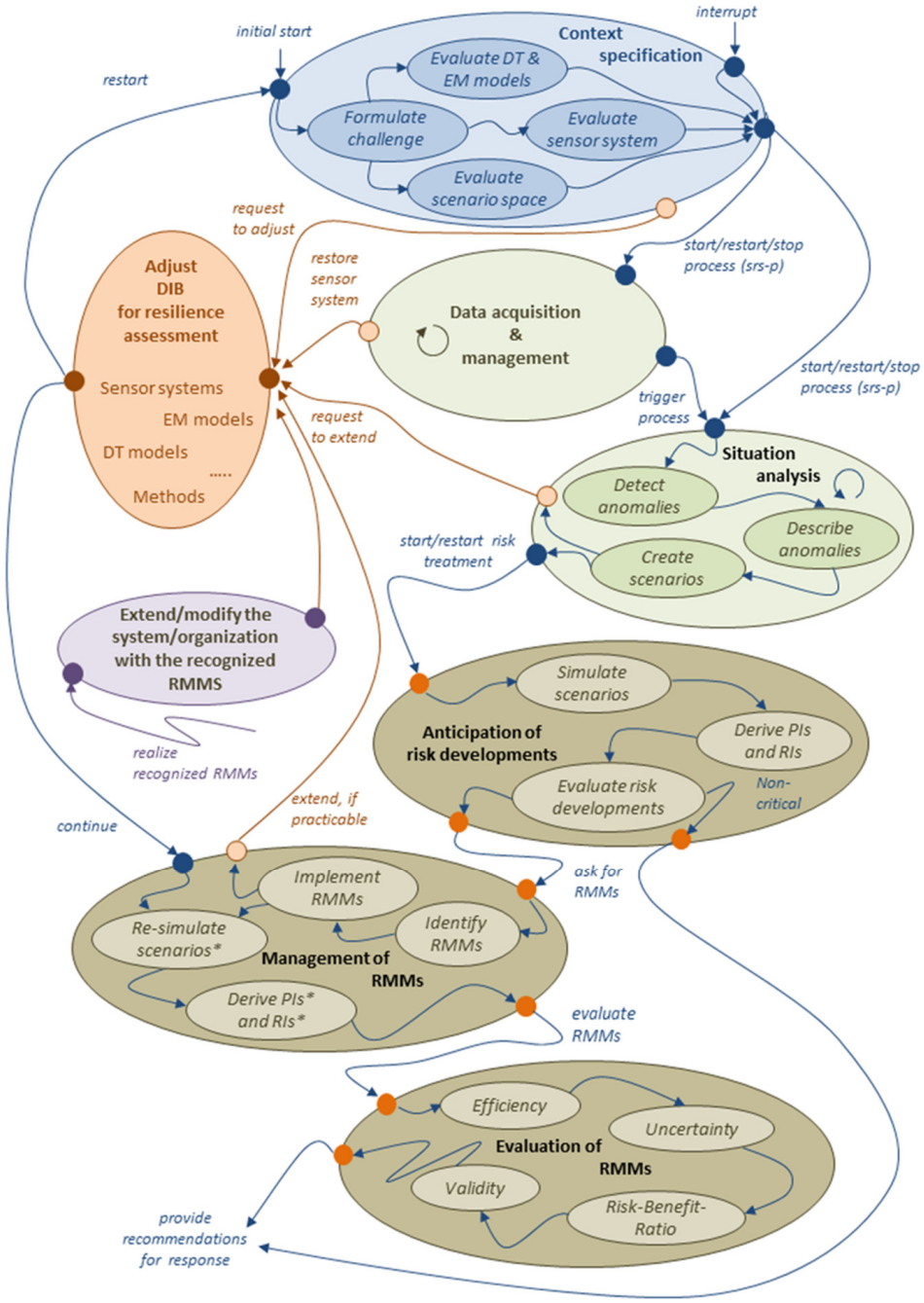

Figure 2. Cycle and main tasks of the resilience management process.

The basic structure of the process follows classical risk management [5] and the proposal of Häring et al. [38]. However, the proposed framework puts a strong emphasis on the actual operability of resilience management processes and thus has to be considered as an additional contributor to the resilience of the CISO. As a consequence, the framework focuses on the implementation of the required process and its tasks into a resilience-enhancing operating procedure.

In this context, it is notable that the system boundaries of a CISO are primarily determined by the components and functions required to fulfill the core task of the CISO, the provision of one or more services. Events that lead to disruptions of these services should be detected predictively or reactively by the framework in order to be able to initiate appropriate recovery measures. The execution of these recovery actions only partially takes place within the system boundaries of CISO and is rather to be considered as an additional service that requires further resources and specific expertise. The proposed ORM framework can provide support for such a service but cannot replace it. The case discussed in Section 5 illustrates the applicability of the framework to CISO operation as well as recovery.

The task "Context specification" provides the evaluation of the framework employed for the resilience management of the CISO under consideration of new or modified challenges on the CISO (blue circle in Figure 2). It is executed whenever changes occur in the CISO, in the environment, or in the requirements of the CISO. Changes can be intentional, e.g., modernization, automation, new standards, and regulations, or quite unexpected, e.g., increased wear out of components, limited supplies, economic embargos. The implementation of such changes is executed in the task "Adjust DIB for resilience assessment", which administrates the adaptation of the employed models (DT, EM), the sensor system, and the applicable scenario spaces (orange circle in Figure 2). This task, which is usually implemented with the help of external service providers, can be initiated by all other tasks with the exception of "Evaluation of Risk Mitigation Measures (RMM)" and "Anticipation of risk developments".

"Data acquisition and management" and "Situation Analysis" are recurring tasks that relate to the operation of the monitoring capability of the CISO (green circle in Figure 2). Both are (re)started by the "Context specification", and thus, both tasks. "Data acquisition and management" continuously provide real-time data from the sensor system to the data and information base. In contrast, "Situation Analysis" continuously monitors and analyses situational changes. It is a central element of resilience management as it enables the identification of critical situations and developments. Its main purpose is the detection and description of anomalies and the identification of how an anomaly relates to the scenario space. The results of this task are then investigated by the following resilience assessment tasks.

Similar to the generic resilience management process proposed by Häring et al. [38], the resilience assessment is carried out with the help of the three consecutively executed tasks (beige circles in Figure 2). However, in the proposed scheme, the emphasis of the tasks is again on the actual operability of resilience management. The task "Anticipation of risk developments" focuses on the anticipation of potential risk developments with the help of scenario analysis. A possible outcome of this analysis might be that the determined risk is tolerable, and therefore the risk assessment is terminated. If this is not the case, the task "Management of Risk Mitigation Measures (RMM)" is initiated, which identifies possible approaches for risk mitigation. Therefore, the identified RMM are implemented in a simulation setup in order to determine corresponding performance and risk indicators [80]. This task can be interrupted when required modifications of the data and information base are required, which will be detailed in subSection 4.5. The consecutive task "Evaluation of Risk Mitigation Measures (RMM)" serves the evaluation of the proposed RMM and supports the decision-making considering efficiency, uncertainties, and risk–benefit ratios. The obtained results are then handed as decision support to the operator or other stakeholders. Proposed and chosen risk mitigation approaches should be stored to enable a posterior analysis of the effectiveness in practice and implementation quality.

The final task, "Extend/modify the CISO with the chosen Risk Mitigation Measures (RMM)", relates to the actual implementation of the measures (purple circle in Figure 2). It is important to note that any consequences of these measures must be integrated into the data and information base of the CISO via the task "Adjust DIB for resilience assessment".

Nominal operation of the CISO may be assumed if "Data collection and management" and "Situation analysis" are performed as specified, and the analysis results prove the overall compliance with the specifications. This can be understood as the first stage of resilience management, which decides on the base of the current situation whether the continued operation of the CISO in its previous form is reasonable and justifiable.

4. Processes of Resilience Management

This section details and discusses the tasks of the proposed resilience management process presented in Section 3.3.

4.1. Context Specification

The purpose of the resilience management in CISO is to appropriately control and manage the CISO's resilience capabilities in order to identify emerging known as well as unknown threats and to initiate appropriate countermeasures. A special challenge is the handling of emerging unknown threats as well as changes in the CISO or its purpose, which often requires an adaptation or extension of the resilience capabilities of the CISO. In such cases, it is necessary to verify whether the DIB still fulfills the requirements resulting from the new situation. For this purpose, the context of resilience management has to be (re)specified by first identifying and formulating the specific objectives and problems of the intended resilience management process (see Figure 3). Next, it must be evaluated whether the DIB corresponds to the specified requirements. This evaluation should be undertaken considering the scenario space, the modelling (DT and EM), as well as the capabilities of the sensor system (see Figure 4). If any of these components does not fulfil the requirements, a corresponding revision is requested, which might lead to the adjustment of the DIB. The realization of these adjustments is not further discussed in this paper, as they are considered an external service activity (see purple activity in Figure 2).

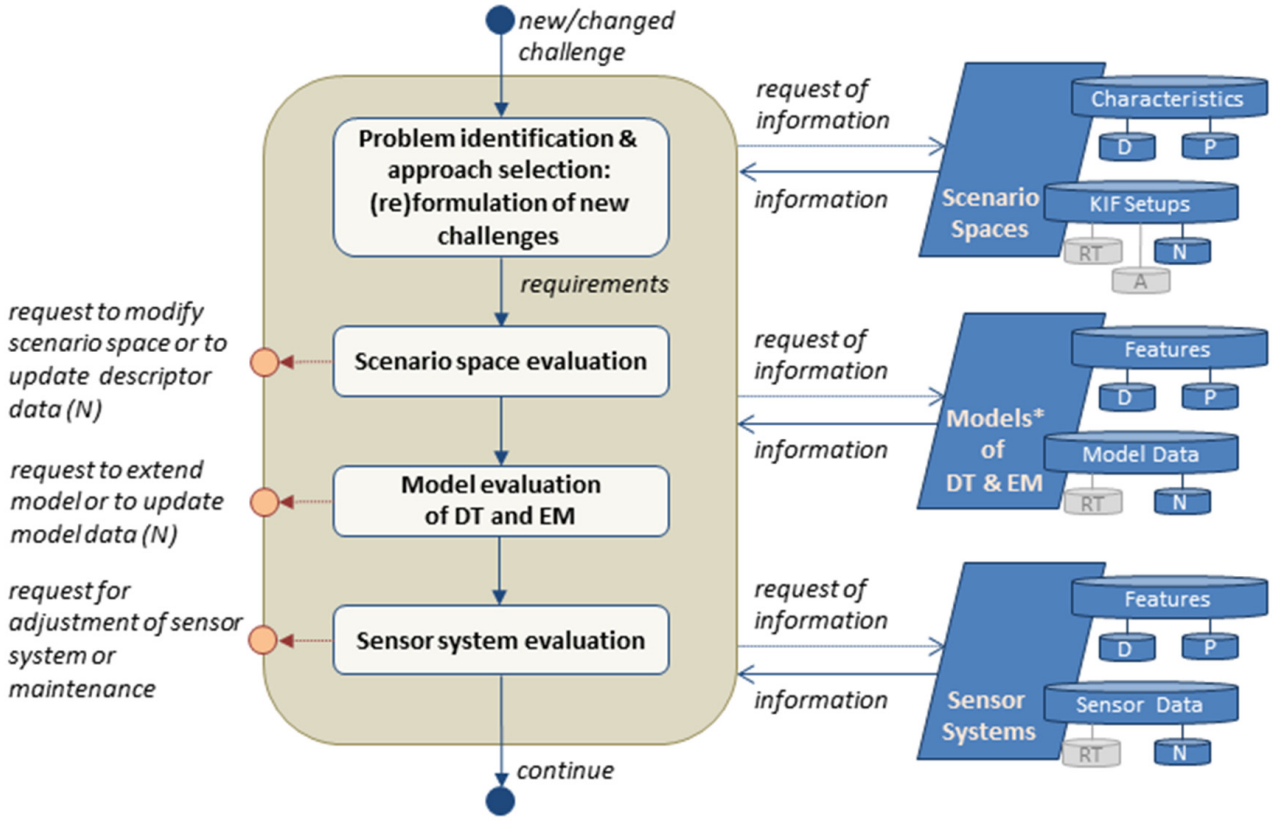

Figure 3. Flow chart of context specification as initial task of the resilience management process.

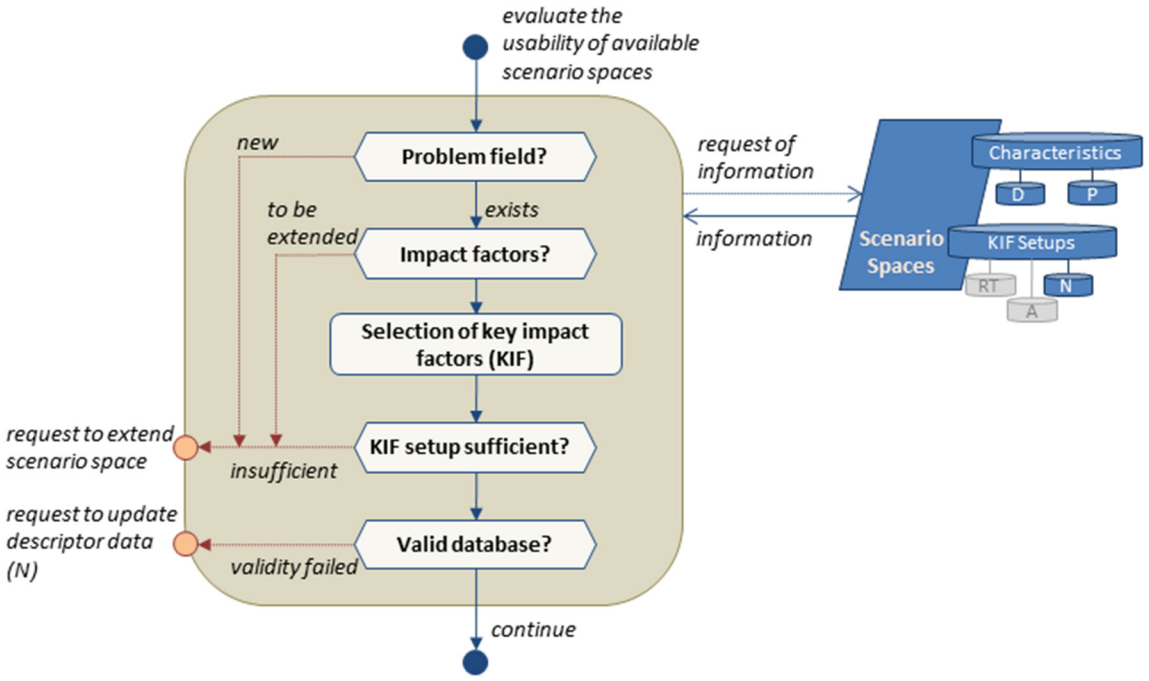

Figure 4. Flow chart of scenario space evaluation as a function of context specification.

4.1.1. Scenario Space Evaluation

Figure 4 details the subprocess for evaluating the usability of the available scenario space based on the concept of general morphological analysis [78,81]. Thus, a scenario space aggregates impact factors of threat scenarios in a multidimensional space, thus using a set of superior key factors for a qualitative and quantitative scenario description [82]. Key factors can comprise factors of the environment as well as factors within the system itself and can thus be of a general as well as a system-specific nature. Therefore, existing scenario spaces reflect the already accumulated and usable competencies about the considered CISO as fields to be formed, about practicable resilience capabilities and their coordination, as well as about already known danger situations as impact factors and possibilities to deal with them. A specific scenario space shall be able to describe all conceivable threats and resulting scenarios, including those characterized as having high impact and low probability of occurrence (HILP) in relation to a considered CISO.

Initially, it must be examined whether one of the existing scenario spaces is, in principle, suitable to be used for investigations of the identified problems in relation to the considered CISO. If not, it is necessary to request the development and implementation of a new scenario space. If a scenario space is principally usable, the next examination checks the covering of the relevant impact factors, e.g., the points where threats or other aspects potentially affect the CISO under consideration. When consistency is not given here, an extension of the impact factors is requested.

Next, the key impact factors (KIF) are selected, e.g., by cross-impact analysis, if the available scenario space supports large numbers of interdependent impact factors of interest. In the following step, the relevant KIFs are checked for sufficient description of all scenarios within the scenario space, e.g., relevant changes in climate or weather conditions, terrorist attacks, or functional failures. Additionally, the KIFs should sufficiently be parametrized according to related variables and parameters of the used models of the system and environment. The description should also include the time-dependent trend of the KIFs for the purpose of scenario development prognosis. An insufficient setup of KIFs leads to process termination and the request for a scenario space extension. Finally, it is checked if a valid database of nominal KIF values (N) representing the nominal state of the system is already provided. If validity is given, the subprocess finishes, and the task continues with

the model evaluation of the used digital twin (DT) and environmental models (EM) (see Figure 5). Otherwise, new descriptor data are requested.

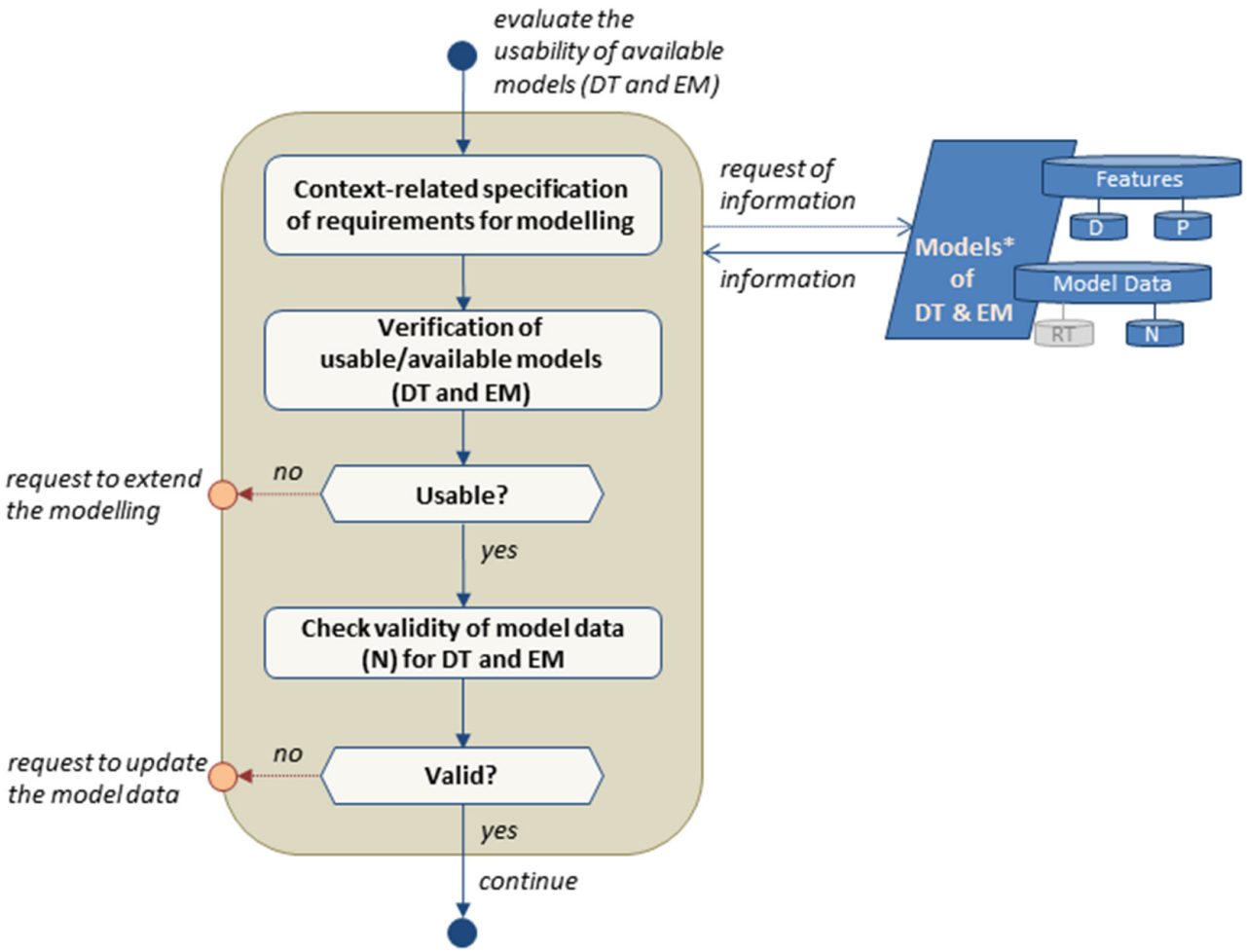

Figure 5. Flow chart of DT and EM model evaluation as a function of context specification.

4.1.2. Sensor System Evaluation

The final subprocess of the task context specification investigates the capability of the sensor system (SeS) to provide the data and information needed for resilience management (Figure 6). It should be emphasized again that "sensor system" is used as a synonym for all sources providing the required data and information.

Initially, a context-related specification of requirements for data and information is executed. The requirements are specifically adapted to the previously evaluated DT and EM models, as the sensor system shall enable the elicitation of all relevant data and information needed by the models to monitor the condition of the considered CISO and its environment as well as actual events and state changes. Thus, the sensor system acts as the bridge between the real system and DT as well as the real environment and EM. In general, the sensor system should provide physical measurement data as well as merged data (sensor fusion) with higher information levels or nonphysical information from other sources.

The fulfillment of requirements is evaluated by a two-step checking of the sensor system. In the first step, the sensor system is analyzed, considering its ability to provide the data and information as needed. In case of a negative outcome, the modification of the sensor system is requested. Next, the operability and capability of the sensors system, e.g., in terms of quality of data provision, is verified, and, if necessary, maintenance is requested.

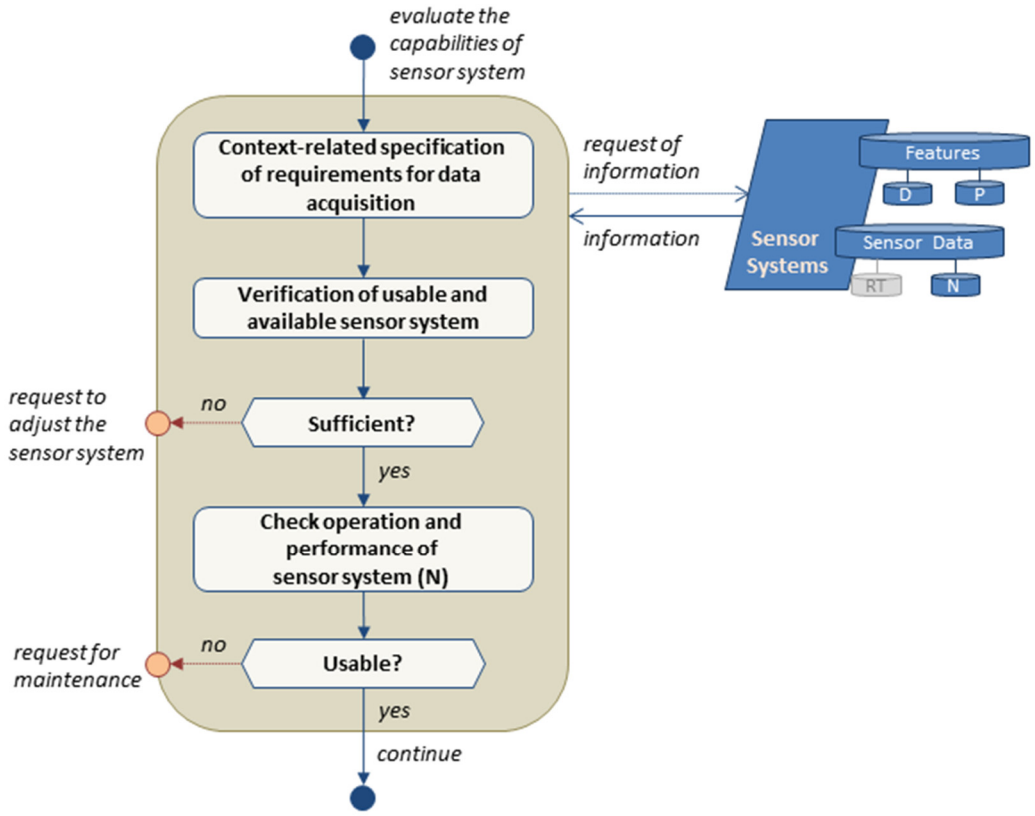

Figure 6. Flow chart of sensor system evaluation as a function of context specification.

4.2. Data Acquisition and Management

The task "Data acquisition and management" serves the monitoring of the considered CISO and its relevant environment in compliance with the specified requirements (Figure 7). Its purpose is the retrieval of data and information needed for the parallel task "Situation analysis". The task starts with the acquisition of the sensor system. Next, the formal requirements on the data provided, such as compliance with the data format, plausible data content, and availability of validity information, are verified. Failed data acquisitions, as well as violations of formal requirements, are reported to the control system, which ultimately decides whether data acquisition should continue or restoring measures are required for the sensor system.

Successfully retrieved actual data may be fused to enable the generation of higher-level information, e.g., geo-referenced as well as time-synchronized data or plausibility, consistency, and integrity information about the actual data. The details of this step strongly depend on the considered CISO, its context, and used models and parameters. Insufficient data quality and unstable data processing can lead to the failure of data fusion and the inability to provide the intended higher quality information. This must also be reported to the control, which decides on the further procedure.

If the data acquisition and processing are performed successfully, the data are provided to the scenario spaces and the DT or EM of the DIB. As a result, the controlling informs the task "Situation analysis" that new data are available for further investigation. It also ensures that data acquisition and processing are continued as cyclical tasks under normal conditions.

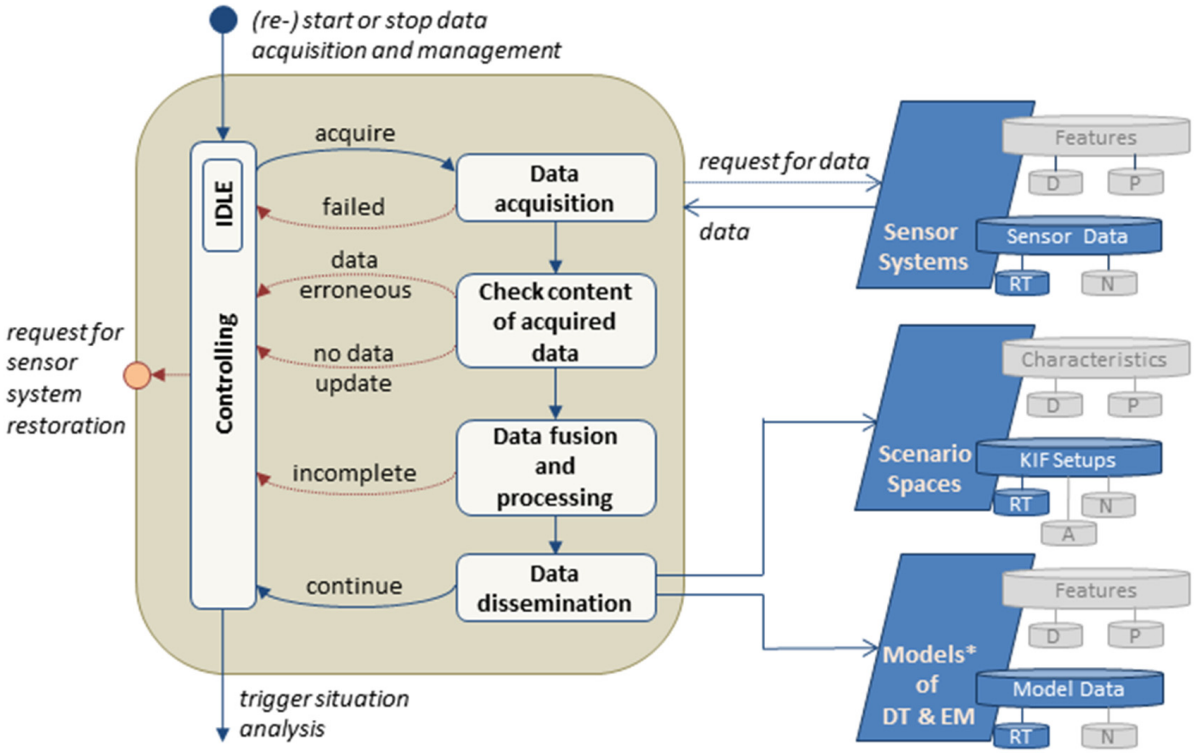

Figure 7. Flow chart of data acquisition and management.

4.3. Situation Analysis

"Situation analysis" is considered a core task of resilience management (Figure 8). Situation analysis is responsible for the identification of developing scenarios and is carried out by consecutively passing through various subprocesses. The current situation is represented by the state of DT and EM modelled with incoming (near) real-time data (RT), while the nominal situation is described via the nominal model data (N). Additionally, sequences of previously logged RT of DT and EM that are still present in the DIB may be used to describe prospective scenario developments.

Next, anomalies are detected by comparing the current and nominal situations. The current and the nominal situation may also include the analysis of time series to determine parameters that describe trends as well as to detect abnormal changes. In principle, various methods are applicable for comparing and evaluating the situation in order to detect anomalies. For example, outlier detection may be a suitable mean for the time-efficient detection of relevant deviations [83,84]. In comparison, the recognition of known and unknown patterns in incoming data indicating abnormal behavior may be conducted by AI-driven processes [85,86]. The choice of comparison methods depends on the type and complexity of the data used as well as the resilience management objectives. Additionally, the comparison results should provide the details needed for the following state assignment in the scenario space. If no anomaly is detected, e.g., the current situation of DM and EM is within the boundaries of the nominal behavior, the process situation analysis switches back into an idle state, waiting to be triggered for a restart by new incoming data.

If anomalies are detected, they are then characterized by a snapshot describing the deviations or found patterns based on key impact factors of a scenario space. The next processing step tries to match the snapshot of a detected anomaly to any feasible states in the scenario space to identify such scenarios which are representative of the current situation and are, therefore, possible developments. This may also include very unlikely scenarios and also scenarios with partial consistency, thus resulting in uncertainties with regards to further scenario development.

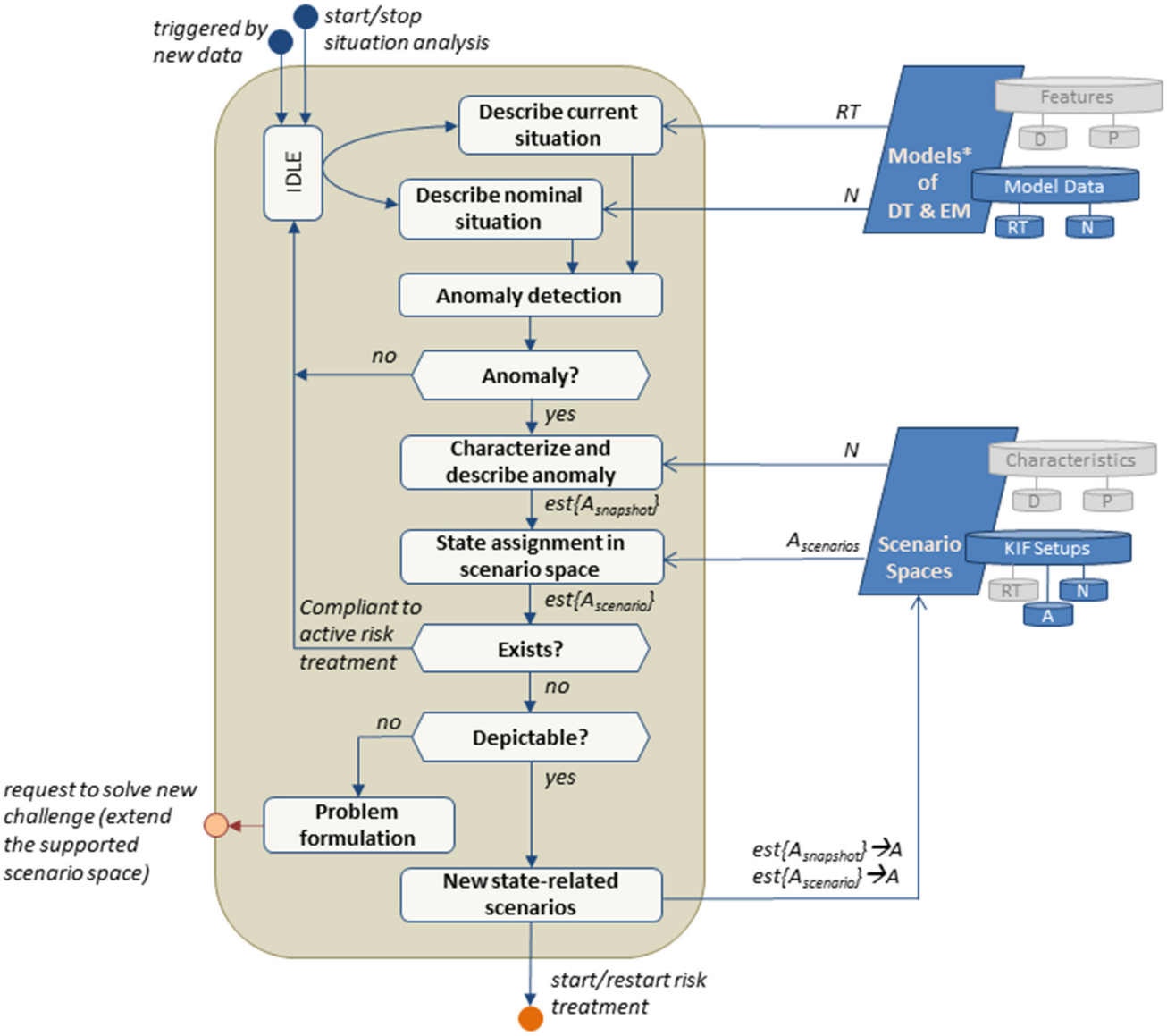

Figure 8. Flow chart of situation analysis.

Additionally, it is reviewed whether matching scenarios were already recognized in an earlier analysis cycle. If this is the case, it is not necessary to start the processes of risk anticipation, RMM identification, and RMM evaluation again. This helps to prevent unnecessary analysis, as compliant risk mitigation measures are already in place or currently under investigation. New scenarios have to be checked for sufficient depiction within the existing scenario space.

A failed depiction should be analyzed to receive a well-formulated problem description needed to request external solution processes, e.g., the extension of the scenario space with additional key impact factors or a changed parametrization. If a depiction is possible, the resulting fully specified new state-related scenarios and their further characteristics are then added to the anomaly database of the scenario space for further analysis.

4.4. Anticipation of Risk Developments

The task, "Anticipation of risk developments", depicted in Figure 9, is triggered either by new or changed scenarios identified by the "Situation analysis" (see Section 4.3).

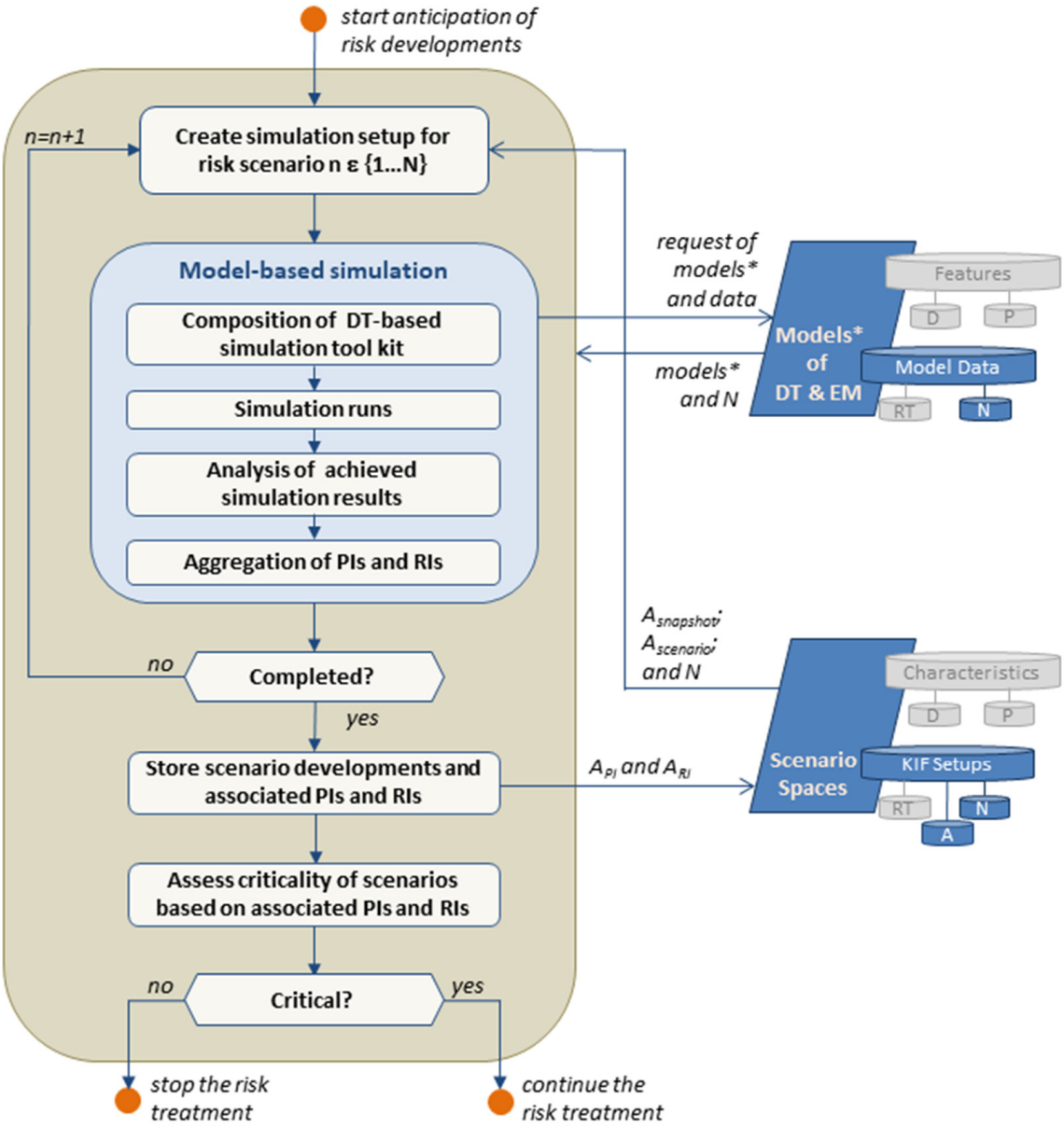

Figure 9. Flow chart of anticipation of risk developments.

The process analyzes the scenarios regarding risk indicators (RIs) related to the criticality of scenario development for the performance indicators (PIs) of the system. Therefore, possible developments of the scenarios are simulated with the help of the DT and EM. The required information for simulating the scenario development is taken from the descriptor database of the scenario space. This comprises the current anomaly data ($A_{Snapshot}$, $A_{Scenarios}$) and the nominal values (N) and includes parameters, variables, and their feasible short-term development, as well as the corresponding likelihoods. The model-based simulations of all parametrized scenarios are conducted in consecutive runs. Each run starts with the composition of a DT- and EM-based tool kit that is sufficient for the simulation of the chosen scenario. This tool kit is an offline copy of parts or the whole DT using its nominal specification. On this base, the scenarios are simulated repeatedly, e.g., by Monte-Carlo simulation, in order to consider different feasible scenario developments and the respective possible outcomes and their likelihoods.

In the next step, all achieved simulation results are analyzed in regard to the resulting course of the PIs and corresponding risks that have an effect. Thus, RIs having an impact

on the course of the PI in different simulated developments are assessed and quantified. In the last step of each run, the PIs, RIs, and their quantified impact, as well as the impact severity likelihood, are aggregated for the various simulated scenario outcomes.

After the finalization of the simulations, the results and associated PIs and RIs are stored in the anomaly database. Finally, a first assessment of the criticality based on the extracted PIs and RIs is done. The risk treatment is stopped if critical risk development within the analyzed scenarios can be ruled out with adequate confidence. The needed level of confidence should depend on individual criteria of the considered system, e.g., its criticality within a higher-level network. Otherwise, the following process of finding appropriate risk mitigation measures (RMM) is triggered.

4.5. Management of RMM

The goal of this task is the identification of RMM which are potentially suitable to reduce the risks in the anticipated risk developments as well as to mitigate resulting consequences. The effectiveness of the RMM has to be proved with respect to PIs and RIs determined by the former scenario-based simulations. In this way, this task decisively contributes to the enhancement of the abilities of the supported system in terms of its ability to react and adapt to emerging critical situations. As not only the mere suitability but also the added value of the measures to overall risk mitigation are relevant, the evaluation of the impact of these measures is additionally conducted within this activity.

In the first step (see Figure 10), potential risk mitigation measures (RMM) are identified. Various methods may contribute to the fulfillment of this rather complex task. These methods are understood as a subprocess, which is not discussed in detail in this paper. Feasible methods range from best practice approaches over state-of-the-art analysis to (variance-based) sensitivity analysis, e.g., described in [87]. The hereby predefined measures could be stored in a list, e.g., suitability for impact on various RIs. Thus, this list of K approaches is generally suitable for the RIs identified in the previous simulations, with a single approach representing a single measure or a combination of them. If no matching RMM is found (K = 0), the task is aborted in order to further continue the risk treatment with the evaluation process.

The identified RMM are further evaluated for their usability and practicability in the current DT model (see Table 2). Here, usability can be assumed if RMM can directly be simulated and analyzed with DT models. Non-usable RMM can still be considered practicable when integration in a timely manner into the DT models is feasible without interrupting the running evaluation process. This evaluation includes the analysis and comparison of links and interfaces between RMM and DT models suitable for the implementation of the measures.

Table 2. Decision matrix about the feasibility of RMM evaluation (usability and practicability).

Identified RMM		**Next Step**
Usable	**Practicable**	
No	No	Reiteration of basic RMM identification
No	Yes	Pausing of the task and request for an extension of the DT. Then, continuation of the task with identified RMM.
Yes	Yes	Continuation of the task with the identified RMM

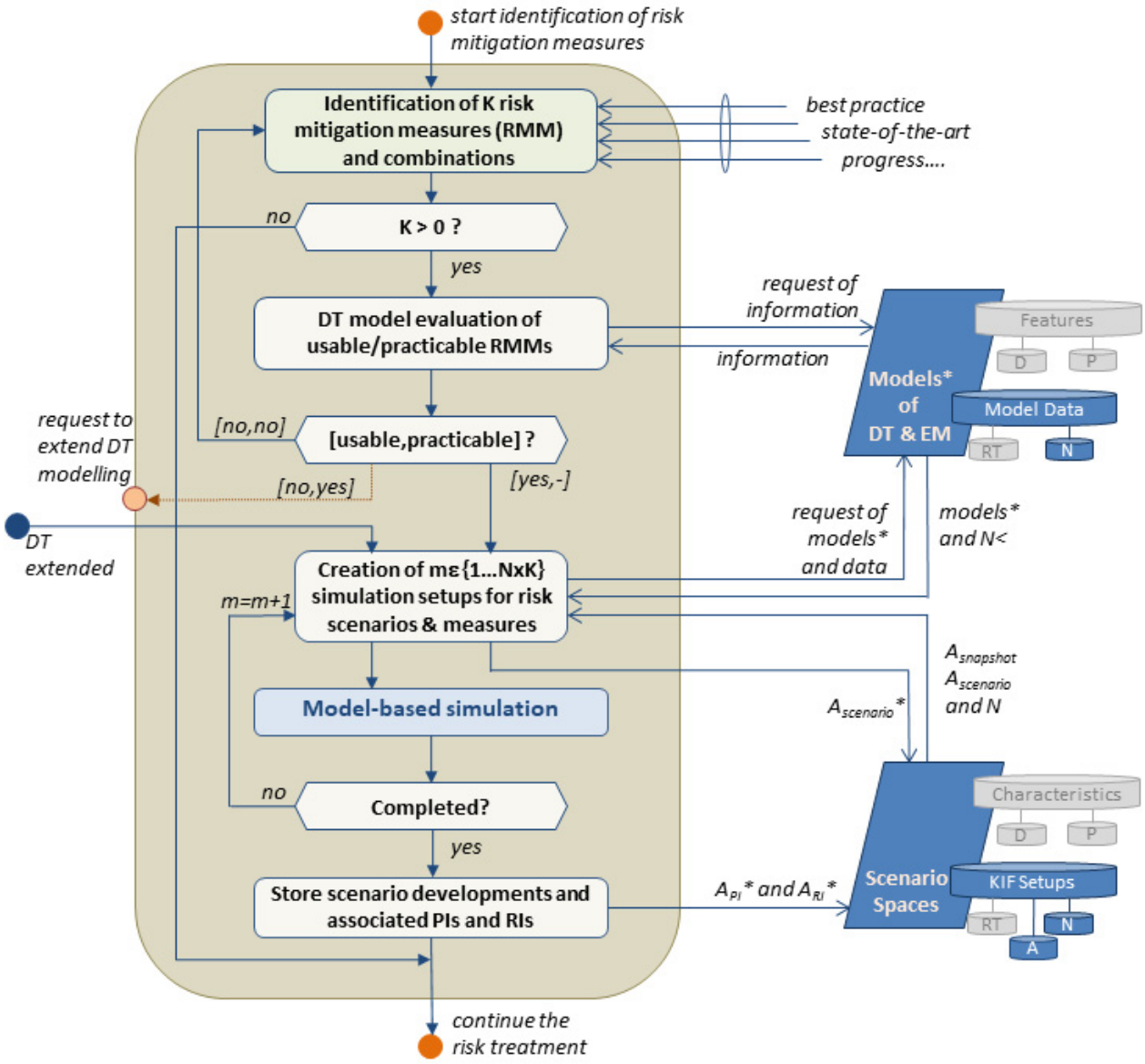

Figure 10. Flow chart of identification of risk mitigation measures.

If at least one usable RMM has been identified, a simulation of the feasible scenario developments is prepared and conducted analogous to the anticipation of development activity (see Section 4.5). The simulation setup now comprises the implemented measures and, if needed, the extended DT models. Furthermore, the simulation setup uses the anomaly database and the nominal values for the key factors for scenario description. The model-based simulation of the RMM-influenced situation developments is iteratively conducted for every feasible scenario. When completed, the activity finishes by storing the scenario developments and associated PIs and RIs ($A_{Scenario*}$, A_{PI*}, A_{RI*}) in the anomaly database of the scenario space.

4.6. Evaluation of RMM

The final task deals with the evaluation of the identified RMM and their simulated impact on situation developments (see Figure 11). The goal is the provision of recommendations for response to developing situations, e.g., emerging threat scenarios, by an optimal choice of RMM.

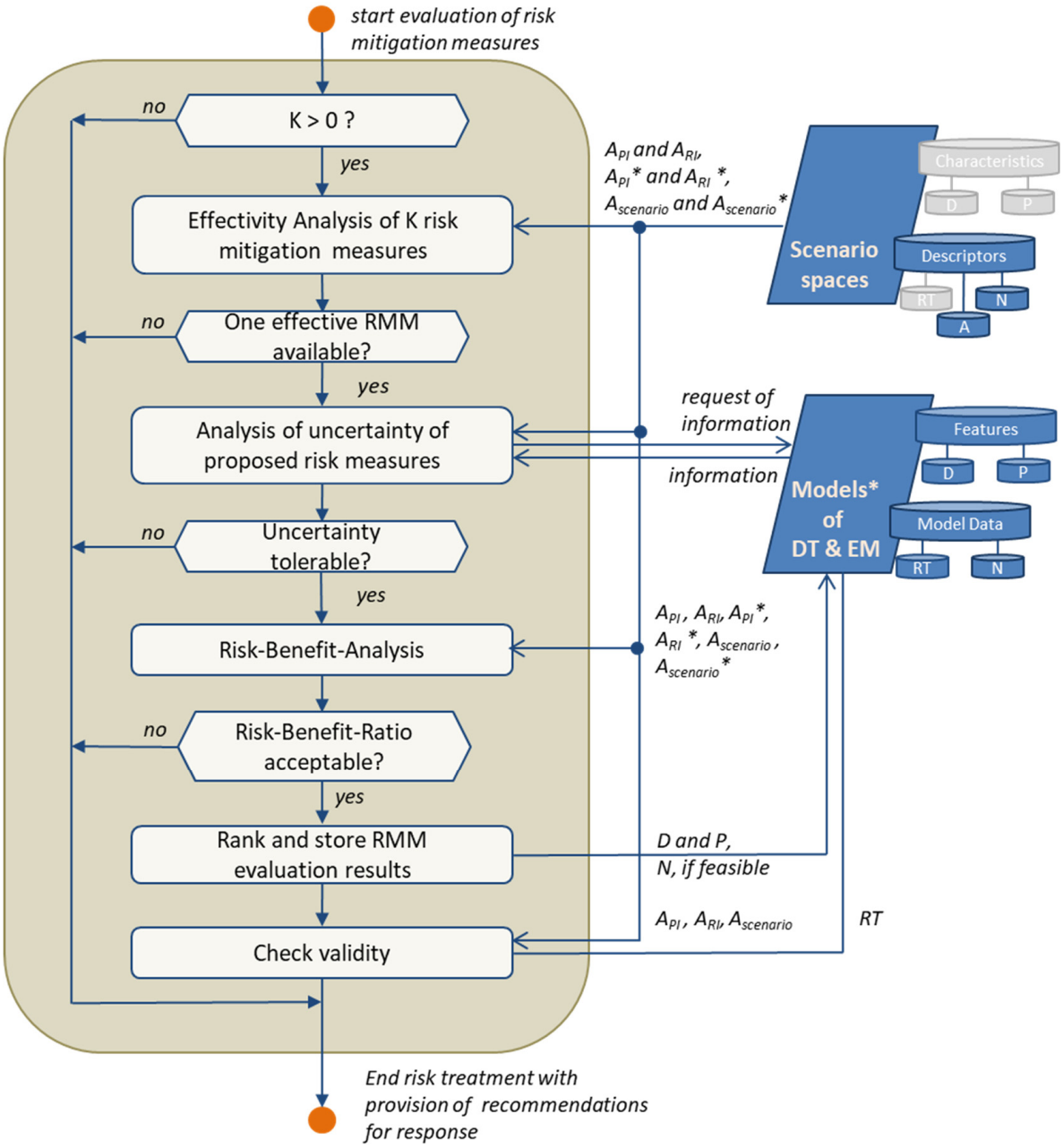

Figure 11. Flow chart for the evaluation of proposed risk mitigation measure (RMM).

The evaluation process itself is multidimensional, having in mind that different influences regarding decision-making have to be considered. Firstly, the effectivity of the proposed RMM is analyzed using the information from the anomaly database, e.g., by comparing the simulated course of PIs and RIs in original developing scenarios ($A_{Scenario}$) and the respective developments with the implemented RMM ($A_{Scenario*}$). Secondly, arising uncertainties from different sources within the framework are evaluated for their impact on decision validity. In this important part of decision analysis, a distinction between epistemic and deep uncertainty is reasonable. While the former is a result of imprecisions in modeling and information, the latter results from unknown scenario development due to incomplete information in the prognosis.

Finally, a Risk-Benefit-Analysis is conducted. Here, the variety of feasible scenario developments ($A_{Scenario}$, $A_{Scenario*}$) and RMM are considered in order to analyze tradeoffs between resulting risks and benefits of RMM implementation on PIs by using the results of

the carried out simulations (A_{PI}, A_{PI*}, A_{RI}, A_{RI*}). Thus, the Risk-Benefit-Analysis considers the uncertain anticipation of threats and the resulting course of scenario development due to incomplete information as well as to measure effectiveness uncertainty. Note that diverging effects of RMM on different PIs or in different scenarios can lead to goal conflicts that can be solved, e.g., by Multi-Criteria Decision Analysis.

All evaluation steps have similar criteria for process abortion and ending risk treatment. Hence, noneffective RMM, too many uncertainties, or not accepted Risk-Benefit-Ratios lead to the recommendation of no RMM implementation. Thus, the decision support of the framework stays neutral and waits for more information on the task "Situation Analysis" (see Section 4.3). If all steps are conducted successfully, the RMM are ranked according to the evaluation results. These results may be stored to track the real achieved RMM effectiveness. This tracking can be used to check the validity of the implementation recommendations by comparing achieved results using real-time data (RT) and expected results of the simulations. A further application of this tracking can support the learning of new best practice RMM solutions.

5. Conceptual Study

This section discusses the feasibility of using the framework for Operational Resilience Management (ORM) in collaboration with dynamic risk management by means of a qualitative analysis of a real event that occurred in a major city in Bavaria (Germany) in February 2021. It is important to note that we assume an implementation of the framework that complies with the requirements presented in the previous section.

5.1. Motivating Scenario Description

The scenario used here as an example was a major fire in a power plant induced by a technical defect that was not detected early enough by the employed condition monitoring system. Regardless of whether the fire could have been avoided or not, the risk management system failed with regard to fire prevention. However, the risk management system worked very well with regard to firefighting as well as the evacuation of employees. Consequently, no personal injuries or major destructions have been reported, with the exception of the power plant unit responsible for the heat supply, which was damaged in such a way that it stopped its operation. Possibly, a post-hazard risk analysis might be able to show to what extent such a fire can be avoided in the future. This analysis might reveal the need for improved monitoring and recognition capabilities of the power plant, i.e., higher resilience against the causes of the fire.

The fire damage to the power plant unit meant that one of several district heating generators in the regional network was no longer available. The power plant unit, which dates back to the 1930s, was primarily in operation to balance peak daytime consumption and contributed to the system margin. Thus, it was expected that at average Central European temperature conditions (~5 °C) and under typical consumption behavior, the failure of this power plant unit would not lead to a noticeable reduction in the district heating supply. However, at the time of the event, the region suffered from freezing cold weather conditions with temperatures constantly below −10 °C. Based on the available information, it is not possible to judge whether risk analyses already carried out by the district heating network operator classified the total failure of the power plant at extremely low temperatures as a rather unlikely event or as a short-term event without significant effects.

The consideration of the damage situation on the part of the power plant led to the estimate that several weeks would be needed to restore and rebuild the unit for heat generation. From the point of view of the district heating network operator and considering the current weather conditions, the district heating supply was no longer guaranteed for two city districts and its critical infrastructures, including a hospital, two old people's and nursing homes, 15,000 households, schools, and businesses. Based on this information, the city declared a disaster situation, established a crisis team, and asked residents to reduce hot water and heating consumption to a minimum. This was undertaken via the catastrophe

warning system KATWARN using mobile communication for messaging. Unfortunately, a radio mast of a mobile phone provider on the roof of the power plant was also destroyed resulting in an interruption of the mobile phone service. In summary, it was difficult to estimate how many of the affected residents would comply with this request. Complicating the situation, the pandemic regulations meant that a large proportion of the population worked from their home offices, resulting in an even higher demand for heat and energy. At the same time, the measure of procuring and installing mobile heating stations began but was delayed due to the unavailability of mobile heat generators on site. Although the risk management of the crisis team had worked quite well up to that point, the uncertainties in the situation impeded the assessment of whether the measures initiated would be sufficient to guarantee a minimum supply of heat. In addition, current pandemic regulations have been suspended in order to provide alternative housing options to the affected population in the event of a total loss of heat supply. This reduced the risk of freezing but increased the risk of being infected with COVID-19.

5.2. Elaboration of Application of the Proposed ORM Framework

In the following, we discuss the possible impact of the ORM framework as specified in Sections 3 and 4 on the presented scenario in a qualitative manner. Therefore, different levels of the scenario are discussed, starting with the power plant as the lowest level, followed by the district heating supply and the urban crisis management.

5.2.1. Power Plant Level

Fire is either caused by the presence of heat, flammable substances, and oxygen in a certain mixture or by physically, chemically, or biologically induced spontaneous ignition processes. The observed outcome indicates that the employed monitoring system and the situation assessment by the operating personnel were not able to perceive and interrupt the ignition process at an early stage. This may be due to several causes: (a) The area where the fire originated was not monitored. (b) The area was monitored, but the data collected were inadequate to detect the emerging fire. (c) The anomaly detected by the monitoring system was an indicator of the emerging fire but was not noticed by the operators. (d) The detected anomaly was perceived as an indicator of an emerging fire by the operating personnel, but the scenario was classified as rather unlikely. (e) The emerging fire was detected too late to be stopped.

In the case of cause (a), the proposed ORM framework could perform the monitoring as needed for risk detection of emerging fires. In contrast, cause (b) could be circumvented via enhanced monitoring capabilities due to improved data acquisition and assessment, which is mainly provided by the tasks "Data acquisition and management" (Section 4.2), "Situation analysis" (Section 4.3), and "Anticipation of risk developments" (Section 4.4). The proposed ORM framework would be particularly helpful in reducing the risks related to causes (c) to (e). Therefore, the framework would initiate a scenario analysis for each detected anomaly with respect to potentially evolving hazards ("Situation analysis" and "Anticipation of risk developments") unless the data and information base contains already explanatory scenarios for the specific type of heat generator. Based on this analysis, adequate risk mitigation measures (RMM) could be proposed and evaluated, mainly via the tasks "Management of RMM" (Section 4.5) and "Evaluation of RMM" (Section 4.6).

5.2.2. District Heating Supply

Modern district heating power plants already optimize the use of local resources with the help of operational support software based on DT or simplified models of the power plant and setpoints for heat generation. Therefore, a district heating supply network is often described by a locally resolved hydrothermal model to ensure that the consumer obtains district heating at the required temperature and pressure. However, the actual heat consumption on the final customer level is unknown within these models. In the exemplary scenario discussed above, the network operator used its operating software to recognize

in the early stages that the district heating supply was at risk under the circumstances described above. However, the pandemic, as well as extreme weather-related deviations to the customer profiles as well as the lack of knowledge of the current consumption of individual customers made it impossible to estimate the emerging restriction of district heating provision reliably. This also applies to the assessment of the extent to which voluntary restriction of heat consumption by customers could contribute to relaxing the critical situation.

The proposed ORM framework could notably improve this situation assessment. Therefore, the applied data and information base (DIB) must provide models not only for heat generators and networks but also for customers in terms of heat consumption. Recent developments indicate the feasibility of such dynamic models [88]. Using the DIB and real-time data also at the customer level, acquired via the task "Data acquisition and management" (Section 4.2), an enhanced description of the current situation and its dynamics is possible and could be provided by the task "Situation analysis" (Section 4.3). Consequently, potential scenarios can be identified and described based on perceived changes in the system and the heat consumption, using the tasks "Situation analysis" and "Anticipation of risk developments" (Section 4.4). This would also offer the possibility of regulatory intervention in times of crisis to avoid consumer behavior that causes additional harm to the stressed system, mainly derived and evaluated within the tasks "Management of RMM" (Section 4.5) and "Evaluation of RMM" (Section 4.6). Other possible risk mitigation measures include the formulation and updating of requirements and the scheduling of mobile heat generation.

5.2.3. Urban Crisis Management

In general, it is very much possible that the current pandemic regulations have been suspended too early, considering the given uncertainties of the developing situation. Enhanced situational awareness, as provided by the proposed ORM framework, could have helped in avoiding or at least delaying the suspension.

6. Conclusions

Recently published works indicate that current risk and resilience research puts high emphasis on uncertainties arising from the lack of knowledge about the behavior of complex networked Critical Infrastructure Systems and Organizations (CISO) and their multifaceted interdependences. As a result, a variety of risk-related as well as resilience-related frameworks offering either method-driven or application-oriented approaches were developed. Alas, these frameworks either lack the focus on operational management, have a rather theoretical approach, or are designed for specific applications. This observation motivated the development of the presented framework for operational resilience management (ORM), which aims at implementing the four cornerstones of resilience, namely responding, monitoring, anticipating, and learning, as operational processes in a CISO. Therefore, the proposed ORM framework provides a process that defines tasks for the proper coordination of the CISO's inherent capabilities to identify and handle adverse as well as surprising events and developments.

Regardless of the context, resilience management requires a minimum of available knowledge. Ultimately, the available knowledge determines the possible performance of the implemented resilience-related capabilities. The framework reflects the importance of knowledge by building a living data and information base (DIB), which includes the digital twin (DT) concept. This DIB enables the description of the current situation and historical events in relation to CISO, environment, and evolving scenarios. Furthermore, the proposed ORM framework also defines operational measures for gathering, maintaining, and extending the available knowledge. This results in the following advantages:

- When starting or resuming ORM, a context specification assesses whether the available knowledge is sufficient to perform the intended resilience management. An identified deficiency leads to the need to expand the DIB, e.g., by collecting additional data,

improving DT and environmental models, or expanding methodological capabilities. This strengthens situational awareness with regard to known and unknown risks.

- The ORM framework provides support for decision-making regarding the need for reassessing possible risk developments due to the current situation. For this purpose, the ACTUAL situation (DIB with real-time data) is compared with the TARGET situation (DIB with nominal data) in order to identify anomalies in the risk indicators used and to anticipate potential risk developments.
- Exhaustive analysis and simulation with the help of DT and environmental models are performed to provide decision support by identification, evaluation, and selection of suitable and practicable risk mitigation measures (RMMs). In this context, novel as well as known RMMs were investigated with regard to their effectiveness. An additional feature is the capability to reduce the influence of uncertainties and to correct implemented measures successively.

All framework-dependent feedbacks between DT and CISO, data and models, as well as analyses and measures of risk mitigation, reflect the crucial resilience feature of a learning CISO. The results of scenario analyses and implementation of identified risk mitigation measures lead to an update of DT models in particular and of the DIB in general. Using the example of a real hazard in a Bavarian district heating power plant, it was shown how the framework could have a positive impact on decision-making processes involving risk mitigation measures as well as measures to increase the resilience of the CISO. One should be aware that the added value of using a framework necessarily depends on the actual implementation of the individual tasks in the context of a specific entity. It should be noted that the enumerated benefits can only be fully achieved if the database is as comprehensive as possible. In practice, limitations and complex implementation may have to be expected here, as deficiencies in data collection can often be identified. Another possible limitation is the lack of knowledge about functional relationships of the complex CISO, which can lead to necessary cutbacks in the accuracy of the system models used. For this reason, it is important to examine the proposed framework and its components in a subsequent step by means of a more detailed implementation on a practical example.

Consequently, to evaluate the effects of these potential limitations in more detail, it is important to subject the proposed framework and its components to a more detailed implementation on a practical example in future works.

Hence, the main contribution of this work is the provision of a methodical approach that paves the way for future research and development on the merging of methods for risk and resilience management as well as the digital twin concept.

Author Contributions: Conceptualization, D.L.; methodology, D.L., F.S.T. and E.E.; validation, D.L., F.S.T. and E.E.; investigation, D.L.; writing—original draft preparation, D.L., F.S.T. and E.E.; writing—review and editing, D.L., F.S.T. and E.E.; visualization, D.L. and E.E.; supervision, D.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. European Commission. Proposal on Directive of the European Parliament and of the Council on the Resilience of Critical Entities—COM(2020) 829 Final. 2020. Available online: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf (accessed on 21 July 2021).
2. White House. Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience, 12 Feb 2013. 2013. Available online: https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf (accessed on 1 July 2021).

3. Nan, C.; Sansavini, G. Multilayer hybrid modeling framework for the performance assessment of interdependent critical infrastructures. *Int. J. Crit. Infrastruct. Prot.* **2015**, *10*, 18–33. [CrossRef]
4. Bell, A.J.; Rogers, M.B.; Pearce, J.M. The insider threat: Behavioral indicators and factors influencing likelihood of intervention. *Int. J. Crit. Infrastruct. Prot.* **2018**, *24*, 166–176. [CrossRef]
5. ISO Norm 31000. *Risk Management—Guidelines*; ISO: Geneva, Switzerland, 2018.
6. SRA. Society for Risk Analysis Glossary. 2015. Available online: https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf (accessed on 17 June 2021).
7. Aven, T. Risk assessment and risk management: Review of recent advances on their foundation. *Eur. J. Oper. Res.* **2016**, *253*, 1–13. [CrossRef]
8. Pomazanov, M. The concept of motivation for effective credit risk management. *Financ. Crédit.* **2020**, *26*, 2567–2593. [CrossRef]
9. Lewis, M.K.; Lundberg, P.; Silver, M.S.L.; Kling, K.S.; Kresge, D.T.; Summers, B.; Wilson, N.; Ekelid, M.; Lind, H.; Lundström, S.; et al. Risk Assessment and Credit Management. In *Risk Behaviour and Risk Management in Business Life*; Green, B., Cressy, R., Delmar, F., Eisenberg, T., Howcroft, B., Lewis, M., Schoenmaker, D., Shanteau, J., Vivian, R., Eds.; Springer: Dordrecht, The Netherlands, 2000; pp. 37–121. [CrossRef]
10. Li, Z.; Feng, H.; Liang, Y.; Xu, N.; Nie, S.; Zhang, H. A leakage risk assessment method for hazardous liquid pipeline based on Markov chain Monte Carlo. *Int. J. Crit. Infrastruct. Prot.* **2019**, *27*, 100325. [CrossRef]
11. Røyksund, M.; Engen, O.A. Making sense of a new risk concept in the Norwegian petroleum regulations. *Saf. Sci.* **2020**, *124*, 104612. [CrossRef]
12. Schlich, T. Objectifying Uncertainty: History of Risk Concepts in Medicine. *Topoi* **2004**, *23*, 211–219. [CrossRef]
13. Katina, P.F.; Pinto, C.A.; Bradley, J.M.; Hester, P.T. Interdependency-induced risk with applications to healthcare. *Int. J. Crit. Infrastruct. Prot.* **2014**, *7*, 12–26. [CrossRef]
14. Thekdi, S.A.; Aven, T. A Risk-Science Approach to Vulnerability Classification. *Risk Anal.* **2020**, *41*, 1289–1303. [CrossRef]
15. Goerlandt, F.; Montewka, J. *Review of Risk Concepts and Perspectives in Risk Assessment of Maritime Transportation*; CRC Press: Boca Raton, FL, USA, 2014; pp. 1559–1566. [CrossRef]
16. Guerra, L.; Murino, T.; Romano, E. Airport system analysis: A probabilistic risk assessment model. *Int. J. Syst. Appl. Eng. Dev.* **2008**, *2*, 52–65.
17. Zsifkovits, M.; Pickl, S. Strategic Risk Management in Counter-Terrorism for the Railbound Public Transport. In Proceedings of the International Conference on Security & Management, Las Vegas, NV, USA, 25–28 July 2016.
18. Palacios, K.E.; Peterson, K.E. An Overview of Security Risk Management Concepts. In *Security Supervision and Management*, 4th ed.; Davies, S.J., Hertig, C.A., Gilbride, B.P., Eds.; Butterworth-Heinemann: Oxford, UK, 2015; pp. 535–548. [CrossRef]
19. Klaver, M.; Luiijf, E. *Analyzing the Cyber Risk in Critical Infrastructures*; Rosato, V., Pietro, A.D., Eds.; Issues on Risk Analysis for Critical Infrastructure Protection; IntechOpen: London, UK, 2021. [CrossRef]
20. Tidwell, V.C.; Lowry, T.S.; Binning, D.; Graves, J.; Peplinski, W.J.; Mitchell, R. Framework for shared drinking water risk assessment. *Int. J. Crit. Infrastruct. Prot.* **2018**, *24*, 37–47. [CrossRef]
21. Thompson, J.R.; Frezza, D.; Necioglu, B.; Cohen, M.L.; Hoffman, K.; Rosfjord, K. Interdependent Critical Infrastructure Model (ICIM): An agent-based model of power and water infrastructure. *Int. J. Crit. Infrastruct. Prot.* **2018**, *24*, 144–165. [CrossRef]
22. Aven, T.; Zio, E. Foundational Issues in Risk Assessment and Risk Management. *Risk Anal.* **2013**, *34*, 1164–1172. [CrossRef]
23. Aven, T. Risk Science Contributions: Three Illustrating Examples. *Risk Anal. Off. Publ. Soc. Risk Anal.* **2020**, *40*, 1889–1899. [CrossRef]
24. Aven, T.; Bouder, F. The COVID-19 pandemic: How can risk science help? *J. Risk Res.* **2020**, *23*, 849–854. [CrossRef]
25. Hansson, S.O.; Aven, T. Is Risk Analysis Scientific? *Risk Anal.* **2014**, *34*, 1173–1183. [CrossRef] [PubMed]
26. Flage, R.; Aven, T.; Zio, E.; Baraldi, P. Concerns, Challenges, and Directions of Development for the Issue of Representing Uncertainty in Risk Assessment. *Risk Anal.* **2014**, *34*, 1196–1207. [CrossRef] [PubMed]
27. Yoe, C. *Uncertainty: Decision Making Under Uncertainty*; CRC Press: Boca Raton, FL, USA, 2019; pp. 29–53. [CrossRef]
28. Aven, T.; Zio, E. Globalization and global risk: How risk analysis needs to be enhanced to be effective in confronting current threats. *Reliab. Eng. Syst. Saf.* **2020**, *205*, 107270. [CrossRef]
29. Aven, T. The Call for a Shift from Risk to Resilience: What Does it Mean? *Risk Anal.* **2018**, *39*, 1196–1203. [CrossRef]
30. Haimes, Y.Y. On the Definition of Resilience in Systems. *Risk Anal.* **2009**, *29*, 498–501. [CrossRef]
31. Hollnagel, E. Prologue: The Scope of Resilience Engineering. In *Resilience Engineering in Practice—A Guidebook*; Hollnagel, E., Paries, J., Woods, D.D., Wreathall, J., Eds.; Ashgate Publishing Co.: Burlington, VT, USA, 2011; pp. 29–39.
32. Hollnagel, E. The four cornerstones of resilience engineering. Preparation and restoration. In *Resilience Engineering Perspectives*; Nemeth, C.P., Hollnagel, E., Aldershot, U.K., Eds.; Ashgate: Farnham, UK, 2009; Volume 2, pp. 117–134.
33. Hosseini, S.; Barker, K.; Ramirez-Marquez, J.E. A review of definitions and measures of system resilience. *Reliab. Eng. Syst. Saf.* **2016**, *145*, 47–61. [CrossRef]
34. Woods, D.D.; Branlat, M. Essential characteristics of resilience. In *Resilience Engineering in Practice—A Guidebook*; Hollnagel, E., Paries, J., Woods, D.D., Wreathall, J., Eds.; Ashgate Publishing Co.: Burlington, VT, USA, 2016; pp. 127–143.
35. Francis, R.; Bekera, B. A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliab. Eng. Syst. Saf.* **2014**, *121*, 90–103. [CrossRef]
36. Ferris, T.L.J. A Resilience Measure to Guide System Design and Management. *IEEE Syst. J.* **2019**, *13*, 3708–3715. [CrossRef]

37. Sun, L.; Stojadinovic, B.; Sansavini, G. Resilience Evaluation Framework for Integrated Civil Infrastructure–Community Systems under Seismic Hazard. *J. Infrastruct. Syst.* **2019**, *25*, 04019016. [CrossRef]
38. Häring, I.; Sansavini, G.; Bellini, E.; Martyn, N.; Kovalenko, T.; Kitsak, M.; Vogelbacher, G.; Ross, K.; Bergerhausen, U.; Barker, K.; et al. Towards a Generic Resilience Management, Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures and Case Studies. In *Resilience and Risk*; Linkov, I., Palma-Oliveira, J., Eds.; NATO Science for Peace and Security Series C: Environmental Security; Springer: Dordrecht, The Netherlands, 2017; pp. 21–80. [CrossRef]
39. Rød, B.; Lange, D.; Theocharidou, M.; Pursiainen, C. From Risk Management to Resilience Management in Critical Infrastructure. *J. Manag. Eng.* **2020**, *36*, 04020039. [CrossRef]
40. Caralli, R.A.; Allen, J.H.; Curtis, P.D.; White, D.W.; Young, L.R. Improving Operational Resilience Processes: The CERT Resilience Management Model. In Proceedings of the 2010 IEEE Second International Conference on Social Computing, Minneapolis, MN, USA, 20–22 August 2010; pp. 1165–1170. [CrossRef]
41. Eisenberg, D.; Seager, T.; Alderson, D.L. Rethinking Resilience Analytics. *Risk Anal.* **2019**, *39*, 1870–1884. [CrossRef]
42. Linkov, I.; Palma-Oliveira, J.M. An Introduction to Resilience for Critical Infrastructures. In *Resilience and Risk*; Linkov, I., Palma-Oliveira, J., Eds.; NATO Science for Peace and Security Series C: Environmental Security; Springer: Dordrecht, The Netherlands, 2009; pp. 3–17. [CrossRef]
43. European Commission. The EU Approach to Resilience: Learning from Food Security Crises. Available online: https://ec.europa.eu/echo/files/policies/resilience/com_2012_586_resilience_en.pdf (accessed on 1 May 2019).
44. International Maritime Organisation. Guidelines for Shipborne Position, Navigation and Timing (PNT) Data Processing. Available online: https://www.transportstyrelsen.se/ (accessed on 1 October 2019).
45. Woods, D.D. Four concepts for resilience and the implications for the future of resilience engineering. *Reliab. Eng. Syst. Saf.* **2015**, *141*, 5–9. [CrossRef]
46. Hollnagel, E.; Leonhardt, J.; Licu, T.; Shorrock, S. From Safety-I to Safety-II, A White Paper; Published by European Organisation for the Safety of Air Navigation (EUROCONTROL). Available online: http://www.skybrary.aero/bookshelf/books/2437.pdf (accessed on 1 August 2019).
47. Levenson, N. Safety III: A Systems Approach to Safety and Resilience. MIT ENGINEERING SYSTEMS LAB. Available online: http://sunnyday.mit.edu/safety-3.pdf (accessed on 12 February 2012).
48. Ouyang, M.; Dueñas-Osorio, L.; Min, X. A three-stage resilience analysis framework for urban infrastructure systems. *Struct. Saf.* **2012**, *36–37*, 23–31. [CrossRef]
49. Toroghi, S.S.H.; Thomas, V.M. A framework for the resilience analysis of electric infrastructure systems including temporary generation systems. *Reliab. Eng. Syst. Saf.* **2020**, *202*, 107013. [CrossRef]
50. Zhu, C.; Wu, J.; Liu, M.; Luan, J.; Li, T.; Hu, K. Cyber-physical resilience modelling and assessment of urban roadway system interrupted by rainfall. *Reliab. Eng. Syst. Saf.* **2020**, *204*, 107095. [CrossRef]
51. Zarei, E.; Ramavandi, B.; Darabi, A.H.; Omidvar, M. A framework for resilience assessment in process systems using a fuzzy hybrid MCDM model. *J. Loss Prev. Process Ind.* **2020**, *69*, 104375. [CrossRef]
52. Tran, H.T.; Balchanos, M.; Domerçant, J.C.; Mavris, D.N. A framework for the quantitative assessment of performance-based system resilience. *Reliab. Eng. Syst. Saf.* **2017**, *158*, 73–84. [CrossRef]
53. Mao, Q.; Li, N.; Peña-Mora, F. Quality function deployment-based framework for improving the resilience of critical infrastructure systems. *Int. J. Crit. Infrastruct. Prot.* **2019**, *26*, 100304. [CrossRef]
54. Almutairi, A.; Collier, Z.A.; Hendrickson, D.; Palma-Oliveira, J.M.; Polmateer, T.L.; Lambert, J.H. Stakeholder mapping and disruption scenarios with application to resilience of a container port. *Reliab. Eng. Syst. Saf.* **2018**, *182*, 219–232. [CrossRef]
55. Yang, D.; Frangopol, D.M. Life-cycle management of deteriorating civil infrastructure considering resilience to lifetime hazards: A general approach based on renewal-reward processes. *Reliab. Eng. Syst. Saf.* **2018**, *183*, 197–212. [CrossRef]
56. Kammouh, O.; Gardoni, P.; Cimellaro, G.P. Probabilistic framework to evaluate the resilience of engineering systems using Bayesian and dynamic Bayesian networks. *Reliab. Eng. Syst. Saf.* **2020**, *198*, 106813. [CrossRef]
57. Hu, J.; Khan, F.; Zhang, L. Dynamic resilience assessment of the Marine LNG offloading system. *Reliab. Eng. Syst. Saf.* **2020**, *208*, 107368. [CrossRef]
58. Häring, I.; Ebenhöch, S.; Stolz, A. Quantifying Resilience for Resilience Engineering of Socio Technical Systems. *Eur. J. Secur. Res.* **2016**, *1*, 21–58. [CrossRef]
59. Boschert, S.; Rosen, R. Digital Twin—The Simulation Aspect. In *Mechatronic Futures*; Hehenberger, P., Bradley, D., Eds.; Springer International Publishing: Cham, Switzerland, 2016; pp. 59–74.
60. Grieves, M.W. *Virtually Intelligent Product Systems: Digital and Physical Twins*; American Institute of Aeronautics and Astronautics, Inc.: Reston, VG, USA, 2019; pp. 175–200. [CrossRef]
61. Grieves, M.; Vickers, J. Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems. In *Transdisciplinary Perspectives on Complex Systems*; Springer: Cham, Switzerland, 2017; pp. 85–113.
62. Schleich, B.; Anwer, N.; Mathieu, L.; Wartzack, S. Shaping the digital twin for design and production engineering. *CIRP Ann.* **2017**, *66*, 141–144. [CrossRef]
63. Rosen, R.; von Wichert, G.; Lo, G.; Bettenhausen, K.D. About The Importance of Autonomy and Digital Twins for the Future of Manufacturing. *IFAC-PapersOnLine* **2015**, *48*, 567–572. [CrossRef]

64. Tao, F.; Sui, F.; Liu, A.; Qi, Q.; Zhang, M.; Song, B.; Guo, Z.; Lu, S.C.-Y.; Nee, A.Y.C. Digital twin-driven product design framework. *Int. J. Prod. Res.* **2019**, *57*, 3935–3953. [CrossRef]
65. Healthcare Solution Testing for Future | Digital Twins in Healthcare, Science Service, Dr. Hempel Digital Health Network, 2017. [Online]. Available online: https://www.dr-hempel-network.com/digital-healthtechnolgy/digital-twins-in-healthcare/ (accessed on 10 March 2021).
66. Air Force Research Laboratory. Condition-Based Maintenance Plus Structural Integrity (CBM + SI) & the Airframe Digital Twin. *88ABW-2011-1428*. 2011. Available online: https://apps.dtic.mil/sti/pdfs/ADA546937.pdf (accessed on 2 April 2021).
67. Smarslok, B.; Culler, A.; Mahadevan, S. Error Quantification and Confidence Assessment of Aerothermal Model Predictions for Hypersonic Aircraft. In Proceedings of the 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference, Honolulu, HI, USA, 23–26 April 2012. Art. No. 1817. [CrossRef]
68. Bruynseels, K.; De Sio, F.S.; Hoven, J.V.D. Digital Twins in Health Care: Ethical Implications of an Emerging Engineering Paradigm. *Front. Genet.* **2018**, *9*, 31. [CrossRef] [PubMed]
69. Zhang, J.; Li, L.; Lin, G.; Fang, D.; Tai, Y.; Huang, J. Cyber Resilience in Healthcare Digital Twin on Lung Cancer. *IEEE Access* **2020**, *8*, 201900–201913. [CrossRef]
70. Ivanov, D.; Dolgui, A.; Das, A.; Sokolov, B. Digital Supply Chain Twins: Managing the Ripple Effect, Resilience, and Disruption Risks by Data-Driven Optimization, Simulation, and Visibility. In *Handbook of Ripple Effects in the Supply Chain, Bd. 276*; Ivanov, D., Dolgui, A., Sokolov, B., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 309–332.
71. Bécue, A.; Maia, E.; Feeken, L.; Borchers, P.; Praça, I. A New Concept of Digital Twin Supporting Optimization and Resilience of Factories of the Future. *Appl. Sci.* **2020**, *10*, 4482. [CrossRef]
72. Francisco, A.; Asce, S.M.; Mohammadi, N.; Asce, A.M.; Taylor, J.E.; Asce, M. Smart City Digital Twin–Enabled Energy Management: Toward Real-Time Urban Building Energy Benchmarking. *J. Manag. Eng.* **2020**, *36*, 04019045. [CrossRef]
73. White, G.; Zink, A.; Codecá, L.; Clarke, S. A digital twin smart city for citizen feedback. *Cities* **2021**, *110*, 103064. [CrossRef]
74. Ruohomaki, T.; Airaksinen, E.; Huuska, P.; Kesaniemi, O.; Martikka, M.; Suomisto, J. Smart City Platform Enabling Digital Twin. In Proceedings of the 2018 International Conference on Intelligent Systems (IS), Funchal, Portugal, 25–27 September 2018; pp. 155–161.
75. Farsi, M.; Daneshkhah, A.; Hosseinian-Far, A.; Jahankhani, H. (Eds.) *Digital Twin Technologies and Smart Cities*; Springer International Publishing: Cham, Switzerland, 2020.
76. El Saddik, A. Digital Twins: The Convergence of Multimedia Technologies. *IEEE MultiMedia* **2018**, *25*, 87–92. [CrossRef]
77. Wang, Y.; Chen, Q.; Hong, T.; Kang, C. Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges. *IEEE Trans. Smart Grid* **2018**, *10*, 3125–3148. [CrossRef]
78. Ritchey, T. Problem structuring using computer-aided morphological analysis. *J. Oper. Res. Soc.* **2006**, *57*, 792–801. [CrossRef]
79. Johansen, I. Scenario modelling with morphological analysis. *Technol. Forecast. Soc. Chang.* **2018**, *126*, 116–125. [CrossRef]
80. Sill Torres, F.; Kulev, N.; Skobiej, B.; Meyer, M.; Eichhorn, O.; Schafer-Frey, J. Indicator-based Safety and Security Assessment of Offshore Wind Farms. In Proceedings of the 2020 Resilience Week (RWS), Salt Lake City, UT, USA, 19–23 October 2020.
81. Alvarez, A.; Ritchey, T. Applications of General Morphological Analysis. *Acta Morphol. Gen.* **2015**, *4*. [CrossRef]
82. Witte, D.; Lichte, D.; Wolf, K.D. Threat Analysis: Scenarios and Their Likelihoods. In Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference, Venice, Italy, 21–26 June 2020.
83. Hodge, V.; Austin, J. A Survey of Outlier Detection Methodologies. *Artif. Intell. Rev.* **2004**, *22*, 85–126. [CrossRef]
84. Gupta, M.; Gao, J.; Aggarwal, C.C.; Han, J. Outlier Detection for Temporal Data: A Survey. *IEEE Trans. Knowl. Data Eng.* **2013**, *26*, 2250–2267. [CrossRef]
85. Bishop, C.M. *Pattern Recognition and Machine Learning*; Springer: New York, NY, USA, 2006.
86. Chandola, V.; Banerjee, A.; Kumar, V. Anomaly detection: A survey. *ACM Comput. Surv.* **2009**, *41*, 15. [CrossRef]
87. Saltelli, A.; Tarantola, S.; Campolongo, F.; Ratto, M. *Sensitivity Analysis in Practice—A Guide to Assessing Scientific Models*; John Wiley & Sons: Chichester, UK, 2007.
88. Mohring, J.; Siedow, N.; Linn, D. *EnEff:Wärme | DYNEFF: Dynamische Netzsimulation zur Effizienzsteigerung und Emissionsreduzierung in der Fernwärmeerzeugung*; AGFW e. V.: Frankfurt am Main, Germany, 2019; Volume 52, ISBN 3-89999-082-X.