infrastructures

MDPI

Review

Finite State Machine Modelling to Facilitate the Resilience of Infrastructures: Reflections

Evelin Engler [1], Michael Baldauf [2], Frank Sill Torres [3,*] and Stephan Brusch [4]

1 Institute of Communications and Navigation, DLR, 17235 Neustrelitz, Germany; Evelin.Engler@dlr.de
2 Institute of Innovative Ship-Simulation and Maritime Systems (ISSIMS), Wismar University of Applied Sciences, 18119 Warnemünde, Germany; Michael.Baldauf@hs-wismar.de
3 Institute for the Protection of Maritime Infrastructures, DLR, 27572 Bremerhaven, Germany
4 Program Coordination Defense and Security Research, DLR, 51147 Köln, Germany; Stephan.Brusch@dlr.de
* Correspondence: Frank.SillTorres@dlr.de; Tel.: +49-471-9241-9910

Received: 13 January 2020; Accepted: 27 February 2020; Published: 29 February 2020

Abstract: The ability of an infrastructure to be resistant against hazards or to accommodate and recover from hazard-induced destructions and disturbances is characterized as resilience. Usually, infrastructures are engineered socio-technical systems or systems-of-systems. Jackson and Ferris consider the use of finite state machine (FSM) modelling as a suitable means to depict and investigate the resilience of such engineered systems. This paper discusses the capabilities and limitations of the FSM model proposed by Jackson and Ferris and if it should be used for the representation and evaluation of the resilience of an infrastructure. The discussion is conducted on a more general level. However, special attention is paid to monitoring because, on the one hand, monitoring is one of the cornerstones of resilience and, on the other hand, Scott and Ferris define a state that is emphasized by an increased level of situational awareness as a result of happened and perceived events. Consequently, the question has to be answered of how the models are able to reflect the need for routine monitoring of the resilience of infrastructures in order to initiate, if necessary, adjustment procedures as an appropriate response to changes in internal and external conditions. The results of this theoretical study are a fundamental step towards the practical application of the FSM approach for the design of resilient infrastructures.

Keywords: infrastructures; resilience; finite state machine modelling; design principles; monitoring

1. Introduction

The paper provides reflections about the usability of finite state machine (FSM) models for the investigation and enhancement of the resilience of infrastructures as proposed in [1,2] by Scott and Ferris. In general, there is a great variety of resilience definitions. They differ in perspective, scope, and objective, and ultimately result in different approaches to describe, evaluate, and enhance the resilience of infrastructure systems [3–14]. The variety of resilience definitions and the large application range of resilience developments has already led to a wide spectrum of resilience models.

To the best of our knowledge, there is no comprehensive resilience model that depicts all aspects in their dynamics. Consequently, the following question is justified: To what extent can the FSM models proposed in [1,2] meet these challenges?

1.1. Resilience

The European Commission considers 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" [3] and highlights the societal view to resilience. Stresses and shocks are the result of normal as

well as unintended developments in relation to technological, socio-technical, socio-economic, as well as socio-ecological aspects. Representative examples for stresses result from: Component failures by disproportionate wear and tear (technological), operating errors due to overload work (socio-technical), destructive attacks by cybercrime and economic crime (socio-economical), or extreme weather events caused by progressing climatic change (socio-ecological). Shocks may also be considered as the human response to accidents and disasters that often occur due to the ineffective handling of stress situations by the infrastructure. A more technological view is supported if resilience is considered 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 [14]. According to the classification of resilience concepts by Woods [15], this definition focuses more on the reliable functioning and robustness of the system under consideration. A more comprehensive view of resilience considers the primary purpose of the system in relation to the current and future behavior of system components, environmental impacts, and resulting interactions. This systemic approach is reflected by the definition given in [16], where resilience is considered 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". Hollnagel elaborated a conceptual framework to accentuate the four cornerstones to become a resilient system [10,17]: Monitoring to "know what to look for", anticipating "to know what to expect", responding "to know what to do", and learning "from what happened". A resulting challenge is the necessity to transform these conceptual requirements, e.g., the capability to perform "sensing-adapting-anticipating-learning", into practicable and assessable processes [10]. Consequently, it is of uttermost importance to have suitable models at one's disposal that sufficiently consider all factors involved that may affect the resilience of an infrastructure during the design, life cycle, and beyond [1,2,5,10–13,16,18–21].

Woods introduced four complementary concepts to classify the variety of resilience views [15]: Robustness, rebound, graceful extensibility as the opposite to brittleness, and sustained adaptability. In general, all these concepts have to be taken into account to achieve comprehensive maintenance of resilience for infrastructures. However, for this purpose, it is important that resilience modelling is conditioned to enable a common consideration of the four resilience concepts taking into account the specific scope of actions defined by "sensing", "adapting", "anticipating", and "learning" [10,17]. This paper analyses to what extent the finite state M=machine (FSM) modelling proposed in [1,2] is capable of meeting the requirements for resilience modelling, whereas the discussion focuses mainly on "sensing" or "monitoring", respectively.

1.2. Finite State Machine Modelling

For decades, classic engineering disciplines have utilized finite state machine (FSM) models for the description of time-variant technical systems [22–25]. An FSM model is specified by a finite number of states, all potential transitions between the states, and causes (e.g., events, actions, conditions, processes) inducing a transition from one state to another. In general, a state is defined by a set of system characteristics, which are described by statements (qualitative) or performance parameters (quantitative) and differ in each state. The finite number of states derives from the considered variety of sets of system characteristics. Therefore, the transition from one state to another represents a change of system characteristics and occurs only if the conditions for a specific transition are satisfied. The transition condition itself results from internal or external events, performed activities and processes, or other changes, and may be considered as input for the FSM model. Meanwhile, a considerable number of FSM model types have been developed to align FSM modelling to concrete problems, e.g., actor or transducer FSM approach, synchronous or asynchronous modelling, deterministic or non-deterministic finite automaton (DFA, NFA), Moore machine or Mealy machine, or a mix or enhancement of them [22–25]. This results in the question of how far FSM modelling is able to reflect the diversity of resilience aspects [10,15,17].

1.3. Modelling of Resilience

In the last decades, a variety of model approaches have been developed in order to meet the different requirements of resilience modelling, which results from the intended scope of model application and the view on resilience. A brief insight into other model developments should only outline the complexity of the subject area. A model comparison in general or with regard to specific requirements is not the subject of this work.

For example, Bayesian networks are identified as suitable models for probabilistic knowledge presentation and used for evaluation of the reliability as well as resilience of a variety of systems and infrastructures [6–8,26]. The stress–strain model developed in [27] is considered as a generic approach to operationalize the four cornerstones of resilience, as outlined in [15] and [16]. A further example is the resilience-driven multi-objective restoration model, which serves the optimization between costs and the resilience of the system of interdependent infrastructure networks [9]. The authors of [10] state that the analysis of an infrastructure's resilience requires common consideration of outcomes, resources, and processes taking into account the interconnections and dependencies between them. Consequently, a common consideration of outcomes, resources, and processes is an additional requirement for dynamic modelling of the resilience behavior of an infrastructure [10].

Jackson and Ferries proposed the use of FSM models for the design of resilient engineered systems [1,2]. In general, the advantage of FSM models is its ability to enable the unambiguous specification of system states, e.g., in relation to a certain level of operational functionality and performance used as an indicator for an infrastructure's resilience. FSM modelling promotes the unambiguous classification of states. In addition, FSM modelling forces the elaboration of causes (e.g., decisions, events, changes) that ultimately may result in transitions between the system states. The latter also directs the attention to additional resources (e.g., support functions and services), machine as well as human made, that may be needed to facilitate and maintain the system's resilience during the life cycle of the system. This covers the functionalities and resources to be prepared for any rebound or to reduce the impacts of unavoidable degradations. In this way, the system boundaries are extended and the number of resilient-relevant aspects to be considered by the model increases. FSM modelling may be considered as a suitable validation tool for the current level of resilience or to assess the effectiveness of resilience-relevant measures. A prerequisite for each validation is a clear differentiation between the states of the FSM model. For this purpose, the system characteristics used as validation criteria have to be defined and scaled to the finite number of states. During the assessment, the probability of the occurrence of each state is determined. Therefore, an improvement is proven if the probability of states with a higher level of functionality and performance is increased.

2. Analysis of Proposed FSM Modelling

Jackson and Ferries propose in [1,2] a non-deterministic finite-state machine (FSM) model, whose condensed version can be represented via a quintuple (Σ, S, s_0, δ, F), where:

- Σ is the input alphabet, i.e., the set of events that can cause state transitions in the system;
- S is the set of discrete states the system can assume;
- $s_0 \in S$ is the initial state of the system;
- δ means the state transition function δ: $S \times \Sigma \rightarrow S$; and
- $F \subseteq S$ is the set of final states (can be empty).

Table 1 lists the state transition table of the condensed FSM model proposed by Jackson and Ferries [1,2]. The model uses "7 possible system states and 31 transitions between states" in order to "describe the relationships related to resilience", i.e., S = {NOS, NOS!, pFDS, d+FS, nFDS, adS↘, tdS↓}, with s_0 = NOS as the initial state of the system. The transitions a to g are transitions discounted by the FSM model presented in [1,2].

Table 1. State transition table of the condensed version of the FSM model proposed in [1,2] consisting of the state names; the indexes 1–31, which represent the transitions associated with the causing event (t for any threats, m for management decisions improving the current functionality and performance, finishing the heightened awareness, or inducing a final state); the transitions a to g together with the inputs ($?_+$), ($?_-$) and ($?_p$), which illustrate the transitions discounted by [1,2].

		Next State						
		NOS	**NOS!**	**pFDS**	**d+FS**	**nFDS**	**adS↘**	**tdS↓**
Current State	NOS	1(m), 3(t)	4(t)	8(t)	19(t)	6(t)	25(m)	26(m)
	NOS!	2(m)	a($?_p$)	29(t)	b($?_-$)	11(t)	27(m)	28(m)
	pFDS	9(m)	31(m)	10(t),18(m)	c($?_+$)	13(t)	14(m)	15(m)
	d+FS	20(m)	d($?_+$)	22(t)	e($?_p$)	21(t)	23(m)	24(m)
	nFDS	5(m)	30(m)	7(m)	f($?_+$)	12(t),g($?_p$)	16(m)	17(m)
	adS↘							
	tdS↓							

The input alphabet of the model proposed in this work is Σ = {t, m, ?+, ?-, $?_p$,} where:

- t means any threat;
- m means management decisions improving the functionality and performance in the current state, finishing the heightened awareness, or inducing a final state; and
- $?_+$, $?_-$, $?_p$ are inputs for transitions discounted by the FSM model in [1,2].

The meaning of each state, as well as the consequences due to the disregarded transitions, will be discussed below.

2.1. States

Two of the proposed states (NOS and NOS!) are allocated to the *nominal operational state* of the system, in which the system or infrastructure operates in compliance with its specification in relation to the conditions, functionality, and performance. Under nominal conditions, a new designed infrastructural system should start its operation with the state NOS, i.e., s_0 = NOS. The state NOS! is specified as the special case, in which the situation awareness has identified one or more impending threats, which are attributed to external or internal causes. Generally, situation awareness "focuses on awareness as *process*, on the notion of *situation*, and on the *subject* of awareness" [28]. The establishment of awareness as a process serves the perception of conditions, changes, and events (internal and external) with respect to time and space to gain a deeper and correct insight of the meaning and potential impact on the situation and its projection into the future [28–30]. The subject of situation awareness is in general the resilience of the infrastructural system and in particular resilience-relevant aspects, e.g., threats, decisions, and measures. This implies that monitoring and surveying as well as analysis and interpretation have to be considered as additional requirements for the design of resilient infrastructures. Certainly, it has to be highlighted that the situation has to be assessed not only in times of nominal operation. A correct evaluation of the situation plays an important role in making the right decisions, especially in phases of degraded operational performance, in order to execute measures of maintenance, repair, and restoration in an effective and efficient manner.

The establishment of situation awareness results in a functional and procedural extension of the infrastructural system. The resilience of the extended infrastructure also requires consideration of the case, in which a missing assessment or a false interpretation of the threat situation occurs due to interrupted or failed monitoring, surveying, analysis, or interpretation. The state NOS! assumes that the observed threats are real and relevant for the safe and efficient operation of infrastructure. However, whether the "heightened situation awareness" is truly necessary depends on the trustworthiness and

correct interpretation of the provided picture of the situation. Likewise, the state NOS leads one to believe in the absence of any threats, even if the situation picture is either missed or distorted.

The proposed model [1,2] uses three states to describe the different losses of functional and/or task-related capacity. The system enters the *partially functional disrupted state* (pFDS) if either the supported functions or human-made tasks are executed with lower performance or one or a subset of supported functions and tasks cannot be performed. However, the retained functionality of the infrastructure is sufficient to provide any usefulness, e.g., by performing the remaining functions or a subset of the tasks. For example, a ferry as an infrastructural component can also transport passengers with a non-functioning entertainment system or without activities from the entertainment personnel. The *damaged but functional state* (d+FS) is a state with special significance for safety-critical infrastructures and reflects the capability to compensate the total loss of infrastructure's functionality for a certain time by alternative means, e.g., by a redundant layout or back-up solutions. A representative example is the use of axillary power in times of an interrupted power supply to continue medical emergency care in hospitals. Another "worst case" scenario is the necessarily takeover of tasks by unqualified or unauthorized personnel. The *non-functional disrupted state* (nFDS) illustrates the total loss of functionality due to damage to infrastructure or a total lack of staff. Consequently, a management decision becomes necessary either to initiate a partial or full restoration of the infrastructure or to decommission the infrastructural component because the end of the life cycle has been achieved.

The role of situation assessment has not been discussed for any of these three modelled states in [1,2]. This includes the pending decision processes nor infrastructure's control and maintenance. However, this gap should be bridged and requires that the creation of situation awareness should be also modelled with respect to technological, human, and socio-technical aspects in order to enhance the FSM model presented in [1,2]. With an increasing complexity of the considered infrastructure, it may be helpful to introduce various levels of performance and functionality in order to illustrate the remaining capacity of the infrastructure and the expenditure needed for a complete or partial repair and restoration.

Different losses of functionality implicate the necessity to make decisions. If the specified functionality and performance should be reinstated (NOS), suitable repair and restoration measures have to be initiated and realized. If not, it may be decided to operate the infrastructure with reduced functionality and/or decreased performance in the *agreed diminished state* (adS$\searrow$). From this point in time, the infrastructure has to be considered as a "new" infrastructure, with altered specifications of functionality and performance. Consequently, this state is part of the set of final states F. The subtle distinction of the *partially functional disrupted state* (pFDS) as well as *damaged but functional state* (d+FS) is part of management's decision to spend no time and money on any repair or restoration measures. Alternatively, it may be decided to remove the infrastructure from service. Then, the infrastructure is set into the *totally decommissioned state* (tdS$\downarrow$), which may correspond with the definitive end of its life cycle, and thus, is also part of the set of final states F.

2.2. Transitions

The FSM model [1,2] specifies 31 event-triggered transitions between the states (see Table 1). Events, which decrease the functionality and performance of the infrastructure, include disturbances, damages, and breakdowns. Events, which may recover or increase the functionality and performance, are successfully performed as maintenance, repair, modernization, and restauration measures, whereby management decisions are a prerequisite for their implementation. Only 26 of the specified transitions correspond to a change of state, while the remaining 5 result in an unchanged state. In principle, an FSM model with 7 states should have at least 49 transitions, if the unchanging states are also taken into account. The proposed model has five functional and two final states. Therefore, a complete specification is achieved if at least 25 transitions between the functional states and 10 transitions between the functional and final states have been specified. Thus, good grounds exist to discuss the transitions proposed or excluded by the proposed FSM model (see Table 1).

As expected, the transition from a final to a functional state may be considered to be impossible in the case that recommissioning after a longer decommissioning phase is considered improbable or unfeasible. It is also quite understandable that threats without a significant influence on infrastructure's current functionality cannot induce a change of state (transitions 1(m), 3(t), 10(t), and 12(t)). This is also valid for the case that only a partial restoration of functions and tasks has been completed (18(m)). It is legitimate to ask for events where a persistence of states ($?_p$, p = persisting) may be achieved at other functional, states such as NOS! and d+FS. For example, the occurrence of a second threat with a potential influence on infrastructure's performance and functionality is a plausible reason to remain in the state NOS!. It may also be expedient to maintain the conditions for the redundant functionality at state d+FS in order to get the time needed for an efficient and effective realization of repair and restoration measures. All transitions proposed in [1,2] are induced by events, such as occurred threats or executed management decisions. The destructive impact of an occurred threat determines the resulting loss of the infrastructure's performance and functionalities with respect to technological functions, human activities, and socio-technical aspects of the infrastructure. A threat has the same disruptive effects on an infrastructure irrespective of whether or not situation awareness exists, therefore a transition from NOS! to d+FS (indicated as ($?_-$)) has to be equally as possible as the transition from NOS to d+FS. As expected, threats may cause additional losses of functionality, e.g., as seen at the transition from pFDS to nFDS (13(t)), d+FS to nFDS (21(t)), or d+FS to pFDS (22(t)).

Transition 4 indicates a special case, where an occurred threat increases the operator awareness (NOS to NOS!) without an immediate impact on the infrastructure's functionality. The monitoring of the infrastructure as well as the surveying of possible impacts is an essential prerequisite in order to get close to an overall or even holistic awareness of the infrastructure's situation [16]. Only on this basis can a correct decision be made at the right time in relation to the infrastructure's operation, maintenance, repair, restoration, or taking out of service. Thus, it makes sense that the state model should also take into account socio-technical processes serving the monitoring and assessment of situations and the use of assessment results in order to make normative as well as descriptive decisions at all functional states of the infrastructure, if necessary. As illustrated in Table 1, a more or less well-functioning infrastructure can be put into a final state of the set F (transitions 14(m), 15(m), 16(m), 17(m), and 23(m)–28(m)), but these transitions can only be initiated by corresponding management decisions. Management decisions also determine whether and when repair measures have to performed in order to recover the infrastructure's functionality and performance partially or even fully (transitions 9(m), 31(m), 20(m), 5(m), 30(m), and 7(m)). At this point, it should be noted that the transition to a state with higher performance and functionality will only be attained if the subjects of management decisions have been implemented and executed.

In summary, the FSM model proposed in [1,2] excludes transitions, indicated by ($?_+$), with increasing functionality (d+FS to NOS!, nFDS to d+FS, and pFDS to d+FS), transitions, indicated by ($?_p$) that prepare only the recovery of functionality (persisting of states NOS!, d+FS, and nFDS), and transitions, indicated by ($?_-$), due to which the resilient design avoids the immediate loss of functionality and performance (NOS! to d+FS). However, an FSM model used for the resilient design of infrastructures as a socio-technical system-of-systems has to encourage the developer, the operator, as well as the service provider to exploit all means for the infrastructure's improvement and protection. Therefore, the design of resilient infrastructures has to start with the consideration of all possible transitions in principle.

2.3. Unambiguous State Classification

The resilience of a system or infrastructure is often evaluated in relation to the required functionality and performance, taking into account that the internal and external conditions are changing. Therefore, it is reasonable that the states of the FSM model [1,2] reflect various levels of functionality and performance, which may occur and have to be clearly specified. Functionality is sometimes considered to be achieved if all system-made functions and human-completed tasks of the infrastructure are

successfully performed in compliance with the specifications. Alternatively, functionality can stand for the capability of a redundant system to provide services with at least a sub-set of successfully performed functions and tasks. The scope of infrastructure modelling, function/task-related or service-related, ultimately determines if a loss of a single function, within a redundant system, has no influence on the NOS or results in any state of degradation, e.g., pFDS, d+FS, or nFDS. Therefore, an important prerequisite for FSM modelling is the unambiguous setting of infrastructure boundaries to fix the requirements to be considered.

It also must be decided if the performance has to be considered either as an intrinsic property of functionality (e.g., provision of situational data with the required performance) or as an additional quality indicator of a performed task (provision of situational data with a certain accuracy and actuality).

If an FSM model is used for the design and operation of resilient infrastructures, a service-related holistic modelling approach is preferred. This implies that the related states have to be defined for each service supported by the infrastructure taking into account the functionalities needed for the service provision. Table 2 proposes the states of such an FSM model. One can note that each of the functionalities represented by the model requires a coordinated use of system-made functions and human-completed activities. Therefore, the states described in Table 2 have to be applied to single functional sub-systems.

Table 2. States of an extended FSM model specifically focusing on the service provision (using a ferry as example).

State of Service	System-Made Functions	Human-Done Tasks	Explanation	Example
Nominal Operational State (NOS)	A set-up of successfully performed functions ensures the service provision.	Humans' activities meet resources and requirements for nominal operation.	The requirements on service provision are met.	The ferry operates on time without intolerable risks and losses.
Sufficient Operational State (SOS)	Performance degradation occurs at one or few functions of the used functional setup.	Humans' activities are applied or performed in a sufficient manner.	The service is provided with a tolerable degradation of performance.	The ferry transportation is slightly delayed due to insufficient consideration of transport volume.
Performance Degraded State (PDS)	Performance degradation occurs at one or a few functions of the used functional setup, or disturbances and break downs decrease the capability of controlling.	Humans' activities are inadequately applied or performed.	The service is provided with a non-negligible degradation of performance.	The ferry is unable to provide the planned transportation service on time and volume due to rough weather conditions.
Functional Degraded State (FDS)	Failures and breakdowns of one or a few functions at the used functional setup results into partial service provision.	Humans' tasks are erroneously performed, or operation-relevant responsibilities are not perceived.	The scope of services is degraded.	One of the ferry ramps cannot be operated, the transportation of trucks is impossible.
Non-operational Disrupted State (nODS)	None of the supported functional setups achieves the ability of service provision.	Humans' lost the ability to perceive the operation-relevant responsibilities.	The provision of services is interrupted.	The staff team of the ferry is on strike or in quarantine.

Table 2. *Cont.*

State of Service	System-Made Functions	Human-Done Tasks	Explanation	Example
Damaged but Operational State* (d+OS)	None of the supported functional setup is able to provide the desired service (nODS), however, the service provision is continued for a certain time.	Humans' lost the ability to perceive the operation-relevant responsibilities (nODS), however, the service provision is continued for a certain time.	The service provision is temporary continued using alternative means.	The outage of ships navigational system is compensated by the support of coast guard.
Controlled Service Disruption (CSD)	-	-	Intended interruption of service provision for repair or maintenance.	

Table 2 does not include the final states introduced in [1,2] that indicate the end of an infrastructure's life cycle or the continued existence as a "new" infrastructure with changed or degraded service provision. An FSM model can renounce on the illustration of these states, i.e., F is empty, if a return to the listed states of service provision is excluded. However, the sole consideration of service provision under the consideration of system-made functions and human-made tasks is an insufficient approach to give guidance for the design of resilient infrastructures and as far as possible reliable service provision.

3. Suitability of FSM Modelling to Analyze Infrastructure's Resilience

FSM modelling of infrastructures promotes the specification of requirements for service provision and, consequently, the specification of the technical and operational requirements and conditions for individual components, functions, processes, and their coordinated interaction. This confirms the theory of [1,2] that FSM modelling can be used for the design of resilient infrastructures. However, if all resilience concepts are taken into account during the design phase, it becomes necessary to extend the boundaries of the infrastructure in order to enable the integrated consideration of core and accompanying services. These cover the complementary use of proactive means as well as reactive means to maintain the resilience of a considered infrastructure [3,4,14,31]. Proactive means are needed to detect degradations and changes and to initiate as soon as possible defensive and adaptive measures. Reactive means are the resources needed to restore, repair, or adjust the infrastructure on the functional or procedural level.

3.1. Situation Assessment

Situation assessment serves as much as possible the realistic ascertainment and assessment of the current state of the infrastructure based on the determined performance parameters and monitored behavioral characteristics of components, system-made functions, human-done activities and responsibilities, as well as internal and external conditions and constraints. The monitoring applies to all phases that may occur during the life cycle; during nominal robust operation, in times of controlled degradation as well as performed rebounding; and if unanticipated perturbations arise in comparison to criteria and assumptions of the initial design.

Comprehensive and realistic situational pictures and the correct sensing and interpretation of observations are essential prerequisites to support the adjustment of system functions and human activities to alternate conditions and to make the right decisions. Therefore, an FSM model used for the design of resilient entities should promote the generation process of current and emerging situation pictures being considered at all states of service provision. In addition, situation-related information should be utilized for the control and management of the infrastructure in and outside the times of service provision. Consequently, the generation and evaluation of situation pictures has

to be considered as an additional functionality whose states (available, comprehensive, true) are an influencing factor for infrastructure's resilience behavior.

This objective requires functions that integrate the monitoring, evaluation, and visualization (MEV) of the infrastructure's behavior at different levels, including the consideration of infrastructure-relevant conditions. Therefore, a second FSM model layer becomes necessary in order to model the states of situation assessment as an informational service in relation to the expected results of supported MEV functions. Principally, the MEV functions may be performed by the infrastructure itself or by external services. The results are used either as input for the control of the infrastructure or to trigger management decisions. In comparison to [1,2], where heightened awareness is considered a special state of nominal operation in times of a detected threat, it is important to perform the situation assessment during the whole life cycle of the infrastructure. Following [32], situation assessment has to serve both the early detection that "some things (may) go wrong" and the identification that "somethings may go better". In order to functionalize both for FSM modelling, the identification of the questions to be answered is required. Table 3 lists the services to be assessed and related subjects of assessment in cases where something goes wrong.

Table 3. Services to be assessed and subject of assessment, if "some things (may) go wrong".

Service to Be Assessed	Subject of Assessment	Purpose
Core Service (Operation)	■ The usability and performance of components and sub-systems ■ The availability of human resources and the effectiveness of their activities ■ The conditions influencing the infrastructure's capability of service provision	Evaluation of the current capability of infrastructure based on indicators recording the target-actual deviations in relation to specifications and conditions.
Core Service (Controlling)	■ The generation of control parameters ■ The selection of alternative usable setups for service provision (redundant, backup) ■ The adjustment capability of the infrastructure to internal and external conditions ■ The selection of best outcomes for service provision	Evaluation of the current capability of a robust infrastructure to adjust its operation to current conditions.
Situation Assessment	■ The completeness and quality of needed information ■ The closeness to reality of provided situation pictures	Evaluation of the trustworthiness of situation pictures
Decision Making	■ The correct interpretation of the situation to make the right decisions ■ The sustainable validity of executed operational decisions ■ The sustainable validity of made management decisions	Evaluation of correctness and validity of situation-based decision making
Operational Management of Infrastructure	■ The feasibility of aimed measures like maintenance, repair or decommissioning ■ The degree of implementation of intended measures ■ The effectiveness of implemented measures	Evaluation of feasibility and implementation degree of measures maintaining the resilience.

As explained before, the situation assessment has to be performed for all different layers of the infrastructure, which are involved either in the service provision or the preservation and protection of the resources in their interaction. Therefore, it is equally important to consider changes of all states (NOS, SOS, PDS, FDS, nODS, d+OS, and CSD) and also changes with respect to and during intended, expected, performed, or occurred transitions.

Table 4 lists the services to be assessed and related subjects of assessment in cases if some things may go better. As illustrated, the establishment and utilization of situational pictures is an essential prerequisite to enable effective maintenance of resilience. This insight is not new with respect to the importance of monitoring as one of the four cornerstones of resilience [15–17,27,31–33]. Thus, models used for the design of resilient infrastructures should consider the infrastructure's ability to monitor and survey.

Table 4. Services to be assessed and subject of assessment, if "some things (may) go better".

Service to Be Assessed	Subject of Assessment	Purpose
Core Service (Operation and (Controlling)	■ The future use of improved components and systems, which become available by the technological progress ■ A more effective adjustment of the infrastructure's operation (functions and human activities) to current and changing conditions (use of practice-proven models, tracing and tracking of models and controlling). ■ A better coordination of human activities due to the use of common situation pictures ■ The adaptability of the infrastructure's operation to diversity of internal and variety of external conditions ■ The adjustment of the infrastructure's controlling to changing targets (achieve as much as possible) ■ Continuously training and qualification of staff (lesson learnt, best practice experience exchanges) for effective working under variable conditions	The identification of possibilities and opportunities to decrease the vulnerability, to increase the performance, to reduce environmental impact or to be adaptable.
Situation Assessment	■ Availability and quality of database (integrity) ■ Performed quality assessment (function and procedures) ■ Relevance and significance of derived observations ■ Trustworthiness and completeness of generated situation pictures ■ Residual scope of interpretation and correctness of situation evaluation	The identification of possibilities and opportunities for the enhancement of situation assessment of infrastructures.
Decision Making	■ The capability to make the right decisions at the right time ■ The ongoing validity of decisions (re-decision or re-adjustment, if necessary) ■ the utilization of gain of knowledge	The identification of possibilities and opportunities for improved decision making.
Management of Infrastructure during its Lifetime	■ The improvement of the demand-controlled and situation-related information and communication culture and management ■ The advanced utilization of monitoring and surveying results for an adaptive maintenance of the infrastructure taking into account the current wear and tear as well as the availability and usability of resources ■ The evaluation of the effectiveness of measures (management feedback and conditioning)	The identification of possibilities and opportunities to increase efficiency and effectivity of infrastructure operation and utilization during its lifetime

As mentioned above, monitoring is responsible for the provision of information necessary for the generation and assessment of situational pictures. For this purpose, data has to be gathered, exchanged, fused, analyzed, and used. The variety of questions to be answered leads to a broad spectrum of situation pictures that differ, for example, in the database, complexity, and data preparation. They have in common that only a correct reflection of reality allows the correct assessment of the situation. A correct reflection of reality is only achieved if the availability and trustworthiness of required information can be ensured on the functional and operational level. Consequently, FSM modelling of resilient infrastructures must not only be able to elaborate the role of MEV functions and activities for monitoring, control, and management but should also consider how malfunctions as well as bad and outdated decisions can be detected and compensated.

3.2. Event-Based Versus Time-Controlled State Modelling

The state machine model introduced in [1,2] considers a state transition as the system response to an occurred event. Effectively, two types of events are discussed: a) Threats that sooner or later result into a loss of functionality and performance, and b) decisions that either change directly the state of infrastructure (switching-off of parts, interruption of service provision, or decommissioning) or initiate an implementation of measures, whose successful realization will result in a state transition. A purely event-driven state machine model is unable to consider and optimize the factor time in the development and operation of resilient infrastructures. However, time plays an important role for the safeguarding of the infrastructure's functionality and performance as well as for the four cornerstones of resilience. For example, early recognition of an emerging bottleneck in relation to the point of no return requires a sophisticated monitoring approach to get the time needed to fend or counterbalance the causes, degradations, as well as consequences.

The monitoring of the situation has to be a routine function/task to be performed in all states as well as in relation to transitions that take place. For this purpose, the acquisition, processing, and exchange of data have to be coordinated and temporally synchronized. Situational pictures (as a snapshot as well as recorded changes) have to be up to date and close to reality. Sophisticated assessment methods have to be used in order to interpret the current situation and to make the right decisions at the right moment. This equally applies to the timely initiation of preventive measures (e.g., maintenance, operation control, and resource management) and reactive measures (e.g., repair, restoration, and damage containment). The effectiveness of measures often depends on its time-efficient realization and requires the consideration of the factor time. This also allows for verification of the sustainability of made decisions in relation to changing conditions and for corrections of these decisions, if necessary.

Thus, it can be concluded that during execution of the FSM model, a synchronous clocking of the transitions is required in order to represent the dependencies and interactions between operation, monitoring, management, as well as the measures of the infrastructure in their temporal context, taking into account time aspects and time constraints. The clocking frequency must be selected such that it is compliant with the update rate needed to monitor the internal as well as external changes of relevance. Monitoring/surveying and evaluation/assessment have to be performed in time. It is then possible to gain the time to initialize and execute preventive measures against emerging threats or to prepare and schedule damage containment and recovery measures in a forward-looking efficient and effective manner. In conclusion, a state model used for the design of resilient infrastructures should be time controlled. This also implies that each state can transition into itself, i.e., the set Σ of transitions must be extended accordingly.

3.3. Infrastructure's State of Service Provision

It is important to consider that an infrastructure usually provides more than one service. Therefore, it is necessary to differ between the set of states S_I representing the abilities of the infrastructure as a system-of-system and the set of states $S_{S(k)}$ representing the abilities of the sub-system providing one of the services (k = 1 . . . K, number of supported services).

In general, the states of infrastructures are determined by the states of subsystems providing the supported services: $S_I = F\{ S_{S(1)}, S_{S(2)} \ldots S_{S(K)}\}$. A set of states, S_I as well as $S_{S(k)}$, covers a certain number N of states: N = 5, if the model in [1,2] is used, or N = 7, if the extended model of Table 2 is applied. A higher number of states enables illustration of the supported levels of functionality and performance with a higher resolution. Assuming that the requirements for provision of each service are clearly specified and the fulfilment of requirements can be proven (offline rather than online by evaluation of the outcome), the current state n (n≤N) of the service-providing sub-system can clearly be determined for each time point within its lifecycle (see Figure 1).

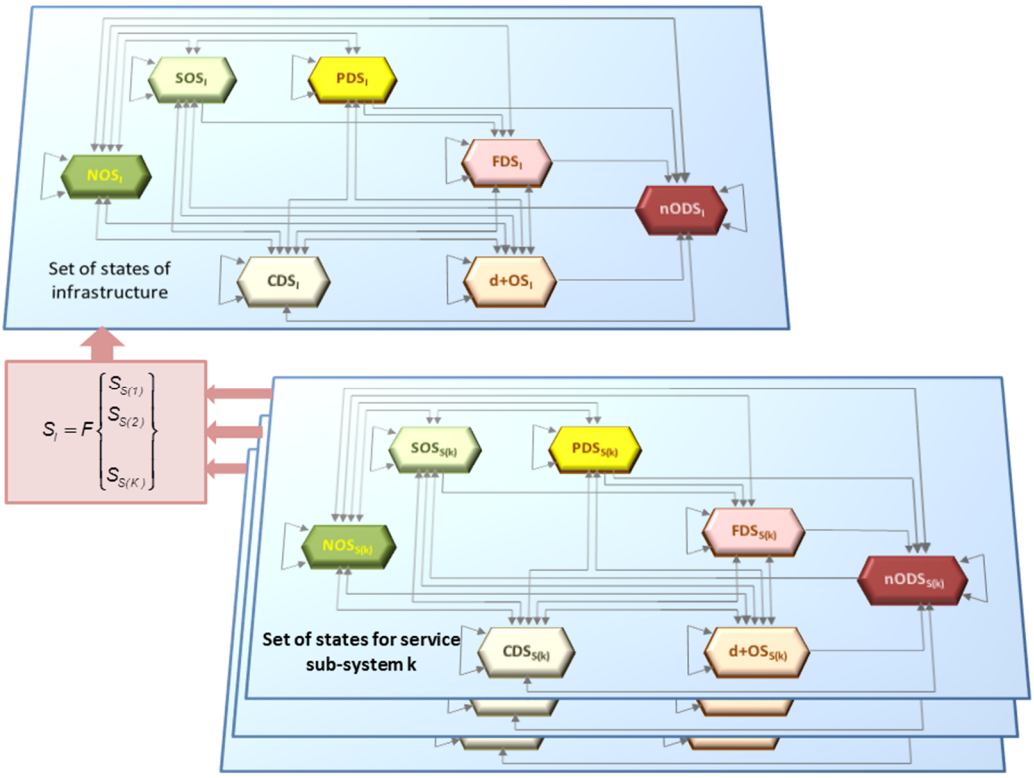

Figure 1. Infrastructure's states of service provision (gray lines indicate the principle bidirectional transitions between states, including the remaining in a state corresponding to Table 2) and the relation to the states of sub-systems.

A complex infrastructure, as shown in Figure 1, has the capability of providing more than one service, e.g., K = 3 services. In compliance with Table 2, each sub-system takes one of the N = 7 states. Therefore, an infrastructure with K = 3 independent services has, principally, up to L = 343 states to illustrate the capability of infrastructure's multi-service provision. This complexity may be reduced ($L \leq N^K$), if either the sub-systems used for service provision are correlated or the variety of states is grouped into a lower number of infrastructure states. In both cases, the interdependencies between the states of sub-systems and the states of infrastructures have to be clarified.

An infrastructure is a priori a complex system, because robust and resilient operation of the core systems requires monitoring of the infrastructure as well as monitoring of the internal and external conditions. The sub-system performing the monitoring and ensuring the access to further information has to be modelled as an accompanying service system with its own states. Consequently, a multi-layer FSM model approach becomes necessary.

3.4. Multilevel Consideration of Infrastructures

Infrastructures are socio-technical systems or systems-of-systems that comprise a multitude of single resources (components, systems, human), needed functionalities, and activities up to their more or less successful coordination on a functional, control, and risk management level within service supply chains and beyond. In order to represent such complex systems, one should apply a hierarchical view on the current state of the infrastructure, defining global states and related sub-states.

Figure 2 illustrates such a hierarchical consideration of states. Here, the system is in the current global state FDS of service provision. This implies that the system properties characterized by indicators should lay in the value ranges, which are assigned to the state FDS. Within the hexagon, each point defines a potential sub-state of the global state FDS with a certain value assignment with regard to the value ranges allowed for the global state FDS. Each point has a directional marker to depict the changes of the system properties due to external or internal events and influences.

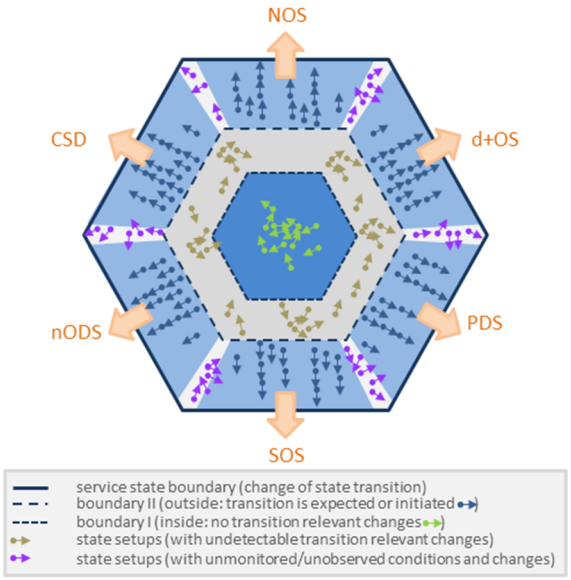

Figure 2. Infrastructure's state setups assigned to state FDS of service provision.

For the resilient operation of an infrastructure, it is desirable to be aware of the current and emerging situation through comprehensive knowledge regarding internal and external conditions, changes, and events. Only then, it can be expected that proper management decisions and effective implementations of identified measures can be made.

Hence, further layers of sub-states are added. A green point inside boundary I (narrow dashed line) represents sub-state setups of the infrastructure, at which changes that are relevant for transitions between global states never occur. From a global view, the infrastructure is in a steady state. Beige points in the area between boundary I and II (dashed line) are sub-state setups of the infrastructure, where changes that are relevant for global transitions already occur. However, these small-scale changes remain undetectable from the global view due to the limited capacity and sensitivity of the applied monitoring and surveying. For these setups, there is the opportunity to use improved monitoring and forecasting in order to increase the scope of actions for a more efficient and effective control and management of the infrastructure. The points between boundary II and the FDS state boundary (thick line) indicate the sub-state setups, where a certain transition to the other global state is in progress or is initiated (made decision with scheduled measures). A routine re-evaluation of ongoing changes, decisions, and actions at these points is an additional means to adjust the infrastructure's operation and management at all layers. The blue points in this area (dark background) represent the cases where the change is recognized from a global view. The purple points in this area (brightened background) represent the cases where undetected threats and changes will result, sooner or later, in an unexpected

degradation or interruption of the entities' service provision. Due to the existing lack of knowledge (incorrect or delayed situation pictures), it is impossible to avoid the emerging transition by a suitable compensation measure and to reduce the losses by effective damage containment.

The example illustrates that the state of change occurs sometime between the start and the end time of the transition process. The time period between the start of the transition process (boundary I) and an occurred state of change (service state boundary) represents the available time period to initiate and perform defensive and protective actions, if the advancing transition has been perceived. In general, it can be expected that the longer the time period, the higher the probability of success.

3.5. Monitoring as Functionality

As a logical consequence of the previous discussion, the monitoring must be considered as an additional functionality of the infrastructure, which the time-controlled FSM modelling must take into account. Functions are needed to monitor the system itself (capacity and performance capability) and the environment (dependencies and influencing factors), ensuring that infrastructure-relevant changes become detectable [17]. At this point, the question arises "What requirements have to be met by the monitoring?". First, it has to be specified what has to be monitored. In general, this may be properties as well as anomalies or forecasted probabilities of negative events or threats. Second, the applied monitoring technique should be able to determine the right identifiers for this purpose. Ultimately, the determination and assessment of identifiers should be performed in such a way that the achieved reliability and accuracy of the monitoring results enables the required situation-adjusted maintenance of resilience. From today's perspective, it is nearly impossible to predict when monitoring becomes necessary. Therefore, the monitoring needs to be conducted routinely. However, monitoring is a time-discrete process, irrespective of who (human-made) or what (machine-made) realizes the monitoring. It has to be remarked that the right selection of the sampling frequency has a decisive influence on the trustworthiness of the monitoring results. Oversampling, which means monitoring is performed more frequently than necessary, ties up resources and is cost intensive. Undersampling occurs if the sampling theorem is violated [34], e.g., the monitoring frequency is not sufficient to detect the occurred change. If undersampling effects remain uncompensated, the resulting loss of information impairs the detection of changes of interest. This implicates that the functionalization of monitoring requires careful consideration of the time aspects.

3.6. Functional Integration of Situation-Based Adjustment Processes into Models

The establishment of situation awareness (monitoring/surveying; evaluation/assessment) and situation-based adjustment (controlling and management of infrastructure) has to be considered as socio-technical processes, which are important factors for the overall infrastructures' resilience. Therefore, both the production of "situation awareness" and the realization of "situation-based adjustment" have to be functionalized and networked with preferably unambiguously specified targets.

- The first target of monitoring is focused on the control of the infrastructure to adjust resources and their interactions to current and emerging conditions in order to achieve the required operability of the infrastructure in relation to the intended service provision. The control serves the efficiency and safety of the infrastructure and is primary a system internal functionality. However, for this purpose, access to additional data and information is often needed to enable the control parameter to be routinely adjusted to internal and external conditions.
- The second target of monitoring aims for efficient adjustment and maintenance of the infrastructure in relation to diverse changes. For this purpose, the performance of the operational service provision, system characteristics, and environmental conditions have to be monitored and assessed. The establishment of these situation pictures may be done by the infrastructure itself (self-monitoring and self-surveying of infrastructure's status and relevant conditions) or by

external services (independent monitoring/surveying of infrastructure and providing of additional information to complete the situation pictures).

- The third target of monitoring serves the surveying of emerging needs and challenges coming from social, economic, ecologic, legal, ethic, or other aspects. They create the informational basis to analyze critically whether, and if so, to what extent, the service providing system has to be modified or even decommissioned, temporally or permanently.

The results of the complementary monitoring processes are the input needed for decision making in relation to infrastructure's operation, maintenance, modernization, or decommissioning as well as to infrastructure's safety and security. The multi-layer system model shown in Figure 3 depicts how the functionalities "situation assessment" and "situation-based adjustment" can be implemented and networked.

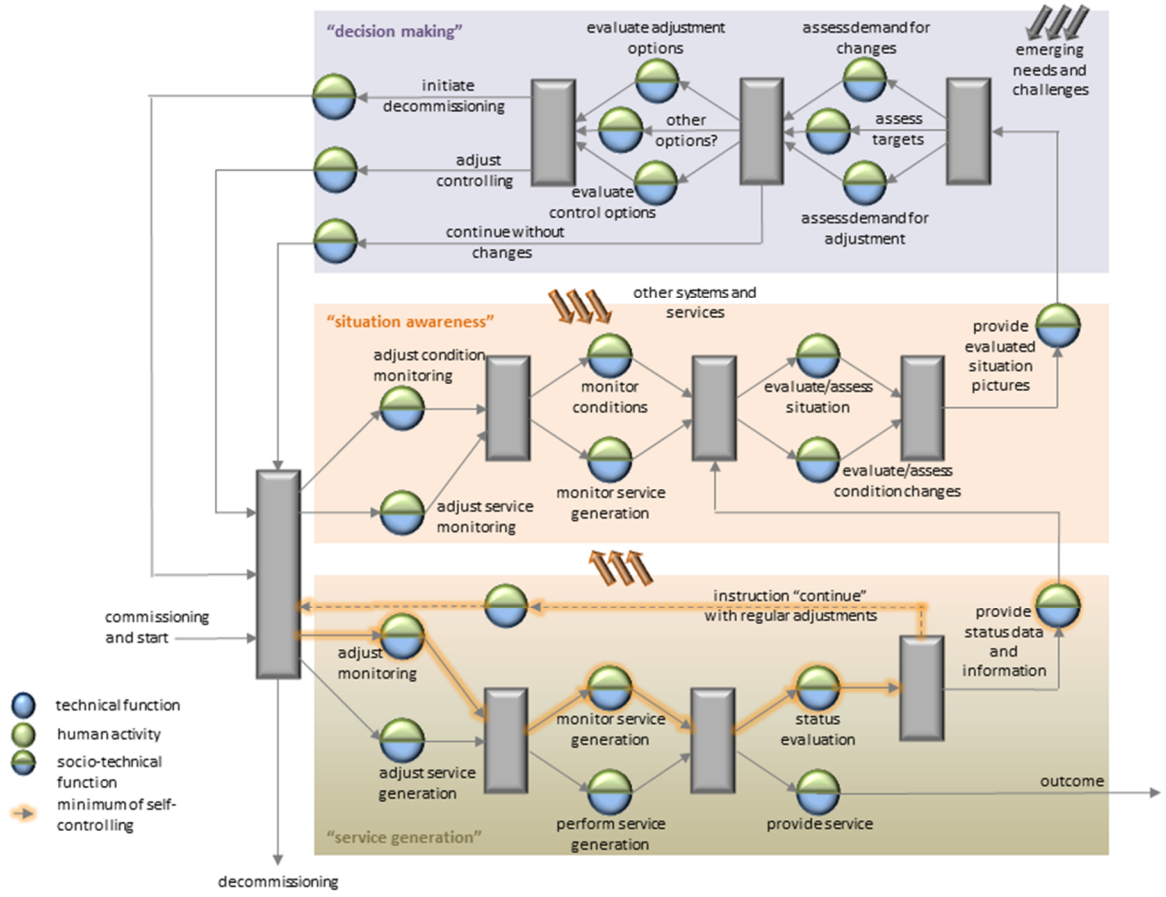

Figure 3. Simplified system model functionalizing situation awareness and decisions about situation-based adjustment processes.

The lower layer "service generation" represents the functions needed to establish the production chain for the provision of an infrastructure's service and the monitoring chain for the operational control of this service provision. As can be seen, if the internal status evaluation of infrastructure leads to no complaints, the service provision can be continued. Otherwise, the situation must be analyzed (medium layer) in order to be able to implement the right compensatory measures (upper layer). In dependence on the applied degree of automatization, each function (shown as a circle in Figure 3) may be performed either by humans (blue circle), technological systems (green circle), or a combination of both (blue/green circle). For the sake of generality, each function is depicted in Figure 3 as a socio-technical function. With growing levels of digitization and automatization, human activities will increasingly restrict observation of the fully automated operation of the infrastructure. Then, it

has to be expected that the layer "service generation" and "situation assessment" will be realized exclusively by technical functions.

The medium layer "situation awareness" represents all additional monitoring and surveying functions arranged outside the "service generation system" and completing the "situation assessment" of the infrastructure. These monitoring and surveying functions enable the provision of accompanying services and can be performed by the infrastructure itself or by external bodies with shared responsibilities. As shown, the layer "situation awareness" addresses services for the independent monitoring of service generation as well as services monitoring various influencing conditions (social, economic, ecologic, legal, ethic, or other aspects). The functions "adjust condition monitoring" and "adjust service monitoring" represent the principal capability to adapt the monitoring to new challenges and influencing aspects.

The high layer "decision making" represents exemplarily a set of functions evaluating and assessing the current situation based on evaluated situation pictures (provided by the medium layer) and additional information in relation to new needs and challenges coming from social, economic, ecologic, legal, ethic, or other aspects. Decision processes are either one or two tiered. The first stage (right-hand functions) assesses the need for changes and a second stage (left-hand functions) evaluates the options for the implementation of changes. The decision process may result in three fundamental decisions: (1) To continue the operation of infrastructure without changes; (2) to adjust the control to new targets and/or conditions; and (3) to initiate a temporary or permanent decommissioning.

Consequently, FSM modelling used for the design of resilient infrastructures requires more than one model layer to illustrate and describe the functioning and interaction between the different system layers of an infrastructure dealing with service generation, situation awareness, and decision making.

3.7. Discussion

If FSM modelling is used for the design of resilient infrastructures, the complete process of service provision has to be taken into account and needs to be converted into functions regardless of whether individual functions and tasks are performed by humans or machines. However, for the effective application of FSM modelling, several problems have been identified, which still need to be solved in an efficient manner. For the proposed FSM model [1,2], a gap is identified in relation to the representation and illustration of monitoring functions as supplementary services for situation assessment and situation-based adjustment. This gap has to be closed, e.g., by using multi-layer FSM models [35,36]. The same applies to the processes of infrastructure preparedness to manage and perform maintenance and recovery activities, to control unavoidable degradations, as well as to avoid or limit damages. The consideration of the factor time is essential to elaborate the dependencies and interactions between operation, monitoring, and management, as well as to consider and optimize measures of the infrastructure in their temporal context, taking into account time aspects and time constraints. A time-controlled multi-layer FSM model extends the applicable toolkit for an even greater improvement of the infrastructure's resilience. On the one hand, forecasting as part of predictive situation assessment can be taken into account as a prerequisite for hazard prevention and damage limitation. On the other hand, additional layers may be used to evaluate the validity and effectiveness of decisions and to consider the possibilities for timely corrections. In summary, from this research, FSM modelling was found to be a suitable approach for the design of resilient infrastructures, if the ability of robust service provision and effective rebounding are addressed. The additional consideration of accompanying services extends the infrastructure's boundaries and may increase the functional complexity to be modelled by FSM. This, however, complicates the handling of modelling, increases the indeterminacy, and requires an abstraction of functional modelling, which is possible in principle.

Another and rather critical point of FSM modelling is the inflexible specification of states, associated setups of characteristics, as well as transition conditions within defined system boundaries. This complicates the use of FSM modelling, if resilience also focuses on the sustained adaptability of an infrastructure or its ability to avoid brittleness. Due to the runtime changes, an infrastructure under

consideration becomes an infinite state machine with a potentially uncountable number of states and transitions. Alternatively, a suitable way has to be found, enabling the the FSM model of the infrastructure to be adapted (e.g., change of external and internal conditions and characteristics) and/or extended (e.g., by temporal activating of additional capacities) during its lifetime.

4. Conclusions

This study identified the potentials and limitations of FSM modelling as proposed in [1,2] in relation to the intended applications: Design of resilient infrastructures [1,2,37] as well as evaluation and indication of the resilience level currently supported by the infrastructure. The ability of FSM modelling to describe technological as well as socio-technical systems in their changeability was identified as a clear advantage. For this purpose, the finite number of states has to be defined in order to represent the entire range of system characteristics under normal routine as well as under disturbed conditions, and after the occurrence of destructive events. The states have to be clearly described by qualitative statements and quantitative performance parameters. In general, transitions between two states correspond to a change of system characteristics and occur only if the specific transition conditions (changes, events) are satisfied. The transition conditions must also be clearly defined, whereby the transition as a process has to be described, e.g., by further FSM models, in order to enable the representation of additional functional layers like monitoring.

The findings of this study are of a theoretical nature, and is a fundamental step in order to pave the way in the future for more practical studies that elaborate on how to integrate the FSM approach into the design of resilient infrastructures.

Author Contributions: For this research article the specifying of the individual contributions of the authors is as follows: conceptualization, E.E., and M.B.; methodology, E.E. and M.B.; investigation, E.E., M.B. and F.S.T.; visualization, E.E.; writing—original draft preparation, E.E., M.B., and F.ST.; writing—review and editing, E.E., M.B. and F.S.T.; supervision, M.B. and S.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by DLR's research program "Maritime Security".

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

References

1. Jackson, S.; Ferris, T.L.J. Designing Resilient Systems. In *Resilience and Risk*; Springer: Dortrecht, The Netherlands, 2017; pp. 121–144. [CrossRef]
2. Jackson, S.; Cook, S.; Ferris, T.L. A Generic State-Machine Model of System Resilience. *INCOSE Insight* **2015**, *18*, 14–18. [CrossRef]
3. European Commission: The eu Approach to Resilience: Learning from Food Security Crises, Communication from the Commission to the European Parliament and the Council, 3.10.2012, Brussels. Available online: http://ec.europa.eu/echo/files/policies/resilience/com_2012_586_resilience_en.pdf (accessed on 1 May 2019).
4. United Nations Office for Disaster Risk Reduction (UNISDR): UNISDR Terminology on Disaster Risk Reduction. Available online: http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf (accessed on 15 July 2019).
5. Sansavini, G. Engineering Resilience in Critical Infrastructures. In Proceedings of the NATO Advanced Research Workshop on Resilience-based Approaches to Critical Infrastructures Safeguarding, Azores, Portugal, 26–29 June 2016. [CrossRef]
6. Baoping, C.; Min, X.; Yonghong, L.; Yiliu, L.; Renjie, J.; Qiang, F. A novel critical infrastructure resilience assessment approach using dynamic Bayesian networks. In *AIP Conference Proceedings*; AIP Publishing LLC: Melville, NY, USA, 2017; Volume 1890. [CrossRef]
7. Hosseini, S.; Barker, K. Modeling infrastructure resilience using Bayesian networks: A case study of inland waterway ports. *Comput. Ind. Eng.* **2016**, *93*, 252–266. [CrossRef]
8. Qiang, F.; Xiujie, Z.; Dongming, F.; Baoping, C.; Yiqi, L.; Yi, R. Resilience design method based on meta-structure: A case study of offshore wind farm. *Reliab. Eng. Syst. Saf.* **2019**, *186*, 232–244. [CrossRef]

9. Almoghathawi, Y.; Barker, K.; Albert, L.A. Resilience-driven restoration model for interdependent infrastructure networks. *Reliab. Eng. Syst. Saf.* **2019**, *185*, 12–23. [CrossRef]
10. Mathias, J.D.; Spierre Clark, S.; Onat, N.; Seager, P. An Integrated Dynamical Modeling Perspective for Infrastructure Resilience. *Infrastructures* **2018**, *3*, 11. [CrossRef]
11. Mostafavi, A. A System-of-Systems Approach for Integrated Resilience Assessment in Highway Transportation Infrastructure Investment. *Infrastructures* **2017**, *2*, 22. [CrossRef]
12. Ngamkhanong, C.; Kaewunruen, S.; Afonso Costa, B.J. State-of-the-Art Review of Railway Track Resilience Monitoring. *Infrastructures* **2018**, *3*, 3. [CrossRef]
13. Thomas, J.E.; Eisenberg, D.A.; Seager, T.P. Holistic Infrastructure Resilience Research Requires Multiple Perspectives, Not Just Multiple Disciplines. *Infrastructures* **2018**, *3*, 30. [CrossRef]
14. International Maritime Organisation (IMO): Guidelines for Shipborne Position, Navigation and Timing (Pnt) Data Processing. Available online: https://www.transportstyrelsen.se/contentassets/46eb2d62cb848309a7749cc85ce6362/1575.pdf (accessed on 1 October 2019).
15. Woods, D.D. Four concepts for resilience and the implication for the future resilience. In *Reliability Engineering and System Safety*; Elsevier: Amsterdam, The Netherlands, 2015; Volume 141, pp. 5–9. [CrossRef]
16. Hollnagel, E. RAG—The resilience analysis grid. In *Resilience Engineering in Practice-a Guidebook*; Hollnagel, E., Paries, J., Woods, D.D., Wreathall, J., Eds.; Publisher Ashgate Pub Co.: Burlington, NJ, USA, 2011.
17. 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.
18. Engler, E.; Göge, D.; Brusch, S. ResilienceN–a multi-dimensional challenge for maritime infrastructures. In *OUR SEA: International Journal of Maritime Science & Technology*; University of Dubrovnik: Dubrovnik, Croatia, 2018. [CrossRef]
19. Fiksel, J. Designing resilient, sustainable systems. *Environ. Sci. Technol.* **2003**, *37*, 5330–5339. [CrossRef] [PubMed]
20. Praetorius, G.; Graziano, A.; Schröder-Hinrichs, J.U.; Baldauf, M. FRAM in FSA—Introducing a Function-Based Approach to the Formal Safety Assessment Framework. In *Advances in Human Aspects of Transportation. Advances in Intelligent Systems and Computing*; Springer: Los Angeles, LA, USA, 2017; Volume 484. [CrossRef]
21. Schröder-Hinrichs, J.U.; Praetorius, G.; Graziano, A.; Kataria, A.; Baldauf, M. Introducing the Concept of Resilience into Maritime Safety. In Proceedings of the 6th Resilience Engineering Association Symposium, Lisboa, Portugal, 22–25 June 2015.
22. Holcombe, W.M.L. *Algebraic Automata Theory*; Cambridge University Press: Cambridge, UK, 1982; pp. 25–71.
23. Lunze, J. *Ereignisdiskrete Systeme: Modellierung und Analyse Dynamischer Systeme Mit Automaten, Markovketten und Petrinetzen*; Oldenbourg Wissenschaftsverlag: München, Germany, 2006.
24. Moore, E.F. Gedanken-experiments on Sequential Machines. In *Annals of Mathematical Studies*; Princeton, N.J., Ed.; Princeton University Press: Princeton, NJ, USA, 1956; pp. 129–153.
25. Wagner, F.; Schmuki, R.; Wolstenholme, P.; Wagner, T.H. *Modeling Software with Finite State Machines: A Practical Approach*; Auerbach Publications: Boca Raton, FL, USA, 2006; pp. 63–75.
26. Baoping, C.; Xiangdi, K.; Yonghong, L.; Jing, L.; Xiaobing, Y.; Hongqi, X.; Renjie, J. Application of Bayesian Networks in Reliability Evaluation. *IEEE Trans. Ind. Inform.* **2019**, *15*, 2146–2157.
27. Woods, D.D.; Chan, Y.J.; Wreathall, J. The Stress-Strain Model of Resilience to Operationalize the Four Cornerstones of Resilience Engineering. In Proceedings of the 5th Symposium on Resilience Engineering: Managing trade-offs, Soesterberg, The Netherlands, 24–27 June 2013.
28. Lundberg, J.O. Situation Awareness States, Systems, and Processes: A holistic framework. *Theor. Issues Ergon. Sci.* **2015**, *16*, 447–473. [CrossRef]
29. Endsley, R.M. *Designing for Situation Awareness: An Approach to User-Centered Design*, 2nd ed.; CRC Press Taylor & Francis Group: Boca Raton, FL, USA; London, UK; New York, NY, USA, 2011; pp. 13–28.
30. Endsley, M.R. Toward a theory of situation awareness in dynamic systems. *Hum. Factors* **2017**, *37*, 32–64. [CrossRef]
31. Woods, D.; Branlat, M. Essential characteristics of resilience. In *Resilience Engineering in Practice-a Guidebook*; Hollnagel, E., Paries, J., Woods, D.D., Wreathall, J., Eds.; Publisher Ashgate Pub Co.: Burlington, NJ, USA, 2011; pp. 21–34.

32. 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).
33. Hollnagel, E. Prologue: The scope of Resilience. In *Resilience Engineering in Practice-a Guidebook*; Hollnagel, E., Paries, J., Woods, D.D., Wreathall, J., Eds.; Publisher Ashgate Pub Co.: Burlington, NJ, USA, 2011.
34. Gallager, R.G. *Principles of Digital Communication*; Cambridge University Press: Cambridge, UK, 2008.
35. Wreathall, J. Monitoring–A critical ability in Resilience Engineering. In *Resilience Engineering in Practice-a Guidebook*; Hollnagel, E., Paries, J., Woods, D.D., Wreathall, J., Eds.; Publisher Ashgate Pub Co.: Farnham, UK, 2011.
36. Engler, E.; Baldauf, M.; Banyś, P.; Heymann, F.; Gucma, M.; Sill Torres, F. Situation Assessment—An Essential Functionality for Resilient Navigation Systems. *J. Mar. Sci. Eng.* **2020**, *8*, 17. [CrossRef]
37. Jackson, S.; Ferris, T.L.J. Resilience Principles for Engineered Systems. *Syst. Eng.* **2013**, *16*, 152–164. [CrossRef]