Applications

Eva Brucherseifer*, Hanno Winter, Andrea Mentges, Max Mühlhäuser and Martin Hellmann

Digital Twin conceptual framework for improving critical infrastructure resilience

Rahmenkonzept für Digitale Zwillinge zur Verbesserung der Resilienz kritischer Infrastrukturen

https://doi.org/10.1515/auto-2021-0104
Received July 27, 2021; accepted October 18, 2021

Abstract: Critical infrastructures are the backbone of our societies with increasingly complex and networked characteristics and high availability demands. This makes them vulnerable to a wide range of threats that can lead to major incidents. Resilience is a concept that describes a system's ability to absorb and respond to disturbances, as well as to learn from the past and anticipate new threats.

In this article, we apply the Digital Twin concept to the infrastructure domain to improve the system's resilience capabilities. We conduct a comprehensive requirements analysis related to infrastructure characteristics, crisis management and resilience measures. As a result, we propose a Digital Twin Conceptual Framework for critical infrastructures. We conclude that the Digital Twin paradigm is well suited to enhance critical infrastructure resilience.

Keywords: digital twin, conceptual framework, critical infrastructure systems (CIPs), disaster management, resilience cycle

Zusammenfassung: Kritische Infrastrukturen sind das Rückgrat unserer Gesellschaften, die zunehmend komplexer und vernetzter werden und hohe Anforderungen an die Verfügbarkeit stellen. Dies macht sie anfällig für ein breites Spektrum an Bedrohungen, die zu größeren Störungen und Großschadenslagen führen können. Resilienz ist ein Konzept, das die Fähigkeit eines Systems beschreibt, Störungen zu absorbieren, auf sie zu reagieren sowie aus der Vergangenheit zu lernen und sich auf neue Bedrohungen vorzubereiten.

In diesem Artikel wenden wir das Konzept des Digitalen Zwillings auf Infrastrukturen an, um die Resilienzfähigkeiten der Systeme zu verbessern. Wir führen eine umfassende Anforderungsanalyse in Bezug auf Eigenschaften der Infrastrukturen, Krisenmanagement und Resilienzmaßnahmen durch. Auf dieser Basis schlagen wir ein Rahmenkonzept für Digitale Zwillinge für kritische Infrastrukturen vor. Wir kommen zu dem Schluss, dass das Paradigma des Digitalen Zwillings gut geeignet ist, die Widerstandsfähigkeit kritischer Infrastrukturen zu verbessern.

Schlagwörter: Digitaler Zwilling, Rahmenkonzept, Kritische Infrastrukturen (KRITIS), Katastrophenschutz, Resilienzzyklus

1 Introduction

Modern societies depend on the unrestricted availability of their critical infrastructures and their services. Critical infrastructures include, for example, water, food and energy supplies, transportation systems, telecommunications systems, and healthcare.

Due to the increasing level of automation and digitalization, infrastructure systems, processes and resources are gaining in complexity and form highly interconnected networks. The behavior and demand of society have a strong influence on the technical systems and must be considered as part of these systems. In addition, humans are involved in service delivery. These complex sociotechnical systems interact with each other while continuously providing essential services to their respective communities [1].

***Corresponding author: Eva Brucherseifer,** DLR Institute for the Protection of Terrestrial Infrastructures, Sankt Augustin, Germany, e-mail: eva.brucherseifer@dlr.de
Hanno Winter, DLR Institute for the Protection of Terrestrial Infrastructures, Darmstadt, Germany, e-mail: hanno.winter@dlr.de
Andrea Mentges, DLR Institute for the Protection of Terrestrial Infrastructures, Sankt Augustin, Germany, e-mail: andrea.mentges@dlr.de
Max Mühlhäuser, Telecooperation Lab, Technical University of Darmstadt, Darmstadt, Germany, e-mail: max@tk.tu-darmstadt.de
Martin Hellmann, DLR Program Coordination Defence and Security Research, Cologne, Germany, e-mail: martin.hellmann@dlr.de

Infrastructures are not only exposed to manageable disruptions and failures, but also to extreme events such as extreme weather events, mechanical failure, human failure, accidents, attacks, and previously unknown and thus non-specified events. Such events can exceed feasible safety and security measures in place. Unexpected and unpreventable disruptions can cause cascading failures that propagate through the infrastructure systems especially in the light of counter-intuitive system behavior [2]. Therefore, it is vitally important to strengthen the resilience of critical infrastructures towards any kind of disruption or catastrophe, to preserve these lifelines during and after disruptive events [1, 3].

In the context of critical infrastructures, resilience describes the ability to continue providing essential services reliably and with little interruptions in the face of disruptive events of any kind [4]. In general, the resilience of a system depends on a set of dynamic skills and coping strategies. A highly resilient system is prepared for disruptions of unknown nature, monitors anomalies, responds and recovers in the immediate situation, learns from the past, and adapts to new threats. Resilience complements the generally accepted design goals of efficiency, usability and sustainability [5].

Since 2017, the new concept of Digital Twins has been increasingly adopted by research and industry for application in many fields such as industrial manufacturing, process industry, building management, health and smart city [6, 7]. Digital Twins are applied as a comprehensive tool that can be used to monitor, analyze, control, and optimize a system throughout its entire lifecycle [8]. Due to the ongoing efforts in the area of digitalization, implementation of Digital Twins of large-scale systems become more and more feasible.

First introduced by Grieves in 2002, the Digital Twin describes a concept of a connected virtual representation of a real system, with both instances coupled to each other in real-time [9]. The virtual instance models and augments the real system in as much detail and accuracy as necessary for the intended use case, i. e., with regard to its form, function and behavior. In contrast to classical models, Digital Twins are bidirectionally coupled by means of a twinning mechanism (Figure 1). This ensures the virtual replica to be in an up-to-date state. Tools utilizing the replica can implement smart functionalities, simulation and control action on the real object.

With its up-to-date nature, integrated smart and adaptive functions, and digital methods, the Digital Twin concept represents a potential approach to the field of infrastructure services. Together with appropriate tools, the virtual object can increase the resilience of infrastructure services at the operational level.

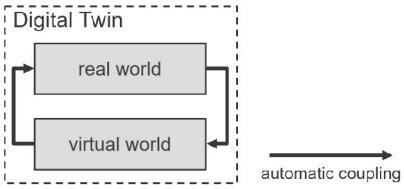

Figure 1: Basic structure of a Digital Twin, following the illustration proposed by Grieves and Vickers [9] and Kritzinger and colleagues [10]. It consists of a *real object* and a *virtual object*, which are bidirectionally coupled in an automatic manner via *twinning components*.

Based on these introductory assumptions, in this paper, we examine in more detail the applicability of the Digital Twin concept to improve resilience of critical infrastructure operation and protection. We first derive implementation requirements from the scope of critical infrastructure, crisis management and resilience methods, which we map to the Digital Twin concept. In Section 4, we introduce a Digital Twin Conceptual Framework for infrastructures consisting of guiding principles and a conceptual model. We show that the Digital Twin paradigm is well suited for a framework that promotes increased resilience in all phases of a crisis.

2 Resilience in critical infrastructure systems

In the following section, we present our understanding of the term *infrastructure* with a particular focus on critical infrastructure systems (CIP), crisis management, and resilience. In addition, the requirements for operational tools to improve infrastructure operations are conducted.

2.1 Critical infrastructures

According to the German government [11], critical infrastructures are defined as "organizational and physical structures as well as facilities of vital importance to a nation's society and economy. Their failure or degradation may result in sustained supply shortages, significant disruptions of public safety and security, or other dramatic consequences". Specifically, the sectors of energy, information and communications technology, water supply and transport on the technical side, but also health, media and culture, food, finance, insurance, state

and administration are considered critical [12]. In addition to this national perspective, some infrastructure networks, such as energy or communications networks, have cross-border interdependencies and span entire continents.

On the one hand, critical infrastructures consist of fixed technical installations required for service provision which are owned and operated by both, the public and private sector. This includes, e. g., roads, bridges, dams, the water and sewer systems, railways and subways, airports, and harbors. On the other hand, these infrastructures also include permanent services provided by their operators, which include maintenance, repair and expansion. In the event of a crisis, emergency services such as disaster relief, civil defense, technical relief organization, ambulance services, fire department and police as well as the military share the task of supporting operations and the population.

Critical Infrastructures form a closely intertwined and interoperating socio-technical network. The various operators and stakeholders within the overall engineered system share the task of ensuring functionality for reliable service provision. Ideally, the failure of one physical component has no influence on the overall functional state [13]. Maintenance and system reconstruction need to be accomplished during operation, only allowing local discontinuity of service. At the same time, data sharing is impeded by data ownership, privacy, provenance, and regulatory requirements.

Table 1: The German Critical Infrastructure Strategy lists the potential hazards to infrastructures in three categories [11].

Natural events	Technical failure/ human error	Terrorism, crime, war
• Extreme weather events inter alia, storms, heavy precipitation, drops in temperature, floods, heat waves, droughts	• System failure inter alia, insufficient or excessive complexity of planning, defective hardware and/or software bugs	• Terrorism
• Forest and heathland fires	• Negligence	• Sabotage
• Seismic events	• Accidents and emergencies	• Other forms of crime
• Epidemics and pandemics in man, animals and plants	• Failures in organization inter alia, shortcomings in risk and crisis management, inadequate co-ordination and co-operation	• Civil wars and wars
• Cosmic events inter alia, energy storms, meteorites and comets		

The recent past has shown that occurring incidents bear the potential to disturb the network of infrastructures and inherent critical processes, thus triggering far-reaching social and economic consequences. Significant damage can be caused in particular by natural events, technical or human failure, deliberate acts with a terrorist or other criminal background, and wars (see also Table 1). The events may be unavoidable, and the focus of crisis management is then on saving lives, emergency supplies, and reconstruction. Current examples are the power failure in mid-February 2019 in Berlin-Köpenick caused by an excavator breaking power cables,[1] or the ransomware attack on the Colonial fuel pipeline from Texas to New York.[2] The flood disaster 2021 in Germany [14] as well as wildfires in 2021 in Southern Europe [15] highlight the impact of extreme weather events on infrastructures [16].

Characteristics of large-scale incidents include large numbers of people injured or otherwise affected by the unavailability of infrastructure services. Uncertainties in forecasting and detection make it difficult to warn the population in a timely and reliable manner and to prepare adequately.

Infrastructures classify as systems-of-systems with complex networked behavior [2]. Complex systems theory describes and analyses such systems and is a field of research gaining significant interest lately [17]. Such networked systems show emergent and self-organizing effects that make them hardly manageable once tipping points have been passed. Fast dynamics and possibly non-linear behavior of events and systems cause standard procedures to fail or at least fail to prevent secondary effects and the crisis can spiral out of control [18]. The resulting situation is difficult to understand and to be handled by humans, with cascade effects taking place. The sheer mass of necessary action and support to communities turns into a challenging task.

Developments such as increasingly complex and interconnected infrastructures, networked communities, climate change, and instabilities in international politics further increase the likelihood of such threat scenarios in the medium and long term. Their occurrence will still be rare [19]. However, due to the high impact by potential disruptions affecting large parts of societies, significant effort is required to protect critical infrastructures against high-impact-low-probability events.

To reproduce critical infrastructure behavior, the following requirements need to be met:

I1) handle **characteristics** of critical infrastructure with a special focus on:
   (a) the variety of systems as well as the coupling between infrastructures;

1 https://www.tagesspiegel.de/berlin/blackout-in-koepenick-der-groesste-und-laengste-stromausfall-in-berlin-seit-jahrzehnten/24019418.html

2 https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

(b) various time and spatial scales such as device, building, area, city, or country, including very large systems;
(c) complex and networked behavior as well as human behavior;

I2) for **regulation**, consider cross-company and cross-country regulatory requirements, data protection and data provenance.

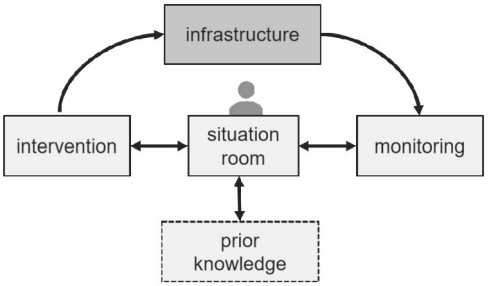

Figure 2: In case of a hazard, a crisis management group is formed, gathering in a situation room with all information from the field monitored and the ability to react fast by interventions based on prior knowledge or emergency plans.

2.2 Crisis management

In the event of disruptions, mitigation measures are required to maintain infrastructure services. In this context, crisis management is the application of strategies to help an organization or community deal with a sudden and significant negative event, with the goal of maintaining operations and reducing damage and injury.

A variety of models have been developed to enhance the reliability of critical infrastructures. Commonly, they are focused on system safety and robustness to determine whether the analyzed infrastructure meets the specified requirements for functionality and performance at the current time or over a period of time. These models have been used in the context of risk assessment to determine the criticality of individual components, functions, and processes and to evaluate the effectiveness of the measures provided to protect operation. This approach is often based on the consideration of cause-effect relationships with the aim of reducing existing or known risks in order to reach a certain level of safety [11]. For example, comprehensive legal regulations for operators of critical infrastructures have been introduced, such as the IT Security Act 2.0 [12], which came into force in May 2021.

Current approaches are essentially based on a consideration from two perspectives: prevention and response. For example, the critical infrastructure strategy of the German government [11] calls for a so-called all-hazards approach. The approach focuses in particular on securing the service provision and thus mirrors the United Nations' "Sendai Framework for Disaster Risk Reduction 2015–2030" approach [20]. This approach is served by prevention frameworks that generally aim at disaster risk reduction to ensure operational safety by risk analyses and resulting measures for a variety of feasible threats. The response perspective focuses on rapid restoration of the functionality of infrastructures and respective services to minimize the negative impact of supply failures.

For the purpose of coordinated disaster response, societies maintain hierarchically organized emergency and relief forces, that have clear command and reporting structures. Regular training strengthens their operational capabilities. In addition, in the event of a crisis, all relevant stakeholders, including politicians, operators, etc., are brought together to form a crisis management group. Such a group should be able to monitor the situation and react fast by deciding on interventions based on prior knowledge and field experience (Figure 2) [21].

The crisis is thus handled in an interdisciplinary manner, relying on established working and communication processes to enable fast and targeted response. As a result, management and decision-making during unforeseen crises rely heavily on expert knowledge to identify and evaluate potential mitigation measures. In addition, the dynamic and uncertain development of the threat situation complicates fast decision-making by requiring cyclical risk analysis and adjustment of decisions and risk measures.

Here, suitable instruments are required that support these processes and include prospective consideration of potential threats and risks as a permanent task into operational processes. Consequently, such a permanent management task includes both normal operations and crisis situations with different tasks, activities, tools and participants. At the same time, infrastructures are subject to constant changes during ongoing operations, which must be taken into account. In the event of a disruption, an infrastructure may even be severely damaged and the information situation unclear. In consequence, support instruments need to adapt to the current structure and state of the infrastructure.

A crisis management tool must be available in the event of a crisis, and thus at all times. It becomes part of the infrastructure service itself and, to serve its purpose, must be as safe, secure and resilient as the infrastructure itself.

Considering the characteristics of critical infrastructures, related threats, and the current state of crisis prevention and management, the following requirements for an efficient crisis management tool can be derived:

C1) include the instrument with permanent tasks into **normal operation** of the infrastructure;
C2) support handling threat and **crisis situations** caused by unforeseen events and potentially resulting in dysfunctional operation;
C3) be a **resilient tool** as part of the infrastructure services.

2.3 Infrastructure resilience

The concept of resilience is applied in a variety of research domains, e. g., ecology, psychology, economics, and national security [22]. Accordingly, the definition of resilience varies from field to field, but also among authors [22]. In the context of critical infrastructures, resilience describes the ability to continue providing essential services reliably and with little interruptions in the face of various non-specified disruptions as well as the ability to recover full functionality after an impact [1]. A key aspect of resilience is to accept that not all future events are predictable and that unexpected events will occur [22, 23, 24]. In contrast to traditional risk management, which strives to identify and limit the impact of specific risks, resilience management aims to generally strengthen the system properties to better deal with future events, whatever form they might take [22]. In contrast to security and safety research, which focus on reducing the risk of specifiable intentional disturbances (e. g., terrorist attacks) or internal disturbances (e. g., accidents) with known underlying scenarios, infrastructure resilience thus deals with a more diverse set of potential disruptions, where the likelihood of occurrence as well as scenario development are uncertain or even unknown.

The resilience of an infrastructure depends on system characteristics, e. g., redundancy [25], as well as a set of dynamic skills and coping strategies, the resilience capabilities. For example, a resilient system is able to anticipate, i. e., identify changes and their potential consequences in advance; monitor, i. e., recognize and track the state of the environment and of the system itself; respond, i. e., effectively handle the actual disruption; and learn, i. e., draw conclusions based on the gathered information and experience [23]. Overall, this underlines that resilience is not a purely static, given property, but can be actively enhanced and acquired [3].

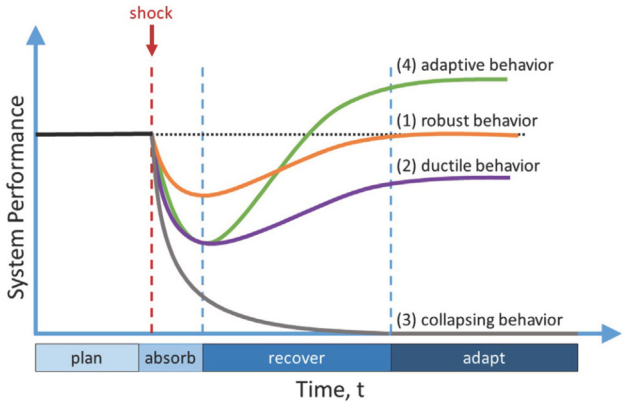

Figure 3: Infrastructure performance in the case of a disruption. As the disruption unfolds, four phases can be distinguished based on the needed actions and resilience capabilities. Figure source: Klimek and colleagues [24], unchanged, license: CC 4.0.

As disruptions unfold, the system performance varies: first the system performance decreases as the impact of the shock is absorbed, then performance increases during the recovery phase, and finally levels off at a lower, equal, or higher level than before the shock, depending on the system behavior (Figure 3). In each of these phases, a different set of capabilities is required and must be activated depending on the requirements of the situation. This is described by the theoretic framework of the resilience cycle.

Typically, this cycle includes a planning phase, an absorption phase, a recovery phase, and potentially an adaption phase. Throughout the cycle, the system activates its resilience capabilities, some of them briefly as the disruptions occurs (e. g., robustness) and some continuously (e. g., monitoring). A highly resilient system will learn from past disruptions and associated system behavior, as well as suffered impacts, and implement changes to the current procedures or technologies, leaving it better prepared to face future disruptions when the cycle begins again [25].

The resilience properties of a system can be assessed based on indicators quantifying sociological aspects (e. g., top management commitment, learning culture, risk awareness, and flexibility [23]) or technical aspects (i. e., redundancy, resource availability, physical resistance [25]). The resilience of the system towards one specific disruption can be estimated using data of the system functionality over time, e. g., how fast the original functionality level is restored (i. e., the slope of the functionality curve) [26]. Such characteristic functionality measures, or key performance indicators, describe the quality and quantity of the services provided by the infrastructure, e. g., the number of households currently sup-

plied with power, the average time to repair a fault in energy transmission, or the number of hospital beds. The resilience of the system towards hypothetical scenarios can be assessed using simulation data. Such simulation can help both to improve preparedness, as well as decision support, i. e., deciding between several options of action. In this case, depending on the chosen system limits, both socio-technical and purely technical systems can be studied. A variety of frameworks have been developed that focus on how to efficiently assess, quantify, manage, and strengthen resilience in critical infrastructure systems [4].

A number of capabilities need to be available in order to maximize the resilience properties and enable infrastructures to loop through the resilience cycle repeatedly and handle disruptions successfully:

R1) for **anticipation**, tools are required that are able to forecast future environmental influences and infrastructure behavior;
R2) for **monitoring**, the timely delivery of highly-resolved environmental data and its interpretation is needed, i. e., anomaly detection and situation awareness [27];
R3) for **response**, a tight coupling of the information gained through situation awareness and the tools providing decision support is required;
R4) for **learning**, feedback tools are needed, that allow to analyze the impact of disruptions and selected counter measures on the system performance indicators and enable the automated comparison of various courses of action.

Research identifying further resilience properties, strategies, capabilities, and the associated technical prerequisites is ongoing, as the concept of resilience, its application, and management are continuously discussed and refined [27].

3 Leveraging the Digital Twin paradigm

Summarizing the previous section, there is a growing demand to improve the protection of critical infrastructures from increasing threats as societies become more dependent on reliable supplies. Driven by these challenges, resilience research has increased in recent years. It has become clear that new methods and tools for crisis management need to be developed, based on a new risk culture that explicitly addresses rare and unforeseen events.

An applied Digital Twin concept and framework for resilient critical infrastructures could help to harmonize existing research efforts and to accelerate innovative realizations of theoretical findings. The concept allows embracing both Data Science and the opportunities created by digitalization.

In this section, we introduce a coarse-grained informal model of the Digital Twin meta-concept, that includes key components and their interworking (Figure 4). This informal model reflects and unifies several definitions of the term Digital Twin [6, 28, 9, 10] and will be used to deduct the key requirements of the Digital Twin Conceptual Framework needed to increase resilience in critical infrastructures.

3.1 Introduction to Digital Twins

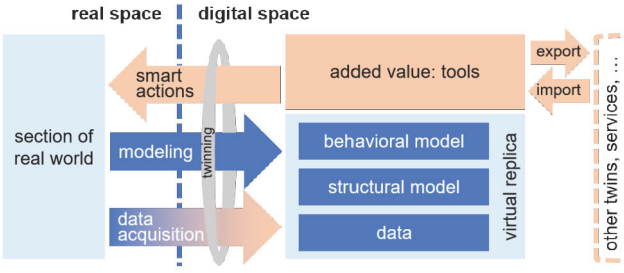

Figure 4: Informal model structure of the Digital Twin meta-concept with the real-world section and its digital correspondence (blue). The added value is ensured by smart tools that leverage the virtual replica's digital-only capabilities (orange); they can be accessed by humans and enable smart actions which impact the real world. Import/export functionality allows interweaving with other Digital Twins, services, or applications.

The term *Digital Twin* was first mentioned in 2002 [29], and became the subject of intense research and development efforts in recent years [6, 8, 28]. For several reasons, there is no consensus on the definition of the Digital Twin concept so far. First, there is considerable overlap with other frequently-used terms such as internet-of-things, cyber-physical systems and digital models, which refer to highly-connected, powerful and partly automated technologies. Second, the term encompasses applications which strongly vary in scope. It includes small, clearly-delimited machineries, as well as large-scale and heterogeneous systems-of-systems, such as production factories, airplanes and smart cities. Therefore, a Digital Twin can be built upon a self-contained, relatively simple technical model or a model with multiple containment levels and blurry system boundaries. The purposes and areas of application are also very diverse, ranging from operational

optimization and support in the design phase to testing and maintenance applications.

Informal model

The Digital Twin gets its name *twin* from its digital correspondence with the section of the real world, digitally reflecting the aspects of that section that are deemed relevant. Based on this leading concept, we define the Digital Twin as a meta-concept that contains both a *real-world section* and a *virtual replica* of it, a *twinning mechanism* to couple both, and accompanied by tools to perform smart actions and ensure the intended *added value* (Figure 4).

The real-world section can involve any set of systems of interest, from individual machine parts to factories, from buildings to cities, from processes to complex interconnected systems-of-systems, and from communities to networked socio-technical systems such as critical infrastructures. It is often alternatively referred to as an *analog system*, *real system*, or *physical system*, even though it may itself contain intelligent control systems implemented in software. The system boundaries define the section of the real world that is captured in the Digital Twin and depend on the use case.

Virtual replica and twinning

Initializing the virtual replica is the first step towards creating a Digital Twin with a modeling step and the launch of data acquisition (Figure 4). Structural models describe the composition and characteristics of the modeled section of the real world, such as a CAD model or a component list. They are accompanied by behavioral models that cover dynamics and functionality, such as simulation models or models created using machine learning or artificial intelligence. A sophisticated Digital Twin typically incorporates both types of models, with the structural model often serving as a semantic container for current and historical state information and the behavioral models. The kind and sophistication of the semantic container depends on the intended use case and the nature of the data, which may range from raw sensor data and unstructured information like natural language text or speech, non-normalized photos, etc., to curated instances of data types, schema-bound data, and ontology-compliant data.

In order to keep the virtual replica in sync with the real world, a twinning mechanism is required. A Digital Twin may capture state data only at distinct times along its life cycle, it may process numerous types of events that occur frequently, it may capture sensor readings at fixed intervals, or it may sample high-resolution time series of data that represent continuous processes related to behavioral models.

Modeling comprises 'the art of abstraction', i. e., the need to include everything necessary in the model to keep it relevant and precise, and to omit everything unnecessary in order to keep it understandable and comprehensible. Due to this abstraction effort, the virtual replica contained in a Digital Twin is always less than the section of the real world it corresponds to.

Added value and HCI

The Digital Twin contains functionality providing *added value*, which is the driving factor when creating Digital Twins. Added value of a Digital Twin is everything it offers that the real-world section does not. It comes into play as soon as the plain structural and behavioral models are augmented by capabilities not present in the non-digital world.

The models within the virtual replica may be fed and 'driven forward' via data acquisition at runtime, such that they keep up with the current state or reflect a past state of the modeled real-world section. Additionally, models may also be 'driven forward' by means of the modeled behavior, simulating future behavior. This is useful for exploring what-if scenarios or for predicting future states in terms of forecasts. This potential to extrapolate is one of the great strengths of Digital Twins.

Further functionality can be provided, pertaining to categories like analysis, monitoring, optimization, prediction, planning, etc. There are three ways in which such added value can be integrated with the Digital Twin and its surroundings (Figure 4, light orange parts):

1. it may be offered to human users in the form of tools by means of a more or less sophisticated human-computer interface (HCI), e. g., AR/VR based;
2. it may directly benefit the real-world section of interest by initiating smart actions on the real-world section, with the real world section converting to a smart system;
3. it may be exported to another Digital Twin to build systems-of-systems on a digital level or vice-versa, a Digital Twin can import added value of other Digital Twins, external services and information sources.

An example of the second variant is a Digital Twin that implements a real-time feedback loop from the real world via data acquisition and corresponding model updates, and returns responses to the real world via smart actions. This case corresponds to the first publication on Digital Twins by Grieves [9].

The third variant allows a system-of-systems approach for Digital Twins, which can be beneficial for several reasons, including modularization, reuse, and multi-tenant support. Import/export functionality can address data exchange, but also services offered and used, especially when software-oriented architectures are used.

Realization details

The conceptualization and implementation of Digital Twins have to reflect the methods and concepts that mark the ongoing digitalization in the domain considered. The data acquisition, model execution, and added value related components may be computationally demanding, and 24/7 availability may be required. Therefore, sophisticated Digital Twins may be realized as modular platforms that leverage cloud architectures [6]. Edge computing may complement the solution stacks, especially in the context of data acquisition and smart actions.

The possible categories of information storage are also diverse, as common terms such as data lake, database, or in-memory storage indicate. The degree of sophistication also depends on the degree of data refinement from raw data to curated data, where elaborate data preprocessing may even be part of the added value.

Table 2 provides a concise list of selected areas that must be considered during the conceptualization and implementation of Digital Twins. Each area is denoted together with a list of keywords indicating important aspects that may be relevant in the area.

Table 2: Selected areas to be considered during the realization of Digital Twins, along with keyword lists for important aspects.

Human-Computer Interaction stakeholder interaction usability, human-design process, visual analytics, immersive reality, serious games, user acceptance, behavior patterns
Tools early warning, situational awareness, scenarios, prediction, fast response, if-then-else questions, virtual interventions, optimization
Modeling and Simulation model structure, model type (structural/behavioural, PDE/agent/etc), multiple scales, surrogate modeling, probabalistic models, uncertainty quantification
Twinning real-time coupling of real and digital world, sensing, acting
Interfaces and Data data ingest and transport, standard interfaces and data formats, semantics, provenance, privacy, cross-disciplinary development workflows, process pipelines
Runtime Environment cloud and virtualization, AI, HPC, data flows, realtime and streaming, data lifecycle, database, modularity of components, elasticity, twin management

3.2 Related work

Digital Twins have been applied to several types of infrastructures, such as transportation [30, 7], buildings [31], energy [30, 7], and water [32]; mainly in the context of city, smart city, or building information modeling (BIM) [6, 33, 30, 7].

In their review on City Digital Twins, Shahat et al. [7, Table 3] list five themes that hint at current potentials of City Digital Twins: data management, visualization, situation awareness, planning and prediction, integration and collaboration. The aspects of situation awareness, prediction, and integration are also included in our technical requirements for the resilience capabilities (R1–R4, Section 2.3). Accordingly, ongoing work on Digital Twins for infrastructures already considers some of the capabilities needed for improved resilience. However, it can also be seen from various survey papers [6, 33, 30, 7] that the main reason for realizing infrastructure Digital Twins is to facilitate their planning and operation. Only few existing publications report on Digital Twin projects that consider resilience as a key goal [34, 35, 36, 37].

In the domain of supply chains, Digital Twins have been discussed as a tool to increase supply chain performance and resilience [37]. The corresponding data structure and modeling framework of a 'digital supply chain twin' follows four major methodological principles [31], which show similarities to resilience capacity design: 1) decision-making support as a viable system model comprised of pre-disruption, disruption, and post-disruption stages – basically following the resilience cycle as described in Section 2.3; 2) integration of physical and cyber data sources with online supply chain modeling – formulating the twinning requirement of a Digital Twin; 3) supply chain models as an integration of physical and cyber networks – modeling supply chains as complex networked systems; 4) data-driven supply chain risk analytics systems support the use of data for learning and disruption pattern recognition – integrating a learning component.

Liu [8] gives a comprehensive overview of use cases of Digital Twins for manufacturing systems and industrial applications throughout the system life cycle. These include real-time monitoring, production planning and control, process evaluation, predictive maintenance, fault detection and diagnosis, state monitoring, performance pre-

diction, and virtual test. Again, there is a certain overlap with the required resilience capabilities listed in Section 2.3. Jones [28] gives a comprehensive overview of relevant aspects to be considered when implementing Digital Twins for manufacturing systems. Also in the area of manufacturing systems, Becue et al. [38] describe how Digital Twins are able to support optimization and resilience. As a core concept, the authors advocate the embedding of human behavior modeling into the Digital Twin. Based on this, a holistic modeling and simulation approach can be taken to identify threats to operations related to fatigue, stress, or suspicious behavior. This approach can in turn be embedded in optimization, quality, safety, and security strategies.

The idea to utilize Digital Twins to deal with characteristics of complex systems, corresponding to requirement I1 (characteristics), has been discussed before in the context of resilient critical infrastructures [1].

The brief literature review above shows that some of the infrastructure and resilience requirements we derived so far are also addressed in works about Digital Twins for other domains and other criteria. Nevertheless, only few related works address Digital Twins in the context of infrastructure resilience in particular, and even fewer address large-scale crises and unknown events. To our knowledge, the present paper is the first to perform a comprehensive analysis regarding the Digital Twin requirements for this application area.

3.3 Requirement analysis

In Section 2, we derived requirements for future assurance of critical infrastructure operations and the need to increase system resilience. In this section, we deduce requirements in the design of a Digital Twin for critical infrastructure resilience by mapping infrastructure and resilience requirements to design alternatives within the Digital Twin concept.

System and purpose

In order to design the components within the Digital Twin system to meet I1 (characteristics), first the system boundaries of the real infrastructure under consideration need to be defined. The surrounding world, outside of the system boundaries, causes changes and disturbing events which impact the system.

In addition, the purpose of the Digital Twin must be defined so that stakeholders, users, use cases, data sources, and design goals for the replica and tools can be derived. In a first step, scenarios with relevance for the respective infrastructure type can be identified. For example, for urban infrastructures near rivers, scenarios related to extreme weather events or flooding are considered. In later versions, the Digital Twin can be enhanced to cover additional types of disruptions and services.

The federation of multiple Digital Twins provides a method for mapping regulatory requirements (I2 regulation) to infrastructures. Along the import/export interfaces, requirements for data governance, privacy and protection as well as regulatory processes can be addressed. With appropriate interfaces, system-of-systems can be connected to build similar virtual systems-of-systems with higher complexity and including sector couplings [39]. It is crucial that the networked Digital Twins and their models represent the emerging or self-organizing behavior of the real system.

Thus, the Digital Twin concept fulfills I1 (characteristics) and contributes to I2 (regulation) when fulfilling the following requirements:

DT1) define the **system** under consideration and the **purpose** of the Digital Twin:
   (a) determine system boundaries and appropriate time and spatial scales such as device, building, area, city or country;
   (b) derive stakeholders and design goals;
   (c) include complex and networked behavior as well as human behavior within the selected real-world section;
   (d) allow the coupling of Digital Twins similar to the coupling of real sectors and subsystems.

Virtual replica

In constructing a virtual replica of a critical infrastructure, I1 (characteristics) requires capturing the relevant processes, structure, and behavior such that its complex and interconnected behavior is virtualized. In the context of Digital Twins, smart tools rely on the virtual replica to satisfy I1 for providing resilience capabilities (R1–R4, anticipation, monitoring, response, learning) and be suitable for the tool use case. C1 (normal operation) and C2 (crisis situation) require modeling of the system behavior both in normal operation and in crisis situations, which include dysfunctional states. Especially for being able to monitor an infrastructure in all phases of a crisis (R2 monitoring) and to respond (R3 response), computing times for simulations and increasing reaction times need to be taken into account when determining type, scale and level of detail of models.

As an example, monitoring and response (R1, R3) are enabled, when for example a purely dynamic model is complemented by temporal-spatial information, which can be used to monitor and navigate relief forces inside an infrastructure building. For this task, a model of the building with pathways and doors as well as firefighting installations, explosive substances, or other persons in the building is useful. The requirement for efficient response (R3) further demands that the possible counteractions or mitigation measures can be simulated by the model, e. g., via changed parameter settings (e. g., adjusting operational parameters), configuration update (e. g., reflecting structural updates of buildings), process changes (e. g., after a new political law has been passed), or by changing the operational mode of the system (e. g., reflecting a shutdown in the event of an attack).

In order to match these use cases and requirements, various model types may be related to each other with regard to semantic containers in terms of a temporal-spacial structure or a graph of relations. This can be achieved when using 3D models to represent the spatial aspect of the real-world section, augmented with semantic, geometric, visual and contextual aspects. Adding the time domain, in terms of geometric changes or movement of objects, they provide a temporal-spatial model and can be used as a structure to integrate other functional or behavioral models. Geometric models can be enhanced by functional modeling, such as mobility, water or electrical network models within the selected area [40]. As a side effect, temporal-spatial models enable VR/AR techniques to immerse into the virtual models within the control center.

Human behavior is an important factor in infrastructure dynamics and add further aspects to the infrastructure characteristics (I1). Agent-based modeling (ABM) is a common micro-modeling approach for socio-technical systems [1, 17] and allows simulating complex behavior in networked systems. Humans within communities cause demand for supply that can be connected through agent-based simulation, resulting in agent-demand models matching the demand towards infrastructure services.

In addition, the human factor in terms of operator error, terrorist or cyber attacks must be taken into account and distinguished from permissible usage patterns. In this case, monitoring (R3) is enhanced by models of behavioral patterns. Machine learning approaches, for example, learn "normal behavior patterns" of humans and allow to detect and classify anomalies.

The validity of the virtual replica in both a functional and a dysfunctional state (C1, C2) requires that rare events are captured by the model. Probabilistic or state modeling techniques can be used for this purpose. Exploring threshold effects of complex systems that lead to dysfunctional states and incorporating them into models will be a necessary task.

Effective monitoring (R2) depends on a timely update of the system status, reflecting all internal states as well as disruptions within the system (safety incident) and outside the system (security incident) shortly after their occurrence. Both the virtual replica and the sensing components must therefore capture the system dynamics and environmental changes in high temporal resolution. A fully synchronized virtual replica represents the current state of all variables of interest of the real object, such as operational measures, maintenance conditions, or visual characteristics.

Requirement C3 requests the Digital Twin to be a reliable and resilient tool. As the core component in the Digital Twin concept, the replica always needs to stay in sync with the real infrastructure. When cloning and decoupling the virtual replica or parts thereof from the real system it is available for a variety of analytics and research without influencing the real system [41]. Such a virtual clone is then a simulation environment, that can be used for forecasts, for scenario simulation of potential attack vectors, potential interventions, or system changes. Optimization tools can make use of the simulators. For the implementation of simulators, classical approaches are suitable, but also ML-based models and predictors, decision support tools, what-if tools, and analysis tools, e. g., based on elaborated models for root-cause analysis.

Summarizing, the Digital Twin replica can be designed such that it meets I1 (characteristics), C1 (normal operation), C3 (resilient tool) and supports all resilience capabilities (R1–R4) by implementing the following requirements:

DT2) construct the **virtual replica** to be an up-to-date projection of the infrastructure:
   (a) model the system such that the model includes all required static information and dynamic behavior in an up-to-date way;
   (b) all replica components need to support normal infrastructure operation as well as partly or totally dysfunctional situations during a crisis;
   (c) provide clones and simulators of the virtual replica.

Twinning

R2 (monitoring) formulates the requirement to monitor the current situation within the system as well as events from the environment at all times. Disruptions might be caused

from within the system or from outside. Therefore, both the replica as well as the sensoring need to cover the system state and dynamics as well as events from the environment in a timely manner. This is realized by the Digital Twin's twinning component.

In order to monitor (R3) a system during normal operation (C1) and crisis (C2), effective sensing components are required and data is as manifold as the models. For functional models, physical sensors may be used. Other sources include weather forecasts, surveillance data, or information resulting from social networks or management systems. It also needs to be mentioned, that sensing of human behavior will remain a challenge due to privacy concerns of surveillance systems and the complexity of the matter. The retrieved data might be uncertain, insufficient, or unobservable (e. g., in crisis situations). Therefore, states must be estimated to some extent by the virtual replica. Ideally, models and tools based on uncertain data and information incorporate this aspect. Furthermore, data provenance, ownership, and privacy of data needs to be ensured and tracked by the Digital Twin.

The response to a disruption (R3) as well as anticipation (R1) require that actions are taken within the real infrastructure. These may include reconfiguring or technical containment, mobilizing relief forces, evacuating communities, or changes of procedures. Actions can take effect on the technical systems of the infrastructure and the operators, or on the communities using the infrastructures.

Because of the manifold types of potential actions and due to rare usage in crisis situations (C2), it is impossible to install automated acting components to cover all potential actions. Instead, we extend the interpretation of smart actions to include human decisions and actions on the real infrastructure. Therefore, requirement R3 (response) additionally demands a decision support system as a tool available to human stakeholders. Defined decision processes with actions executed by humans establish an alternative acting mechanism within the Digital Twin concept. Defined processes ensure de-facto automated twinning.

The twinning mechanism increases the resilience of critical infrastructures with regard to the monitoring (R2), response to disruptions (R3), and anticipation (R1). In addition, it can be designed to meet I1 (characteristics), C1 (normal operation), and C2 (crisis situation) by implementing the following requirements:

DT3) implement **twinning** to ensure the replica is up-to-date and actions on the infrastructure can be taken:
   (a) provide a sensing mechanism to capture the current state of the system as well as events resulting from the environment including uncertainty and provenance information; update the replica accordingly;
   (b) provide an acting mechanism such that interventions can be applied to the real-world section and are available for human control; make sure, the Digital Twin replicates these changes.

Toolbox

The general purpose of the Digital Twin in the context of this paper is to improve resilience capabilities of critical infrastructures in terms of requirements R1 to R4 (anticipation, monitoring, response, learning). This added value is implemented as smart tools within the Digital Twin concept. The activities of those tools must be orchestrated over time to have maximum effect during the different phases of the resilience cycle (see Section 2.3). Some activities, such as monitoring, are performed continuously throughout the resilience cycle, while others are performed only briefly (e. g., response). Therefore, there is no direct correspondence between the phases of the resilience cycle and the activity types. Each activity type can contribute to the overall resilience capabilities of the infrastructure in the course of events (Figure 5).

Figure 5: Sequence of activities during and after a crisis. These activities are supported by the Digital Twin, and help to maximize resilience of the respective critical infrastructure.

Ongoing activity monitoring (R2 monitoring) needs to be performed continuously, such that potential incidents will be detected based on the virtual replica's state and the sensing data. The tools include anomaly detection, risk and resilience monitoring, scenario identification, and scenario forecast. Situation awareness should be established in an all-hazards-approach (C2 crisis) and in case of an incident inform about the characteristics of the disruption and the affected system dynamics.

Within threat and crisis situations, additional activities are required in order to respond to the incident in a timely manner (R3 response). Depending on the nature of the crisis, responses may be aimed at containing the threat, intervening in the sequence of events, shutting

down parts of the infrastructure to prevent further damage, providing aid and assistance to injured people, providing replacement services, or rebuilding the infrastructure. These responses must then be transformed into an action plan that can be executed automatically with the help of the acting component or manually in the real infrastructure. In case sufficient measures and knowledge are provided by the Digital Twin, or when the incident and its dynamics are managable by standard procedures, the crises can be appropriately handled. In case of an unforeseen type of crisis, new mitigation approaches must be developed and provided in short time – which depends on how well the Digital Twin is prepared for the unexpected e. g., by offering modular mitigation modules and deep, fast, and informed intervention for humans; otherwise, a major disruption may result, which may impair services, affect, or even injure the users and population concerned. At this stage, the tools provide simulation of the identified interventions, decision support, and assistance in creating an action plan. Alignment of stakeholders ensures a common approach among all organizations (I2 regulation).

After crisis situations, a learning activity (R4 learning) follows. The goal is to understand the causes and reactions during the crisis and the risk development. The course of events and developments is saved to a scenario database. Based on the improved understanding of the crisis, the system can be enhanced (R1 anticipation). System optimization and adaption by, e. g., technical changes, procedure updates, stakeholder and citizen participation, and staff training, deliver a refined system better prepared for future crises.

To support resilience of the infrastructure (R1 to R4) and effective crisis management (C1 to C2), the following requirements for the toolbox are derived:

DT4) the **toolbox** should include smart tools, which are operable at any point during the resilience cycle, and:
   (a) include the ability to monitor the status of the system and its environment, provide situation awareness, and enable response in case of a disruption;
   (b) provide the ability to analyze and learn from past crises, to increase preparedness and adaptability.

Control center

The control center is the human computer interface (HCI) of the Digital Twin and as such a key component to ensure the purpose of the Digital Twin. It helps to understand the situation and to use the tools to perform the appropriate activities according to R1 to R4 (resilience capabilities). The situation room (Figure 2) is extended by the Digital Twin and transformed into a situation control center (Figure 6).

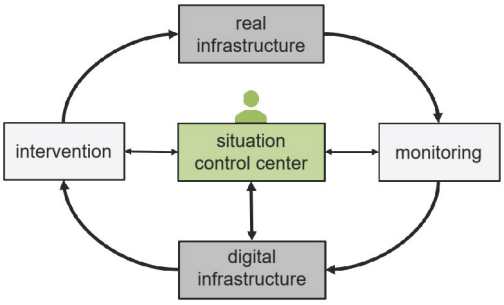

Figure 6: Control center for effective crisis management. As part of the Digital Twin concept, a situation control center provides stakeholders with up-to-date information and access to the tools needed to handle the crisis. The control center contains both information from the real infrastructure and a digital infrastructure.

To meet requirement C1 (normal operation) the control center makes the Digital Twin available for everyday interaction with stakeholders as well as in crisis situations (C2 crisis). Stakeholders are for example crisis management teams, operators, emergency and relief forces, citizens, and decision-makers from economy. In crisis situations, stakeholders might be overwhelmed by information and grasping dynamics thus the user interfaces need to be carefully crafted. Human-centered design processes should be used to design the control center, to meet use case requirements, establish well-defined processes, and ensure acceptance of both the Digital Twin and the resilience concept [42].

If the virtual replica contains 3D models they can be integrated into the control center for immersive interaction. A 3D-enriched clone of the current situation, past, or what-if scenarios is ideally suited to deal with rare and unforeseen events. Such events cannot be effectively countered on the basis of past experience alone. Instead, ingenuity and experimentation are called for. A virtual clone allows to test the implications of a wide variety of possible actions, immersively visualize the results (e. g., via VR and AR), and decide between several options. Serious games can be used to provide effective training for changed processes and optimized damage control.

The control center represents the interface between humans and the toolbox and addresses R1 to R4, C1 and C2, with the following requirements:

DT5) **control center** providing human-computer interaction and visualization:
- (a) a control center, providing the stakeholders with tools to gain control of the current situation, visualization techniques, and decision support;
- (b) up-to-date information and appropriate tools throughout all stages of crisis development and the resilience cycle;
- (c) innovative learning processes, e. g., training of selected scenarios using VR or AR methods.

Platform and data management

The Digital Twin is required to meet C3 (resilient tool), which can be achieved by modularity and standardization for the software implementation, elastic hardware resources, and defined processes for development and operation. The overall Digital Twin concept consists of both software and hardware components, where the latter is the real world with the acting and sensing components. In this paper, we concentrate on the software aspects of the core components, i. e., the replica, the clone simulators, the tools, and the user interfaces.

From a software architecture point of view, a Digital Twin concept is best implemented as a service oriented architecture (SOA). Services implement simulators, tools, HCI, databases, and connectors to external services and components. Data streams connect those services, thus handling real-time data and control communication to form workflows. Ideally, all components are loosely coupled and modular, in order to ease implementing Digital Twins for new real-world sections and adding more tools.

To ensure consistent and reproducible data handling complying with regulation (I2), standards need to be followed for data semantics and formats, modular and reusable components, interfaces and protocols. For example, standardized APIs simplify the use of data from geo servers or sensors and allow federation of several Digital Twins. Possibly, new standards need to be formulated and established.

To meet the C3 requirement, the software services are operated in a cloud infrastructure with elastic hardware resources or in a network of edge devices. Such virtualized or distributed infrastructures provide, among other things, elastic computing and storage resources that can accommodate the high dynamics of resource requirements resulting, for example, from recurring large-scale simulations. The software services and the computing infrastructure together form a Digital Twin platform, that can be connected to the real infrastructure and is then available for use. The operation of the platform needs to follow IT standard methods to secure operation and integrity as well as support continuous change regarding software components. The DevOps approach might be suitable to orchestrate development and operation processes.

To enable learning from past incidents (R4 learning), historic data needs to be archived and readily available. Ideally, the full course of events in a crisis situation can be analyzed retrospectively, by storing data on environmental context, system status, and taken countermeasures in the infrastructure as well as the protocol of how the Digital Twin has been used.

The resulting requirements on Digital Twin software components are:

DT6) provide a Digital Twin **platform** to operate the core software services including **data management**:
- (a) a modular and flexible architecture for replica, clones, tools, data lakes, user interfaces and connectors, operated on elastic hardware resources;
- (b) standardized interfaces and protocols;
- (c) the ability to record and replay historic crisis situations as scenarios, storing scenario data in a scenario database;
- (d) service and life cycle management of Digital Twin components, tools and data to ensure resilient Digital Twin development and operation.

Table 3 shows that the main components of a Digital Twin can be designed to meet the formulated requirements. Thus, it is feasible to use the Digital Twin concept as a key instrument to significantly increase the resilience of critical infrastructures and make it a central concept for further research in this application area.

Table 3: The components of the Digital Twin concepts fulfill the requirements to increase critical infrastructure resilience, making the Digital Twin a valuable approach for the given task. Components marked with 'x' contribute to the resp. requirement, 'X' marks core elements to the task.

	Digital Twin					
	DT1 System Bound., Coupling	DT2 Virtual Replica	DT3 Twinning	DT4 Toolbox	DT5 Control Center	DT6 Platform, Data Mgmt
Infrastructure						
I1 characteristics	X	x	x			
I2 regulation	x					X
Crisis Management						
C1 normal operation		X	X	x	x	
C2 crisis situations		X	X	x	x	
C3 resilient tool		x				X
Resilience						
R1 anticipation	x	x		X	X	
R2 monitoring		x	X	X	X	
R3 response		x	X	X	X	
R4 learning		x		X	X	x

4 Digital Twin conceptual framework for infrastructures

In this section, we derive a Digital Twin framework for managing resilient infrastructures. The Digital Twin is introduced as an instrument to provide support during normal operation as well as during a crisis. In particular, we derive a conceptual model which embeds the virtual replica in a Digital Twin platform. As a continuous service, it integrates with the infrastructure and is accompanied with resilience, interaction and management tools. The framework aims to optimize and manage the performance of infrastructures, with the ultimate goal of increasing their resilience.

4.1 Guiding principles

For the successful application of Digital Twins to existing infrastructures, we propose a set of four guiding principles.

Human in the loop control
We suggest that the Digital Twin should prioritize human interaction. This means that only lower-level decisions should be automated within a control loop, while crucial decisions should be made by humans. As a result, this implements human-in-the-loop control [43].

In order to closely integrate stakeholders in major decision processes, the Digital Twin needs to firstly provide reliable, understandable and well-prepared information as a basis for the decision-making processes, and secondly enable human intervention upon request. The control loop aims to optimize multiple criteria, such as the quality of service, risk level, and resilience.

Principle of parsimony and accepted uncertainty
The principle of parsimony, also known as Occam's razor, describes, simply put, a heuristic in which, among several possible explanations of a phenomenon, the simplest is preferred over options that require more assumptions. We advocate that this principle should be applied when choosing among several options in model design, detail, and the amount of external sensor data.

However, a simpler model and tool design comes along with increased uncertainty with regard to the performance of, e. g., the monitoring system or forecasting results. Therefore, we suggest to determine a level of accepted uncertainty when it comes to decisions. The uncertainty information should be made transparent within the decision making processes.

Prepared for complexity, emergence and self organization
As the Digital Twin captures the dynamics of complex, networked infrastructures, the Twin too likely shows properties of complex, networked systems itself, such as emergence and self-organization. This is even more likely when Digital Twins are coupled, forming a system-of-systems themselves. Thus, a certain degree of unpredictability can be expected and methods to anticipate such effects as a cause to cascades need to be developed [2].

Safe experiments and training
We propose to design the Digital Twin to provide a safe experimentation and training environment for uncertain situations and crises in addition to normal operations. It needs to be guaranteed that the experiments leave the actual system untouched until a decision is made. Due to the high uncertainty associated with the future course of events and the data collection processes, a variety of potential future system changes and intervention strategies exist. Crisis teams might need to take action in stressful situations. Training of situations beforehand and guidance through all processes support safe Digital Twin operation as well as effective responses in crisis situations.

4.2 Digital Twin conceptual model

We propose a conceptual model for infrastructure Digital Twins consisting of the real infrastructure, building blocks and interface components (Figure 7), together forming a functioning system. All components are designed following the descriptions and requirements DT1 to DT6 (Section 3). A Digital Twin implemented according to this conceptual model operates continuously and covers all phases of infrastructure operation, including normal operation and crisis situations. Normal operation involves, e. g., continuous monitoring of the real-world section. Some components are activated only when needed, depending on the phase of the resilience cycle and the activity required.

A Digital Twin platform provides the environment to implement Digital Twin building blocks as services following the service oriented architecture (SOA) pattern. This platform can be implemented within a cloud infrastructure running those core services and connecting the real

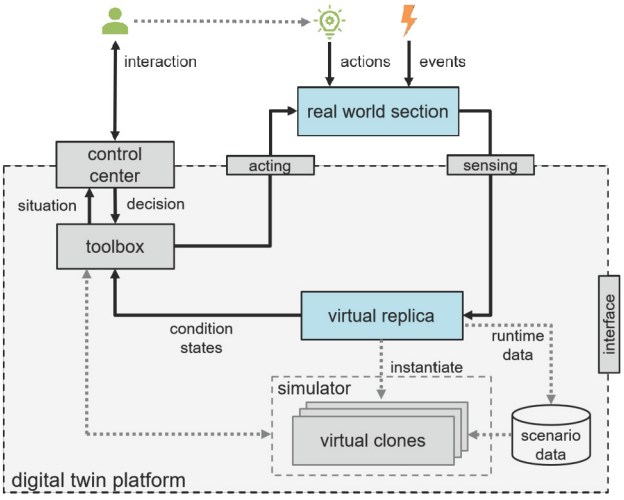

Figure 7: Digital Twin Conceptual Model for infrastructure operation supporting improved resilience for crisis situations. Together, the individual building blocks form a functioning system for normal operation (black) and on-demand activities (grey).

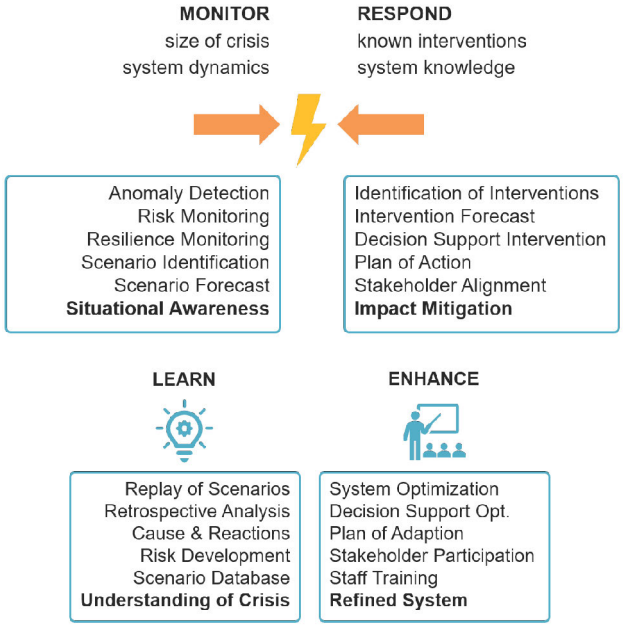

Figure 8: Smart Digital Twin Tools can offer four types of activities to support infrastructure resilience along the resilience cycle.

world part of the Digital Twin via acting and sensing interfaces, as well as via direct human interaction in the control center. Furthermore, the functionality of the Digital Twin can be partially implemented in edge nodes. At the heart of the architecture, the virtual replica receives and distributes data through streaming services and stores it in databases.

In our architecture design, the virtual replica is not directly synced back to the corresponding real world-section. Instead, changes are applied to the real-world section either by tools using the acting component or by human intervention outside the Digital Twin. The Digital Twin then will be notified by the changes through the sensing component.

The toolbox provides the option to clone the virtual replica of the infrastructure and to initialize it with the current state of the real-world if needed. Such a clone is then used for forecasts, simulation of alternative system set-ups or interventions. Optimization algorithms can be used to identify system improvement options in addition to novel out-of-the-box actions suggested by system experts. Further, the clone is used to simulate the expected sequence of events based on modified initialization and runtime data, either from previous records or from a designed hypothetical scenario database.

The control center resembles the interface to the stakeholders, guides through all situations, and provides access to the toolbox. It contains a situation room enriched by the monitoring and analysis results of the Digital Twin. The control center can be shared remotely such that it enables aligned action of stakeholders distributed in various organizations.

The toolbox supports monitoring and response activities, such as anomaly detection, action planning, scenario forecast, and decision support (Figure 8). For learning and adaptation, another suite of tools must be added, performing replay of scenarios, retrospective analysis, system optimization and training. The scenario database stores information characterizing selected events, supporting the retrospective evaluation of past events. This evaluation can lead to an optimization of future processes, e. g., enhanced staff training, and thus helps to prepare the system for future crises.

5 Conclusion

In this paper, we present requirements for the operation and crisis management of critical infrastructures, to enhance their resilience towards unforeseen events. We propose the use of the Digital Twin concept and deduce functional requirements, tailored specifically to the application to critical infrastructures. To our knowledge, such a comprehensive analysis with regard to Digital Twin requirements for a specific field of application and in particular for critical infrastructure management has been performed for the first time.

Based on these requirements, we derive a Digital Twin Conceptual Framework for infrastructures, which is based on the construction and interconnection of a virtual replica and the real-world section, virtual clones, a toolbox of smart tools, and a human-operated control center. The conceptual framework is composed of guiding principles for the construction and planning phases and a conceptual model of the digital twin for infrastructures. The advantages and new opportunities posed by Digital Twins are thus integrated to an instrument for managing and strengthening resilience of critical infrastructures.

The key challenges we see are the requirements for integrating a variety of uncertain data sources and system model types into one Digital Twin framework, evaluating intelligent tools to support the resilience cycle, and IT platform scalability and reliability. Federated Digital Twins are a promising approach to address these challenges, instead of 'one solves it all' implementations.

We emphasize that the human factor plays a significant role in the management and prevention of crisis situations. Our Digital Twin conceptual model includes supportive tools and human-computer interaction as a central component, and thus implements human-in-the-loop control. We suggest human-centered design to develop specific control center implementations for both continuous activities as well as for tools providing support within rare event situations.

One advantage of the proposed Digital Twin model is that it is well-suited both for daily use and for use during rare crisis events. As the user interfaces and functionalities are well-known from daily interaction, the handling of the tools is easier in situations where mental pressure is high. Furthermore, a Digital Twin clone together with VR/AR technologies allows training for rare events, so that stakeholders, staff members, and relief forces can practice system behavior out of normal operation and can memorize procedures to react.

Another key element of the Digital Twin conceptual model for infrastructures is scenario recording. It allows retrospective analysis of causes and risks, weaknesses during response can be identified, tipping points for emergent behavior can be derived, resilience KPIs can be developed and analyzed, and optimizations can be performed.

As part of the Digital Twin, simulators based on virtual clones can serve as a valuable playground for experiments and optimization, helping to prepare for rare events and crisis situations. It can be used to simulate virtual attacks, similar to the Red Team approaches [44], analyze their impacts and develop specific enhancements to meet these potential scenarios.

Overall, applying the Digital Twin concept to critical infrastructures enables learning from mistakes and developing new approaches. As such, it promises to play an important role in addressing the challenges posed by increasingly interconnected and complex infrastructures and societies. The smart tools improve resilience capabilities, rendering the Digital Twin a key instrument to systematically promoting resilience.

References

1. Min Ouyang and Zhenghua Wang. Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis. *Reliability Engineering & System Safety*, 141: 74–82, Sep. 2015. 10.1016/j.ress.2015.03.011.
2. Dirk Helbing, Dirk Brockmann, Thomas Chadefaux, Karsten Donnay, Ulf Blanke, Olivia Woolley-Meza, Mehdi Moussaid, Anders Johansson, Jens Krause, Sebastian Schutte and Matjaž Perc. Saving human lives: What complexity science and information systems can contribute. *Journal of Statistical Physics*, 158 (3): 735–781, Jun. 2014. 10.1007/s10955-014-1024-9.
3. David D. Woods. Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*, 141: 5–9, Sep. 2015. 10.1016/j.ress.2015.03.018.
4. Royce Francis and Behailu Bekera. A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, 121: 90–103, Jan. 2014. 10.1016/j.ress.2013.07.004.
5. Dimitris Gritzalis, Marianthi Theocharidou and George Stergiopoulos, editors. *Critical Infrastructure Security and Resilience*. Springer International Publishing, 2019. 10.1007/978-3-030-00024-0.
6. Aidan Fuller, Zhong Fan, Charles Day and Chris Barlow. Digital twin: Enabling technologies, challenges and open research. *IEEE Access*, 8: 108952–108971, 2020. 10.1109/access.2020.2998358. URL https://doi.org/10.1109/access.2020.2998358.
7. Ehab Shahat, Chang T. Hyun and Chunho Yeom. City digital twin potentials: A review and research agenda. *Sustainability*, 13 (6), 2021. ISSN 2071-1050. 10.3390/su13063386. URL https://www.mdpi.com/2071-1050/13/6/3386.
8. Mengnan Liu, Shuiliang Fang, Huiyue Dong and Cunzhi Xu. Review of digital twin about concepts, technologies, and industrial applications. *Journal of Manufacturing Systems*, 58: 346–361, Jan. 2021. 10.1016/j.jmsy.2020.06.017.
9. Michael Grieves and John Vickers. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. In *Transdisciplinary Perspectives on Complex Systems*, pages 85–113. Springer International Publishing, August 2017. 10.1007/978-3-319-38756-7_4. URL https://doi.org/10.1007/978-3-319-38756-7_4.
10. Werner Kritzinger, Matthias Karner, Georg Traar, Jan Henjes and Wilfried Sihn. Digital twin in manufacturing: A categorical literature review and classification. *IFAC-PapersOnLine*, 51

(11): 1016–1022, 2018. 10.1016/j.ifacol.2018.08.474. URL https://doi.org/10.1016/j.ifacol.2018.08.474.
11. Federal Republic of Germany Federal Ministry of the Interior. National strategy for critical infrastructure protection (cip strategy), June 2009.
12. Gesetz über das bundesamt für sicherheit in derinformationstechnik (bsi-gesetz - bsig), 2021. original 2009.
13. Scott Jackson and Timothy L. J. Ferris. Resilience principles for engineered systems. *Systems Engineering*, 16 (2): 152–164, Oct. 2012. 10.1002/sys.21228.
14. Emergency Response Coordination Centre (ERCC). Western Europe | floods and UCPM assistance, 2021a. URL https://erccportal.jrc.ec.europa.eu/ercmaps/ECDM_20210716_western-Europe_Floods.pdf.
15. Emergency Response Coordination Centre (ERCC). South-East Europe | forest fires and EU response (1–6 August), August 2021b. URL https://erccportal.jrc.ec.europa.eu/ercmaps/ECDM_20210806_Forestfires_SouthernEurope.pdf.
16. Michael Dietze and Ugur Ozturk. A flood of disaster response challenges. *Science*, 373 (6561): 1317–1318, Sep. 2021. 10.1126/science.abm0617.
17. Hiroki Sayama. *Introduction to the Modeling and Analysis of Complex Systems*. Open SUNY Textbooks, Milne Library, State University of New York at Geneseo, Geneseo, 2015. ISBN 9781942341093.
18. Dave Butry, Craig A. Davis, Sanjeev R. Malushte, Ricardo A. Medina, Mahmoud Reda Taha, John W. Van de Lindt, Cory R. Brett, Sherif Daghash, Caroline Field, Juan Fung, Paolo Gardoni, Sue McNeil, Fernando Moreu, Ali Mostatavi, Yalda Saadat, Neetesh Sharma, Kenichi Soga, Eslam Soliman, Elaina J. Sutley, Armin Tabandeh, Douglas Thomas, Eric Vugrin and Richard N. Wright. *Hazard-Resilient Infrastructure*. American Society of Civil Engineers, May 2021. 10.1061/9780784415757.
19. Stephen Hudson, David Cormie, Edward Tufton and Stuart Inglis. Engineering resilient infrastructure. *Proceedings of the Institution of Civil Engineers – Civil Engineering*, 165 (6): 5–12, Nov. 2012. 10.1680/cien.11.00065.
20. United Nations. Sendai framework for disaster risk reduction 2015–2030, 2015.
21. Adam Widera, Sandra Lechtenberg, Gaby Gurczik, Sandra Bähr and Bernd Hellingrath. Integrated logistics and transport planning in disaster relief operations. 05 2017.
22. Morten Wied, Josef Oehmen and Torgeir Welo. Conceptualizing resilience in engineering systems: An analysis of the literature. *Systems Engineering*, 23 (1): 3–13, May 2019. 10.1002/sys.21491.
23. Erik Hollnagel. *Resilience Engineering in Practice: A Guidebook*. Taylor & Francis Group, 2010.
24. Peter Klimek, János Varga, Aleksandar S. Jovanovic and Zoltán Székely. Quantitative resilience assessment in emergency response reveals how organizations trade efficiency for redundancy. *Safety Science*, 113: 404–414, March 2019. 10.1016/j.ssci.2018.12.017. URL https://doi.org/10.1016/j.ssci.2018.12.017.
25. David Rehak, Pavel Senovsky, Martin Hromada and Tomas Lovecek. Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection*, 25: 125–138, Jun. 2019. 10.1016/j.ijcip.2019.03.003.
26. Cen Nan and Giovanni Sansavini. A quantitative method for assessing resilience of interdependent infrastructures. *Reliability Engineering & System Safety*, 157: 35–53, Jan. 2017. 10.1016/j.ress.2016.08.013.
27. Evelin Engler, Michael Baldauf, Paweł Banyś, Frank Heymann, Maciej Gucma and Frank Sill Torres. Situation assessment — an essential functionality for resilient navigation systems. *Journal of Marine Science and Engineering*, 8 (1): 17, Dec. 2019. 10.3390/jmse8010017.
28. David Jones, Chris Snider, Aydin Nassehi, Jason Yon and Ben Hicks. Characterising the digital twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology*, 29: 36–52, May 2020. https://doi.org/10.1016/j.cirpj.2020.02.002.
29. Michael Grieves. Digital twin: manufacturing excellence through virtual factory replication. *White paper*, 1–7, 2014.
30. Adil Rasheed, Omer San and Trond Kvamsdal. Digital twin: Values, challenges and enablers from a modeling perspective. *IEEE Access*, 8: 21980–22012, 2020. 10.1109/access.2020.2970143. URL https://doi.org/10.1109/access.2020.2970143.
31. Min Deng, Carol C. Menassa and Vineet R. Kamat. From BIM to digital twins: a systematic review of the evolution of intelligent building representations in the AEC-FM industry. *Journal of Information Technology in Construction*, 26: 58–83, February 2021. 10.36680/j.itcon.2021.005. URL https://doi.org/10.36680/j.itcon.2021.005.
32. Congcong Sun, Vicenç Puig and Gabriela Cembrano. Real-time control of urban water cycle under cyber-physical systems framework. *Water*, 12 (2): 406, February 2020. 10.3390/w12020406. URL https://doi.org/10.3390/w12020406.
33. Roberto Minerva, Gyu Myoung Lee and Noel Crespi. Digital twin in the IoT context: A survey on technical features, scenarios, and architectural models. *Proceedings of the IEEE*, 108 (10): 1785–1824, October 2020. 10.1109/jproc.2020.2998530. URL https://doi.org/10.1109/jproc.2020.2998530.
34. Ishii Kazuhiko and Yamanaka Atsushi. Building a common smart city platform utilizing FIWARE (case study of Takamatsu City). *NEC Technical Journal*, 13: 28–31, 11 2018.
35. Youngjib Ham and Jaeyoon Kim. Participatory sensing and digital twin city: Updating virtual city models for enhanced risk-informed decision-making. *Journal of Management in Engineering*, 36 (3): 04020005, May 2020. 10.1061/(asce)me.1943-5479.0000748. URL https://doi.org/10.1061/(asce)me.1943-5479.0000748.
36. David N. Ford and Charles M. Wolf. Smart cities with digital twin systems for disaster management. *Journal of Management in Engineering*, 36 (4): 04020027, July 2020. 10.1061/(asce)me.1943-5479.0000779. URL https://doi.org/10.1061/(asce)me.1943-5479.0000779.
37. Dmitry Ivanov and Alexandre Dolgui. New disruption risk management perspectives in supply chains: digital twins, the ripple effect, and resileanness. *IFAC-PapersOnLine*, 52 (13): 337–342, 2019. 10.1016/j.ifacol.2019.11.138. URL https://doi.org/10.1016/j.ifacol.2019.11.138.
38. Adrien Bécue, Eva Maia, Linda Feeken, Philipp Borchers and Isabel Praça. A new concept of digital twin supporting optimization and resilience of factories of the future. *Applied Sciences*, 10 (13): 4482, Jun. 2020. 10.3390/app10134482.
39. Leif-Thore Reiche, Claas Steffen Gundlach, Gian Mewes and

Alexander Fay. The digital twin of a system: A structure for networks of digital twins. 09 2021.
40. Stefan Boschert and Roland Rosen. Digital twin — the simulation aspect. In *Mechatronic Futures*, pages 59–74. Springer International Publishing, 2016. 10.1007/978-3-319-32156-1_5. URL https://doi.org/10.1007/978-3-319-32156-1_5.
41. Hao Zhang, Qiang Liu, Xin Chen, Ding Zhang and Jiewu Leng. A digital twin-based approach for designing and multi-objective optimization of hollow glass production line. *IEEE Access*, 5: 26901–26911, 2017. 10.1109/access.2017.2766453.
42. Simon Nestler. Mensch-technik-interaktion und zivile sicherheit: Bedeutung von usability und user experience in forschungsprojekten zu ziviler sicherheit. 09 2019.
43. Sirajum Munir, John A. Stankovic, Chieh-Jan Mike Liang and Shan Lin. Cyber physical system challenges for human-in-the-loop control. In *8th International Workshop on Feedback Computing (Feedback Computing 13)*, San Jose, CA, June 2013. USENIX Association. URL https://www.usenix.org/conference/feedbackcomputing13/workshop-program/presentation/munir.
44. European Central Bank. TIBER-EU framework. how to implement the european framework for threat intelligence-based ethical red teaming, May 2018. URL https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf.

Bionotes

Eva Brucherseifer
DLR Institute for the Protection of Terrestrial Infrastructures, Sankt Augustin, Germany
eva.brucherseifer@dlr.de

Prof. Dr.-Ing. Eva Brucherseifer (born 1973) is a full professor at the University of Applied Science in Darmstadt. After her PhD at the Department of Control Methods and Robotics at the TU Darmstadt, she founded and operated a software engineering company with focus in embedded HMI systems for industry. Her main research interests since 2017 are embedded systems engineering, artificial intelligence and human machine interaction. In the German Aerospace Center (DLR) she is Head of the Department Digital Twins for Infrastructures in the Institute for the Protection of Terrestrial Infrastructures. The research group focuses on methods, concepts and applications to utilize Digital Twins in responding to threats and improving the resilience of infrastructures.

Hanno Winter
DLR Institute for the Protection of Terrestrial Infrastructures, Darmstadt, Germany
hanno.winter@dlr.de

Hanno Winter received his Master's degree in electrical engineering from TU Darmstadt, Germany, in 2014. Afterwards he worked on sensor fusion methods for the localization of rail vehicles at the Control Methods and Robotics group at TU Darmstadt. Since 2021 he is with the Institute for the Protection of Terrestrial Infrastructures at the German Aerospace Center where he is particularly concerned with the creation of Digital Twins for cities.

Andrea Mentges
DLR Institute for the Protection of Terrestrial Infrastructures, Sankt Augustin, Germany
andrea.mentges@dlr.de

Andrea Mentges studied environmental sciences (B. Sc.) and marine environmental sciences (M. Sc.) at the University of Oldenburg, Germany, specializing in mathematical modeling. After receiving the master's degree in 2014, she started a PhD in geochemistry and biodiversity at the Institute for Chemistry and Biology of the Marine Environment in Oldenburg, Germany. After this, she moved on to a Postdoc position at the Center for Integrative Biodiversity Research (iDiv) in Leipzig, Germany. Since 2020, she's a researcher at the Institute for the Protection of Terrestrial Infrastructures of the German Aerospace Center (DLR) in Sankt Augustin, Germany, where she focuses on describing and modeling the resilience of critical infrastructures.

Max Mühlhäuser
Telecooperation Lab, Technical University of Darmstadt, Darmstadt, Germany
max@tk.tu-darmstadt.de

Max Mühlhäuser received his diploma and doctoral degrees from University of Karlsruhe (now KIT). From 1986 on, he managed the first European research and tech transfer center for Digital Equipment Corp., the second largest computer manufacturer at the time. Since 1989, he worked as a professor or visiting professor in Germany, France, Austria, Canada, Australia, and the US. Since 2000, he is a full professor of computer science at TU Darmstadt. In his work on ubiquitous computing, he develops and integrates with his team members novel concepts from networked and intelligent systems, security and privacy, and human computer interaction.

Martin Hellmann
DLR Program Coordination Defence and Security Research, Cologne, Germany
martin.hellmann@dlr.de

Since 2010, Martin Hellmann is the Coordinator of Civil Security Research and Dual-Use at the German Aerospace Center's (DLR) overall Program Coordination for Defence & Security Research. He is also a reserve officer (Major d. R.) in the German armed forces. In his current DLR position, he is coordinator for civil security research, dual-use and EU-related topics. As a strategy and security analyst for the DLR Executive Board, he is the contact person for ministries, industry, and national and European research institutions. He is DLR representative in various national and European think tanks, working groups. Mr Hellmann holds a Diploma Degree as well as a PhD Degree in Electrical Engineering.