Resilient Cities and Structures 3 (2024) 1–19

Contents lists available at ScienceDirect

Resilient Cities and Structures

journal homepage: www.elsevier.com/locate/rcns

Full Length Article

Protecting critical infrastructure against cascading effects: The PRECINCT approach

Meisam Gordan[a,*], Djibrilla Amadou Kountche[b,*], Daniel McCrum[a], Stefan Schauer[c], Sandra König[c], Shirley Delannoy[d], Lorcan Connolly[e], Mircea Iacob[f], Nicola Gregorio Durante[g], Yash Shekhawat[h], Carlos Carrasco[i], Takis Katsoulakos[j], Páraic Carroll[a]

[a] School of Civil Engineering, University College Dublin, Belfield D04 V1W8 Dublin, Ireland
[b] AKKODIS Research 1, 7 Boulevard Jean Ziegler, Blangac 31700, France
[c] Austrian Institute of Technology (AIT), Safety & Security Department, Vienna, Austria
[d] VIAS Institute (VIAS), Haachtsesteenweg 1405, Bruxelles 1130, Belgium
[e] Research Driven Solutions Limited (RDS), 1A Saint Kevin S Avenue, D08 TX29 Dublin, Ireland
[f] Interuniversitair Micro-Electronica Centrum (IMEC), Kapeldreef 75, Leuven 3001, Belgium
[g] Engineering - Ingegneria Informatica Spa (ENG), Piazzale Dell'agricoltura 24, Roma 00144, Italy
[h] NUROGAMES GMBH (NURO), Schaafenstrasse 25, Cologne 50676, Germany
[i] Barcelona Supercomputing Centre (BSC), Jordi Girona 31, Barcelona 08034, Spain
[j] Inlecom Commercial Pathways (ICP), Core B Block 7, The Plaza Park West, D12 WDN2, Ireland

ARTICLE INFO

Keywords:
Critical infrastructure protection
Serious games
Digital twins
Blueprints
OASIS TOSCA
Industry 4.0
Resilience
Interdependencies
Cyber-physical

ABSTRACT

Critical Infrastructures (CIs), which serve as the foundation of our modern society, are facing increasing risks from cyber threats, physical attacks, and natural disasters. Additionally, the interdependencies between CIs throughout their operational lifespan can also significantly impact their integrity and safety. As a result, enhancing the resilience of CIs has emerged as a top priority for many countries, including the European Union. This involves not only understanding the threats/attacks themselves but also gaining knowledge about the areas and infrastructures that could potentially be affected. A European Union-funded project named PRECINCT (Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyber-Physical Threats), under the Horizon 2020 program, tries to connect private and public stakeholders of CIs in a specific geographical area. The key objective of this project is to establish a common cyber-physical security management approach that will ensure the protection of both citizens and infrastructures, creating a secure territory. This paper presents the components of PRECINCT, including a directory of PRECINCT Critical Infrastructure Protection (CIP) blueprints. These blueprints support CI communities in designing integrated ecosystems, operating and replicating PRECINCT components (or toolkits). The integration enables coordinated security and resilience management, incorporating improved 'installation-specific' security solutions. Additionally, Serious Games (SG), and Digital Twins (DT) are a significant part of this project, serving as a novel vulnerability evaluation method for analysing complicated multi-system cascading effects in the PRECINCT Living Labs (LLs). The use of SG supports the concentrated advancement of innovative resilience enhancement services.

1. Introduction

Infrastructure systems are the foundation for the management, organization, and efficient running of cities. Such systems are considered as complex socio-technical ones that strongly contribute to the supply of goods and services to both the public and private. In infrastructure sectors where assets and networks are crucial for the security and well-being of the city, their failure would negatively impact economics, public health, or security [1,2]. Therefore, the term Critical Infrastructures (CIs) are used to indicate this importance [3–8]. Moreover, due to these facts, the protection of CIs is considered by decision makers and urban planners to be of primary concern [9]. The CIs are physical sectors along with cyber and organizational subsectors and services that a country or community needs to function properly. Each sector and the corresponding subsectors have critical dependencies with other sectors. For instance, the healthcare sector is highly dependent on communications, emergency services, energy, food and agriculture, Information Technologies (IT), transportation, and water sectors. Therefore,

* Corresponding authors.
E-mail addresses: meisam.gordan@ucd.ie (M. Gordan), Djibrilla.AMADOU-KOUNTCHE@akkodis.com (D.A. Kountche).

https://doi.org/10.1016/j.rcns.2024.04.001
Received 10 November 2023; Received in revised form 7 April 2024; Accepted 23 April 2024
Available online 16 May 2024

each CI is in collaboration with other sectors due to its functionalities [10,11].

The protection of CIs is increasingly recognized as a critical issue, particularly given their fundamental role in social and economic development [12]. Technological advancements in recent decades have made infrastructure management more challenging, requiring innovative and efficient monitoring methods [13–15]. The Industrial Control Systems (ICS) used in CIs have evolved across three generations, i.e., Monolithic, Distributed, and Networked, and are thus interconnected [16]. CIs are increasingly connected which can make them more vulnerable to cyber-physical threats, human error, faulty equipment, and natural disasters. Extensive disruptions to these interconnected infrastructures can cause cascading effects [17,18]. Therefore, it is imperative to enhance Critical Infrastructure Protection (CIP) strategies to mitigate the impact of cascading effects.

In the past decade, the focus of research on CI and their various aspects such as resilience, protection, security, and vulnerability has developed significantly [19]. Researchers have established various approaches for CI risk assessment, with some studies focusing on different infrastructure types, e.g., water [20], electricity [21,22], energy [23], ports [24], and oil and gas networks [25]. El-Maissi et al. [26] proposed an innovative methodological perspective for CI integrated assessment models by using digital technologies during multi-hazard incidents. In their work, a holistic gaming scenario application was presented, using virtual reality for improved data visualization, and incorporating big data analytics for predictive and prescriptive management. Henriques et al. [27] detailed a review of existing literature on Forensics and Compliance Auditing (FCA) for CIP. The authors introduced a blueprint for building FCA platforms that address the specific needs of CI security. In a separate report by Yang et al. [28], a state-of-the-art review on indicator-based CI resilience assessment was conducted to achieve two main goals, i.e., understand the current landscape, and identify the need for standardization. In addition, interdependency modelling of CI networks has been a topic of research in several studies. For example, Brunner et al. [29] investigated modelling cascading failures that occur in interconnected infrastructure systems after extreme events, while Xu et al. [30] focused on improving the decision-making process for restoring interdependent CIs after disasters.

Serious Games (SG) are becoming increasingly data-driven, intelligent, and immersive, developing into Digital Twins (DTs) [31]. Both have been used in hazard mitigation strategies. For example, a novel approach for construction safety training was developed by [32] using DT and a virtual training environment within a game engine. The proposed approach was capable of generating realistic virtual training environments for minimal manual effort, offering benefits beyond safety awareness training through data analysis. A virtual reality-based safety education and training was also presented in [33] using SG. It was shown that SG with automated data analysis could be used for risk prevention in construction. Another study [34] applied a DT of a construction site to create a SG with real-time collision risk assessment for bored pile installation. Brucherseifer et al. [35] proposed a DT framework for CI to improve resilience against unforeseen events. It analyzed requirements for infrastructure operation, crisis management, and resilience, then detailed a conceptual framework with virtual replicas, smart tools, and a human-operated control centre. The outcome of their work was a system that could learn from past incidents, optimise responses, and train personnel for rare events, ultimately enhancing infrastructure resilience.

According to the literature, various CIP tools, frameworks and approaches have been developed to improve the protection of CIs and their interdependencies. Some specific examples of these existing CIP tools and their respective sectors are: SAURON [36], focuses on enhancing security in ports; STOP-IT [37], addresses security challenges in the water sector; DEFENDER [38], aims to enhance security measures in the energy sector; SAFECARE [39], focuses on improving security and resilience in hospitals; RESISTO [40], aims to enhance security and resilience in communication systems; INFRASTRESS [41], focuses on the security and resilience of industrial plants; SATIE [42], addresses security challenges in airports and the aviation sector; SAFETY4RAILS [43], focuses on enhancing safety measures in the rail transportation sector; IMPETUS [44], aims to enhance urban safety and security; 7SHIELD [45], focuses on the security of ground segments of space systems; and ENSURESEC [46], addresses security challenges in e-commerce. These tools are examples of research and development initiatives focused on enhancing the security, resilience, and safety of CI sectors. Each of the aforementioned approaches is dedicated to a specific sector and aims to address the unique challenges and vulnerabilities within that domain.

Despite the existence of various CIP tools and frameworks, there remains a significant gap in integrated cyber-physical security and resilience management platforms. This paper addresses this gap by introducing a model-driven cooperative and integrated platform from the PRECINCT project [47] that leverages developments from existing CIP tools to protect CIs from cascading effects. PRECINCT stands for Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyber-Physical Threats. The PRECINCT project is developing the concept presented in this paper. The PRECINCT project connects both private and public stakeholders involved in critical infrastructures within a specific geographic area. The goal is to establish a unified cyber-physical security management approach, creating a secure environment for citizens and infrastructures. This approach, called "PRECINCT," can be efficiently reproduced throughout Europe to enhance safety. The PRECINCT project aims to achieve the following objectives: (1) develop a framework plan for efficient safety and resilience management of CIs, aligning with industry requirements, (2) establish a collaborative cyber-physical security and resilience management infrastructure that enables CI stakeholders to create artificial intelligence-powered PRECINCT ecosystems. This infrastructure will also offer enhanced support services for resilience, (3) create a vulnerability assessment tool that utilizes SGs. This tool will identify potential vulnerabilities and quantify measures to enhance resilience, considering cascading effects, (4) implement PRECINCT's DT that represents the network topology and metadata profiles of CIs. The DT will employ continuous feedback-loop machine learning methods to identify anomalies, provide optimised reaction and mitigation quotas, and facilitate computerised analysis, (5) deploy innovative PRECINCT ecosystems within four real-world application scenarios, i.e., living labs (LLs) located in Antwerp, Ljubljana, Athens, and Bologna. These ecosystems will serve as validation demonstrators, generating measurement-based evidence of the targeted benefits. Active participation from emergency services and city administrations will ensure that the results contribute to ongoing DT developments, (6) produce outputs related to sustainability, comprising capacity building, dissemination activities, resilience strategies, exploitation strategies, and standardization recommendations. In summary, the PRECINCT project aims to create a comprehensive and replicable approach for managing the security, resilience, and sustainability of CIs, ensuring the safety of citizens and supporting the development of smart cities across Europe [48–52].

Based on the explanations provided above, this study aims to discover the connection between CIs and their interdependencies and cascading effects in Section 2. The PRECINCT approach is presented in Section 3, which includes the ecosystem platform, specific interdependencies in the context of LLs, and the calculation of resilience management. This Section also covers the architecture and components of SG, DT as well as their integration. The experimentation conducted in the PRECINCT LLs using blueprints is discussed in Section 4. A scenario showcasing how PRECINCT evaluates risks and strengthens resilience during a flood event is presented in Section 5, and conclusions are drawn in Section 6.

2. Interdependency graphs and cascading effects

CIs are growingly at risk from various intentional cyber-physical attacks and risks from natural hazards. However, assessing and coping

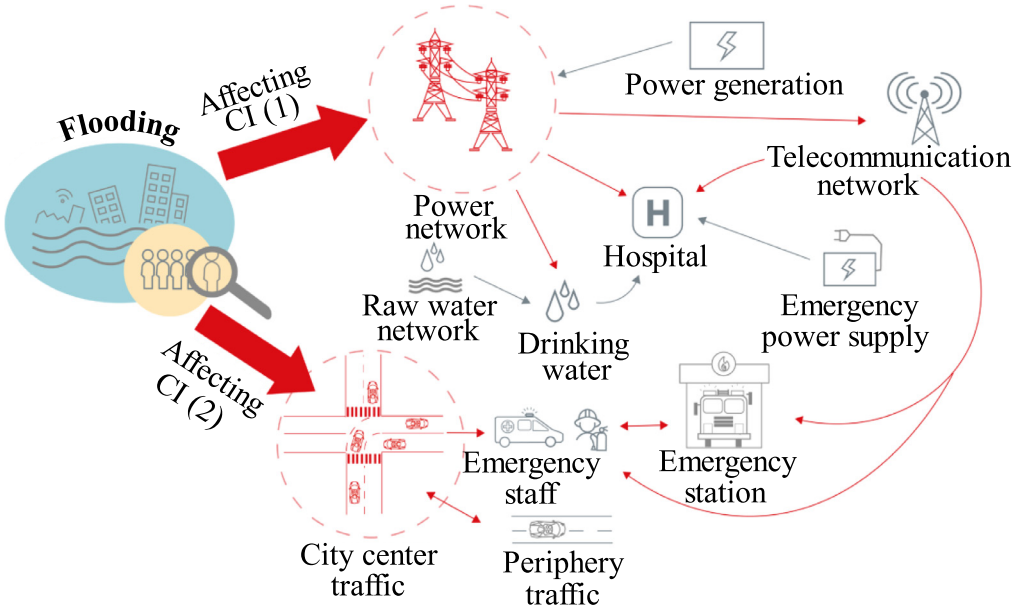


Fig. 1. An example of dependency graph [59].

with the influence of cascading effects arising from the interdependencies among various types of CIs and different types of hazard/threats and their resilience for 'rapid recovery' is becoming increasingly pertinent and is extremely difficult, particularly in terms of specified geographical areas such as cities. The increasing vulnerability of urban centres focuses the importance of deep public-private cooperation to ensure a coordinated multi-sector response and enhanced protection of CIs [52,53].

Identification of the various impacts of an event such as a flood involves knowledge about the hazard, the region and infrastructures that will be affected [54]. Modern CIs are strongly interconnected due to their dependency on each other, the pursuit of efficiency and optimization of resources, the need for information exchange, economic considerations, technological advancements, and the desire to enhance services and user experience [55]. Therefore, if one CI experiences reduced operation, it can potentially impact others in the network [56]. Hence, a thorough threat analysis must consider all relevant CIs and their interdependencies. In this paper, a graph-based model is employed to represent these interdependencies, with nodes symbolizing CIs and edges denoting dependencies. Fig. 1 shows a general example of such a dependency graph. The flooding event depicted in Fig. 1 has a direct impact on both the power network and city centre traffic, as evident from the graph. As a result, any service disruption occurring in these two CIs will directly or indirectly affect other CIs, such as hospital and telecommunication network.

Most CIs rely on and are dependent of information and communication technologies for their daily operation. These information and communication technologies are considered as CIs [57]. A threat may affect these CIs and indirectly influence people living in the area. Different nodes react in different ways to a specific threat, so it is necessary to describe the dynamics of each node through an individual "inner" model. The approach here uses Mealy automata models [58], as these describe reactions to an incoming alarm (e.g. notification of a sensor) and inform dependent nodes in case the functionality or availability of the node changes due to that alarm. Knowing the local reaction to a cyber-threat and/or physical hazard, i.e., how the state changes due to a specific threat and/or hazard, the simulation acknowledges an approximation of the overall response of the whole system.

3. Methodology and results

3.1. Applying a precinct to critical infrastructure

Cascading effects are considered in threat scenarios involving multimodal transport, energy, water, and telecommunications networks, considering the interdependencies between these prominent and highly interconnected sectors. These scenarios contain cyber, physical, and hybrid threats. An effective approach to collaborative cyber-physical security management requires the creation of public-private partnerships [60], which is based on a nested-scales strategy to obtain coherence among the social organisation and economic development. This approach also needs harmony between various factors such as cost, risk, and security. To achieve this, PRECINCT builds upon recent and progressive CIs within the four proposed LLs, as shown in Table 1.

The PRECINCT project's main outputs contain various components (see Fig. 2). These components include a PRECINCT framework description for efficient safety and resilience monitoring of CIs, integrating industry obligations and insights from EU projects. This project also assists CI stakeholders to generate AI-driven PRECINCT ecosystems and gain access to developed support services through an integrated cross-facility platform for cyber-physical security and resilience management. A vulnerability measurement tool utilizing SGs is implemented to identify vulnerabilities and resilience enhancements at the CI level. Additionally, PRECINCT's DT represents CI network topology and metadata, employing continuous feedback-loop Machine Learning (ML) for anomaly detection, response optimization, and automated forensics. The project implements cutting-edge PRECINCT ecosystems in four LLs and employs validation demonstrators to showcase measurement-driven evidence of the anticipated benefits. Sustainability-related outcomes, including capacity building, dissemination, standardization recommendations, and resilience strategy, are also incorporated.

The PRECINCT Ecosystem Platform is composed of a set of re-usable IT tools such as:

- A Knowledge Graph to model CIs interdependencies and cascading effects using an instance of Neo4J [62].
- A message broker and a Complex Event Processor to securely connect CI systems that need to share data in the context of collabora-

Table 1
PRECINCT Living labs.

Living lab (LL)	Critical infrastructure system involved	Relevant hazard (s)
LL1 Ljubljana	• City bus transport and national rail • Electricity Distribution System Operator • Telecommunication infrastructure • Municipality Police • First responder services	Terrorist attack (bomb threat and cyber threat)
LL2 Antwerp	• Traffic (Tunnel) • Water Infrastructure • Energy Distribution • Telecoms • Police • Fire Department • Emergency services	• Natural disaster (flooding)
LL3 Athens	• Athens International Airport • Athens Metro • Attiki Odos Roadway	• Natural disaster (earthquake) • Terrorist attack (cyber threat)
LL4 Bologna	• Bologna Airport • Roads to the airport • Rail (Marconi Express) • Telecommunication network	• Natural disaster (intense rain, high intensity wind) • Accidental damage to infrastructure (e.g., break in wiring) • Cyber-attack to TLC network

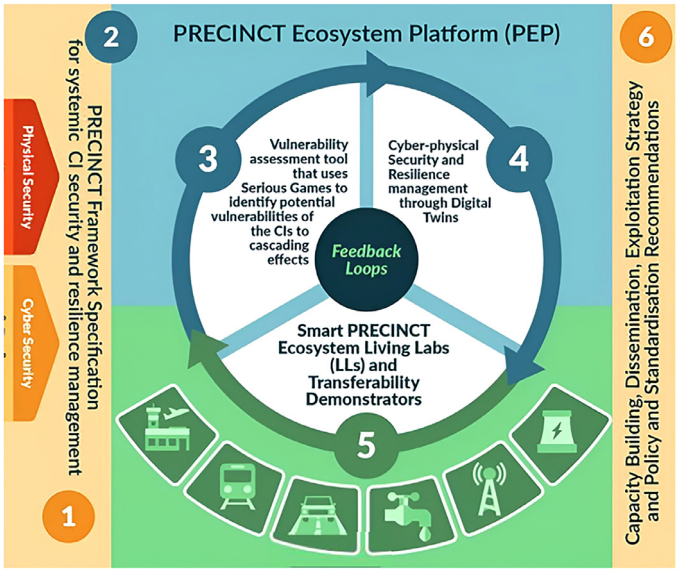


Fig. 2. PRECINCT componets [61].

tively managing vulnerabilities to Cascading Cyber Physical Threats. Apache Kafka is used as message broker [63] and can support additional security mechanisms based on public and private keys. The Event Processor used in PRECINCT is Esper [64].

- A Complex Event Processor determine complex event from CIs data received from the message broker.
- An Intelligent Security Monitoring tools to capture a form of IoT systems deployed in the CIs as well as to filter and extract events and statistics from these data and visualise them.
- A Big Data Infrastructure to store CIs data and AI/ML algorithms/models provided as libraries and applied on data provided by CIs.
- A Design studio for CIP software engineers to integrate existing CIP tools / services with the PRECINCT Blueprints Directory which contains the description this ecosystem as OASIS TOSCA service templates and Node types.
- A Unified PRECINCT situation awareness user interface (UI) for all Ecosystem participant secured by an Identity and Access Management (IAM) system.

Therefore, this ecosystem is a set of IT tools which are used as building blocks by other PRECINCT components (for e.g., the DT exploit Kafka, and the Big Data Infrastructure) and supports territory CIs, emergency responders and other stakeholders to adopt a common security and resilience management approach and harmonizing CIs emergency processes.

3.2. The precinct approach to critical infrastructure protection

3.2.1. CI interdependencies in the context of precinct living labs

Before detailing the involved technologies in PRECINCT, it is important to elaborate on the provided database population from the LLs (i.e., Ljubljana, Antwerp, Athens, and Bologna) as the input parameters. These data include cascading effects using mathematical methods (e.g., automaton theory, Markov chains and Markov processes) to model the transitions among pre-defined operational states to indicate the effects of various incidents on CIs, CI interdependencies applying a graph-based approach, and the Resilience Methodological Framework (RMF). Fig. 3 shows the interdependencies of CIs. All attack threats such as (1) cyber and physical threats/attacks, (2) natural/technological hazards, and (3) threats towards humans have been considered accordingly. All threats/hazards have been ranked according to their relevance and severity for each LL by LL experts. Fig. 4 shows an example of an interdependency graph for a flooding scenario within a city with a focus on transportation, water supply, and energy supply infrastructure as well as rescue services. The calculated Resilience Index (RI) based on the resilience modelling and cascading effect/ interdependencies are detailed in the following subsection.

The main purpose of the CI Interdependency Graph is to gain an understanding of the global behaviour of the CI network based on local dynamics (i.e., the local behaviour or performance of the CI). Local dynamics are described through an inner model inside each node. Nodes represent the CI and the edges of dependencies among them. A qualitative scale is used to characterize the state of each node, ranging from 1 (best) to 5 (worst). Depending on the type of node, the levels represent functionality or availability of a component. Some possible interpretations are provided in Table 2. The transitions among each state represent

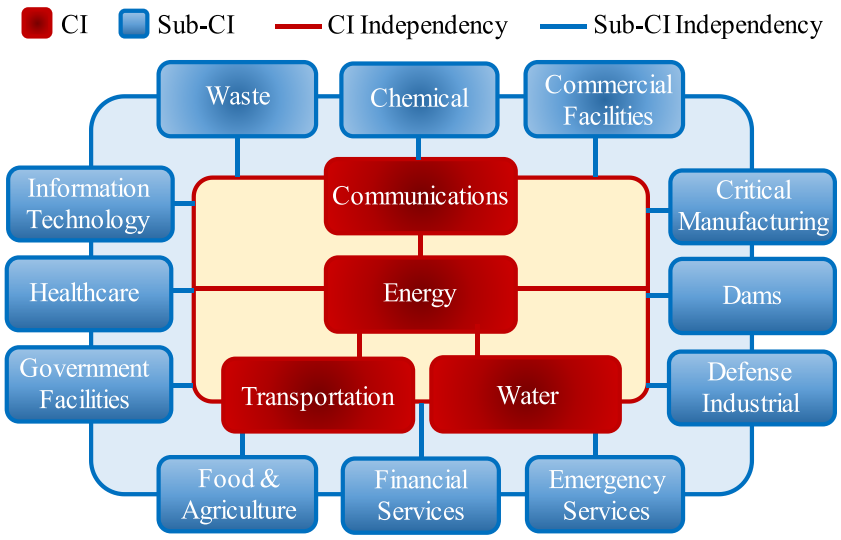


Fig. 3. Critical infrastructure independency.

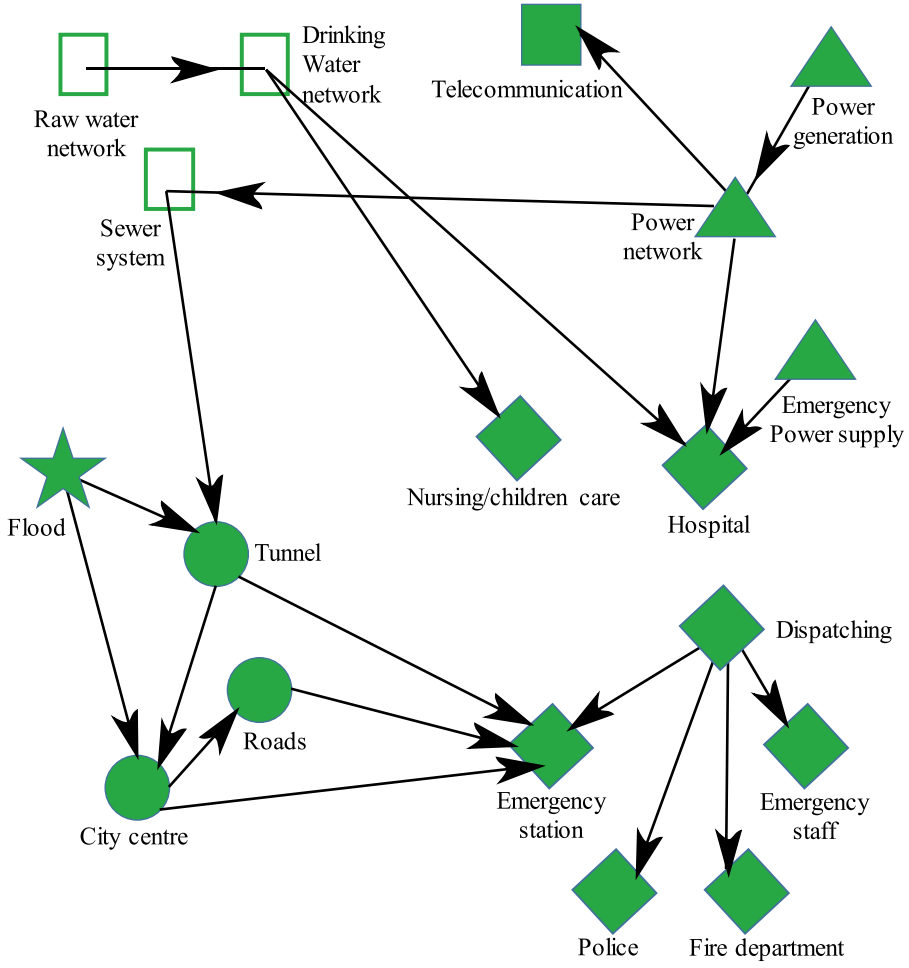


Fig. 4. Interdependency model of flooding scenario, adopted from [65].

the inner dynamics of each CI when affected by a specific incident. CIs are all interconnected, and their widespread disruptions cause cascading effects. Interdependent infrastructures are vulnerable to risk of a cascading nature. The cascading effects are used to update nodes inside CIs by changing the state of the node. The transitions among the functionality of each node represent the inner dynamics of each CI when affected by a specific severe incident, e.g., a bombing or fire. Hence, based on the inner dynamics, the cascading effects of the afore-mentioned incident affecting one of the assets in the system can be simulated for the entire network of assets.

The state of the node will change by reducing the specification of the node's dynamic, i.e., when the condition gets worse. Such a change is

Table 2
Interpretation of states of a node.

State	Functionality	Availability	Loss / Damage
1	Full functionality	Normal	None or negligible
2	Slightly reduced	Slight delay	Some minor damage, repairable
3	Some limitations, but still operating	Some interruption or delay, but still satisfactory	Some severe damage or multiple smaller problems, repair takes considerable time or money
4	Strong limitations	Strong interruption or delay, not satisfactory	Severe or long-lasting damage, repair time consuming or expensive
5	Not working at all	Not available	Failure, needs to be replaced or substituted (at least temporarily)

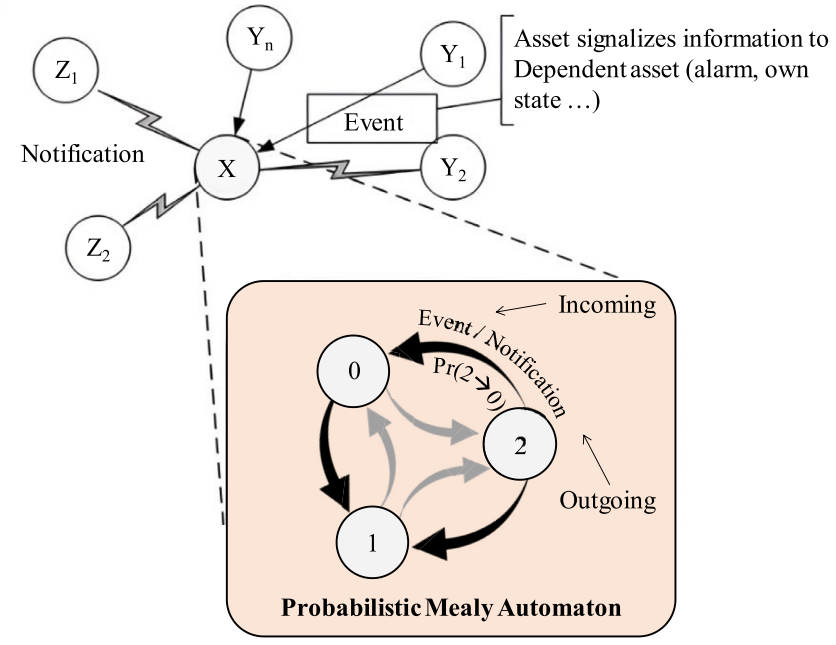


Fig. 5. Interdependency graph with probabilistic Mealy automaton model [67].

triggered by the afore-mentioned incident, either directly or indirectly through the state of a node it depends on. Furthermore, the reaction to the threat may depend on the circumstances, i.e., on the current state of the node. Such behaviour is best modelled through a probabilistic Mealy automaton [66], as it changes the node's state upon a given input and returns an output. Therefore, it is appropriate to model a node's behaviour by adding probabilities to the state changes of the automaton model, i.e., through a probabilistic Mealy automaton [58]. Fig. 5 illustrates an example of a probabilistic Mealy automaton.

Formally, the local dynamics in a node are described through a tuple $M = (S, \Sigma_{in}, \Sigma_{out}, \lambda, \delta, s_0)$ where;

- S represents a limited and non-empty group of states, e.g., $S = \{1, 2, 3, 4, 5\}$
- Σ_{in} is a limited and non-empty input alphabet encoding the threats, where $\Sigma_{in} \subset \{0, 1\}$
- Σ_{out} is a limited and non-empty output alphabet
- $\delta : S \times \Sigma_{in} \to \Delta(S)$ represents a transition function that maps a pair of state and input word to a probability distribution over the states (i.e., an element of the simplex $\Delta(S)$)
- $\lambda : S \times \Sigma_{in} \to \Sigma_{out}$ is an output function that maps a pair of state and input word to an output word
- $s_0 \in S$ is the initial state

It is recommended to choose the same set of states, S, for all nodes as it allows comparing the condition of different components. Further, it is convenient, and in most cases sufficient, to set $\Sigma_{in} = \Sigma_{out} = \Sigma \subset \{0, 1\}$. A state change of assets is defined by an incident (i.e., an alarm clarifying the aspects of the occurred incident). Σ is composed from possible strings (e.g., the kind of threat, its criticality, a timestamp) to describe alarms. The transition function, δ, can be considered as a set of mappings, $\delta_a : S \to \Delta(S)$ for each $a \in \Sigma$, where δ_a can be characterized through a stochastic matrix P_a, where each row describes the distribution of the next state. This representation typically makes it more understandable for users, as they can fill these transitions matrices row by row, each corresponding to a concrete situation, described by the node's state.

As an example, consider a node that receives information relating to a fire. If the node is currently in State 1 (operating smoothly/ efficiently) with a probability of occurrence of 20 %, it goes to the worst state, State 3 with a probability of occurrence of 70 % and to the intermediate state, State 2 with probability of 20 %. The remaining probability of 0.1 or 10 % is allocated to the condition where the state is not changed. These numbers are summarized in the initial row of the transition matrix, P_{fire}, as the starting state was 1. If the node is originally in State 2 (i.e., already facing some issues), there is a probability of 80 % that it changes to the worst state, State 3. If we assume that a fire alarm will not improve the node's state (i.e., the transition probability to State 1 is zero), there is a probability of 20 % that it stays in the current state. These numbers are summarized in the second row of the transition matrix, P_{fire}. If the node is already in the worst state, a new fire alarm will not affect the probability, so that the last row of the transition matrix assigns all probability to State 3. The transition matrix, P_{fire}, is described through a table as shown in Table 3. Each row describes a state change including the input and output messages that are relevant for the detection of cascading

Table 3
An example of transition.

Input	Current State	Next State	Output	Probability of occurrence
Fire	1	2	Fire	20 %
Fire	1	3	Fire	70 %
Fire	2	3	Fire	80 %

effects. The conditions where the state is not changed are defined implicitly through the fact that the sum of all transition probabilities being 100 % but could also be added explicitly. Whenever the node goes to a new state, it notifies its neighbors through the output 'Fire'.

$$P_{fire} = \begin{pmatrix} 0.1 & 0.2 & 0.7 \\ 0 & 0.2 & 0.8 \\ 0 & 0 & 1 \end{pmatrix}$$

The current model does not explicitly consider the intensity of the fire when determining state transitions. In this paper, the focus is on using incident types like fire alarms to trigger transitions based on predefined probabilities. The estimation of transition probabilities is a particularly challenging task often due to the lack of data that is often seen in the context of CIs. Therefore, multiple approaches are proposed to solve the problem of a specific threat, depending on the amount of data available (see Table 4).

3.2.2. Quantification of resilience

Over the past decade, the concept of resilience has rapidly evolved in the context of CIs [68,69]. Within the PRECINCT project, a review of recent work in the space of resilience was carried out to identify a strategy for resilience calculation. The following definition for resilience was adopted: "Resilience is the ability to continue to provide service if a disruptive event occurs" [50]. The PRECINCT project builds upon work which has preceded it in order to define a quantitative Resilience Methodological Framework (RMF) which defines a RI based on a monetary representation of the losses due to break down in the service delivered by the CI. Some samples of service measures are provided below for different CIs:

- Railway network: Passenger miles, ticketing.
- Road network: Delay times, safety of road users.
- Electricity/telecom network: Availability of power.

Service measures tend to vary from one CI type to the next. The monetary estimation used within PRECINCT allows summation of all service measures involved in the assessment of a multi-modal CI. To describe the resilience-relevant parts of the CI, "resilience indicators" are used. These are separate aspects to the RI, as they are essentially representative parts of the CI which indicate how resilient the CI is to the posed threats. Resilience indicators may be classified as Infrastructural, Environmental or Organisational. Each indicator is assigned a score based on the baseline state. Table 5 provides some examples of indicators for various infrastructure types. The various potential states of each indicator are listed in the table, as well as the context/meaning of each state. Wherever possible, the indicators states should be based upon existing standards and codes of practice relating to the indicators. For example, the indicator states for "Bridge Condition" may be based upon the states listed within the inspection protocol already in place for the bridge.

Table 5 also indicates the state to which the indicator impacts the resilience of the system. For example, the "Bridge Condition" indicator impacts the "Absorb" phase of the resilience cycle, as a higher bridge condition increases the resistance to a triggering event (e.g. flood and earthquake), while the "Number of City Police" impacts the "Recovery" phase. That is, more police mean that the aftereffects of a triggering event can be limited, bringing the service back into place more quickly.

Once the resilience indicators have been assigned, their impact on the service measure for a given triggering event must be determined. In this respect, the RMF works in conjunction with the interdependency graph simulation described in Section 3. Each indicator may be modelled as a node within the graph. In this way, the impact of changes to the indicator values can be modelled, considering the interconnected and time dependant nature of the problem. By simulating the various outcomes of indicator changes, the relative weight of each indicator on the service can be determined. The service measure used to quantify the resilience can also be determined from the cascading effects simulation as monetary values can be assigned to the output state of the nodes which are related to the service provided. This output data can then be fed to the backend of the serious game in order to acknowledge users to investigate the impact of various combinations of actions taken before, during and after a hazard/threat event. Cost benefit assessment can be combined with machine learning algorithms to train models to predict optimum strategies for the various actions that can be taken, subject to budgetary constraints.

There is a trade-off between model complexity and ease of use. Using a 5-point scale offers advantages in terms of clarity and applicability. In real-world scenarios, detailed data on CI components might be limited. This simplified approach makes the model easier to understand and implement by practitioners, thus enhancing its usability. However, the model itself is flexible and could be adapted to incorporate a wider range of values in future work, provided more granular data becomes available. Despite the limited value range, the model's strength lies in its comprehensiveness, capturing various resilience aspects through di-

Table 4
Parametrization of probabilistic models, adapted from [66].

Estimation Method	Description
Direct Estimation	The simplest way to characterize the transition regime is direct estimation of the transition probabilities $p_{ij} = p_{(i \to j)}$ that a node changes its state from i to j. In situations where data is sparse, such estimation is subjective and therefore prone to error. Whenever possible, multiple assessments should be collected and combined in a way that is not sensitive to outliers (e.g., a median).
Qualitative Estimation	One way to consider the uncertainty in human estimates is to let experts indicate how certain they are about their prediction. The predicted values are the most likely ones, but neighboring values are also considered as potential outcomes. Based on the confidence, the distribution over all possible states is of different forms, i.e., the weight put on other values increases when confidence decreases.
Identification of Similar Scenarios	In some situations, threats are explicitly characterized through variables, e.g., through the configuration of a system. In this case, the state of a node can be estimated through the number of scenarios that potentially caused a specific degree of disruption or loss.
Counting Threats	In a situation where experts or tools support the evaluation of the threats an asset faces, the estimation of probabilities can be based on the number and type of threats that affect a specific asset. For a given configuration describing the current state of the node and potentially considering the states of neighboring notes, the threats affecting an asset are evaluated to determine the new state of the node.
Logistic Regression	Collecting experts' implicit knowledge on system threats can be challenging, as they often hesitate to make precise estimates. However, utilising a "parametrization by example" approach, evaluating different configurations and analyzing the data with logistic regression, can provide valuable insights without requiring full configuration coverage.

Table 5
Sample Resilience Indicators.

Part	Indicator	Phase	Possible values	Meaning
Infrastructure	Telecom ICS Protection Systems (firewalls)	Absorb	4	State of the art
			3	Slightly outdated
			2	Very outdated
			1	Not in place
	Bridge Condition	Absorb	5	Like new
			4	Slightly deteriorated
			3	Average
			2	Poor
			1	Alarming
	Rail control centre backup power supply	Recovery	3	Automatic back up
			2	Manual back up plan
			1	No back up system
Environment	Ease of physical access to Telecom staff area	Absorb	5	Very low risk
			4	Low risk
			3	Average risk
			2	Moderate risk
			1	Severe risk
	Accessibility of bridge infrastructure	Recovery	4	Fully accessible after event
			3	Fully accessible with specialist equipment
			2	Semi-accessible
			1	Not accessible
Organisation	Telecom staff crisis training	Recovery	3	Constant training
			2	periodic training
			1	No monitoring
	Monitoring of threat level	Absorb	4	Every week
			3	Every month
			2	Every 3 months or more
			1	No monitoring
	Number of city police staff	Recovery	5	More than 200 staff
			4	150–200 staff
			3	100–150 staff
			2	50–100 staff
			1	Less than 50 staff

verse indicators, while remaining scalable for application to different CIs.

The PRECINCT RMF (see Fig. 6) computes resilience with respect to the service measures delivered by the CI, such as the number of passengers moved by a transport system, or the hospital's patient load. Every single service measure is computed in financial expressions to evaluate resilience improvements across different CIs. Subsequently, resilience can be assessed by quantifying the service losses caused by a particular cyber-physical incident. Resilience indicators can be applied to allocate the losses to particular elements of the CI, and targets can be set for these indicators to improve resilience. The proportion of indicators met can be used to estimate the relative impact of a cyber-physical incident on CIs. Each step of the RMF is described in the following.

a) Define CI System

The first step in assessing CI resilience is to define the CI system being assessed. This includes identifying the physical assets, cyber systems, and organisations that contribute to the CI's resilience (e.g., fire departments, police departments, emergency services, and first responders). For example, bridges and road sections form part of a transport network, central control rooms form part of a motorway, and power plants supply electricity to CI elements. The CI system should also consider the physical environment in which it operates, such as the risk of floods or deliberate physical attacks, as well as the organisational environment to which the infrastructure management organisation is subject. This includes regulations/codes impacting the infrastructure. The definition step should also identify the relevant hazards of interest to the multimodal system of CIs and interdependencies between events. For example, an urban tram system with sufficient flood defenses may not be impacted by a 1 in 100-year flood event, but the power network supplying electrification to trams may potentially be at risk of shutdown.

b) Quantify Service

PRECINT evaluates CI resilience by assessing the quality of service provided, which can range from travel time and user safety to uninterrupted internet access. This assessment involves three main steps: defining the service, quantifying the service, and valuing the service. The service definition should be based on stakeholder input and can be measured using indicators or simulations. The service value is then assigned a monetary value based on published data or valuation techniques. This standardised approach allows for a comparable assessment of CI resilience across different types of CI.

c) Quantify Resilience

The RMF quantifies resilience using indicators or simulations. As described in Table 5, various resilience indicators can be used to assess the state of a CI and its impact on service provision. These indicators can be assigned scores based on their states (e.g., "Like New" vs. "Alarming" for Bridge Condition) and then weighted based on their impact on service provision. When using indicators, the user must identify, check for relevancy, estimate values, and quantify resilience using weights. Indicators provide an indication of the difference between the service provided and the intervention costs. An example indicator is the condition state of the infrastructure. Indicators must be checked for relevance to ensure they are worthwhile to include. The number of scores possible for each indicator may vary for each hazard. The final step of measuring resilience with indicators involves correlating indicator scores with measures of resilience, generally in monetary units representing differences in intervention costs or measures of service. For differentiated weights, estimating the relative impact of each indicator on resilience is essential. The weight of an indicator is determined by the difference between the reduction in service and intervention costs with the indicator at its worst value and the reduction with the indicator at its best value.

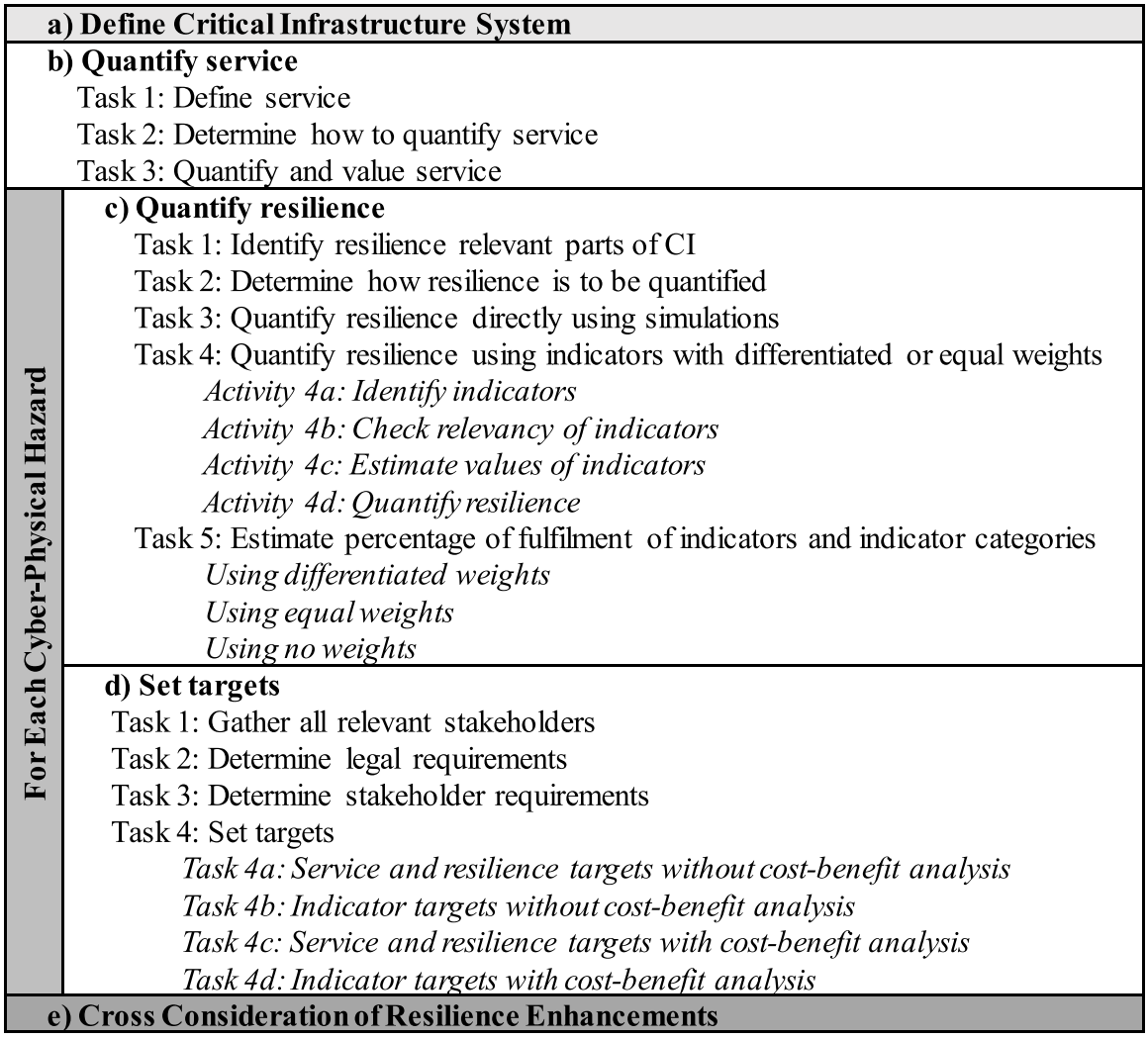


Fig. 6. Precinct RMF [50].

d) Set Targets

The RMF sets targets for resilience to ensure the goals of the CI organisation are achieved and to incorporate codified norms. The process involves gathering stakeholders, identifying legal requirements, determining stakeholder requirements, and setting targets. Legal requirements typically involve minimum condition states for infrastructure assets and minimum assessment loads. Targets can be set against measures of service and resilience, or against indicators. Cost-benefit analysis (CBA) can be used to determine the optimal target for each indicator.

e) Cross Consideration of Resilience Enhancements

The RMF's final step involves considering and implementing resilience enhancements to the CI system, taking into account the resilience quantification and targets. This can be done either for each hazard individually or across multiple hazards simultaneously. Then, the resilience of the entire system can be weighted according to the likelihood of each event. The identification of appropriate resilience enhancements can then be made by analysing the statistical representation of resilience across all indicators.

The PRECINCT cascading effects pattern, a central component of the RMF (see Fig. 7), assesses the impact of resilience enhancements on overall expected losses given a triggering event, considering budget constraints. Resilience targets are set resulting from stakeholder concerns, monetary evaluations, and endorsed obligations. Fig. 7 shows the relationship between the cascading effect simulation and the RMF. It indicates how the cascading effect simulation is used to quantify resilience and to inform the setting of resilience targets. Specifically, the cascading effects interdependency initially provides a conceptual ontology to describe the context of the CI system in terms of hazards and key infrastructure nodes/boundaries. This is step (a) of the RMF. Subsequently, the interdependency graph is used with steps (b) and (c) of the RMF in terms of quantifying the service and quantifying the resilience, with consideration of the specific hazards modelled in the graphs. Finally, targets are set (RMF step (d)) by considering the impact of enhancements on the resilience of the system.

3.2.3. Serious games (SG)

Gamification can be defined as "using game-based mechanics and theory to engage people, motivate action, and promote learning" [70]. In 1987, the term "Serious Game (SG)" was introduced by researcher Abt [71]. In 2002, the US Army developed a serious game in the form of a video game named America's Army. Then, the SG Initiative was founded in 2002 by the Woodrow Wilson Center for Scholars in Washington, D.C. [72]. They described serious games as "games that do not have entertainment, enjoyment, or fun as their primary purpose" [73]. Nevertheless, "entertainment" has been considered a significant factor of SGs in other definitions, e.g. "serious game is a mental contest, played with a computer in accordance with specific rules, that uses entertainment to further government or corporate training, education, health,

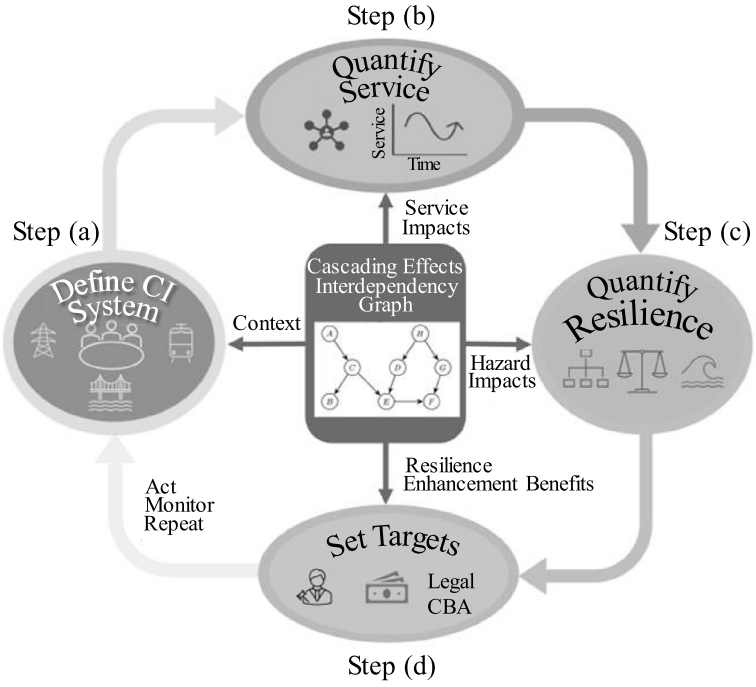


Fig. 7. Incorporating PRECINCT cascading effects and interdependency graphs into RMF modeling.

public policy, and strategic communication objectives" [74]. It can explore entertainment for different purposes, such as training, education and skills development [75]. Since 2002, SGs have been successfully introduced for different domains such as education, scientific research, environmental science, healthcare, government, politics, military, entertainment, religion, security, marketing, culture and art [76,77]. The authors of [77] proposed the main characteristics of a serious game, as follows:

- An action language for communication between game and player;
- Assessment tracks the number of correct answers;
- Conflict or challenge;
- Control, or the ability for the players to alter the game;
- Environment;
- Game fiction or story;
- Human interaction among the players;
- Immersion in the game; and
- Rules and goals of the game provided to the player.

In Fig. 2, the PRECINCT project's comprehensive framework was showcased, which included a range of components designed for the systematic security and resilience management of CIs. One major tool within this framework is the SG module. This module can identify the unanticipated combinations of threats or cascading effects in CIs [78]. In PRECINCT, a SG design concept was proposed to improve CI resilience which has been outlined in six main steps, i.e. (1) fit player's data to train machine learning, (2) generate clusters, (3) create prediction models, (4) identify vulnerabilities, (5) discover trends, and (6) create visualisations. The methodology followed to develop the SG was based on the principles of SGs and gamification. The game was intentionally designed to be challenging and engaging, while also providing players with the opportunity to learn about CI resilience. The gamification techniques were used to motivate players and help them to develop the skills and knowledge they need to improve the resilience of CI systems. The end users (CI operators & emergency responders) needs and learning objectives relating to the SG as a training environment for CIP was assessed in specific workshops. Feedback from the workshops was aligned with SG pedagogical approaches [79–84] to design the SG for CIP. These approaches ensure users are motivated to learn, understand the environment, improve resilience outcomes, and gain valuable feedback.

To implement the game, it is required to feed various key contributors, i.e., player attributes, different threats, resilience indicators, threshold levels, attack and defence strategies, and available budget. Game play records will be analysed, and data will be mined to produce training material and understanding of how interventions can change the resilience index (see Fig. 8).

A brief overview of the sequencing of gameplay and potential gameplay options are provided here to enable the reader to understand the potential gameplay interactions and data. In the SG, firstly, a registered user logs in by entering their username, email, and password (Fig. 9(a)), then selecting a character, either the Game Director, an Attacker or Defender (Fig. 9(b)). Once a player is logged in, the game will present the qualified director with a director's dashboard to select the type of physical or cyber-attack, the location, and the budget for the attacker and the defender for each CI. The attacker's dashboard (Fig. 9(c)) enables the attacker to select tools for the initial attack, use upgraded tools for changing the attack. The defender is presented with a game's initial balance, the player's ranking, the attack type, and the level set by the director (Fig. 9(d)). Next, the defender must enter their job role and the number of years in this position. Then, the defender is presented with the opening attack scenario, e.g., "flooding" set by the director using the rainfall selected by the attacker to launch the initial attack. The game provides a set of analysis tools to help the defender decide, including geospatial visualisation, the impact location and the size, the risk level concerning each CI's resilience, and the live update of the traffic condition of the attack's assets. The game uses the interaction of the attacker and the defender to simulate an attack's cascading effect. After the defender implements a solution to counteract the attacker's first attack, the attacker intensifies the attack by increasing the level of attack. Consequently, CI is damaged due to the additional attack. The size of the affected area, the change in resilience for each CI, the links of affected CIs, and the detailed cascading effect between different CIs can also be displayed using the proposed SG.

The SG was validated by living labs (LLs) user testing to gather feedback on its usability, effectiveness, and overall experience, as well as expert review by CI resilience experts to ensure its accuracy. The main

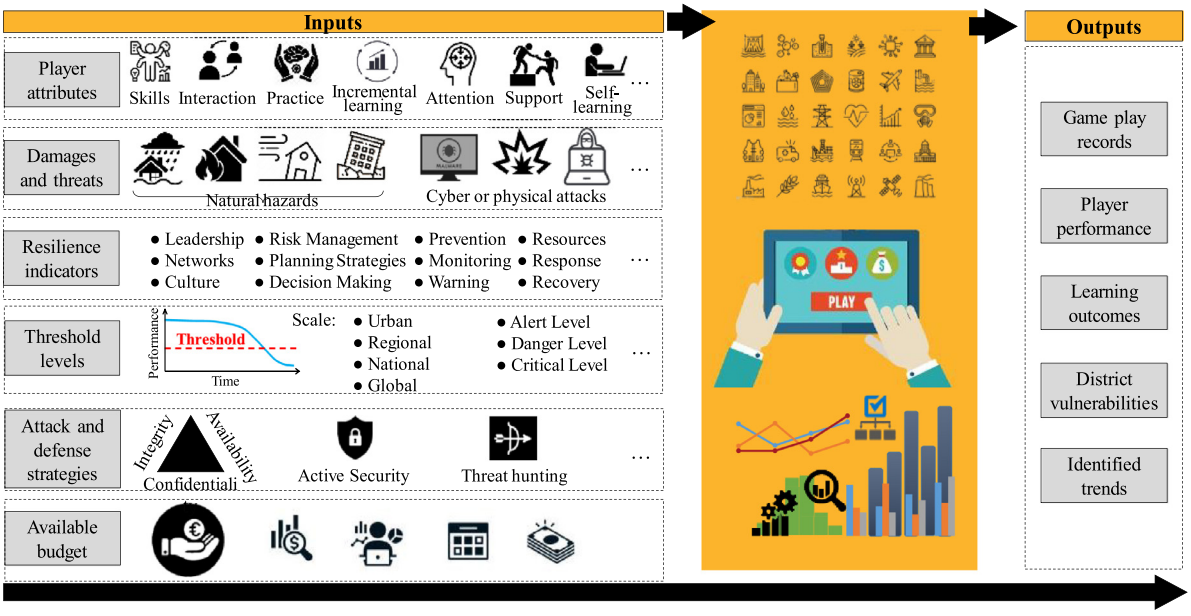
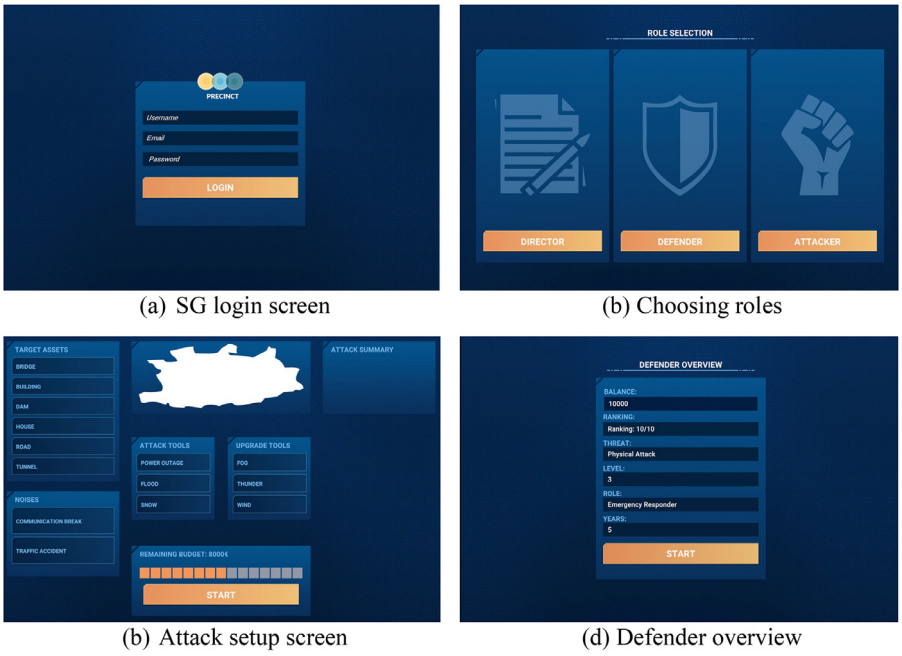


Fig. 8. SG design concept.



(a) SG login screen (b) Choosing roles

(b) Attack setup screen (d) Defender overview

Fig. 9. PRECINCT Serious Game.

contribution of this SG is that it is specifically designed for CI resilience. This means that the game is focused on enabling players to understand, evaluate, analyse, and create solutions about the threats and vulnerabilities of CI systems, and how to mitigate the threats. The game also provides players with the opportunity to practice their skills in a simulated environment. To the best of our knowledge, there is no existing SG in the same or a related domain that validates the contribution made by this study.

3.2.4. Digital twins (DT)

A Digital Twin (DT) is a virtual model of a physical asset or process, hosted in the cloud, that mirrors the entity's current state and behaviour, enabling simulation, prediction, and optimisation. In other words, the DT is an integrated multi-physics, multi-scale, probabilistic simulation of a real physical system that uses the best available physical models, sensor updates, data and events history to represent the life of the corresponding twin [85]. A DT acts as a container for integrating information from different sources at different lifecycle stages. The information contained in the DT can be used to analyse the current status of a real system and derive a model in order to build an improved version of the system capable of managing the risks detected with suitable mitigation strategies. The idea of DT can be traced back to the early 2000s, when NASA and the U.S. Air Force organised its implementation in the aerospace industry for their spacecraft and aircraft systems [86]. Then, DT has been gradually expanded into diverse application domains, including Smart Cities, Industry 4.0, Healthcare, and Smart Manufacturing. NASA, a pioneer in DT adoption, integrated it into its technology roadmap for simulation, modelling, processing, and information technology [87]. DTs

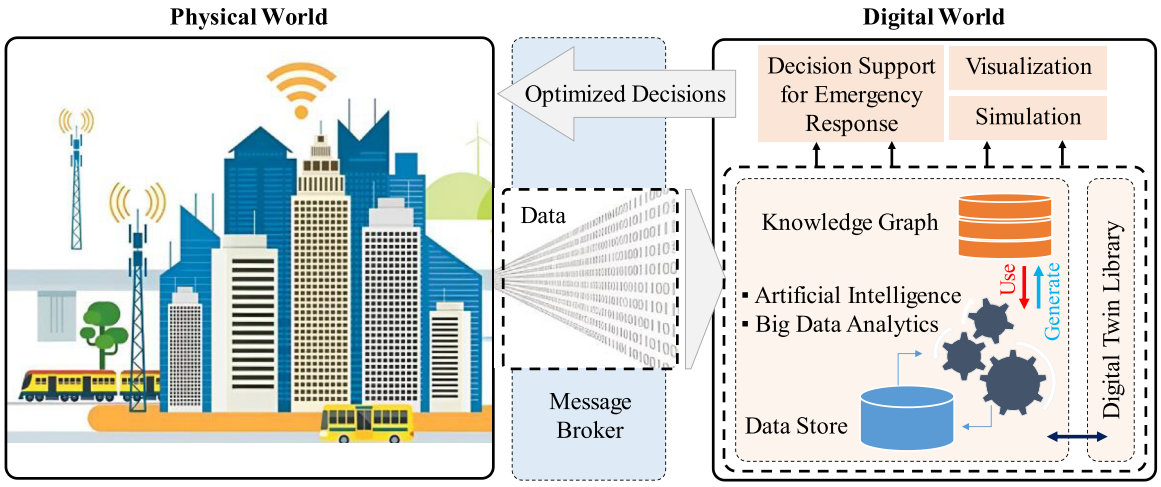


Fig. 10. Overview of DT concept.

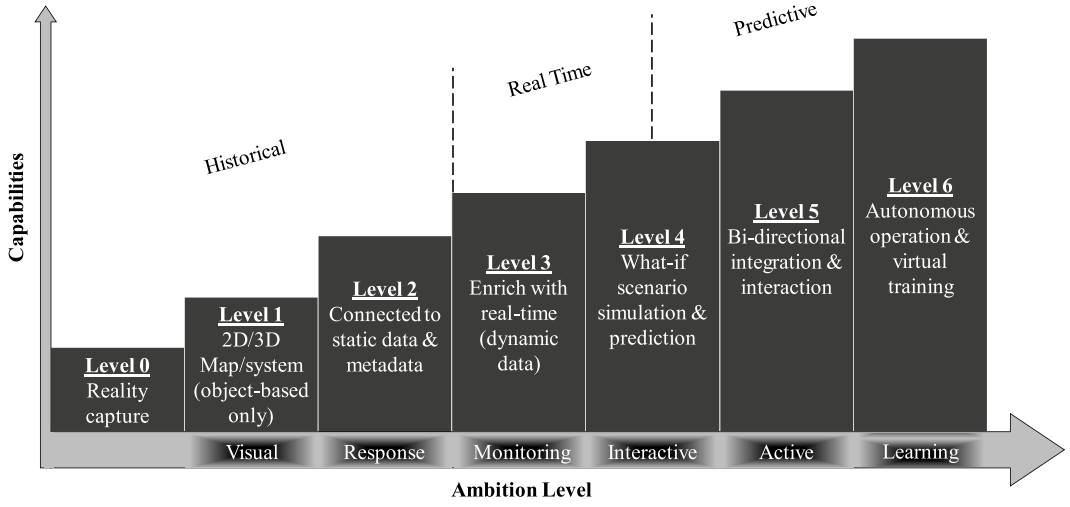


Fig. 11. OPEN Local DT.

have emerged as transformative decision-support tools, enabling companies to create real-time simulations that predict object or process performance using data from the physical world. Hence, DTs serve as a bridge between the physical and digital worlds, advancing a better understanding and enhanced control of real-world systems (see Fig. 10).

A DT architecture and related instantiation (system of systems) is not a single-ended collection of components, or a centralised platform. It is a collection of processes based on important principles. These processes need capabilities (functional and technical) and related components that can fulfill these capabilities. DT frameworks also come in different variants. Fig. 11 presents a classification based on the capabilities of the DTs, categorized into six levels. In PRECINCT, the level needed is level 4 to be able to simulate cascading effects on CIs caused by events and assess the RI of possible mitigation actions. Which means that static and dynamic data is needed, but also simulation models to see the impact of "What-If" analysis.

The DT module stands as a principle of PRECINCT framework, serving as the digital counterpart to physical CI networks. As depicted in Fig. 2, the DT is connected to the CI network topology and metadata, employing closed-loop ML for anomaly detection, response optimisation, and automated forensics. A high-level conceptual architecture of the PRECINCT DT is shown in Fig. 12. As can be seen from Fig. 12, the PRECINCT DT architecture highlights the DT, and its interaction with CI systems and the PRECINCT ecosystem platform components. The salient parts of the architecture are the DT platform and the solution accelerators labelled CI_1, CI_2 and CI_n. Each of these solution accelerators measures a specific CI and handles the CI data in the appropriate way through custom algorithms.

4. Blueprints, deployment, and transferability of precinct components

A PRECINCT blueprint is defined by a reference architecture for PRECINCT components that employs a description language, i.e., Topology and Orchestration Specification for Cloud Applications (TOSCA). Blueprints facilitate the deployment of PRECINCT applications on resources provided by CI stakeholders. Additionally, they offer an effective solution for scaling and maintaining large applications. Hence, the implementation of CIP applications is assisted with blueprints as they can enable the collaboration of the partners during the development procedure to reduce the overall development period as well as to standardize CIP assets. In other words, PRECINCT components are described as TOSCA service templates to manage the deployment and orchestration of these components. A service template is illustrated by Fig. 13.

A service template is defined for the DT, SG, the PRECINCT ecosystem platform, and the composition of all these outcomes using a YAML based grammar and contains the description of a topology model, Interfaces, Operations, and Workflows. A topology model is a directed acyclic

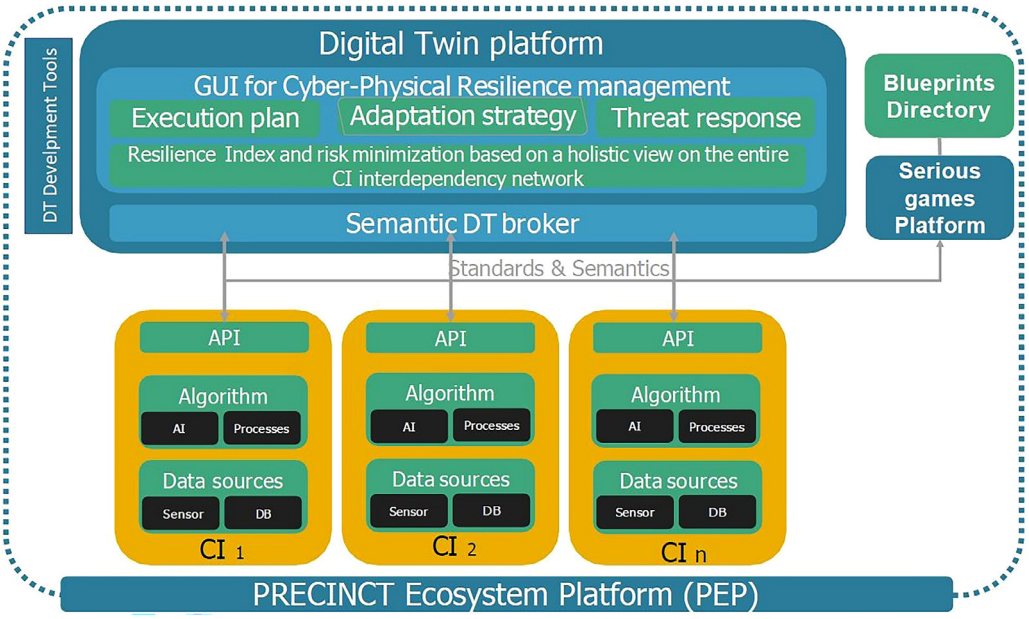


Fig. 12. High-level conceptual PRECINCT DT Architecture [61].

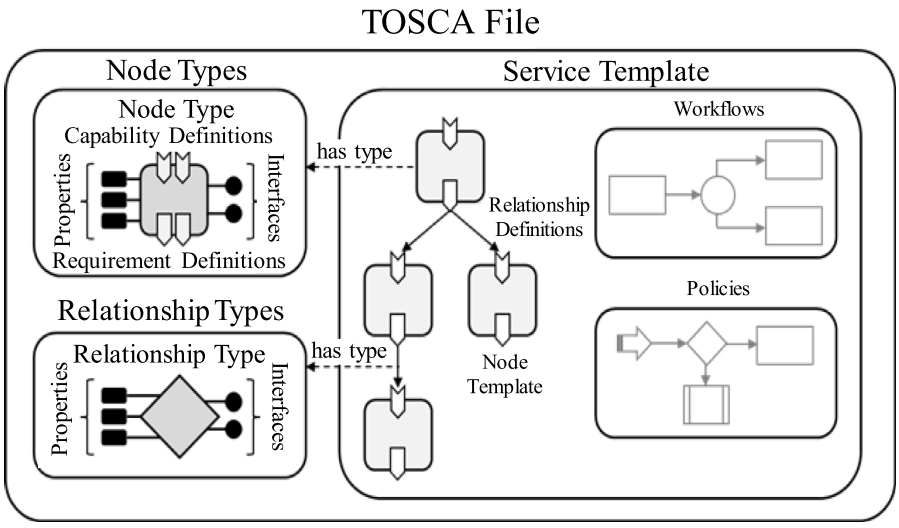


Fig. 13. Illustration of an OASIS TOSCA service template [88].

graph where the node are instances of Node Types (i.e., the definition of properties and operations provided by the component) and the edges are defined as relationships which can also be generalized into Relationship Types [88]. A topology used to deploy the Knowledge Graph is illustrated on Fig. 14, where the graph shows the nodes and their relationships (connection to TCP ports and hosting) in a deployment scenario where Docker to host Neo4J, the graph database and a REST API server. The computer, networking and storage resources are provided by CIs operators in on-premises, private or public cloud as well as the definition of the Policies through the adaptation of the service templates.

The architecture is modelled using TOSCA within a Service Template, incorporating CIP assets such as the Cascading Effect Simulator, SG, and DT, along with their relationships (e.g., the sequence of instantiation for tools). This modelling also captures the interfaces used by these tools to exchange data, such as the interdependency graph, which can be communicated via APIs or MQTT. In addition, TOSCA's Service Template emphasises the management of the lifecycle of CIP assets, while the interdependency graph is represented as an artifact in a JSON file and is not modified by TOSCA's orchestrator, which lacks an understanding of the semantic of this JSON file. Consequently, acyclic and interdependency graphs are not directly correlated.

Furthermore, in a service template, Interfaces, Operations and Workflows define how a service described by the topology is instantiated, terminated, and managed during its entire lifecycle. Finally, Policies defines the services aspects such as its quality-of-service, performance, and security objectives [88]. Thus, a PRECINCT blueprint manages the life cycle of the PRECINCT components deployed in a LL as well as the dedicated infrastructure used by the LL to host the components. Fig. 15(a) illustrates some of the node Types defined for the PRECINCT Ecosystem Platform components and Fig. 15(b) shows the service templates describing the deployment of PRECINCT component in LLs.

The PRECINCT blueprints are stored in a Gitlab repository named the PRECINCT Blueprint repository from which the service template can be downloaded and deployed using an OASIS TOSCA orchestrator such as xOpera [89]. Finally, the PRECINCT Blueprints contain documentation

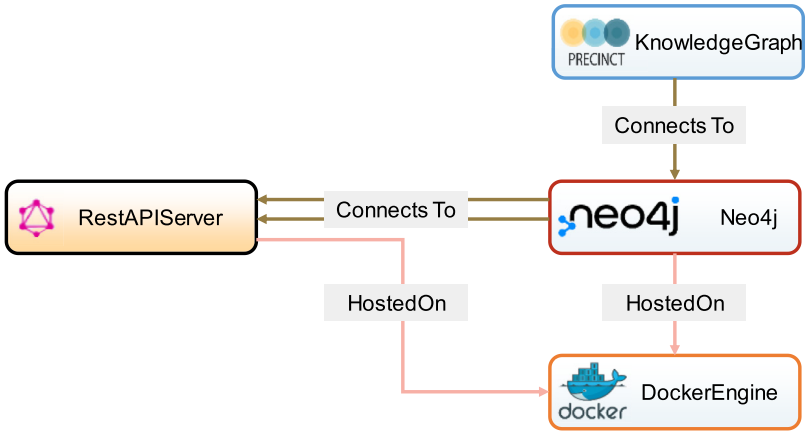


Fig. 14. Visualisation of the topology of deployment of the Knowledge Graph.

Fig. 15. Illustration of (a) node types, and (b) service template defined in PRECINCT.

which described the reference architecture as well as lessons learned during the deployment to facilitate the adoption of PRECINCT solutions in several CIP use cases.

5. Illustrative scenario: PRECINCT's role in a flood event

An illustrative scenario showcasing how PRECINCT evaluates risks and strengthens resilience during a flood event is presented in this section. Imagine a severe storm triggering flash flooding in a riverside city. This scenario can be considered to show the application of the PRECINCT model in a real-world context. Flooding is selected here as a representative natural disaster due to its complex and cascading effects on interdependent CIs. Floods can have devastating consequences, disrupting transportation networks through road closures and bridge failures. Additionally, flooding can damage power grids, water treatment plants, and communication towers, creating a domino effect that cripples entire communities [90,91]. Given the widespread disruption floods cause to CIs, they serve as a relevant example for showcasing PRECINCT's capabilities.

5.1. PRECINCT in action

The PRECICNT initiative in action can be observed through four aspects, i.e., identifying cascading effects, resilience assessment, mitigation strategies, and an e-learning module.

a) Identifying Cascading Effects

A major flood event lasting for a long time could disrupt CI systems. The cascading effects could be significant, with disruptions in other CIs. Analysing the knowledge graph, PRECINCT determines the potential consequences of flooding on various CIs, as follows:

- Transportation networks: Road closures due to submerged roads, bridges, and tunnels, leading to total gridlock traffic congestion on the city streets.
- Power grid: Disruptions from flooded substations and downed power lines.
- Water treatment plants: Potential contamination of water sources and damage to treatment facilities.
- Communication networks: Disruptions due to flooded communication towers and damaged cables.

b) Resilience Assessment

PRECINCT employs the RMF to calculate the city's infrastructure RI before and after the flood. This considers service measures (such as disruptions in power supply, water availability, transportation, and communication services), resilience indicators (scores assigned to aspects corresponding to flood barriers around critical facilities, redundancy in power lines, and public awareness campaigns), and monetary estimations. The RI reflects the economic losses due to service disruptions across affected CIs.

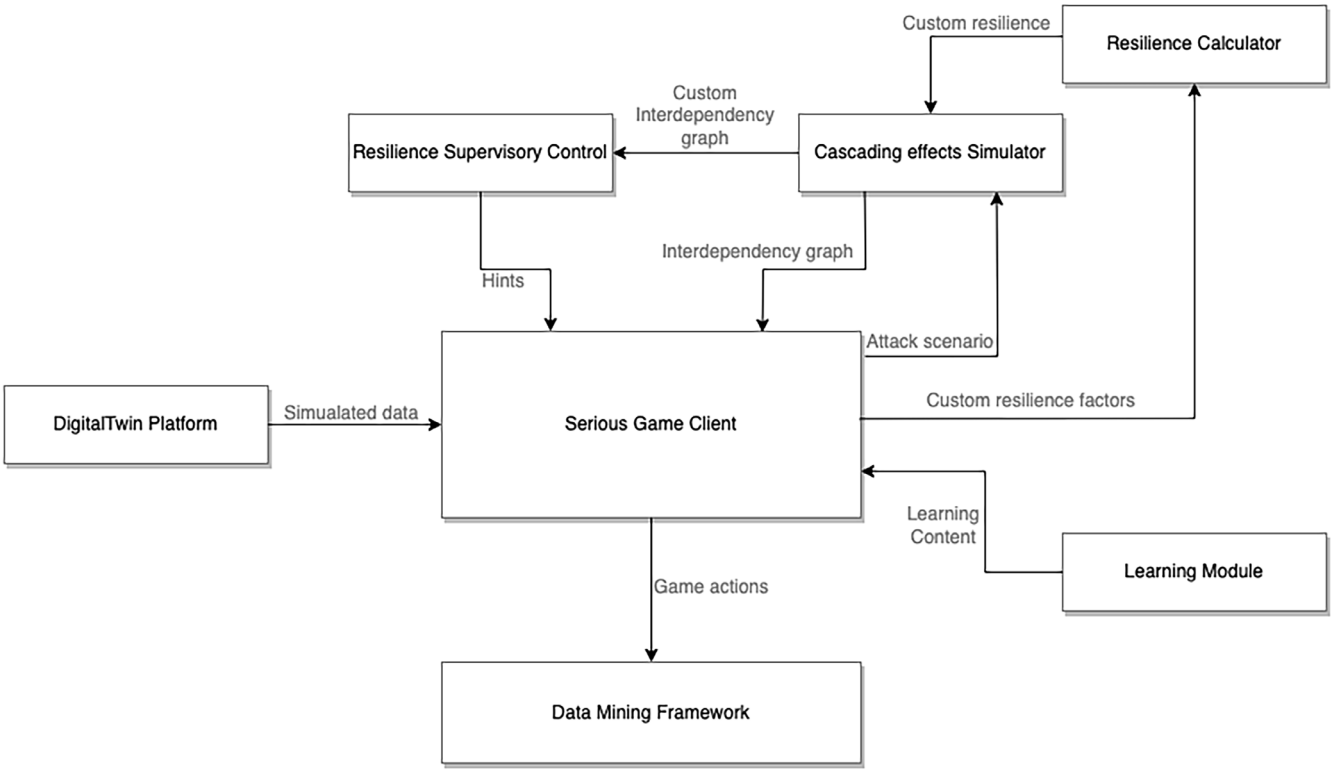


Fig. 16. Integration architecture of the SG.

c) Mitigation Strategies

PRECINCT utilises simulations to support decision-making. In this scenario, the PRECINCT model's DT would play a vital role. The DT would continuously monitor real-time data from various CIs. By analysing this data, the DT could identify potential cascading effects early on, allowing for timely mitigation strategies, as follows:

- Emergency response coordination: Facilitating communication between emergency services, public utilities, and residents for evacuation and resource allocation.
- Deployment of resources: Activating mobile water treatment plants, deploying temporary communication towers, and setting up sandbag barriers to protect CI.
- Resource Management: Optimising the allocation of rescue crews, medical supplies, and evacuation shelters based on the severity of flooding in different areas.

d) E-learning Module

The SG component of the PRECINCT model would also be crucial in this situation. The SG could simulate a flood event and its cascading effects, allowing CI operators and emergency responders to practice their response under realistic conditions. This immersive training would enable them to identify critical decision points, refine communication protocols, and enhance overall preparedness for unforeseen events.

e) Blueprints for *Re*-usability of PRECINCT's CIP Assets

The previously described IT tools (i.e., DT, SG, etc.), data and documentation used during this scenario can be described using TOSCA. This will allow the scenario to be readily re-used when a redeployment of the tools is needed by another city or by a researcher for testing the overall PRECINCT approach. In fact, beyond this scenario, TOSCA allows to change several parameters: either using the tools as provided or deployment them using new resources and configurations (changes the data sources, simulation parameters, etc.). The Blueprints are then stored in a dedicated PRECINCT repository.

5.2. Outcomes

By simulating flood scenarios and identifying vulnerabilities, PRECINCT empowers stakeholders to proactively enhance the city's resilience from the following perspectives:

- Prioritizing investments: Directing resources towards flood protection measures for CIs, early warning systems, and flood-resistant building codes.
- Developing emergency response plans: Creating well-coordinated plans for evacuation, rescue operations, and damage assessment.
- Enhancing community preparedness: Educating residents about flood risks, evacuation routes, and safety protocols.

The PRECINCT SG frontend application acts as a face to the various backend components such as cascading effects simulator, DT data, and the user/usage backend system. The overall integration architecture of the SG is shown in Fig. 16 which includes communication with backend components to obtain the data for all the players in the SG to perform various tasks in the game and send the data collected to enable a data mining tool to analyse the gameplay records.

When a user registers/logs in, the backend is used to verify the credentials and the role assigned to that user. The user can be assigned one or more of the three major roles (i.e., Director, Attacker, and Defender). Once the login is successful, based on the role assigned to the user, the backend sends the attack data, defends available and other information about the scenario created by the director. An attacker can then create and save a new attack to the backend as well as attach it to one or many defenders.

When a defender logs in, the backend sends all the attacks available for defending available. Once the defender chooses an attack, the system sends all the attack information to the cascading effects simulator and runs the simulation. The cascading effects simulator returns the various effects of the attack on the geospatial nodes in the city. The defender can take various defensive actions on the action nodes, this sends the current state of the dependency graph (which includes the nodes) along

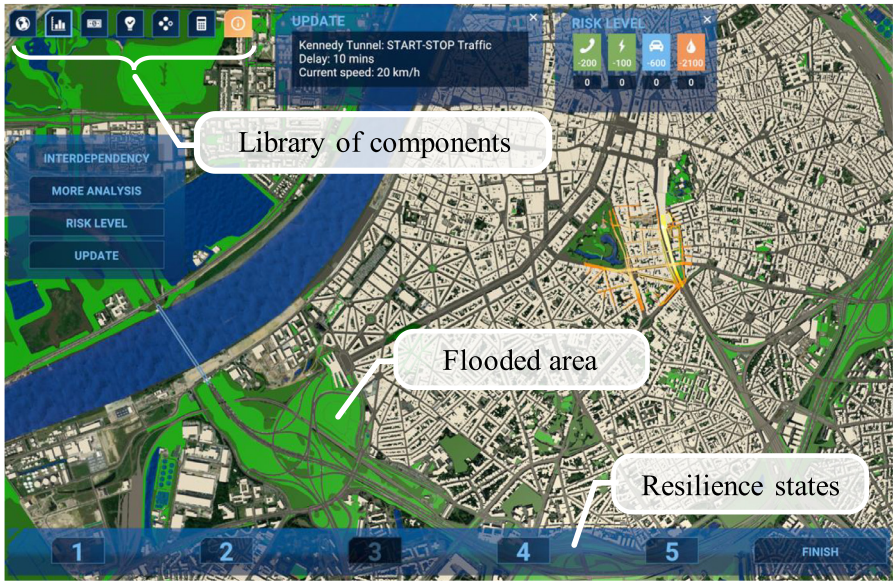


Fig. 17. PRECINCT SG.

Characters	Dashboards and Roles
Director	- Setup damage scenario(s), i.e., type of attack and location (Damage identification) - Define budget for defender and attacker for each CI
Attacker	- Select the CI target (Damage location) to lunch an initial attack - Select the attack type (Damage severity) - Can lunch additional attack by selecting destructive option(s) or increasing the severity of damage
Defender	- Provide the player's information, i.e., the initial budget balance, ranking, type of threat, job role, years of experience - Select gameplay options to play, pause, restart, speed or quit the game - Use the provided tutorial, control elements, time slider and play buttons - Finish the game and get the report (game score)

Control Elements Information

Map button: Geospatial analysis - Provide the geospatial visualization based on: ▪ Damage location (Affected size) ▪ Damage severity (Degree of damaged area) ▪ Level of Resilience	Tool button: Potential solutions - Suggest suitable action(s) such as: ▪ Warning/Evacuation ▪ Sending Food, Medicine, etc. ▪ Police patrolling ▪ Sending technician(s) for maintenance/repair ▪ Providing Shelter
Analysis button: Current condition and analysis - Present the following updates: ▪ Interdependency graph (Model of linked CIs) ▪ Risk level and affected size (Damage detection) ▪ Resilience meter	Sub-CIs button: - Present the relevant sub-CIs, e.g. ▪ CI: Water (Damage type: Flooding) ▪ Sub-CIs: Drain, Reservoir, Sewer
Additional resources button - Allow to requests limited additional budget with an interest rate	Bookkeeping button: Expenses distribution - Allow to implement the aforesaid potential solution(s) in tabular or map-based format - Allows to enter the amount of expenditure for each CI

Fig. 18. Library of components of the PRECINCT SG.

with the defensive actions to the cascading effects simulator backend to run more simulations and calculate the change in the resilience.

Each action done by the defender along with the attack and scenario information is sent to the backend as well and saved, which allows the mining of the data to be analysed by the data mining framework. The flow of data is through REST APIs and use https authentication for security.

Fig. 17 shows the PRECINCT SG including a library of components, flooded areas, and resilience states. The player can click on any component (e.g., map button, analysis button, additional resources button, tool button, and bookkeeping button) to get more detailed information as described in Fig. 18. For example, if the player clicks on the analysis button, the information about Risk Level will display what each colour represents, the value inside the colored square indicates the probability of occurrence and the change in resilience (see Fig. 19). As can be seen from Figs. 17 and 19, the resilience is shown using a probability range associated with a state from 1 to 5.

5.3. PRECINCT's advantages and challenges

By integrating knowledge graphs, flood vulnerability assessments, and dynamic simulations, PRECINCT provides a powerful framework for

Colour	State	Accessibility	Minimum Probability	Maximum Probability
	1	Good	90% ≤ Resilience	
	2	Minor	70% ≤ Resilience	< 90%
	3	Moderate	40% ≤ Resilience	< 70%
	4	Major	30% ≤ Resilience	< 40%
	5	Inaccessible	Resilience	< 30%

Fig. 19. CI's state colour representation and resilience conversion probabilities.

managing flood risks and bolstering the resilience of CI networks. The modelling of cascading effects is one of the most significant benefits of PRECINCT. The PRECINCT framework identifies the cascading effect of flooding on interconnected CIs, enabling proactive mitigation strategies. Supporting decision-making is another benefit of PRECINCT as it can provide real-time simulations to guide resource allocation and response actions when flood events occur. PRECINCT also offers Blueprints to CIP research communities and other CI stakeholders. These Blueprints are TOSCA Service Template which facilitate the customization and deployment of CIP assets to fit the needs of a CI stakeholder. Another advantage is the ability of CI operators and emergency responders to train under realistic conditions.

While PRECINCT offers a powerful framework for flood preparedness and response, it is important to acknowledge some potential limitations and challenges. Data quality and availability is one of the most important challenges of PRECINCT. The effectiveness of PRECINCT relies on the quality and comprehensiveness of its underlying data. Inaccurate or incomplete data on CIs, their interdependencies, and historical flood events can lead to flawed risk assessments and mitigation strategies. The complexity of real-world scenarios is also challenging as flood events can be highly unpredictable, and real-world situations may involve unforeseen factors not fully captured by the model. PRECINCT's ability to adapt to these complexities is crucial for its effectiveness. Human decision-making, cybersecurity threats, cost implications and implementation challenges are other limitations. PRECINCT provides valuable insights and recommendations, but ultimately, human decision-making plays a critical role in implementing mitigation strategies and responding to flood events. Effective communication and trust between stakeholders are essential for utilising PRECINCT's recommendations effectively. PRECINCT's reliance on real-time data and simulations could make it vulnerable to cyberattacks. Robust cybersecurity measures are necessary to protect the integrity of the system and the data it utilises. Deploying and maintaining a comprehensive framework in PRECINCT can be resource-intensive and the blueprints proposed to alleviate these burdens also need to be maintained. Careful consideration of costs and benefits is essential, particularly for smaller communities.

6. Conclusions

PRECINCT's central idea is that the SG and DT both distinguish and track events within and across system boundaries, using ML principles. The autonomous nature of the PRECINCT solution regarding detection (pattern matching and learning capabilities) and mitigation (DT approach) addressed limitations in existing systems to provide timely and 'automated' responses to cascading effects, to support automated forensics and to provide improved protection measures for individual CIs. Based on the presented information, the following conclusions can be drawn.

A methodological framework was developed to facilitate quantification of resilience (1) during normal operations, and (2) for threats with short-term or long-term impacts. The RI calculated before and after events based on the Use Cases from the LLs were defined before playing the SG. The main function of the DT was to provide data (e.g. resilience index; cascading effects; metadata; etc.) for use in the SG. The SG was proposed as a training and learning tool for emergency responders and CI operators.

The PRECINCT blueprints provided an approach for designing reusable CIP software assets by: (1) defining a reference architecture for PRECINCT components based on the outcomes of past CIP research projects, (2) describing the concreate implementations of these reference architectures using OASIS TOSCA and to manage their lifecycle in a LL, and (3) documenting the lessons learned during deployment to facilitate the maintainability, transferability of knowledge, and re-usability of the PRECINCT components in different deployment scenarios. Moreover, these PRECINCT blueprints were centralised in a repository to be used by CIP communities.

Relevance to resilience

This paper presents a novel approach to improving the resilience of critical infrastructures using serious games and digital twins. The provided framework presents a holistic approach to critical infrastructure security and resilience management by considering the interdependencies between critical infrastructures and the potential for cascading effects. The serious game and digital twin components of the framework are particularly relevant to resilience in the following ways:

- Serious games provide a novel and engaging platform for training emergency responders and critical infrastructure operators on how to respond to cyber-physical attacks and other disruptions. This helps to improve their preparedness and response capabilities, which is essential for mitigating the impacts of disruptive events on critical infrastructures.
- Digital twins provide a realistic simulation environment for assessing the resilience of critical infrastructures under different scenarios. This information can be used to develop and implement resilience enhancement measures, such as identifying and addressing critical vulnerabilities, developing contingency plans, and improving coordination between critical infrastructure operators.

In addition to the serious game and digital twin components, the presented framework also introduces other features that are relevant to resilience, such as:

- A methodological framework for quantifying resilience under different scenarios.
- Reusable critical infrastructure protection software assets through the blueprints.

Data availability

Due to security considerations, the inclusion of specific data in this paper is restricted, and we are prohibited from publishing it.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Meisam Gordan: Conceptualization, Investigation, Methodology, Visualization, Writing – original draft, Writing – review & editing. **Djibrilla Amadou Kountche:** Formal analysis, Software, Writing – review & editing. **Daniel McCrum:** Supervision, Writing – review & editing. **Stefan Schauer:** Data curation, Formal analysis. **Sandra König:** Conceptualization, Data curation, Formal analysis, Visualization. **Shirley Delannoy:** Investigation, Project administration. **Lorcan Connolly:** Conceptualization, Formal analysis, Writing – review & editing. **Mircea Iacob:** Formal analysis, Software, Validation. **Nicola Gregorio Durante:** Formal analysis, Software, Validation. **Yash Shekhawat:** Software, Validation, Visualization. **Carlos Carrasco:** Formal analysis, Investigation, Validation. **Takis Katsoulakos:** Investigation, Resources. **Páraic Carroll:** Funding acquisition, Resources, Supervision, Writing – review & editing.

Acknowledgements

PRECINCT is funded by the European Commission , Horizon 2020 research and innovation programme under grant agreement No. 101021668.

References

[1] Puchol-Salort P, O'Keeffe J, van Reeuwijk M, Mijic A. An urban planning sustainability framework: systems approach to blue green urban design," *Sustain.* Cities Soc. 2021;66 102677. doi:10.1016/j.scs.2020.102677.
[2] Ince R, Marvin S. Constructing domestic retrofit as a new urban infrastructure: experimentation, equitability and contested priorities. Local Environ 2019;24(9):825–42. doi:10.1080/13549839.2019.1648401.
[3] Chowdhury N, Gkioulos V. Cyber security training for critical infrastructure protection : a literature review. Comput. Sci. Rev. 2021;40 100361. doi:10.1016/j.cosrev.2021.100361.
[4] Chaoqi F, Yangjun G, Jilong Z, Yun S, Pengtao Z, Tao W. Attack-defense game for critical infrastructure considering the cascade effect. Reliab. Eng. Syst. Saf. 2021;216 107958. doi:10.1016/j.ress.2021.107958.
[5] Yamin MM, Katt B, Nowostawski M. Serious games as a tool to model attack and defense scenarios for cyber-security exercises. Comput. Secur. 2021;110 102450. doi:10.1016/j.cose.2021.102450.
[6] van Riel W, Post J, Langeveld J, Herder P, Clemens F. A gaming approach to networked infrastructure management. Struct. Infrastruct. Eng. 2017;13(7):855–68. doi:10.1080/15732479.2016.1212902.
[7] Kumar N, Poonia V, Gupta BB, Goyal MK. A novel framework for risk assessment and resilience of critical infrastructure towards climate change. Technol. Forecast. Soc. Chang. 2021;165 120532. doi:10.1016/j.techfore.2020.120532.
[8] Deelstra A, Bristow DN. Assessing the effectiveness of disaster risk reduction strategies on the regional recovery of critical infrastructure systems. Resilient Cities Struct 2023;2(3):41–52. doi:10.1016/j.rcns.2023.05.001.
[9] Li Y, Qiao S, Deng Y, Wu J. Stackelberg game in critical infrastructures from a network science perspective. Physica A 2019;521:705–14. doi:10.1016/j.physa.2019.01.119.
[10] Nipa TJ, Kermanshachi S, Subramanya K. Development of innovative strategies to enhance the resilience of the critical infrastructure. In: Construction Research Congress. ASCE; 2022. p. 111–20.
[11] Song Y, Wu P. Earth observation for sustainable infrastructure : A review. Remote Sens 2021;13(1528):1–20.
[12] Ani UD, Watson JDMK, Nurse JRC, Cook A, Maple C. A review of critical infrastructure protection approaches: improving security through responsiveness to the dynamic modelling landscape. PETRAS/IET Conference Living in the Internet of Things: Cybersecurity of the IoT; 2019. doi:101049/cp20190131.
[13] Shirzad-Ghaleroudkhani N, Mei Q, Gul M. A crowdsensing-based platform for transportation infrastructure monitoring and management in smart cities. In: The Rise of Smart Cities. Butterworth-Heinemann; 2022. p. 609–24. doi:10.1016/B978-0-12-817784-6.00005-9.
[14] Gordan M, Sabbagh-Yazdi S-R, Ghaedi K, Thambiratnam DP, Ismail Z. Introduction to Optimized Monitoring of Bridge Infrastructure Using Soft Computing Techniques. Applied Methods in Bridge Design Optimization - Theory and Practice. London: IntechOpen Limited; 2022. doi:105772/intechopen104905.
[15] Gordan M. State-of-the-art review on advancements of data mining in structural health monitoring. Measurement 2022;193 110939. doi:10.1016/j.measurement.2022.110939.
[16] Miller T, Staves A, Maesschalck S, Sturdee M, Green B. Looking back to look forward: lessons learnt from cyber-attacks on Industrial Control Systems. Int. J. Crit. Infrastruct. Prot. 2021;35 100464. doi:10.1016/j.ijcip.2021.100464.
[17] Nguyen TN, Liu B-H, Nguyen P, Dumba B, Chou JT. Smart grid vulnerability and defense analysis under cascading failure attacks. IEEE Trans. Power Deliv. 2021;36(4):2264–73.
[18] Reis C, Lopes M, Baptista MA, Clain S. Towards an integrated framework for the risk assessment of coastal structures exposed to earthquake and tsunami hazards. Resilient Cities Struct. 2022;1(2):57–75. doi:10.1016/j.rcns.2022.07.001.
[19] Setola R, Luiijf E, Theocharidou M. Critical infrastructures, protection and resilience. In: Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach. Springer International Publishing; 2016. p. 1–18. [Online]Available.
[20] Tidwell VC, Lowry TS, Binning D, Graves J, Peplinski WJ, Mitchell R. Framework for shared drinking water risk assessment. Int. J. Crit. Infrastruct. Prot. 2019;24:37–47. doi:10.1016/j.ijcip.2018.10.007.
[21] Correa-Henao GJ, Yusta JM, Lacal-Arántegui R. Using interconnected risk maps to assess the threats faced by electricity infrastructures. Int. J. Crit. Infrastruct. Prot. 2013;6(3–4):197–216. doi:10.1016/j.ijcip.2013.10.002.
[22] Othman A, El-Saoud WA, Habeebullah T, Shaaban F, Abotalib AZ. Risk assessment of flash flood and soil erosion impacts on electrical infrastructures in overcrowded mountainous urban areas under climate change. Reliab. Eng. Syst. Saf. 2022;236:2023 109302. doi:10.1016/j.ress.2023.109302.
[23] Hughes L, de Jong M, Wang XQ. A generic method for analyzing the risks to energy systems. Appl. Energy 2016;180:895–908. doi:10.1016/j.apenergy.2016.07.133.
[24] Romero-Faz D, Camarero-Orive A. Risk assessment of critical infrastructures – New parameters for commercial ports. Int. J. Crit. Infrastruct. Prot. 2017;18:50–7. doi:10.1016/j.ijcip.2017.07.001.
[25] Urlainis A, Shohet IM, Levy R. Probabilistic risk assessment of oil and gas infrastructures for seismic extreme events. Procedia Eng 2015;123:590–8. doi:10.1016/j.proeng.2015.10.112.
[26] El-Maissi AM, Kassem MM, Nazri FMohamed. Resilient critical infrastructures: an innovative methodological perspective for critical infrastructure (CI) integrated assessment models by inducing digital technologies during multi-hazard incidents. MethodsX 2024;12 January102561. doi:10.1016/j.mex.2024.102561.
[27] Henriques J, Caldeira F, Cruz T, Simões P. A survey on forensics and compliance auditing for critical infrastructure protection. IEEE Access 2024;12:2409–44 January. doi:10.1109/ACCESS.2023.3348552.
[28] Yang Z. Indicator-based resilience assessment for critical infrastructures – A review. Saf. Sci. 2023;160 January. doi:10.1016/j.ssci.2022.106049.
[29] Brunner LG, Peer RAM, Zorn C, Paulik R, Logan TM. Understanding cascading risks through real-world interdependent urban infrastructure. Reliab. Eng. Syst. Saf. 2023;241:2024 June109653. doi:10.1016/j.ress.2023.109653.
[30] Xu M, Li G, Chen A. Resilience-driven post-disaster restoration of interdependent infrastructure systems under different decision-making environments. Reliab. Eng. Syst. Saf. 2023;241:2024 June109599. doi:10.1016/j.ress.2023.109599.
[31] Mayer IS. Digital Twins in the Real World. Tilburg University; 2022. doi:1026116/fv8m-fq41.
[32] Speiser K, Teizer J. An efficient approach for generating training environments in virtual reality using a digital twin for construction safety. Proc. CIBW099W123 Digit. Transform. Heal. Saf. Constr. 2023;21:481–90. [Online]Available https://books.fe.up.pt/index.php/feup/catalog/book/978-972-752-309-2 .
[33] Golovina O, Teizer J. Serious game in Virtual Reality for Safe, Active, and Personalized Learning related to Pedestrian Workers Struck By Equipment and other Construction Hazards. In: 22nd Conference on Construction Application of Virtual Reality (CONVR); 2022. p. 260–71.
[34] Leonardo M, Berardo N, Alessandro C, Luigi R, Giuseppe Martino DG. Development of a digital twin model for real-time assessment of collision hazards. Creative Construction e-Conference 2020:14–19 2020. doi:10.3311/ccc2020-003.
[35] Brucherseifer E, Winter H, Mentges A, Mühlhäuser M, Hellmann M. Digital Twin conceptual framework for improving critical infrastructure resilience. At-Automatisierungstechnik 2021;69(12):1062–80. doi:10.1515/auto-2021-0104.
[36] "SAURON: Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports." [Online]. Available: https://www.sauronproject.eu/
[37] "The STOP-IT Project." [Online]. Available: https://stop-it-project.eu/
[38] "DEFENDER." [Online]. Available: https://cordis.europa.eu/project/id/740898
[39] "SAFECARE: SAFEguard of Critical heAlth infrastructure." [Online]. Available: https://cordis.europa.eu/project/id/787002
[40] "RESISTO: RESIlience enhancement and risk control platform for communication infraSTructure Operators." [Online]. Available: https://www.resistoproject.eu/
[41] "InfraStress: Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats, by means of an open testbed stress-testing system." [Online]. Available: https://cordis.europa.eu/project/id/833088
[42] "SATIE: Security of Air Transport Infrastructure of Europe." [Online]. Available: https://satie-h2020.eu/
[43] "SAFETY4RAILS: Data-based analysis for SAFETY and security protection FOR detection, prevention, mitigation and response in trans-modal metro and RAILway networkS." [Online]. Available: https://safety4rails.eu/
[44] "IMPETUS: Intelligent Management of Processes, Ethics and Technology for Urban Safety." [Online]. Available: https://www.impetus-project.eu/

[45] "7SHIELD: Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats." [Online]. Available: https://www.7shield.eu/
[46] "ENSURESEC: End-to-end security of the digital single market's e-commerce and delivery service ecosystem." [Online]. Available: https://www.ensuresec.eu/
[47] PRECINCT, "Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats and effects with focus on district or regional protection." [Online]. Available: https://www.precinct.info/
[48] P. Carroll, D. McCrum, Y. Shekhawat, "Serious Gaming for Inredependent Critical Infrastructure (CI) Resilience Determination," U.S. Patent Application No. 17/736,943, 2023
[49] PRECINCT consortium, "Preparedness and resilience enforcement for critical infrastructure cascading cyberphysical threats and effects with focus on district or regional protection." [Online]. Available: https://www.precinct.info/en/publications/
[50] Gordan M. A serious game conceptual approach to protect critical infrastructure resilience in smart cities. *14th International Conference on Applications of Statistics and Probability in Civil Engineering, ICASP14*, Dublin, Ireland; 2023.
[51] Soroudi M, Gordan M, Ko I, Carrol P, McCrum D, Pilla F. A Sustainable GIS-based serious game approach to improve railways resilience. In: The Fifth International Conference on Railway Technology. Montpellier, France: Elseiver; 2022. p. 1–6. doi:10.4203/ccc.1.27.18.
[52] König S. Risk management with multi-categorical risk assessment. In: Advances in Modelling to Improve Network Resilience: Proceedings of the 60th European Safety, Reliability, & Data Association (ESReDA) Seminar. Grenoble, France: University Grenoble Alpes; 2022. p. 105–13. doi:10.2760/503700.
[53] Cassottana B, Balakrishnan S, Aydin NY, Sansavini G. Designing resilient and economically viable water distribution systems: a Multi-dimensional approach. Resilient Cities Struct 2023;2(3):19–29. doi:10.1016/j.rcns.2023.05.004.
[54] Malek K. Design and implementation of sustainable solar energy harvesting for low-cost remote sensors equipped with real-time monitoring systems. J. Infrastruct. Intell. Resil. 2023;2(3) 100051. doi:10.1016/j.iintel.2023.100051.
[55] Osei-kyei R, Tam V, Ma M, Mashiri F. Critical review of the threats affecting the building of critical infrastructure resilience. Int. J. Disaster Risk Reduct. 2021;60:102316. doi:10.1016/j.ijdrr.2021.102316.
[56] Mowll R, Becker J, Wotherspoon L, Stewart C, Johnston D, Neely D. Creating a 'planning emergency levels of service' framework – a silver bullet, or something useful for target practice? Resilient Cities Struct 2023;2(2):1–12. doi:10.1016/j.rcns.2023.05.002.
[57] Alcaraz C, Zeadally S. Critical infrastructure protection: requirements and challenges for the 21st century. Int. J. Crit. Infrastruct. Prot. 2015;8:53–66. doi:10.1016/j.ijcip.2014.12.002.
[58] König S, Rass S, Rainer B, Schauer S. Hybrid dependencies between cyber and physical systems. In: Intelligent Computing-Proceedings of the Computing Conference. Cham: Springer; 2019. p. 550–65. doi:10.1007/978-3-030-22868-2.
[59] PRECINCT, "Newsletter, April 2022, Issue #02," 2022.
[60] Ng ST, Wong JMW, Wong KKW. A public private people partnerships (P4) process framework for infrastructure development in Hong Kong. Cities 2013;31:370–81. doi:10.1016/j.cities.2012.12.002.
[61] European Commission, "Grant Agreement - PRECINCT," 2021.
[62] "Neo4j: The world's leading graph database." [Online]. Available: https://neo4j.com/
[63] Open-source stream processing platform, "Apache Kafka." [Online]. Available: https://kafka.apache.org/
[64] Complex event processing (CEP) platform, "EsperTech." [Online]. Available: https://www.espertech.com/esper/
[65] König S, Schauer S, Connor AO, Carroll P, McCrum D. Combining cascading effects simulation and resilience management for protecting cis from cyber-physical threats. In: Proceedings ofthe 32nd European Safety and ReliabilityConference (ESREL 2022; 2022. p. 2741–8. doi:10.3850/978-981-18-5183-4.
[66] König S, Shaaban AM. Parametrization of Probabilistic Risk Models. *17th International Conference on Availability, Reliability and Security*, Vienna, Austria; 2022.
[67] König S. D1.2 Critical Infrastructure Interdependencies and Cascading Effects Interdependency Graphs. PRECINCT 2022.
[68] Mentges A, Halekotte L, Schneider M, Demmer T, Lichte D. A resilience glossary shaped by context: reviewing resilience-related terms for critical infrastructures. Int. J. Disaster Risk Reduct. 2023;96:103893. doi:10.1016/j.ijdrr.2023.103893.
[69] Casciati F, Casciati S, Faravelli L. Resilience resilience and sustainability for educational buildings. J. Infrastruct. Intell. Resil. 2022;1(1):100005. doi:10.1016/j.iintel.2022.100005.
[70] Diaz-romero DJ, María A, Rincón R, Miguel-cruz A, Yee N, Stroulia E. Recognizing emotional states with wearables while playing a serious game. IEEE Trans. Instrum. Meas. 2021;70.
[71] Abt CC. Serious Games. University Press of America; 1987.
[72] Susi T, Johannesson M, Backlund P. Serious Games – an Overview. Sweden: University of Skövde; 2007.
[73] Zubković BR, Kolić-vehovec S, Smojver-ažić S, Dorčić TM, Pahljina-reinić R. The role of experience during playing bullying prevention serious game : effects on knowledge and compassion. Behav. Inf. Technol. 2022;41(2):401–15. doi:10.1080/0144929X.2020.1813332.
[74] Zyda M. From visual simulation to virtual reality to games. Computer (Long. Beach. Calif). 2005;38(9):25–32.
[75] Bianchi I. AnemiaAR : a serious game to support teaching of haematology. J. Vis. Commun. Med. 2022:1–20. doi:10.1080/17453054.2021.2021798.
[76] Yanes N, Bououd I, Alanazi SA, Ahmad F. Fuzzy logic based prospects identification system for foreign language learning through serious games. IEEE Access 2021:63173–87. doi:10.1109/ACCESS.2021.3074374.
[77] Bedwell WL, Pavlas D, Heyne K, Lazzara EH, Salas E. Toward a taxonomy linking game attributes to learning : an empirical study. Simul. Gaming 2012;43(6):729–60. doi:10.1177/1046878112439444.
[78] Wehrle R, Wiens M, Schultmann F. Application of collaborative serious gaming for the elicitation of expert knowledge and towards creating Situation Awareness in the field of infrastructure resilience. Int. J. Disaster Risk Reduct. 2021;67:102665 October2022. doi:10.1016/j.ijdrr.2021.102665.
[79] Ávila-pesántez D, Rivera LA, Alban MS. Approaches for serious game design: a systematic literature review. Comput. Educ. J. 2017;8(3).
[80] Behl A, Jayawardena N, Pereira V, Islam N, Del Giudice M, Choudrie J. Gamification and e-learning for young learners: a systematic literature review, bibliometric analysis, and future research agenda. Technol. Forecast. Soc. Change 2022;176:121445. doi:10.1016/j.techfore.2021.121445.
[81] Taxonomy "Bloom. In: Serious Games and Lean Learning: What Do These Topics Have in Common?," in *Learning in the Digital Era: 7th European Lean Educator Conference, ELEC 2021*. Trondheim, Norway: Springer International Publishing; 2021. p. 308–16.
[82] Zhonggen Y. A meta-analysis of use of serious games in education over a decade. Int. J. Comput. Games Technol. 2019;2019(3). doi:10.1155/2019/4797032.
[83] Armstrong MB, Landers RN. An evaluation of gamified training: using narrative to improve reactions and learning. Simul. Gaming 2017;48(4):513–38. doi:10.1177/1046878117703749.
[84] Hirdes EM, Thillainathan N, Leimeister JM. Towards Modeling Educational Objectives in Serious. In: *Proceedings of the 1st International Workshop on Pedagogically - driven Serious Games*, Saarbrücken, Germany; 2012.
[85] Liu C, Zhang P, Xu X. Literature review of digital twin technologies for civil infrastructure. J. Infrastruct. Intell. Resil. 2023;2(3):100050. doi:10.1016/j.iintel.2023.100050.
[86] Glaessgen EH, Stargel DS. The digital twin paradigm for future NASA and U . S . air force vehicles. In: The 53rd Structures, Structural Dynamics, and Materials Conference: Special Session on the Digital Twin; 2012. p. 1–14.
[87] Shafto M. Modeling, Simulation. *Information Technology & Processing Roadmap NACA*. National Aeronautics and Space Administration; 2012.
[88] TOSCA Verison 2.0, "OASIS OPEN." [Online]. Available: https://docs.oasis-open.org/tosca/TOSCA/v2.0/TOSCA-v2.0.html
[89] Web-based hub for version control using Git, "GitHub." [Online]. Available: gitHub - xlab-si/xopera-opera: xOpera orchestrator compliant with TOSCA YAML v1.3 in the making
[90] Klemas V. Remote sensing of floods and flood-prone areas: an overview. J. Coast. Res. 2015;31(4):1005–13.
[91] Deng L, Wang W, Yu Y. State-of-the-art review on the causes and mechanisms of bridge collapse. J. Perform. Constr. Facil. 2016;30(2):04015005. doi:10.1061/(asce)cf.1943-5509.0000731.