Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-5183-4_S20-03-343-cd

Combining Cascading Effects Simulation and Resilience Management for Protecting CIs from Cyber-Physical Threats

Sandra König

Center for Digital Safety and Security, AIT Austrian Institute of Technology, Austria. sandra.koenig@ait.ac.at

Lorcan Connolly

Research Driven Solutions Ltd., Ireland. lorcan.connolly@researchdrivensolutions.ie

Stefan Schauer

Center for Digital Safety and Security, AIT Austrian Institute of Technology, Austria. stefan.schauer@ait.ac.at

Alan O'Connor

Research Driven Solutions Ltd., Ireland. alan.oconnor@researchdrivensolutions.ie

Páraic Carroll and Daniel McCrum

School of Civil Engineering, University College Dublin, Ireland, {paraic.carroll, daniel.mccrum}@ucd.ie

This article investigates a way to develop a cascading effects simulation tool for a network of interdependent critical infrastructures that explicitly incorporates resilience aspects. To that end, an existing simulation tool for cascading effects, that builds on a graph representation of the network of critical infrastructures, is extended based on a resilience methodological framework in such a way that the resilience indicators directly influence the local behaviour of the components of the network and therefore the reaction of the entire network to an incident. This refined simulation model provides feedback on the effectiveness of the resilience indicators and at the same time provides input for the design of serious games. These games let players interact with the system to better understand the consequences of their actions, but also provides valuable information on the user's reactions to threats. This can in turn be used to identify ways to protect an infrastructure system against cyber physical threats.

Keywords: Cascading effects, resilience framework, serious games, critical infrastructures, cyber-physical threats

1. Introduction

Understanding the manifold direct and indirect effects of a hazard such as a flooding does not only require knowledge about the threat itself, but also about the environment. An incident may influence the operational behaviour of infrastructures (CIs), for example, reducing their availability. In urban areas CIs are strongly interconnected, limited operation of one CI is likely to affect other CIs. Therefore, an in-depth analysis of threats requires modelling of the exposed CIs as well as their interdependencies.

In the current work, a graph model is employed to describe CI networks. Once the reaction of each component is known, the dependency model allows simulation of cascading effects of an incident. Many factors influence the local reaction of a CI to a threat, one of the most crucial is its resilience. This paper investigates the combination of a cascading effect simulation with a Resilience Methodological Framework (RMF) to obtain a comprehensive understanding of how a system of CIs reacts to threats, depending on the resilience of the components.

The relation between resilience and cascading effects has been recognised in many areas. The resilience of power systems to extreme temperature is analysed based on a cascading failure model in (Khazeiynasab and Qi 2021), and a robustness and a resilience model for power systems after cascading failures are presented in (Beyza and Yusta 2021). Monte Carlo simulations of cascading failures in power networks can be used to train a Machine Learning approach for preventive actions to improve resilience (Noebels, Preece, and Panteli 2022). Recent models for cascading failures also form the basis for resilience assessment and optimization research of Cyber-Physical Power Systems (Wu and Li 2021). Resilience is also considered in simulation of cascading failures (Hu, Li, and Zheng 2021)b. However, a general simulation framework of cascading failures that explicitly incorporates detailed information about resilience is currently unavailable in the literature. This extended simulation framework provides information about the impact of threats for different resilience setups, and therefore enables refinement of the RMF. Further, the simulation may be used to identify additional ways to protect the system besides removing nodes or edges using topological features (Kumar et al. 2022). The simulation results allow identification of vulnerable components, i.e., components that are affected most frequently or most seriously, or have the most significant impact on service. More advanced protection strategies may be identified using serious games.

The paper is organized as follows. Section 2 presents existing approaches cascading effects modelling and resilience, while Section 3 shows how these two methods can benefit from one another. Section 4 shows a combined approach that may help protection of the system using serious games. All steps are illustrated through an example from the RECINCT project. Section 5 shows the direction of future work.

2. Interdependent Modelling of Cascading Effects and Resilience Management

This section describes an approach to modelling cascading effects and an approach to measure resilience. The two will be combined in Section 3 to obtain a more comprehensive understanding on the consequences of cyber-physical threats on a network of CIs.

2.1. Cascading Effects Simulation

The Cascading Effects Simulation (CES) builds on an *interdependency graph* where nodes represent CIs (or relevant parts of CIs) and edges represent dependencies, such as exchange of resources or providing services, e.g., a hospital needs electricity and water for operation, but also depends on the transportation system for staff and medication. In recent years, digitalization induced further dependencies, e.g., through the application of electronic control systems for physical processes. Since the graph is the basis for the simulation of cascading effects, edges are directed in the sense that an edge from X to Y means that a problem in X may affect Y, i.e., it propagates. Figure1 shows an example of an interdependency graph for a city with a focus on transportation, water supply, energy supply, and rescue services in a city, drawn with the Sauron tool (AIT 2021).

During PRECINCT, the most relevant threat for this city is a flooding. This directly affects the transportation network and particularly a tunnel at the city centre. Due to the geographic proximity of CIs, it is also possible that the flooding affects the power network or the sewer system (i.e., both physical and cyber parts).

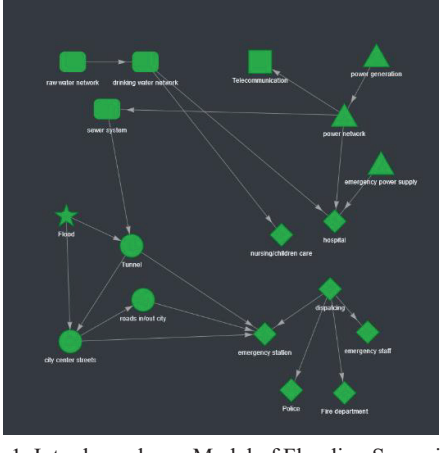

Fig. 1. Interdependency Model of Flooding Scenario

For a more detailed analysis, refinements of this high-level model are needed, especially more information on the component level is required. To this end, nodes have an 'inner model' describing their local behaviour. The form of this inner model depends on the problem at hand. For the analysis of consequences of an incident, a Mealy automata model proves to be useful as it

reacts to triggers (König et al. 2019). The states of the automata correspond to the 'health' of the component. This state can be interpreted as functionality level or availability of a service, depending on the components function. The states are described on a 5-tier scale, where 1 describes the best situation and 5 the worst (intermediate numbers represent intermediate limitations). Since consequences of rare events in complex environments are challenging to predict precisely, we use a probabilistic model to describe the local dynamics. Let $P_{n,t}$ denote the matrix of transition probabilities between states for node n and threat t. The i-th row of $P_{n,t}$ shows the distribution over the next state when the current state is i. In large networks it makes sense to categorize nodes and assign transitions to the group rather than to individual nodes.

When a node changes its state, it notifies its neighbours by sending an output. This output may be the same as the trigger, e.g., in case of a fire, but it may also be different. In the context of the flooding example, consider the component 'Tunnel' in the dependency graph shown in Figure 1. If it is hit by a flooding, the resulting output is that streets are blocked. How strongly the streets are affected also depends on the current condition of the node. If everything worked fine before the flooding (state 1), we assume a 50% chance that roads cannot be used at all (new sates is 5), a 30% chance that there is a strong affection, but still some operation is possible (state 4), and a 20% chance that limitation is average (state 3). If there are already some problems (the node is in state 3, 4, or 5 before the flooding), the new state will be 5 for sure. The table representation of this dynamics in the Sauron tool is shown in Figure 2.

Trigger	From	Go To	Output	%
flood	1	5	blocked	50%
flood	1	4	blocked	30%
flood	1	3	blocked	20%
flood	2	5	blocked	60%
flood	2	4	blocked	40%
flood	3	5	blocked	100%
flood	4	5	blocked	100%

Fig. 2. Local dynamic of node 'Tunnel'

2.2. Resilience Methodological Framework

The PRECINCT Resilience Methodological Framework (RMF) is outlined in Figure 3.

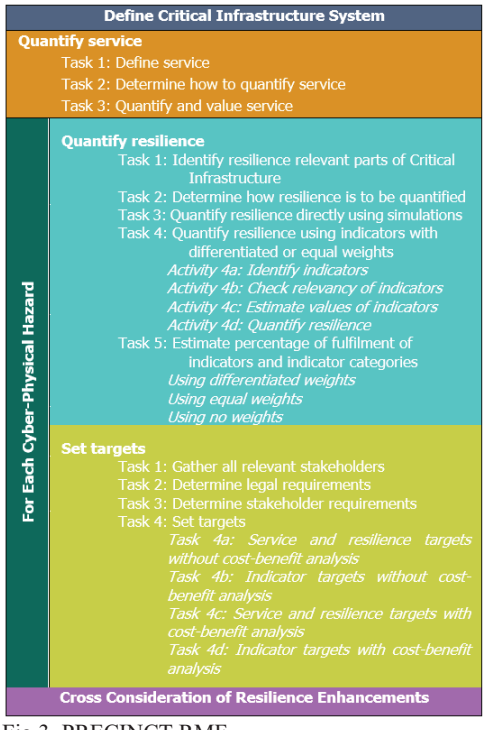

Fig 3. PRECINCT RMF

It is based on the CWA 17819 framework used for transportation infrastructures (Committée Européen De Normalisation 2021). Each step of the process is described in the following.

2.2.1. Define Critical Infrastructure System

The first step in the process is the definition of the CI system being assessed. Organisations responsible for the resilience of the CI and the people served also contribute to the resilience of the CI and, as such, should be considered as part of the CI system. This may include police departments, first responders, emergency services, fire departments etc. The various parts of the infrastructure should be categorised according to Infrastructure, Environment and Organisation

Infrastructure describes the physical assets and cyber systems required to provide service. Examples include bridges and road sections forming part of a transport network, central control rooms forming part of a motorway Intelligent Transport System (ITS). The Environment consists of the physical environment in which the infrastructure is embedded that might affect the provision of service as well as the organisational environment in which the

infrastructure management organisation is subject to. Items to be considered include the occurrence of floods or likelihood of deliberate physical attacks to infrastructure elements, as well as the regulations/codes impacting the infrastructure. The Organisation category covers the organisation(s) responsible for ensuring that the infrastructure provides service, as well as responders responsible for resilience. Indicators in this category include emergency plans, maintenance activities etc.

The Definition step should describe all resilience-relevant aspects of the CI, including contextual information. It should also define the hazards of interest to the multimodal system of CIs. Interdependencies between events should be considered where relevant. For example, an urban tram system with sufficient flood defences may not be impacted by a 1 in 100-year flood event. However, the power network supplying electrification to trams may potentially be at risk of shutdown.

2.2.2. Quantify Service

In PRECINCT, Resilience is benchmarked against the service provided by the system being assessed. This may include time spent travelling, safety of users etc. The various steps in measuring the service within the PRECINT RMF are as follows:

1. Define the service that the CI system provides.
2. Determine how the service is to be quantified.
3. Quantify and value service.

The definition of the service provided by a CI requires consideration of the most basic reason for the system being in place. The service definition should ideally be obtained through discussion with the CI stakeholders. A sample definition of service for a fibre broadband network may be described as follows; the primary reason for the CI is to provide uninterrupted 50MB internet services. The primary measure of service in this case may be the length of time for which connection remains stable throughout the year. This may be further assigned a cost for simplicity.

Next, the user must determine how to quantify the service. This requires a decision on whether service will be quantified using simulations or indicators. Should indicators be used, the assessor must also decide what indicators best model the service in question and determine how data for the indicators will be obtained. Measures of service should also include intervention costs.

The final step is the calculation / valuing of the service itself, either by way of simulations or indicators. In either case the outcome is a numeric estimation of the service provided by the CI each year. An example may include a telecom system which is expected to deliver broadband to 100 users for 364 days in a year. The service provided is then equal to 36,400 user days. To allow comparison and equal consideration of intervention costs and different measures of service across different CI types, the units used to quantify service should be expressed in monetary values wherever possible. The estimation of the values should, as far as possible, be related to published values, or collected using one or more valuation techniques, such as hedonic pricing.

2.2.3. Quantify Resilience

For the PRECINCT project, resilience is quantified in terms of relative reductions in the provision of each CI service during (and after) a disruptive event. The tasks involved to quantify resilience are as follows, for each hazard:

1. Identify resilience relevant parts of the CI.
2. Determine how resilience is to be quantified.
3. Quantify resilience directly using simulations.
4. Quantify resilience using indicators with differentiated or equal weights.
5. Estimate percentage of fulfilment of indicators. (optional)

The resilient relevant parts of the CI should be identified according to the global division listed for the parts of each CI assessed. This step allows consideration of the areas which impact on the service in general when carrying out the resilience analysis.

The assessor decides whether to directly quantify the reductions in level of service and the increased intervention costs due to a disruptive event, or to indirectly quantify these properties using indicators. Direct quantification of resilience is the most time-consuming method which requires significant expertise, resources and data availability. If insufficient time, data or expertise is available, indicators may be used instead. Indicators may be summarised in terms of weights, depending on the accuracy required, time and resources available. Where there are numerous complex interactions between different CIs, it is recommended to use indicators. On this basis, the simulation method will not be discussed further in this paper.

Indicators are parts of the CI system that give an indication of the difference between the service provided, and the intervention costs. While some indicators may manifest in a similar fashion across multiple CIs and hazards, a separate list of indicators should be produced when analysing each hazard individually, as the weight assigned to each indicator may change depending on the hazard analysed. The steps involved in measuring resilience using indicators are as follows:

a) Identify indicators
b) Check relevancy of indicators
c) Estimate values of the indicators
d) Quantify resilience using weights.

An example of an indicator under the "Infrastructure" part of the CI would include the condition state of the infrastructure.

Indicators must be checked for relevance to the system to ensure it is worthwhile to include them, and also to investigate if they provide a sufficient overview of the CI. This should be done by investigating how indicators change the measures of service being investigated and the intervention costs following the disruptive event. The next step involves the selection of the indicator score for each indicator. 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. The process for assigning monetary values to each indicator can be done assuming equal weights or assuming differentiated weights. For differentiated weights, the relative impact of each indicator on resilience must be estimated. This is achieved as follows, for each indicator:

i. Set all indicators to their best values and estimate the reduction in service and additional intervention costs, if the disruptive event occurs.
ii. Set all indicators to their best values except one and set that indicator to its worst value, and then estimate the reduction in service and additional intervention costs, if the disruptive event occurs.
iii. Assuming a relationship between the worst and best values for each indicator and using the actual values of the indicators, quantify the resilience in terms of expected total costs.

The weight of the indicator is then given by the difference between the value of reduction in service and intervention costs if the indicator has its worst value and the value of the reduction in service and intervention costs if the indicator has its best value. This essentially provides a monetary value for the minimum and maximum score for each indicator, allowing a monetary value to be allocated to the actual score.

2.2.4. Set Targets

The setting of targets for resilience is very useful to ensure the goals of the CI organisation are achieved, and to allow the framework to inherently consider codified norms which the bound the problem. The steps involved in setting targets are as follows, for each CI and each hazard:

1. Gather all relevant stakeholders.
2. Determine legal requirements.
3. Determine stakeholder requirements.
4. Set targets.

The first step is the gathering of relevant stakeholders. As for earlier steps, this should include anyone affected by any of the CI modes. Subsequently, relevant legal requirements should be identified in consultation with relevant stakeholders. Examples of legal requirements on indicators include minimum condition states an infrastructure asset must achieve, minimum assessment load, etc. These targets will quickly highlight areas where resilience enhancements must be put in place. Finally, targets are set either against measures of service / resilience, or against indicators. Additionally, for each of these cases, targets can be set either with or without Cost Benefit Analysis (CBA). The process is based on incrementally calculating the benefit / cost ratio of raising each indicator by 1 level. The indicator target is then selected as the one which maximises the benefit cost ratio while satisfying all legal and stakeholder requirements.

2.2.5. Cross Consideration of Resilience Enhancements

The final step in the RMF involves the consideration and putting in place of resilience enhancements to the CI system, considering the resilience quantification and targets. This step can be carried out either individually for each hazard or alternatively a cross consideration can be performed over multiple hazards. The cross

consideration of resilience requires the likelihood of the hazards to be quantified. The determination of the likelihood of hazard events is outside the scope of this methodology.

Once the likelihoods of each threat have been determined, the resilience of the entire system may be weighted according to the likelihood of each event. The delineation of appropriate resilience enhancements can then be performed by examining the statistical representation of resilience across all indicators.

3. Combining Cascading Effects Simulation and Resilience Framework

CES and RFM tackle important problems in CI networks, that are strongly related. It is therefore worth investigating how to combine the two approaches to develop a simulation framework that incorporates resilience.

3.1. Extension of Simulation

The resilience of a component influences its local reaction to a threat. In the case where resilience is measured through an indicator with values in a finite set of small size, the information can be incorporated into the CES by letting the transition matrices depend on it, e.g., use a set of transition matrices $P_{n,t,r}$ that depend on $r \in R$, where R is the set of all possible values of the resilience index. The implementation of this idea could look as follows. Indicators are built into the interdependency graph as *resilience indicator node* having a few potential states representing the indicator score. The indicator score can be set by the user (with a probability of 1.0). The state of each indicator will impact the various state probabilities within the infrastructure nodes in the graph.

For the considered example, we extended the dependency graph (Figure 1) by adding the nodes indicator tunnel (influencing the tunnel), availability of resources (affecting the emergency station), and a failure warning system (affecting the power network), as shown in Figure 4.

The values of all the resilience indicator nodes are set through an artificial node 'resilience setup'. This allows to run the CES for different indicator values and therefore provides information on which combinations reduce the impact of an incident.

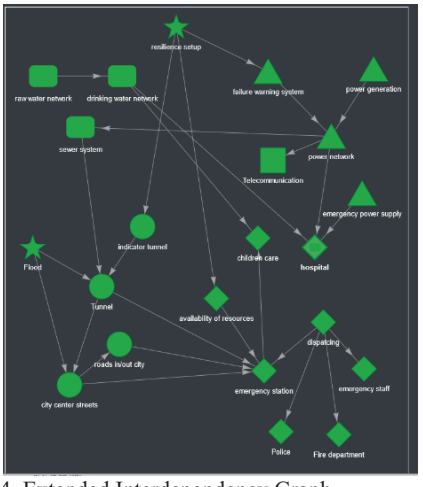

Fig. 4. Extended Interdependency Graph

Implementation of this extended simulation framework will be done in the PRECINCT project. The main change is that the transition matrix in each node is replaced by a set of matrices (one for each value of the resilience indicators) and the simulation return a pair of state and resilience index (s, r). This new approach increases the number of parameters but provides more information on the cascading effects for different resilience settings.

3.2. Extension of Resilience Framework

The Cascading Effects Simulation is an integral part of the Resilience Methodological Framework. In the first instance, interdependency graphs for the CI provide the context for the problem. Subsequently, when quantifying the baseline service, the interdependencies in services are quantified. The interdependency graphs can be appraised semi-quantitatively to assist in this process, evaluating the relative impact one service has on the running of another. This assists in deciding which measures of service should be quantified to measure resilience, and which ones can be excluded from this quantification since they are already having a significant impact on the overall service provided by the precinct. An example may include an electricity network which impacts the urban transport as well as hospitals and emergency services ability to assist the public in the event of a cyber-physical hazard. Should a measure of service already be

quantified for the transport network, hospital, and emergency services, it is advisable to not include an additional measure of service for the electricity network should this already have a significant indirect impact on the other measures of service. At this stage the interdependency graph is used to quantify the relative impact (weight) of each indicator on the overall measure of service.

To evaluate the resilience to a specific trigger event, the procedure in listed section 2.2.3 would be initiated by setting all indicator nodes to the best value and reading the outcome probabilities of being in each state for each infrastructure node. There will be a certain level of monetary loss associated with each state beyond state 1, associated with a loss in service for that infrastructure node. The total loss associated with the event is evaluated by multiplying the associated outcome probabilities by the associated monetary losses and summing for all measures of service included in the assessment. The losses associated with repair would also be summed. Subsequently, indicator 1 would be set to a value of state 1 and the state probabilities will again be read and multiplied by the associated monetary losses. This produces the relative weight of indicator 1 and each subsequent indicator analysed.

The final step involves the setting of resilience targets based on stakeholder issues, legal requirements, and CBA. All indicators are set to their actual values. The resulting state probabilities are read, and the resilience calculated in terms of the service losses for each measure of service. This is carried out for each indicator to populate the CBA requirements. Figure 5 illustrates the relations between CES and RMF.

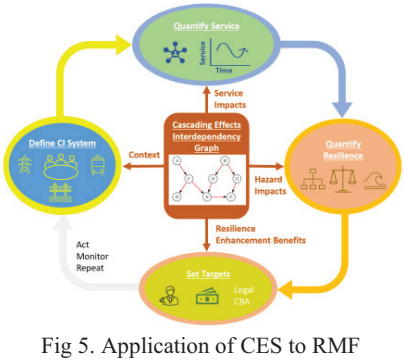

Fig 5. Application of CES to RMF

4. Evaluation of Models using Serious Games

A serious game is a game that is designed for a primary purpose other than pure entertainment. Serious Games are primarily used for training purposes as a form of experiential learning that employ simulation techniques as a cost-effective alternative to often high risk and costly real-life activities. Many examples existing using serious games for training. The global market growth of serious games is expected to reach $9167 million in 2023 (Allied Market Research 2022). Serious games typically have three main aims; (1) help players deduce optimal strategies while dealing with budgetary, temporal regulatory, technical constraints, and conflicting interests; (2) enable players to assume realistic roles, tackle issues, make decisions, and get quick feedback on their actions, and (3) support the game's evolution over time and balance the seriousness and entertainment (Yusoff 2010). The challenges of developing serious games are capturing the complexity, long-term uncertainties and balancing the seriousness with interest/entertainment. Research has shown that three significant factors influence the usefulness of serious games: transfer of skills, learner control, and ease of use (Merabti, Kennedy, and Hurst 2011).

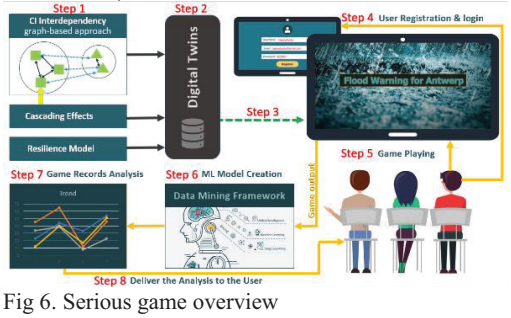

Fig 6. Serious game overview

Figure 6 shows that the interdependencies, cascading effects simulation and resilience scores provide input to serious game via a digital twin, which will store the outputs of the modelling before being passed to the serious game. Such inputs ensure that the complexity of the interdependencies and cascading effects between critical infrastructures is captured. Resilience is a key metric that is used in the serious game to help game players (e.g., CI operators, emergency responders, etc) interpret complex information in more intuitive and understandable formats (i.e., in

geographical format in the serious game). The serious game players are trusted members of CIs, emergency responders, governmental official etc, within the urban region being considered. Importantly, the empirical results of the game play records will provide important experiential learning in terms of operational strategies and cost/benefit analysis of decisions made to enhance the resilience of their CI systems (e.g. deploying sandbags during a flooding event). The gaming records will be data mined to identify trends in attack and defence scenarios and will auto-generate periodic reports of trends identified. Furthermore, the outputs of the game will be analysed via the RMF, to quantify the system resilience during and after the game is played. Such empirical results will also be fed back to interdependency and cascading effects modelling to improve the simulation and validate it by comparing the model results with independent data not used in calibration process, which will be done iteratively as each user will have the opportunity to play the serious game multiple times.

5. Conclusion and Future Work

Through the combination of a simulation tool for cascading effects and a resilience framework we develop a model that incorporates resilience indicators directly into the simulation of the consequences of an incident in a CI network. This refined simulation provides feedback about the impact of different resilience settings.

Future work focuses on two aspects: the implementation of the new model and the design of serious games based on the model. The latter is especially useful since it enables training and at the same time collects data on user behaviour.

Acknowledgement

The PRECINCT project has received funding from the European Union's HORIZON 2020 research and innovation program under Grant Agreement No 101021668.

References

AIT. 2021. 'SAURON Propagation Engine Editor'. 2021. https://atlas.ait.ac.at/sauron/#/.

Allied Market Research. 2022. 'Serious Games Market'. *Allied Market Research* (blog). February 2022.

Beyza, Jesus, and Jose M. Yusta. 2021. 'Integrated Risk Assessment for Robustness Evaluation and Resilience Optimisation of Power Systems after Cascading Failures'. *Energies* 14 (7): 2028.

Committée Européen De Normalisation. 2021. 'CWA 17819, Guidelines for the Assessment of Resilience of Transport Infrastructure to Potentially Disruptive Events'.

Hu, Yashan, Yan Li, and Jiaqi Zheng. 2021. 'Resilience-Constrained Economic Dispatch for Cascading Failures Prevention'. In *2021 IEEE Sustainable Power and Energy Conference (ISPEC)*, 1692–97. Nanjing, China: IEEE.

Khazeiynasab, Seyyed Rashid, and Junjian Qi. 2021. 'Resilience Analysis and Cascading Failure Modeling of Power Systems Under Extreme Temperatures'. *Journal of Modern Power Systems and Clean Energy* 9 (6): 1446–57.

König, Sandra, Stefan Rass, Benjamin Rainer, and Stefan Schauer. 2019. 'Hybrid Dependencies Between Cyber and Physical Systems'. In *Intelligent Computing*, 998:550–65. Cham: Springer.

Kumar, Shriram Ashok, Maliha Tasnim, Zohvin Singh Basnyat, Faezeh Karimi, and Kaveh Khalilpour. 2022. 'Resilience Analysis of Australian Electricity and Gas Transmission Networks'. *Sustainability* 14 (6): 3273.

Merabti, Madjid, Michael Kennedy, and William Hurst. 2011. 'Critical Infrastructure Protection: A 21st Century Challenge'. In *2011 International Conference on Communications and Information Technology*, 1–6. Aqaba, Jordan: IEEE.

Noebels, Matthias, Robin Preece, and Mathaios Panteli. 2022. 'A Machine Learning Approach for Real-time Selection of Preventive Actions Improving Power Network Resilience'. *IET Generation, Transmission & Distribution* 16 (1): 181–92.

Wu, Gongyu, and Zhaojun S. Li. 2021. 'Cyber—Physical Power System (CPPS): A Review on Measures and Optimization Methods of System Resilience'. *Frontiers of Engineering Management* 8 (4): 503–18.

Yusoff, Amri. 2010. 'A Conceptual Framework for Serious Games and Its Validation'. University of Southampton.