DOI: 10.1111/mice.12999

RESEARCH ARTICLE

COMPUTER-AIDED CIVIL AND INFRASTRUCTURE ENGINEERING WILEY

A simulation-based generalized framework to model vulnerability of interdependent critical infrastructure systems under incomplete information

Prasangsha Ganguly | **Sayanti Mukherjee**

Department of Industrial and Systems Engineering, University at Buffalo, The State University of New York (SUNY), Buffalo, NY, USA

Correspondence
Sayanti Mukherjee, Department of Industrial and Systems Engineering, 411 Bell Hall, University at Buffalo (SUNY), Buffalo NY 14260, USA.
Email: sayantim@buffalo.edu

Funding information
National Science Foundation, Grant/Award Number: Award#2308524; Center for Geohazards Study, University at Buffalo (SUNY)

Abstract

This paper proposes a novel simulation-based hybrid approach coupled with time-dependent Bayesian network analysis to model multi-infrastructure vulnerability over time under physical, spatial, and informational uncertainties while considering cascading failures within and across infrastructure networks. Unlike existing studies that unrealistically assume that infrastructure managers have full knowledge of all the infrastructure systems, the proposed approach considers a realistic scenario where complete information about the infrastructure network topology or the supply–demand flow characteristics is not available while estimating multi-infrastructure vulnerability. A novel heuristic algorithm is proposed to construct a dynamic fault tree to abstract the network topology of any infrastructure. In addition, to account for the unavailability of exact supply–demand flow characteristics, the proposed approach constructs the interdependence links across infrastructure network systems using different simulated parameters considering the physical, logical, and geographical dependencies. Finally, using parameters for geographical proximity, infrastructure managers' risk perception, and the relative importance of one infrastructure on another, the multi-infrastructure vulnerability over time is estimated. Results from the numerical experiment show that for an opportunistic risk perception, the interdependencies attribute to redundancies, and with an increase in redundancy, the vulnerability decreases. On the other hand, from a conservative risk perspective, the interdependencies attribute to deficiencies/liabilities, and the vulnerability increases with an increase in the number of such interdependencies.

1 | INTRODUCTION

Modern society is critically dependent on lifeline infrastructure systems such as the electric power, telecommunication, water, transportation, and others. In recent years, the construction and operation of such interdependent infrastructure system in a sustainable way are becoming integral for assuring the overall sustainability of the society (Zavadskas et al., 2018). Most of these infrastructure systems comprise multiple components interconnected by physical, logical, geographical, or cyber interdependencies, rendering them suitable to be modeled as a network of networks or "system-of-systems" as described by Eusgeld et al. (2011). To enhance the resilience of a community, analyzing multiple infrastructure systems' vulnerability in conjunction while considering the interdependencies between them is of paramount importance (Mahmoud & Chulahwat, 2018).

In a network-of-network system, failure of a key component may lead to a cascading failure of the entire system, which is not desirable (Dong et al., 2020; Faturechi & Miller-Hooks, 2014). In literature, modeling the reliability of an infrastructure is well studied (O'Connor & Kleyner, 2012). One of the most popular methods used to model system reliability is the fault tree (FT) method (Dugan et al., 1992). In a FT analysis, a top event (failure of the whole system) is represented as a Boolean combination (AND, OR, NOT) of the basic events (e.g., failure of some switch(s), substation(s), transformer(s)). In this method, at first, the failure probabilities are assigned to the basic events and then the failure probability of the top event is calculated through Boolean modeling and calculations of probabilities (Watson, 1961). The main *advantage* of such deterministic models is that they are easily interpretable and encourage a procedural way of modeling the dependencies of components in an infrastructure. However, the main *disadvantage* is that being static models, they cannot capture the dynamics of failure propagation with time. Several research studies have extended the static FTs into dynamic fault trees (DFTs) that use different advanced gates (e.g., the spare gates, priority gates) to capture the temporal dynamics of the failure propagation (Dugan et al., 1992). Time-dependent Bayesian networks (BNs) such as the discrete-time Bayesian networks, the continuous time Bayesian networks (CTBNs), and the dynamic Bayesian networks (DBNs) have been used to model the DFT in the literature (Codetta-Raiteri & Portinale, 2015). However, the methods for developing a FT or DFT are not generalized enough to be applied to different infrastructure systems. Even for a single infrastructure system like electricity infrastructure, different FTs are proposed based on the components or events considered, such as the failure of generators, switches, and substations (Volkanovski et al., 2009) or the disruption of distribution generators and output flow paths (Song et al., 2014). Nonetheless, a generalized approach to construct a DFT would be particularly useful for infrastructure managers. Moreover, the exact DFT of one infrastructure may not be available to the other infrastructure managers. In this case, for understanding the vulnerability of interdependent infrastructure systems, a heuristic algorithm to construct an approximate DFT of the other interdependent infrastructures can be useful for the infrastructure managers. Hence, to address this research gap, a procedural approach to construct an approximate DFT, which can be applied to multiple infrastructure systems in the absence of exact information, is proposed in this paper.

Since the infrastructure systems are interdependent, analyzing a single infrastructure system is not ideal as it underestimates the risk of failure. Hence, recently several studies have focused on modeling the vulnerability and reliability of multiple interdependent infrastructure systems in conjunction (Galbusera et al., 2018; Lu et al., 2018) and accordingly optimize the recovery process of interdependent infrastructure system (Sharma et al., 2020). Rinaldi et al. classified infrastructure interdependencies into four categories: (1) *physical interdependency*, which emerges from physical linkages or connections among elements of the infrastructures; (2) *cyber interdependency*, when the state of one infrastructure depends on information/data transmitted from/through another infrastructure; (3) *geographical interdependency*, if there exists close spatial proximity between elements of different infrastructures; and (4) *logical interdependency*, when the state of one infrastructure depends on the state of others via mechanisms that are not captured by the physical, cyber, or geographic connections (Rinaldi et al., 2002). Although there exist distinct characteristics for each of these interdependencies, they are not mutually exclusive as mentioned by Rinaldi et al. (2002). Different other types of interdependencies such as functional interdependency have also been studied in the literature (Wallace et al., 2003; Zhang & Peeta, 2011). Furthermore, several interdependencies may arise while considering the repair process of an infrastructure (Xiong et al., 2020). Nocera et al. considered that the interdependencies between different infrastructures can exist at the interfaces, or the boundaries where the different infrastructure networks interact with one another (Nocera & Gardoni, 2022). Ouyang provided a thorough survey of the literature focusing on the interdependent infrastructure systems modeling (Ouyang, 2014). Previous studies also established that for accurate estimation of overall system performance, the connections between different networks need to be considered by analyzing the overall system and individual network performance (Hernandez-Fajardo & Dueñas-Osorio, 2013; Krishnamurthy et al., 2016). Yagan et al. identified that the robustness of an interconnected system is dependent on the bidirectional interdependencies existing between the networks of the system (Yagan et al., 2012).

As depicted by Zio and Sansavini (2011), according to the methodology of modeling the critical infrastructure systems, the existing literature can be broadly classified into six categories: (1) *aggregate supply–demand methodology*, which considers the supply–demand relationships by evaluating the total required demand for infrastructure services in a region, and the ability to satisfy that demand by the infrastructure system (Adachi & Ellingwood, 2008; Apostolakis & Lemon, 2005); (2) *dynamic simulations*, which employ simulation techniques like discrete event simulation or system dynamics techniques (Dueñas-Osorio et al., 2007); (3) *agent-based models*, which consider the physical components of an infrastructure to be modeled as agents and allow them to interact for the analysis of the operational characteristics and physical states of infrastructures (Casalicchio et al., 2007; Nan & Sansavini, 2017); (4) *physics-based models*, which consider the physical aspects of infrastructure using standard engineering techniques (Yang et al., 2020); (5) *population mobility models*, which capture the movement of entities through geographical regions considering a very high resolution of modeling approach (Casalicchio et al., 2009); (6) *Leontief input–output models*, which consider the economic flows among infrastructure sectors to provide a linear, aggregated, time-independent analysis of the generation, flow, and consumption of various commodities in the various sectors (Haimes & Jiang, 2001).

Along with the above-mentioned methods for modeling the infrastructure interdependencies, several other modeling techniques like economic inoperability input–output model (IIM) (Barker & Haimes, 2009a) and the dynamic inoperability input–output model (DIIM) (Barker & Haimes, 2009b) have been used in the literature to capture the inoperability that propagates through interdependent infrastructure systems in a quantitative manner. Duenas-Osorio et al. analyzed the performance of interdependent infrastructure systems for different network topologies exposed to external or internal disruptions (Dueñas-Osorio et al., 2007). Utne et al. developed a simplified cascade diagram–based model for risk estimation of an interdependent infrastructure system. However, their model does not account for the within-infrastructure failure propagation (Utne et al., 2011). Aghababaei et al. considered the interaction and dynamics between several systems like schools, households, businesses, healthcare, and lifeline infrastructures (e.g., water supply network and electric power network) within a community using an agent-based model (Aghababaei & Koliou, 2022). A spatial network model has been proposed by Fu et al. to simulate the growth and evolution of interdependent critical infrastructure systems like electricity transmission and distribution system, gas infrastructure, and transportation infrastructure systems (Fu et al., 2016).

A considerable fraction of literature that aims to model the interconnected infrastructure systems uses the supply–demand modeling approaches by explicitly identifying the interconnections or interdependencies between different infrastructure systems (Cavallaro et al., 2014; Cavdaroglu et al., 2013). For example, Lee et al. proposed a detailed mathematical programming formulation for a network flow–based model that explicitly incorporates the interdependencies among a set of civil infrastructure systems. However, this model requires a large set of parameters to be known in advance for the model to run (Lee II et al., 2007). Mixed integer linear programs (MILPs) (Ouyang & Fang, 2017), multistage optimization models (Fang & Zio, 2019), and other optimization techniques (Alinizzi et al., 2018) have been widely used in the literature for modeling a resilient system of interdependent infrastructure systems. Chen et al. proposed an MILP model for optimal mitigation and restoration strategies of interdependent infrastructure networks considering time-dependent strategies (Chen et al., 2021). Similar methodologies focusing on mathematical programming have been widely used for interdependent network design problem (INDP) (González et al., 2016), network reconstruction, restoration, and reliability modeling (Veremyev et al., 2014), resilience assessment of an interdependent infrastructure system (Wang et al., 2022), and integrated interdependent network design and scheduling problem (Nurre et al., 2012). Najafi et al. proposed a framework to evaluate flood-induced risk of an interdependent infrastructure system, where the interdependencies are obtained through expert opinions (Najafi et al., 2021). Zhang et al. proposed a multiobjective optimization model for community resilience enhancement considering the water and traffic network (Zhang et al., 2022). Leveraging a genetic algorithm, they analyzed the impact of the interdependence of services among buildings to enhance the resilience of a community under earthquake disaster. Another multiobjective optimization model for minimizing the construction cost and number of repairs for an interdependent infrastructure system in a post-earthquake scenario is considered by Wang et al. (2017). In these flow-based models incorporating deterministic optimization techniques, all the connector variables between different infrastructure systems are required to be known in advance (González et al., 2017). Such methods assume that the entire set of functional dependency links between the two infrastructure systems is known beforehand. Furthermore, these flow-based models require large amounts of data for realistic modeling of the interdependent infrastructure systems (Ouyang et al., 2009).

However, one of the main challenges related to vulnerability assessment of interdependent infrastructure systems is the unavailability of data (Rinaldi et al., 2002). Reilly et al. reviewed different types of aleatory and epistemic uncertainties that may arise during the vulnerability assessment of interdependent infrastructure systems. They identified that uncertainty is vastly understudied in literature and often the exact interdependencies are assumed to be well known for modeling convenience, which in reality is not a realistic assumption (Reilly et al., 2021). Baroud et al. proposed a mechanism to generate a synthetic critical infrastructure network under unavailability of data.

However, the proposed methodology cannot incorporate the within-infrastructure failure propagation (Wang et al., 2022). Talebiyan et al. considered operational decisions under uncertainty in an interdependent context using a Bayesian hierarchical model (Talebiyan & Duenas-Osorio, 2020). Furthermore, there are uncertainties associated with natural hazards, which can impact the infrastructure systems, and are often modeled using stochastic methods in literature (Allen et al., 2022; Zhang & Alipour, 2023). Hence, considering the importance of information sharing between different infrastructure systems (Sharkey et al., 2015), and the lack of it in the real-life scenario (Bjerga et al., 2018), a new holistic framework is needed to capture the vulnerability of interdependent infrastructure systems under uncertainties. The dynamic simulation-based approaches solve this problem by abstracting the physical details of the services provided by the infrastructures in almost all aspects—making the model simple and feasible to use (Brown et al., 2004; Dueñas-Osorio et al., 2007). Franchin et al. developed an object-oriented model to capture the interactions between different interconnected systems and analyzed the impact of sources of uncertainty and key vulnerability factors on the resilience of such systems through simulation (Franchin & Cavalieri, 2022). However, often such methods are inherently incapable of capturing most of the dimensions of physical, logical, and geographical interdependencies between the infrastructure systems (Zio & Sansavini, 2011). Hence, a hybrid approach is required that can model most of the interdependence dimensions of the infrastructure systems while considering that a minimal number of parameters is known beforehand.

Therefore, although the interdependent infrastructure reliability and vulnerability assessment is well studied in the literature, there exist notable research gaps. Hence, in this paper, a generalized framework is proposed *to model the vulnerability of an infrastructure system arising from both the cascading failure within the network and the failure of its components induced by other interdependent infrastructure component failures*. In the proposed model, instead of assuming that all the flow characteristics are available to the infrastructure managers, different scenarios can be realized to estimate the vulnerability of interdependent infrastructures according to the risk perception of infrastructure managers. Specifically, considering the vulnerability estimation problem from the perspective of the manager of a child infrastructure that is dependent on other parent infrastructures, we aim to address the following research gaps, identified through our comprehensive literature review, in a systematic manner as listed below. Note, in this paper, when an infrastructure provides service to another infrastructure, the *service-providing infrastructure* is termed as a *parent infrastructure*, and the *service-receiving infrastructure* is termed as a *child infrastructure*. Furthermore, we consider single-commodity infrastructure systems in our study, where every infrastructure system produces one type of commodity.

- * *Gap*: There is a lack of a holistic framework to estimate the vulnerability of interdependent infrastructure systems. A significant fraction of literature considering the vulnerability of interdependent infrastructure systems either focuses on a single infrastructure system vulnerability or only the vulnerability induced by the interdependent infrastructure systems. Not being able to model the infrastructure vulnerability from a holistic perspective often underestimates the compound risk of failure induced by multiple interdependent infrastructure systems failures. * *Contribution*: We propose an integrated framework to calculate the time-dependent vulnerability of infrastructure systems measured by the probability of service failures while considering both the within-infrastructure cascading failure and the failure induced by other interdependent infrastructures' failures. The within-infrastructure vulnerability is efficiently measured using DFTs, whereas using a simulation framework, the cross-infrastructure vulnerability is estimated. Finally, both these estimates of vulnerability are integrated into a single metric such that it can encapsulate both the within-infrastructure cascade and failure induced by other infrastructure systems. This overall estimate of vulnerability is referred to as the *comprehensive vulnerability* for the subsequent discussions in this paper.
- * *Gap*: To estimate the failure propagation within a network, DFTs are well studied. However, depending on the infrastructure under consideration, the component and connectivity of the DFTs can significantly vary. For several infrastructure systems, DFTs do not even exist in the literature. Furthermore, complex DFTs may suffer from state space explosion problems. The lack of a generalized approach for constructing DFTs for all types of infrastructure systems may hinder efficient assessment of the reliability and vulnerability of the infrastructure systems. * *Contribution*: Therefore, to address this gap, a heuristic algorithm to construct a DFT of an infrastructure, which is generalized enough to be applied to multiple infrastructure systems is presented. Although the DFTs developed using the proposed heuristic approach are not exact, in the absence of data, this method can provide a close approximation of the exact DFT, and thus can aid in efficient vulnerability and reliability assessment of the infrastructure systems under incomplete information. Furthermore, for more realistic modeling, we extended the derivation of the closed-form solutions

of the failure probabilities of the DFT gates from the existing literature as depicted in Section 2.

- * *Gap*: In contrary to the real-life scenario, often the most realistic models assume that all the supply–demand characteristics are well known to all the infrastructure systems' managers in advance. In doing so, such models relax the intrinsic dimensions of the interdependencies while trying to abstract the supply–demand characteristics. Not considering all the dimensions of interdependencies may underestimate the actual risk of failure of the infrastructure systems. Additionally, when a child infrastructure depends on multiple parent infrastructures at the same time, the relative importance of dependencies of different infrastructures may not be the same. * *Contribution*: To address this problem, a generalized framework that can capture most of the dimensions of the interdependencies, while requiring minimal data, is proposed. To estimate the vulnerability of the interdependent infrastructure systems, it is assumed that the managers only have knowledge of the types of existing interdependencies; however, the exact supply-demand flow characteristics between different infrastructures are unknown and simulated according to the manager's risk perception. Specifically, leveraging different parameters decided by themselves, the infrastructure managers can efficiently model the physical, logical, and geographical dimensions of interdependencies across multiple infrastructure systems while accounting for their relative importance.

According to Reilly et al., *physical uncertainty* is related to the quantities characterizing the flow between the systems, thus dictating how the failure may cascade from one infrastructure to another. In our study, we have accounted for this type of uncertainty (Reilly et al., 2021). Specifically, we assumed that the exact supply–demand flow from one infrastructure to another is unknown, and simulated the flow links according to the risk perception of the infrastructure managers. Furthermore, the *spatial uncertainty*, which depicts the uncertainty related to the spatial distribution (i.e., proximity vs. farness) of the collocated infrastructure systems, is also considered in our analysis. It is done through the introduction of a parameter in the modeling approach, which controls the neighborhood size as considered by the infrastructure managers. Finally, the *informational uncertainty*, which accounts for the unavailability of information from the perspective of the manager of a child infrastructure about the state of the parent infrastructure, is also considered in our proposed framework. To do so, first, it is assumed that the exact DFT of the parent infrastructure is not available to the child infrastructure manager, which is often the case in reality. Second, rather than fixing the importance of one infrastructure on another, a relative importance matrix is proposed, using which the impact of one infrastructure on another can be simulated by the manager of the child infrastructure. To implement the proposed generalized vulnerability assessment framework, we leverage the Bayesian network (BN) to model the DFTs for each infrastructure system, which can efficiently capture the failure propagation dynamics within a particular infrastructure referred to as the *intra-infrastructure failure*. Then, over a grid-based geo-map, a network of interdependent infrastructure networks is created, which can quantitatively measure the *physical, logical, and geographical* interdependencies that may exist between every pair of infrastructure systems. Thereafter, using a simulation-based approach, the failure dynamics of the components of the child infrastructure that may be induced by the failure of interdependent infrastructure systems, referred to as the *inter-infrastructure failure*, is calculated. Finally, the compound risk of failure, that is, the comprehensive vulnerability of a network of infrastructure systems, which may be caused by either the intra-infrastructure failure or inter-infrastructure failure is computed. The proposed framework is implemented and validated using existing synthetic data on electricity, water, and supply chain networks. The remainder of the paper is organized as follows. In Section 2, the detailed methodology employed in this paper is described. In Section 3, the data collection and preprocessing methods for the specific case study are described, followed by summarizing the results and key findings in Section 4. Finally, the paper is concluded in Section 5.

2 | METHODOLOGY

In this section, a detailed description of the methodology to calculate the vulnerability of an infrastructure due to intra- and inter-infrastructure failures is presented. As mentioned before, the proposed framework is flexible enough to incorporate modifications in terms of the number and types of the infrastructure systems under consideration, any type of spatiotemporal characteristics, and even the lack of adequate data availability. First, to capture the failure propagation within an infrastructure, a DFT is constructed, and then using a DBN, the time-dependent vulnerability is modeled (Section 2.1). To model the inter-infrastructure vulnerability where the *exact supply-flow characteristics are not known*, a heuristic network of networks is created considering the physical, logical, and geographical dependencies between the infrastructures (Section 2.2). Thereafter, leveraging a simulation approach, multiple cases are constructed to calculate the best, average, or worst-case inter-infrastructure failures. Finally, the intra- and inter-infrastructure failures

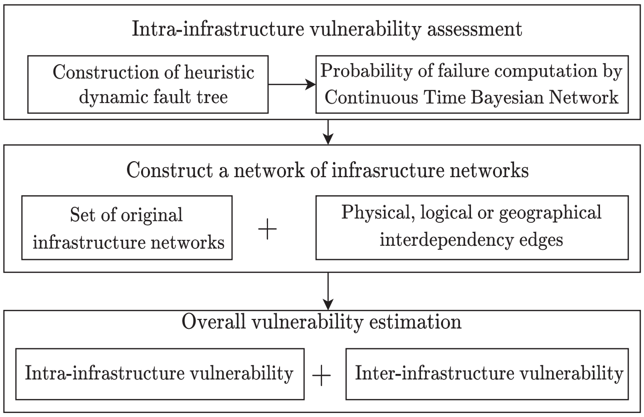

Intra-infrastructure vulnerability assessment
Construction of heuristic dynamic fault tree
Probability of failure computation by Continuous Time Bayesian Network
Construct a network of infrasructure networks
Set of original infrastructure networks
+
Physical, logical or geographical interdependency edges
Overall vulnerability estimation
Intra-infrastructure vulnerability
+
Inter-infrastructure vulnerability

FIGURE 1 The overall research framework.

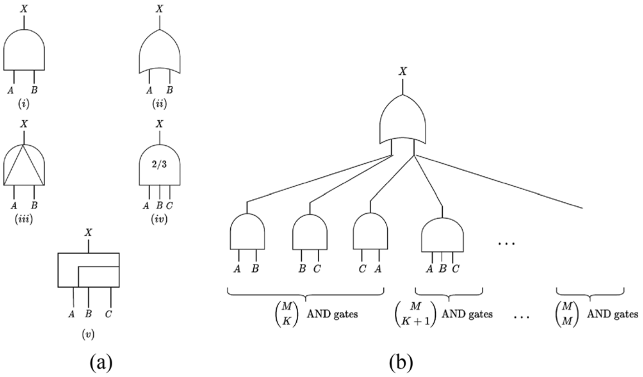


FIGURE 2 (a) The gates in the dynamic fault tree (DFT): (i) AND gate, (ii) OR gate, (iii) PAND gate, (iv) VOTING gate, and (v) WSP gate; (b) the depiction of the VOTING gate using a combination of AND and OR gates.

are combined to estimate the comprehensive vulnerability of an infrastructure (Section 2.3). The three parts of the overall methodology are depicted in Figure 1. Details of each part are described in the following subsections.

2.1 | Intra-infrastructure failure probability

In this section, the proposed method of leveraging a DFT and a CTBN to estimate intra-infrastructure vulnerability under incomplete information is described. A DFT consists of several gates as depicted in Figure 2a. A brief description of the gates commonly used in a DFT is depicted below.

- In a DFT, if two inputs A and B are connected via AND (Figure 2a(i)) gate to produce output X, then X fails if both A and B fail.
- On the other hand, if A and B are connected via OR gate (Figure 2a(ii)) to produce X, then X fails if either A or B fails.
- In a PAND or priority AND gate (Figure 2a(iii)), the output fails if all of its inputs fail in a particular order. Often the order of failure of the inputs is considered from left to right as depicted in the diagram of the PAND gate (Boudali et al., 2010).
- In a K/M VOTING gate (Figure 2a(iv) depicting a 2/3 VOTING gate), the output fails, if at least K of its M inputs fail (Boudali et al., 2010). Being a derived gate, the VOTING gate can be easily constructed using the basic AND and OR gates as depicted in Figure 2b. If $M = 2$ and $K = 1$, then the VOTING gate is an OR gate, and if $K = 2$, then the VOTING gate is an AND gate. Essentially, a VOTING gate is an OR combination of the $\binom{M}{K} + \binom{M}{K+1} + \cdots + \binom{M}{M}$ number of AND combinations of the inputs. From the available M inputs, if any combination of K such inputs fails, or any combination of $K + 1$ to M of such combinations fails, then the output fails.
- In a WSP or warm spare gate (Figure 2a(v)), there is one primary input (A) and multiple spare inputs (B and C). Initially, the primary input is switched on and the spares operate in a dormant or standby mode where the failure rate of the spare is reduced by a factor $\alpha \in [0, 1]$ called the dormancy factor (α). When the primary unit fails, the first available spare becomes active. The output X fails if all of the inputs fail (Boudali et al., 2010).

2.1.1 | Constructing a DFT

When any critical component of a particular infrastructure fails, then the failure propagates within the infrastructure network. In any infrastructure network, commodities or services flow from one component to another. Often, some types of commodities are generated at the source nodes and then the commodities flow through multiple intermediate nodes before they are consumed or utilized by the customers in the terminal node. This general architecture is the backbone of the operation mode for several infrastructure systems like electricity distribution and transmission systems, water distribution, or the supply chain network. For example, in an electricity infrastructure, generators are connected to the loads via buses, and buses are connected via power lines in between them. The power generated at a generating station satisfies the loads connected to that particular bus and may be transferred to other buses via the transmission lines to satisfy the demands of the other buses. When a generator goes off, other generators connected to the bus try to make up for the potential demand of the bus (Wood & Wollenberg,

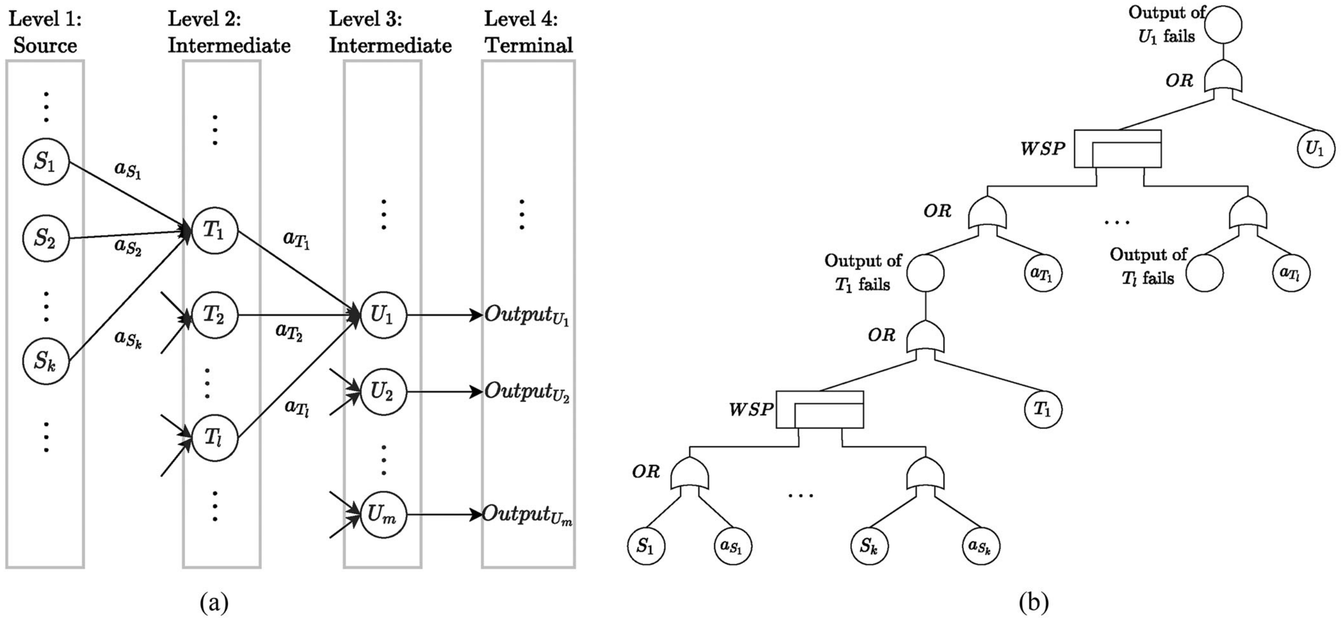


FIGURE 3 (a) A multipartite directed acyclic graph constructed according to the material/service flow in a general infrastructure system, and (b) the dynamic fault tree (DFT) constructed from the network of the general infrastructure system under consideration.

2012). Thus, these generators can be considered as the sources of electricity flowing through the network, the buses can be considered as the intermediate nodes, and finally, the loads connected to the buses can be considered as the consumers. Similarly, for a water distribution system, the water flows from the sources to the treatment plants, then to the storage reservoirs, and finally to the distribution reservoirs from where the water is dispatched to the consumers (Sincero & Sincero, 1995). A similar underlying network architecture also exists for a supply chain network, where the raw materials flow from the supplier to the manufacturer for processing the commodities and then the commodities are supplied to the retailers who supply the commodities to the customers (Tang et al., 2016).

Based on the flow of the commodities or services (e.g., electricity or water) from the source node to the terminal node via multiple intermediate nodes and connecting arcs, it is evident that *different network infrastructure systems share a common representation*. In this paper, we present a *generalized framework that can abstract a network topology for any such infrastructure when exact information on the nodes, arcs, and interdependencies is not available.* Our approach to model the intra-infrastructure vulnerability of different infrastructure systems does not require the exact knowledge of all the components and their connections within the infrastructure networks considered in the study. Alternatively, in the presence of scarce information about the parent infrastructure, using a heuristic approach, the child infrastructure manager can come up with a logical representation of the parent infrastructure network as shown in Figure 3a and calculate the intra-infrastructure vulnerability by deriving a DFT as shown in Figure 3b, and Algorithm 1. First, according to the flow of the commodities or services within an infrastructure, a topological ordering (Cormen et al., 2001) of the nodes is created. From that topological ordering, a multipartite graph is constructed where the nodes of the graph are partitioned into multiple disjoint sets or levels say, $B_1, \ldots, B_l$. There exist directed edges from the nodes of level B_b to B_{b+1} for $b \in \{1, \ldots, l-1\}$. For example, for a water distribution network, the first level consists of the sources, and the second level consists of the treatment plants. As water flows from the sources to the treatment plants, there exist directed edges from the nodes in the first level to the nodes in the second level. Similarly, edges exist between the nodes of the second level to the third level (e.g., reservoirs for water infrastructure) and finally to the layer of the terminal nodes (e.g., consumers). This similar representation technique can also be applied to several other infrastructure systems wherever there exists a flow of commodities or services from one set of nodes to the others like electricity infrastructure where electricity flows from generators to buses and loads. Such a common logical representation of a general infrastructure system has been shown in Figure 3a.

Consider that the source nodes $S_1, S_2, \ldots, S_k$ are connected to the intermediate node T_1 via the arcs $a_{S_1}, a_{S_2}, \ldots, a_{S_k}$, respectively. If either S_1 or the arc coming out of S_1, that is, a_{S_1} fails, then the output of S_1 cannot reach T_1. Similarly, the output of S_2 cannot reach T_1 if

ALGORITHM 1 IntraModel($I_i, \varkappa$)

```
Input: An infrastructure $I_i$ with the nodes and the edges
    connecting the nodes. and the initial probabilities of failure
    for each node and arc of $I_i$ denoted here as $\varkappa$.
Output: For each node of $I_i$, the probabilities of failure arising
    from intra-infrastructure cascade.
    /* Construction of the dynamic fault tree (DFT) for a
       general infrastructure */
    According to the material/service flow within $I_i$ find a
       topological ordering of the nodes of $I_i$
    According to the topological ordering, partition the nodes
       of $I_i$ into disjoint sets (levels): $B_1, \ldots, B_l$, such that there
       exist arcs from nodes in $B_b$ to $B_{b+1}$
    for $lv \in \{2, \ldots l\}$ do
        for every node $T_v \in B_{lv}$ do
            Input to $T_v$ fails $\leftarrow WSP(\, OR(\varkappa(S_k), \varkappa(a_{S_k})))$ , where
            $S_k$ are the parent nodes of $T_v$ in the level $B_{lv-1}$ and $a_{S_k}$
            are the arcs between $S_k$ and $T_v$
            Output of $T_v$ fails $\leftarrow OR$(Input to $T_v$ fails, $\varkappa(T_v)$)
            $\varkappa(T_v) \leftarrow$ Output of $T_v$
        end for
    end for
    /* Calculating probabilities of failure using continuous
       time Bayesian network */
    for every node in the DFT starting from the bottom level
        do
        Using the closed form solutions in Section 2.1.2,
        calculate the probabilities of failure of intermediate and
        top events
    end for
    for every node $n_{ij} \in I_i$ do
        return probabilities of failure due to
        intra-infrastructure cascade
    end for
```

either S_2 or the arc associated with it, a_{S_2} fails; and if either S_k or the arc associated with it, a_{S_k} fails, then the output of the source S_k cannot reach the destination T_1. Considering the single-commodity network and all the sources are of the same type, when one of the sources in $S_1, S_2, \ldots, S_k$ or the associated arcs $a_{S_1}, a_{S_2}, \ldots, a_{S_k}$ fail, then the other sources try to compensate for the loss owing to the breakdown of such a source. Hence, the other sources start working in a more stressful condition than the dormant state to make up for the loss of supply. Due to this, the failure rate of the current functional units, which are in standby mode, increases by a factor (α). This situation can be modeled by leveraging a DFT, using the warm spare (WSP) gate. Using a DFT, the infrastructure network described in Figure 3a can be modeled using Figure 3b. If any source of $S_1, S_2, \ldots, S_k$ or the associated arc with it $a_{S_1}, a_{S_2}, \ldots, a_{S_k}$ fails, then the output of the particular source cannot reach the intermediate node T_1. If all the sources connected with T_1 fail, then the input to T_1 fails. Furthermore, if one input fails, the failure rate of the other inputs increases by a certain factor. Hence, the input to T_1 failing is a result of a WSP gate output. Then, if the input to T_1 fails or the node T_1 itself fails, the output of T_1 fails. If either the output of T_1 fails or the arc coming out of T_1, that is, a_{T_1} fails, then the output of T_1 cannot reach the destination U_1. Similar to the previous layer, there are multiple nodes $T_1, T_2, \ldots, T_l$ connected to U_1 via the arcs $a_{T_1}, a_{T_2}, \ldots, a_{T_l}$. If any of the nodes of $T_1, T_2, \ldots, T_l$ or the arcs associated fails, then the output of that node may not reach U_1. Using a similar logic to the previous layer, the failure of the input to U_1 is modeled as a WSP gate output of its parent nodes or the incoming edges. Therefore, in this architecture, the output of U_1 fails if either the input of U_1 fails or the node U_1 itself fails. Thus, in this paper a recursive procedure is proposed to convert the nodes and the arcs of an infrastructure network into a DFT following the commodity or service flow patterns within the infrastructure network.

Though such an algorithm can be used to construct a DFT for any infrastructure network, such a DFT is not accurate. A more complex and accurate DFT can be constructed considering the accurate topology and the service–demand flow of the infrastructure if they exist. Such a situation may arise when the number of intermediate levels considered by the infrastructure manager as depicted in Figure 3a is not adequate. For example, though a basic supply chain network consists of suppliers, manufacturers, and retailers, often other sets of nodes like plants or distributors are also considered as components of the supply chain network (Gong et al., 2014). Hence, the accurate construction of DFT is dependent on the prior knowledge of the infrastructure manager. However, the accurate DFT can be easily substituted in the overall framework of the paper as described in Figure 1, without loss of generality when more accurate information is available.

2.1.2 | Construction of a CTBN

In order to construct a CTBN from the DFT of the infrastructure (Boudali & Dugan, 2006), we extended the methodology proposed by Boudali et al. in this paper. In the CTBN, the state space is continuous, which depicts the failure time of a component of the DFT. In a CTBN, the random variable ξ is in state x means that the system component represented by ξ failed in the time instant x, where x is a nonnegative real number (Boudali & Dugan, 2006). Here, the closed-form solutions of the probabilities of failure of the output for each of the gates used in our DFT are presented. A detailed derivation is provided in the

TABLE 1 For each gate of our dynamic fault tree (DFT), the probabilities of failure of the output in time $[0, t]$.

Gate	Probability of failure of output in $[\mathbf{0}, \boldsymbol{t}]$
AND	$1 - e^{-\lambda_A t} - e^{-\lambda_B t} + e^{-(\lambda_A+\lambda_B)t}$
OR	$1 - e^{-(\lambda_A+\lambda_B)t}$
WSP	$(1 - e^{-\lambda_A t})(\frac{\alpha\lambda_B(e^{-t(\lambda_A+\alpha\lambda_B)}-1)}{-\lambda_A-\alpha\lambda_B} - \frac{\lambda_A(-(e^{-\lambda_B t}-1)(\lambda_A+\alpha\lambda_B)+\lambda_B e^{-t(\lambda_A+\alpha\lambda_B)}-\lambda_B)}{(\lambda_A+\alpha\lambda_B)(\lambda_B-\lambda_A-\alpha\lambda_B)})$

Appendix. Considering a two-input AND, OR, and WSP gate, Table 1 depicts the probabilities of failure of the output in time $[0, t]$. It is considered that the inputs to the gates are A and B, where the time of failure of A follows an exponential distribution with rate λ_A, and the time of failure of B follows an exponential distribution with rate λ_B. Then, for the WSP gate if B is the spare unit with dormancy factor α, the probability of failure of the output X in time $[0, t]$ is depicted in Table 1. For the WSP gate, while deriving the closed-form solution of the probability of failure, Boudali et al. considered both the inputs A and B to have the same failure rate λ. This assumption is not practical in a real-life scenario. In this study, the work is extended by considering the inputs A and B having different rates of failure: λ_A and λ_B, respectively. The detailed derivation is provided in the Appendix. It is noteworthy that, when $\lambda_A = \lambda_B = \lambda$, our closed-form solution reduces to the solution provided by Boudali and Dugan (2006). The dormancy factor (α) for a two-input WSP gate is considered as 0.5, which is also considered in the literature (Boudali & Dugan, 2006).

To summarize, the overall procedure to estimate the probabilities of intra-infrastructure failure has been depicted in Algorithm 1.

ALGORITHM 2 `CreateNetwork` $(I_1, I_2, \dots, I_s, \Gamma)$

Input: The infrastructure networks $I_1, I_2, \dots, I_s$, the threshold $\Gamma \in [0, 1]$ of the interdependency edge strength.

Output: A network of infrastructure networks (G) with the intra-infrastructure and inter-infrastructure links.

```
1:  $G = I_1 \cup I_2 \cup \dots \cup I_s$
2:  for every two infrastructure networks $I_i$ and $I_k$ $(i \neq k)$ do
3:    for each node $n_{kl}$ of $I_k$ do
4:      for each node $n_{ij}$ of $I_i$ do
5:        if the node $n_{kl}$ may require service from the node $n_{ij}$ or the state of the node $n_{kl}$ may be affected by the state of the node $n_{ij}$ then
6:          $d$ = (The Euclidean cell distance between $n_{ij}$ and $n_{kl}$) + 1
7:          Interdependency strength $(\gamma_{kl}^{ij}) = \frac{1}{d}$
8:          if $\gamma_{kl}^{ij} \geq \Gamma$ then
9:            Add the interdependency edge of strength $\gamma_{kl}^{ij}$ from $n_{ij}$ to $n_{kl}$ in $G$
10:         end if
11:       end if
12:     end for
13:     if the node $n_{kl}$ may require service from at least one node in $I_i$ or the state of the node $n_{kl}$ may be affected by the state of the node $n_{ij}$ then
14:       if $\nexists$ an edge from at least one node of $I_i$ to $n_{kl}$ then
15:         Add the interdependency edge of highest strength $= \frac{1}{d}$ from $n_{ij}$ to $n_{kl}$ in $G$; where $n_{ij}$ is the nearest node of $I_i$ from $n_{kl}$, and $d$ = the Euclidean cell distance between $n_{ij}$ and $n_{kl}$ +1
16:       end if
17:     end if
18:   end for
19: end for
20: return $G$
```

2.2 | Constructing an interdependent network of networks

In the second step of the overall research framework, where we estimate the *inter-infrastructure vulnerability*, first, a framework to construct a network-of-networks that can capture the physical, logical, and geographical interdependencies as depicted in the Algorithm 2 is proposed. To start with, it is considered that there are s interdependent infrastructure systems, $I_1, I_2, \dots, I_s$. Each infrastructure system is a network of components. Let us consider that there are N_1 number of nodes in I_1, N_2 number of nodes in I_2, …, N_s number of nodes in I_s. The jth node of infrastructure I_i is denoted by n_{ij}. As mentioned above, the **physical** interdependency between two infrastructure systems exists, if materials or services produced by one infrastructure are consumed by another infrastructure. On the other hand, the **logical** interdependency between two infrastructure systems exists if the state of one infrastructure is affected by the change of state of another infrastructure. First, the algorithm checks if infrastructure I_k is **physically** or **logically** dependent on the infrastructure I_i. In Algorithm 2, Line 5, if node n_{kl} may require service from node n_{ij}, then according to the definition of the physical interdependency, infrastructure I_k is physically dependent on I_i. Furthermore, if the state of node n_{kl} is affected by the change of state of node n_{ij}, then according to the definition of logical interdependency, infrastructure I_k is logically dependent on I_i. The infrastructure managers should be able to decide these criteria based on their previous experience and expert knowledge. For example, the water distribution infrastructure may be physically and logically dependent on the electricity infrastructure

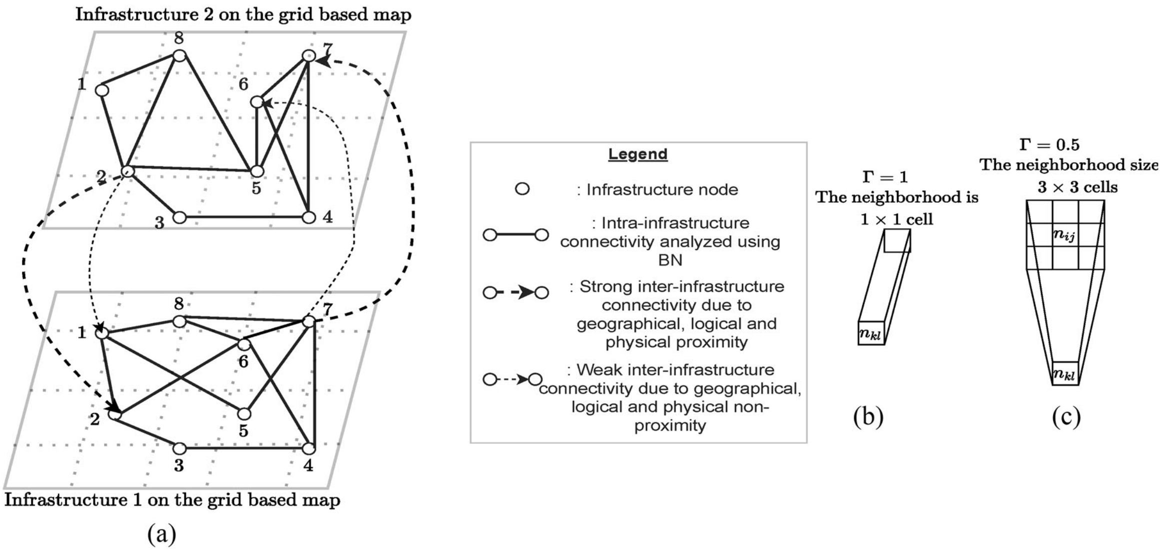

Infrastructure 2 on the grid based map
1
2
3
4
5
6
7
8
Infrastructure 1 on the grid based map
(a)
Legend
: Infrastructure node
: Intra-infrastructure connectivity analyzed using BN
: Strong inter-infrastructure connectivity due to geographical, logical and physical proximity
: Weak inter-infrastructure connectivity due to geographical, logical and physical non-proximity
Γ = 1
The neighborhood is 1 × 1 cell
n_{kl}
(b)
Γ = 0.5
The neighborhood size 3 × 3 cells
n_{ij}
n_{kl}
(c)

FIGURE 4 (a) The network of infrastructure networks on a grid-based map with intra- and inter-infrastructure edges, (b) the neighborhood size for Γ = 1, and (c) the neighborhood size for Γ = .5.

system in the sense that the pumps of the water distribution infrastructure require electricity services to operate. In this context, it is assumed that the manager of the water distribution infrastructure knows that there exists physical dependency of water infrastructure over the electricity infrastructure. If infrastructure I_k is dependent on infrastructure I_i, then there exist interdependency edges from components of I_i to I_k. Furthermore, note that even if I_k is dependent on I_i, all the nodes of I_k may not require services from I_i; and all the nodes of I_i may not provide service to a node of I_k. As an example, for electricity infrastructure to operate, water is required for cooling and also for the generators; however, all the nodes of a water distribution infrastructure cannot provide the required service to the electricity infrastructure. Water can be dispatched from the reservoirs but not directly from the treatment plants. These physical and logical dependencies are specific to the infrastructure systems under consideration and expert opinion may be helpful in this regard.

The infrastructure networks are placed on a grid-based geo-map as shown in Figure 4 using the quantum geographic information system (QGIS) (QGIS, 2021). The grid cells have a specific size, which is to be kept constant for all the infrastructures. The grid cells with the smallest resolution essentially represent the geographical coordinate of each node of the infrastructure. Using a larger resolution, it is allowed to discretize the geographical space into cells where each node of infrastructure belongs to a specific cell of the grid. The cell-based distance between every node (n_{ij}) of I_i and every node (n_{kl}) of I_k is calculated as the Euclidean distance. By add-one smoothing, the effective distance is modified such that the distance $d \geq 1$. The interdependency edge strength between the components n_{ij} and n_{kl} is calculated as $1/d$, where the add-one smoothed distance d can be used. If the components n_{ij} and n_{kl} are geographically distant, then the cell-based distance (d) will be more, which in turn results in low interdependency edge strength. On the other hand, if the nodes n_{ij} and n_{kl} are in geographical proximity, then the cell-based distance (d) will be less, which results in a strong interdependent edge from n_{ij} to n_{kl}. In this way, the geographical interdependencies are taken into consideration, which results from the geographical proximity of two infrastructures. Finally, the strong interdependency edges are considered and the weak interdependency edges are removed from the system by using the threshold Γ, a user-defined parameter. In this context, the underlying assumption is that, for a child infrastructure dependent on a parent infrastructure, the material/service flows from the parent to the child infrastructure only if the components are in a certain geographical proximity. The interdependency edges from n_{ij} to n_{kl} are only added if the interdependency edge strength (γ^{ij}_{kl}), calculated according to the geographical proximity, is greater than or equal to the threshold Γ. However, it is noteworthy that for a large threshold Γ, there can be a situation where no interdependent edges are added as all the interdependency edge strengths are less than Γ. Such a situation may not be practical for modeling the interdependent infrastructure systems. For example, consider the dependency of water distribution infrastructure on the electricity infrastructure system. All the water pumps require electricity to operate; however, due to the high value of Γ, if no interdependency edge can be added from any bus of the electricity infrastructure to the water pumping stations, then it will not be practical to model the interdependency. Hence, in such a situation, (where the physical or logical interdependencies must exist, but are not added due to larger geographical distance), the interdependency edge of strength $\gamma_{kl}^{ij} = \frac{1}{d}$ from the nearest node $n_{ij} \in I_i$ to the node n_{kl} is added. Here, d is the add-one smoothed Euclidean distance between the cell of n_{ij} and n_{kl}, even though $\gamma_{kl}^{ij} < \Gamma$. To summarize, if there exist physical or logical interdependencies between the infrastructures, then the interdependency edges are added with the strength proportional to their geographic proximity. However, note that the infrastructure systems considered by the infrastructure managers do not have the exact infrastructure layout as described previously in Algorithm 1. Thus, the physical or logical interdependencies considered by the infrastructure managers may not be exact in the presence of incomplete/imperfect information about the infrastructure topology and the exact interdependency relationships. However, without the loss of generality of the overall framework, more accurate interdependencies can be incorporated upon the availability of information.

2.3 | Infrastructure systems vulnerability assessment

After the network of infrastructure networks (G) is obtained using Algorithm 2, a framework to estimate the vulnerability of each infrastructure due to both the intra- and inter-infrastructure cascading failures is created. In this process, three probabilities of failure are considered, including (1) P_{ij}^{intra}—the probability of failure of node n_{ij} due to intra-infrastructure cascade effect at time $[0, t]$, where $t \in [0, 24]$; (2) P_{ij}^{inter}—the probability of failure of node n_{ij} due to inter-infrastructure failure propagation from one infrastructure to another at time $[0, t]$, where $t \in [0, 24]$; and (3) P_{ij}^{fail}—the comprehensive probability of failure arising from both intra- and inter-infrastructure cascade at time $[0, t]$, where $t \in [0, 24]$. It is assumed that for a particular node n_{ij}, the intra-infrastructure failure probability is independent of the inter-infrastructure failure probability of the same node n_{ij}. This is a reasonable assumption because the source of the intra-infrastructure failure probability is any parent node of n_{ij} within the same infrastructure I_i, whereas the inter-infrastructure failure probability is obtained from a node of a different network. Using the independence assumption, the probability of failure occurring from both the intra- and inter-infrastructure cascades is calculated as $P_{ij}^{intra} * P_{ij}^{inter}$.

Furthermore, when an infrastructure (I_k) receives service from another infrastructure (I_i), there can be generally three cases that may occur if multiple interdependency links exist. Say $\mathcal{N}_i$ be the set of nodes of I_i from which there exist interdependency links to node n_{kl} of I_k (i.e., $\exists n_{ij} \in \mathcal{N}_i$ such that $n_{ij} \rightarrow n_{kl}$ exists). In this scenario, there may be any of the following three cases that may arise:

1. *Best case*: The node n_{kl} fails if all the nodes of $\mathcal{N}_i$ fail. In this case, the node n_{kl} fails after the node in $\mathcal{N}_i$, with the minimum probability of failure, fails.
2. *Worst case*: The node n_{kl} fails if any one of the nodes in $\mathcal{N}_i$ fails. In this case, the node n_{kl} fails after the node in $\mathcal{N}_i$, with the maximum probability of failure, fails.
3. *Average case*: The functionality of node n_{kl} is partially dependent on every node of $\mathcal{N}_i$. For example, if the nodes in $\mathcal{N}_i$ include certain types of supply facility locations; n_{kl} are demand nodes and the demand of these nodes can be satisfied by multiple service nodes operating in conjunction. Without loss of generality, it can be assumed n_{kl} is equally dependent on all the nodes of $\mathcal{N}_i$.

The infrastructure manager considers either of these cases according to their *risk perception and prior experience*. For example, a risk-averse infrastructure manager who is interested to design a robust system shall consider the *worst -case scenario* of the supply–demand characteristics from other infrastructures. On the other hand, a risk-seeking and opportunistic manager may consider the *best -case scenario*; whereas, the *average -case scenario* is well suited for a risk-neutral design of interdependent infrastructure systems. After considering a particular scenario of supply–demand characteristic, a simulation environment is created where the probability of failure is calculated for each node of the infrastructures, and how the failure probabilities evolve over the days is analyzed. As mentioned before, the failure probabilities depict the probability of a component failure at time $[0, t]$ where $t \in [0, 24]$, depicting the hourly probabilities of failure for each component. The intra-infrastructure failure probability for the *first day (i.e., iteration 1)* is computed considering the initial failure probability follows an exponential distribution, as indicated in previous studies (Boudali & Dugan, 2006). Then, the inter-infrastructure failure probability of node n_{kl} due to n_{ij} is calculated as the product of the strength of the interdependency links between them (γ) and the probability of failure of the parent node n_{ij}.

$$V_{kl}^{ij} = \gamma_{kl}^{ij} * P_{ij}^{fail}$$

According to the case of simulation (best, worst, or average), the inter-infrastructure failure probability is calculated. As mentioned before, if the best-case scenario is considered, the failure of the node happens if all the interconnected parent nodes fail. Hence, the probability of failure is the minimum of the failure probabilities of the parent nodes. On the other hand, the worst-case situation may happen when a node fails if any one of the parent nodes fails. In this case, the failure probability of the node is the same as the maximum probability of failure of the parent nodes. Finally, there can be an average case, where the failure of a node is dependent on all the parent nodes. In this case, a uniform distribution over all the parent nodes is assumed, and the failure probability is estimated as the average of the probabilities of failure of all the parent nodes. If there are two infrastructures I_i and I_k, such that there exist interdependency edges from the nodes of I_i to I_k, we have described how to calculate the probabilities of failure of the nodes of I_k induced by the failure of the nodes of I_i (refer to Section 2.2). However, as described before, the infrastructure I_k may be dependent on multiple infrastructure systems, not a single infrastructure I_i. Now, the importance of one infrastructure on another infrastructure may be different. For example, for three interdependent infrastructure systems, I_i, I_k, and I_m, where I_m is dependent on both I_i and I_k, the importance of dependency of I_m on I_i may be more than the dependency of I_m on I_k and vice versa. To capture the combined effect of all the other infrastructure systems on a particular infrastructure, we introduce the relative importance matrix R of dimension $s \times s$, where s is the total number of infrastructures considered in the analysis. The importance of infrastructure I_i on I_k (or, the importance of dependency of I_k on I_i) is depicted by the entry in the ith row and kth column, that is, R_{ik}. Furthermore, it is considered that the construction of R follows the following properties.

(1) The diagonal entries of R are 0, that is, $R_{ii} = 0 \; \forall i \in \{1, \dots, s\}$, indicating a particular infrastructure is not dependent on itself for inter-infrastructure failure.
(2) The sum of every column in R is 1, that is, $\sum_i R_{ik} = 1 \; \forall k \in \{1, \dots, s\}$, indicating that the importance of interdependencies of the infrastructure I_k over the other infrastructures must sum up to 1. Note, without loss of generality, if the column sum is not 1, it can be normalized to 1.

Now, the inter-infrastructure probability of failure of the node n_{kl} of infrastructure I_k due to all the parent infrastructures in time $[0, t]$ for either the best-, worst-, or average-case scenario (P_{kl}^{inter}) can be estimated as

$$P_{kl}^{inter} = \sum_{i=1}^{s} R_{ik} P_{kl}^{i}$$

where P_{kl}^{i} is the inter-infrastructure failure probability of the node n_{kl} induced by I_i in either the best-, worst-, or average-case scenario.

Finally, the probability of failure of a node may result from either intra- or inter-infrastructure cascade or both.

$$P_{ij}^{fail} = P_{ij}^{intra} + P_{ij}^{inter} - \left(P_{ij}^{intra} * P_{ij}^{inter}\right)$$

After the probabilities of failure P_{ij}^{fail} for the *first day (i.e., iteration 1)* are realized, they are considered as the initial failure probabilities of the components for the *next day (i.e., iteration 2)* and again the intra-infrastructure, inter-infrastructure, and combined/comprehensive probabilities of failures are calculated. This process is iterated over multiple iterations depicting the effects of multiple days of service outage of interdependent infrastructure systems. Finally, the sensitivity of the user-defined parameters considered in our model, including the threshold of the interdependency edge strength Γ and the relative importance of one infrastructure on another R_{ik}, is considered. It is noteworthy that, as Γ is changed, the inter-infrastructure probabilities of failure change corresponding to the best-, worst-, or average-case scenarios under consideration. The following Proposition 1 says that, with increasing Γ (decrease in the neighborhood size), the inter-infrastructure failure probabilities will increase for the best-case scenario, and the inter-infrastructure failure probabilities will decrease for the worst-case scenario. In the best-case scenario where the child node fails if all the parent nodes fail, the parent nodes act as redundancies. Hence, in that case, the more the number of parent nodes, the less vulnerable is the child node. In the worst-case scenario where a child node fails, if any one of the parent nodes fails, the parent nodes act as nonredundancies or deficiencies. In such a scenario, the more the number of parent nodes, there is a higher chance of finding a critical node with a high probability of failure, which can cause the failure of the child node. Hence, in the worst case, the more the number of the parent nodes, higher is the vulnerability of the child node.

Proposition 1. *Consider two infrastructures I_i and I_k, where there exist interdependency edges from I_i to I_k. Say $\mathcal{N}_{\Gamma z1}$ is the neighborhood of a node $n_{kl} \in I_k$ such that the interdependency edge strength from any node $n_{ij} \in I_i$ is $\geq \Gamma z1$ for a given $\Gamma z1$; and $\mathcal{N}_{\Gamma z2}$ is the neighborhood of a node $n_{kl} \in I_k$ such that the interdependency edge strength from any node $n_{ij} \in I_i$ is $\geq \Gamma z2$ for a given $\Gamma z2$. Furthermore, let us consider that $P_{\Gamma z}^{b}$ and $P_{\Gamma z}^{w}$ denote the average inter-infrastructure failure probabilities of the nodes of I_k for the given Γz in time $[0, t]$, for the best- and worst-case scenarios, respectively. Then,*

$$P_{\Gamma z1}^{b} \leq P_{\Gamma z2}^{b}, \text{ where } \Gamma z1 \leq \Gamma z2$$

$$P_{\Gamma z1}^{w} \geq P_{\Gamma z2}^{w}, \text{ where } \Gamma z1 \leq \Gamma z2$$

Proof. Below, the formal proof of the proposition is presented. It can be proved that any node that belongs to the $\Gamma z2$ neighborhood is always contained in the $\Gamma z1$ neighborhood. Hence, with increasing Γ, the probabilities of failure are monotonically increasing for the best-case scenario; and the probabilities of failure are monotonically decreasing for the worst-case scenario. There can be four cases that may arise for $\Gamma z1 \leq \Gamma z2$ as follows. (1) If $\mathcal{N}_{\Gamma z2} \neq \phi$, $\mathcal{N}_{\Gamma z1} \neq \phi$, in this case, according to the construction in Algorithm 2, if there exist some nodes $n_{ij} \in I_i$ in the $\Gamma z2$ neighborhood ($\mathcal{N}_{\Gamma z2}$) of n_{kl}, then that node must also exist in the $\Gamma z1$ neighborhood ($\mathcal{N}_{\Gamma z1}$) of n_{kl}. (2) If $\mathcal{N}_{\Gamma z1} = \phi$, then, according to the construction, $\mathcal{N}_{\Gamma z2} = \phi$. In this case, let $\mathcal{N}^A_{\Gamma z1}$ and $\mathcal{N}^A_{\Gamma z2}$ be the auxiliary neighborhoods that are created by adding the then $n_{ih} \in I_i$, which is the nearest node of n_{kl} to the neighborhoods $\mathcal{N}_{\Gamma z1}$ and $\mathcal{N}_{\Gamma z2}$. Hence, both $\mathcal{N}^A_{\Gamma z1}$ and $\mathcal{N}^A_{\Gamma z2}$ consist of n_{ih}. (3) If $\mathcal{N}_{\Gamma z2} = \phi$ and if $\mathcal{N}_{\Gamma z1} \neq \phi$. In this case, say $n_{ih} \in I_i$ is the nearest node added to $\mathcal{N}_{\Gamma z2} = \phi$ to ensure at least one interdependency edge exists, forming the auxiliary neighborhood $\mathcal{N}^A_{\Gamma z2}$. Now, as $\mathcal{N}_{\Gamma z1} \neq \phi$, then we conclude n_{ih} must belong to $\mathcal{N}_{\Gamma z1}$, that is, $n_{ih} \in \mathcal{N}_{\Gamma z1}$. (4) If $\mathcal{N}_{\Gamma z2} = \phi$ and if $\mathcal{N}_{\Gamma z1} = \phi$, then similar to a previous case, let $n_{ih} \in I_i$ which is the nearest node of n_{kl}, be added to the neighborhoods $\mathcal{N}_{\Gamma z1}$ and $\mathcal{N}_{\Gamma z2}$ to form the auxiliary $\mathcal{N}^A_{\Gamma z1}$ and $\mathcal{N}^A_{\Gamma z2}$. Hence, both $\mathcal{N}^A_{\Gamma z1}$ and $\mathcal{N}^A_{\Gamma z2}$ consist of n_{ih}.

From the above four cases, we conclude that, $\mathcal{N}_{\Gamma z2} \subseteq \mathcal{N}_{\Gamma z1}$ or $\mathcal{N}^A_{\Gamma z2} \subseteq \mathcal{N}_{\Gamma z1}$ or $\mathcal{N}^A_{\Gamma z2} \subseteq \mathcal{N}^A_{\Gamma z1}$. Now, according to the definition, in the best case, node n_{kl} fails if all the nodes in the neighborhood fail. That is, from Algorithm 3, $P^b_{\Gamma z} = \min_{n_{ij} \in \mathcal{N}_{\Gamma z}} V^{kl}_{ij}$. As we have a minimization problem here, we conclude $P^b_{\Gamma z1} \leq P^b_{\Gamma z2}$, where $\Gamma z1 \leq \Gamma z2$. Similarly, according to the definition, in the worst case, node n_{kl} fails if at least one of the nodes in the neighborhood fails. That is, from Algorithm 3, $P^b_{\Gamma z} = \max_{n_{ij} \in \mathcal{N}_{\Gamma z}} V^{kl}_{ij}$. As we have a maximization problem in this scenario, we conclude $P^w_{\Gamma z1} \geq P^w_{\Gamma z2}$, where$\Gamma z1 \leq \Gamma z2$. Hence, proved. □

ALGORITHM 3 `CalculateVulnerability` (G, M, λ, R)

```
Input: $G$, the maximum number of iterations ($M \geq 1$), mean
  time of failure for the root nodes to start with ($\lambda$), and the
  relative importance matrix $R$.
Output: The probability of failure $P^{fail}_{ij}$ for each node of each
  infrastructure in $G$.
iterations = 0
while iterations $\leq M$ do
  if iterations = 0 then
    The initial probabilities of failure $\varkappa \sim \mathrm{Exp}(\lambda)$
  else
    The initial probabilities of failure $\varkappa \leftarrow P^{fail}$ of last
      iteration
  end if
  for each infrastructure network $I_i \in G$ do
    for each node $n_{ij} \in I_i$ do
      $P^{intra}_{ij} \leftarrow$ IntraModel($I_i, \varkappa$)
      $P^{fail}_{ij} \leftarrow P^{intra}_{ij}$
    end for
  end for
  for every two network $I_i$ and $I_k$ do
    if The edge $n_{ij} \rightarrow n_{kl}$ exists then
      $V^{ij}_{kl} = \gamma^{ij}_{kl} * P^{fail}_{ij}$
      for each node $n_{kl}$ do
    /* Simulate either the best, average or worst case
      scenario */
        if Best case then
          $P^i_{kl} = \min_{(j)} V^{ij}_{kl}$
        else if Worst case then
          $P^i_{kl} = \max_{(j)} V^{ij}_{kl}$
        else if Average case then
      /* Considering uniform distribution*/
          $P^i_{kl} = \frac{1}{|\mathcal{N}_k|} \sum_{n_{i,j} \in \mathcal{N}_k} V^{ij}_{kl}$
        end if
      end for
    end if
  end for
  /* Weighted sum over the relative importance of the parent
    infrastructures */
  for every infrastructure $I_k$ do
    for every infrastructure $I_i$ from where $\exists$
      interdependency edge to $I_k$ do
      for every node $n_{kl} \in I_k$ do
        $P^{inter}_{kl} = \sum_{i=1}^{s} R_{ik} P^i_{kl}$
      end for
    end for
  end for
  /* Combining intra-infrastructure and
    inter-infrastructure vulnerability */
```

3 | DATA COLLECTION AND PREPROCESSING

To implement our proposed framework, a case study with three infrastructure systems, electricity, water, and a small-scale supply chain network, is considered.

3.1 | Electricity infrastructure

A typical electricity infrastructure system consists of generators, buses, lines, and loads (Wood & Wollenberg, 2012). The buses are connected to each other via lines and both the generators and the loads are connected to the

ALGORITHM 3 Continued

```
    for every infrastructure $I_k$ do
        for every node $n_{kl} \in I_k$ do
            $P_{kl}^{fail} = P_{ij}^{intra} + P_{ij}^{inter} - (P_{ij}^{intra} * P_{ij}^{inter})$
        end for
    end for
    $iterations = iterations + 1$
end while
for each node $n_{ij}$ in each infrastructure network $I_i \in G$ do
    return $P_{ij}^{final}$
end for
```

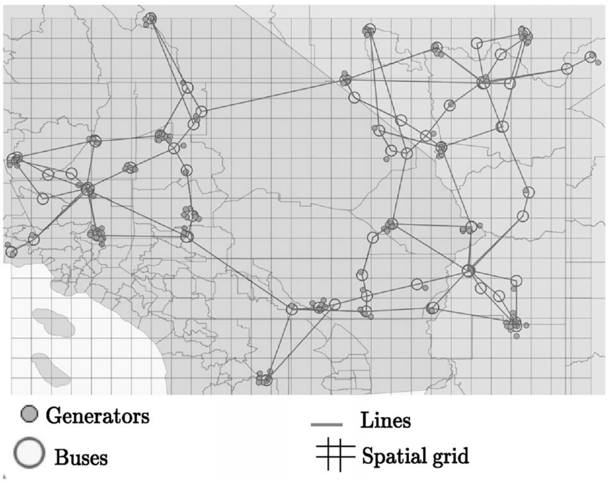


FIGURE 5 The layout of the electricity infrastructure system placed over the maps of the states of Arizona, California, and Nevada.

buses. Each line is originating from a source bus and ends up at a destination bus. The hypothetical node–network data representing a typical power grid is leveraged for our analysis. These data are obtained from the Reliability Test System Grid Modernization Lab Consortium (RTS GMLC) (RTS-GMLC, 2021). The data are geocoded and a failure probability is associated with each component (generators, buses, and lines). Using QGIS, a grid with 0.25° horizontal and vertical spacing is constructed. This power grid is placed over the maps of California, Arizona, and Nevada as shown in Figure 5. The initial hourly failure rates of the components (generators, buses, and lines) are obtained from the RTS-GMLC data set. A summary of the initial failure rates of the components is provided in Table 2.

3.2 | Water distribution network

In the literature, for water distribution network (WDN), hypothetical networks like Anytown, Colorado Springs Utilities, EXNET, or Richmond are extensively used with different types of topologies like grid iron, ring system, radial system, or dead-end system (Mazumder et al., 2018). However, none of these hypothetical networks are geocoded. In a general WDN, water is brought to the treatment plants from the sources using a pumping or gravity system. Then, from the treatment plants, water is stored in storage reservoirs. Finally, the water is brought and temporarily stored in distribution reservoirs to meet the fluctuating demands (Sincero & Sincero, 1995). In this study, a hypothetical WDN with a total of 30 nodes, out of which three are sources, five are treatment plants, six storage reservoirs, and 16 distribution reservoirs with a topology similar to the radial system is considered. The simulated WDN is placed on the same geographical boundary of the electricity infrastructure for the ease of analysis. In Figure 6, the spatial distribution of the WDN is shown. In Table 3, the mean and the standard deviation of the hourly rates of failure for different components of the WDN are depicted. Note that, these hypothetical values are arbitrarily selected by the researchers of this study, and may not depict the actual failure rates of the components in a real-life scenario. However, not to mention that these parameters can be updated easily in the presence of actual

TABLE 2 Summary of the initial failure rates of the components of the electricity infrastructure.

Component	Mean failure rate (λ_{base})	Maximum failure rate	Minimum failure rate	Standard deviation (σ_{base})
Generators	.003	.012	.001	.001
Lines	.007	.02	.001	.003
Buses	.002	.01	.001	.001

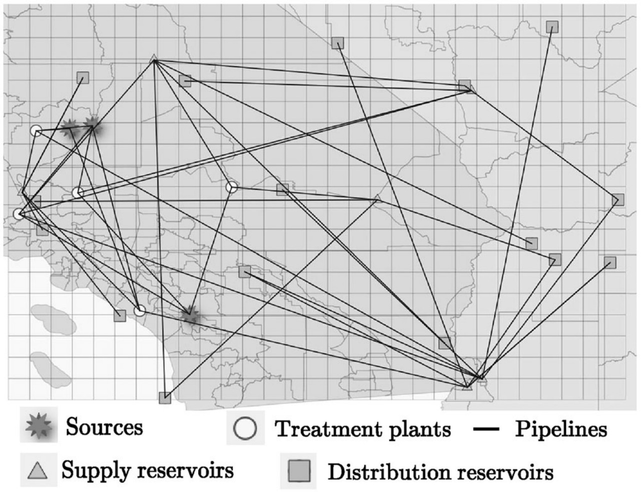


FIGURE 6 The layout of the water distribution system.

TABLE 3 Summary of the initial failure rates of the components of the water distribution network.

Component	Mean failure rate (λ_{base})	Standard deviation (σ_{base})
Sources	.005	.001
Treatment plants	.008	.001
Storage reservoirs	.009	.002
Distribution reservoirs	.01	.002
Pipelines	.01	.001

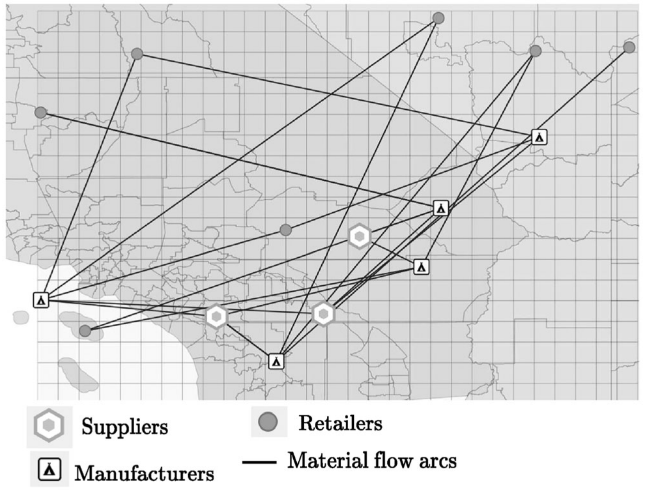


FIGURE 7 The layout of the supply chain network.

data or expert opinion without loss of generality of the overall framework.

3.3 | Supply chain network

A typical supply chain network (SCN) consists of suppliers, manufacturers, and retailers, where material flows between the suppliers and manufacturers, and between manufacturers and retailers as represented by the arcs of the network (Tang et al., 2016). In this study, a hypothetical single-commodity SCN with a total of 15 nodes, out of which there are three supplier nodes, five manufacturer nodes, and seven retailer nodes, is considered. The SCN is placed over the same geo-grid of the electricity and water distribution network as depicted in Figure 7. In Table 4, the mean and standard deviation of the initial hourly failure rates of the components of the hypothetical supply chain network considered in this study are summarized. Again, in the presence of an actual network and data, the rates can be updated according to the user inputs.

TABLE 4 Summary of the initial failure rates of the components of the supply chain network.

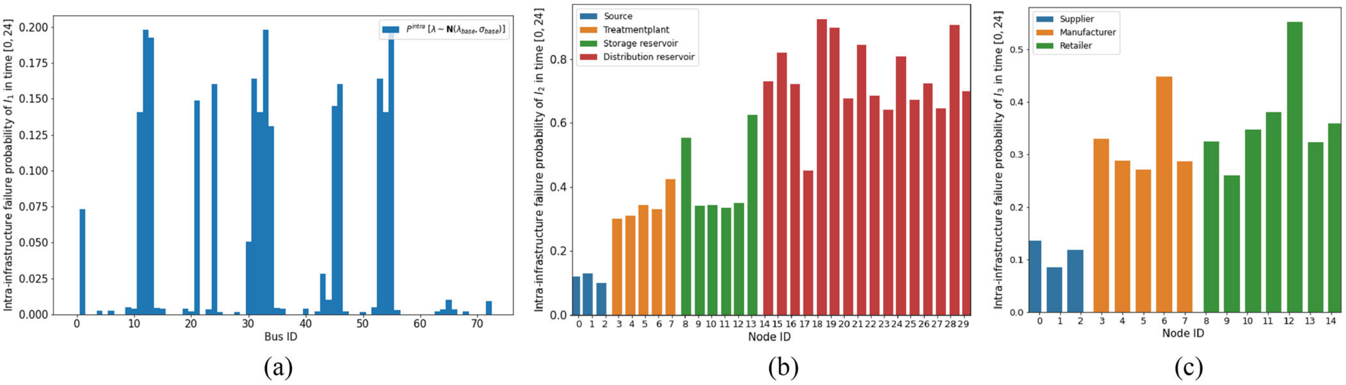
Component	Mean failure rate (λ_{base})	Standard deviation (σ_{base})
Suppliers	.005	.001
Manufacturers	.008	.001
Retailers	.009	.002
Material flow arcs	.01	.001

4 | RESULTS

Following data pre-processing, the intra- and inter-infrastructure vulnerability and finally the comprehensive vulnerability are estimated as described in Section 2. As mentioned before, in this study, the vulnerability of infrastructure represents the dynamic probability of failure as a function of time, which is the failure probability of each of the infrastructure components in time $[0, t]$, where $t \in [0, 24]$.

4.1 | Intra-infrastructure failure probability estimation

In this section, our key findings on the failure probabilities of each infrastructure arising from the intra-infrastructure connections and the cascade propagation within a network are presented. For the *electricity infrastructure* (I_1), the mean failure rates of the different buses, generators, and transmission lines are obtained from sampling with replacement from a normal distribution with mean λ_{base} and standard deviation σ_{base} as depicted in Table 2. The chi-square goodness-of-fit test (Pearson, 1900) is performed to identify that the mean rates of failure depicted in the RTS-GMLC data can be approximated using a normal distribution. For example, for the generators, the rate is assumed to be normally distributed with mean 0.003 and standard deviation 0.001, and the actual failure rates of each generator are obtained from a sampling of this normal distribution. Similarly, for the WDN (I_2) and the supply chain network (I_3), the initial failure rate of each individual component is obtained from a sampling of a normal distribution with mean and standard deviation as depicted in Tables 3 and 4, respectively. The failure time of each infrastructure component follows an exponential distribution with the realized rate of the particular component, which is well considered in literature (Boudali & Dugan, 2006). That is, the initial probability of failure due to intrainfrastructure cascade in time $[0, t]$ is $P^{intra}(t) = 1 - e^{-\lambda t}$, where $\lambda \sim \mathbf{N}(\lambda_{base}, \sigma^2_{base})$. The distribution of λ



(a)

(b)

(c)

FIGURE 8 The component (node) wise probabilities of failure in time [0,24] due to intrainfrastructure cascade for (a) the electricity infrastructure considering the buses as the components; (b) the water distribution network where the node IDs 0 to 2 represent the source nodes, 3 to 7 represent the treatment plants, 8 to 13 are the storage reservoirs, and 14 to 29 represent the distribution reservoirs; and (c) the supply chain network, where the node IDs 0 to 2 represent the supplier nodes, 3 to 7 represent the manufacturer nodes, and 8 to 14 are the retailer nodes.

can be identified using a goodness-of-fit test. Furthermore, the sensitivity of the parameter λ can be identified using a sensitivity analysis framework by alternating the mean of the distribution of λ (e.g., in case of a disaster, it is reasonable to assume that the mean failure rate increases, i.e., say, $\lambda \sim \mathbf{N}(\lambda_{base} + \sigma_{base}, \sigma^2_{base})$). Ganguly et al. described such a sensitivity analysis framework in detail for sensitivity analysis of model parameters applied to crime analysis (Ganguly & Mukherjee, 2021) and mental health prediction (Mukherjee et al., 2021). Such a framework has also been used in the scientific domain of infrastructure risk assessment using data-driven techniques (Masoud-vaziri et al., 2020; Mukherjee & Nateghi, 2019). However, in this paper, the failure rate λ is considered to follow a normal distribution with mean λ_{base} and standard deviation σ_{base} identified using the chi-square goodness-of-fit test. Using Algorithm 1, a DFT is constructed for each of the infrastructures and the failure probabilities for each component of the networks due to the failure propagation within the network are obtained. The failure probabilities of each infrastructure component in time [0,24] or within 24 h due to the cascading failure within the network have been depicted in Figure 8. Furthermore, a diagnostic test is performed where it is found that the intra-infrastructure vulnerability of a node is particularly sensitive to the amount of redundancy associated with it, and the vulnerability decreases with increasing redundancy. This observation holds true because of the properties of the WSP gates used in the DFT, which also may hold true if OR gates are used in that context. The redundancy depicts the number of parent nodes associated with a particular node. This supports the findings from previous studies and thus validates our results under the assumptions considered in the study mentioned above (O'Connor & Kleyner, 2012; Rausand et al., 2020). Intuitively, as there exist more parent nodes for a particular node, the failure probability of the input decreases, resulting in a decrease in the vulnerability of the child node as expected (see Figure 9).

4.2 | Inter-infrastructure vulnerability modeling

For an electricity infrastructure to operate successfully, it is assumed that water is required for power-generating operations and cooling the system. Hence, every bus of the electricity infrastructure requires a certain type of service from the distribution reservoirs of the WDN. Similarly, for a WDN to operate, pumps require electricity (Rinaldi et al., 2002). It is considered that the pumps are associated with all the nodes of the WDN, that is, the sources, treatment plants, storage reservoirs, and distribution reservoirs. Hence, all the nodes of the WDN require services from the electricity infrastructure. As a first step of estimating the inter-infrastructure vulnerability, the network of networks is constructed as depicted in Algorithm 2. As the value of Γ is changed, the number of interdependent edges from one infrastructure to the other changes. It is identified that for a high value of Γ, the neighborhood size of a cell is small, and hence, the number of interdependent edges is also small; on the other hand, as Γ decreases, the neighborhood size increases and there can be many potential nodes of a parent infrastructure, which may provide service to a node of the child infrastructure. In Figure 10a and b, respectively, how the number of interdependent edges from the electricity infrastructure (I_1) to the W (I_2) and the SCN (I_3), and from the WDN (I_2) to the electricity infrastructure (I_1) and the SCN (I_3) vary according to Γ have been depicted.

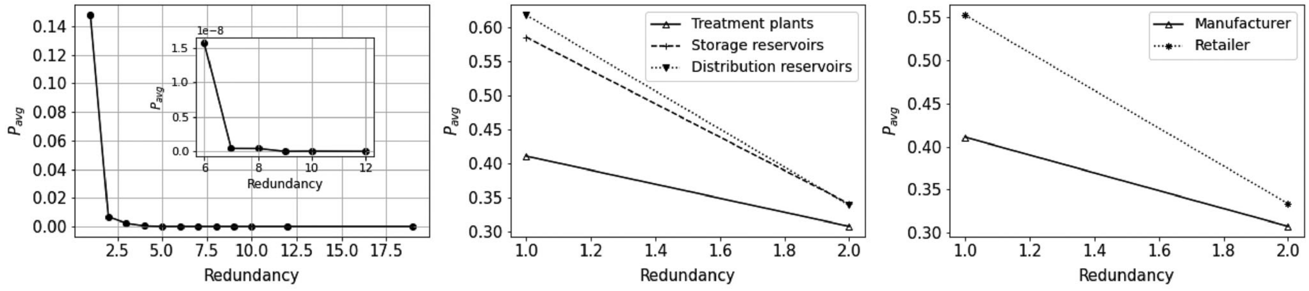


FIGURE 9 Redundancy versus intrainfrastructure failure probabilities of the components for (a) electricity infrastructure, (b) water distribution network, and (c) supply chain network.

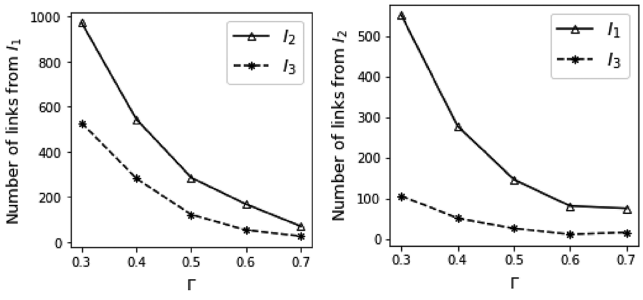
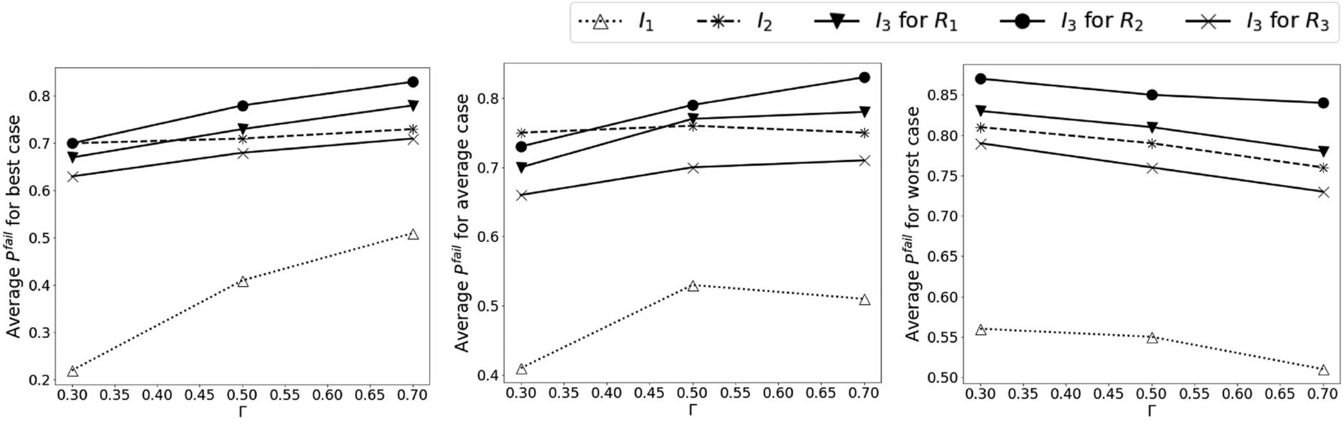


FIGURE 10 Variation in the number of interdependent edges versus Γ, for the parent infrastructure: (a) electricity distribution infrastructure and (b) water distribution network (WDN), considering I_1 as the electricity infrastructure, I_2 as the WDN, and I_3 as the SCN.

TABLE 5 Average interinfrastructure probabilities of failure of one infrastructure induced by another versus Γ for different scenarios after one iteration.

Γ	Scenario	$I_1 \rightarrow I_2$	$I_2 \rightarrow I_1$	$I_1 \rightarrow I_3$	$I_2 \rightarrow I_3$
.3	Best case	$1.01 * 10^{-6}$	.12	$2.3 * 10^{-6}$	.13
	Average case	.04	.38	.043	.33
	Worst case	.11	.40	.099	.35
.5	Best case	$9.2 * 10^{-4}$	.26	$8.8 * 10^{-4}$	.25
	Average case	.046	.37	.044	.32
	Worst case	.08	.39	.073	.33
.7	Best case	$9 * 10^{-3}$	.35	$9 * 10^{-4}$	.31
	Average case	.037	.36	.032	.32
	Worst case	.05	.36	.035	.32

After constructing the network of networks for $\Gamma = 0.5$ (starting point), the inter-infrastructure probabilities of failure induced by one infrastructure to another are estimated as described in Algorithm 2 and Algorithm 3. Table 5 depicts the inter-infrastructure failure probabilities averaged over the nodes of the infrastructure induced by one infrastructure on the other corresponding to the best-, worst-, and average-case scenarios. The column $I_i \rightarrow I_k$ denotes the vulnerability (average probability of failure of the nodes in time [0,24]) of the infrastructure I_k induced by the vulnerability of the interdependent infrastructure network (I_i), that is, $\frac{\sum_{l=1}^{N_k} P^i_{kl}}{N_k}$, where N_k is the number of nodes in infrastructure I_k, and P^i_{kl} is the inter-infrastructure probability of l th node $n_{kl} \in I_k$ induced by I_i. In this study, I_1 is the electricity infrastructure, I_2 is the WDN, and I_3 is the SCN. For example, the column $I_1 \rightarrow I_2$ denotes the vulnerability (average probability of failure of the nodes in time [0,24]) of the WDN (I_2) induced by the vulnerability of electricity infrastructure network (I_1). Various important phenomena regarding the inter-infrastructure failure probabilities for the best-, worst-, and average-case scenarios for different values of Γ are observed. According to Proposition 1, as Γ increases, the average inter-infrastructure failure probabilities of an infrastructure in time $[0, t]$ for the best-case scenario increases. On the other hand, as Γ increases, the inter-infrastructure failure probabilities for the worst-case scenario in time $[0, t]$ decreases. Furthermore, it can be noted that, for a particular value of Γ, the best-case scenario inter-infrastructure failure probability is the lowest, while the worst-case inter-infrastructure probability of failure is the highest. Though the inter-infrastructure failure probabilities are summarized here, for I_3, there exist two different columns $I_1 \rightarrow I_3$ and $I_2 \rightarrow I_3$. Using the relative importance matrix, the inter-infrastructure failure probability is calculated for I_3 as depicted in Algorithm 3. In this study, three relative importance matrices are considered. As I_1 is only dependent on I_2, and I_2 is only dependent on I_1, the entries corresponding to I_1 and I_2 in all the three matrices are 1. According to the construction, all the other entries for the columns corresponding to I_1 and I_2 are 0. In R_1, it is considered that I_3 is equally dependent on I_1 and I_2. Hence, the importance of I_1 and I_2 on I_3 is 0.5 each. However, in R_2, it is assumed that I_1 is less important for I_3 compared to I_2; and in R_3, it is assumed that I_1 is more important for I_3 compared to I_2. While constructing R_2 and R_3, it should be noted that the column sum of the I_3 has to be 1.



(a) (b) (c)

FIGURE 11 The probabilities of failure for each infrastructure versus Γ for different relative importance matrices under consideration for the scenarios: (a) best case, (b) average case, and (c) worst case considering I_1 as the electricity infrastructure, I_2 as the water distribution infrastructure, and I_3 as the supply chain network for different relative importance scenarios of R_1, R_2, and R_3.

$$R_1 = \left[\begin{array}{cccc} & I_1 & I_2 & I_3 \\ I_1 & 0 & 1 & .5 \\ I_2 & 1 & 0 & .5 \\ I_3 & 0 & 0 & 0 \end{array}\right] \quad R_2 = \left[\begin{array}{cccc} & I_1 & I_2 & I_3 \\ I_1 & 0 & 1 & .3 \\ I_2 & 1 & 0 & .7 \\ I_3 & 0 & 0 & 0 \end{array}\right]$$

$$R_3 = \left[\begin{array}{cccc} & I_1 & I_2 & I_3 \\ I_1 & 0 & 1 & .7 \\ I_2 & 1 & 0 & .3 \\ I_3 & 0 & 0 & 0 \end{array}\right]$$

As depicted in Figure 11, the average failure probabilities of the nodes of each infrastructure versus Γ, considering different relative importance matrices R_1, R_2, and R_3, are plotted. As I_1 is only dependent on I_2, and I_2 is only dependent on I_1, the entries in the relative importance matrix are the same for R_1, R_2, and R_3 for the columns corresponding to I_1 and I_2. Hence, in Figure 11a–c, there exists one curve each for I_1 and I_2. However, as I_3 is dependent on both I_1 and I_2, the entries in the R_1, R_2, and R_3 are different, and in each of Figure 11a–c, we have three curves for I_3 each corresponding to the three relative importance matrix. The two important observations from these plots are as follows: (1) The failure probabilities increase as Γ increases for the best-case scenario as depicted in Figure 11a and the failure probabilities decrease as Γ increases for the worst-case scenario, as depicted in Figure 11c. This supports Proposition 1; and (2) for I_3, as we have different curves for the different relative importance matrices, it is observed that the probability of failure is highest for R_2. This is because, in R_2, the importance of I_2 is more and the inherent failure probability of I_2 is more compared to I_1. Hence, the induced vulnerability to I_3 is higher for R_2 compared to R_1 and R_3.

4.3 | Comprehensive vulnerability estimation

Before proceeding with the final step of estimating the comprehensive vulnerability of the interdependent infrastructure systems, first, we hold some of the parameters used in our study constant, depicting our base case, to understand the failure propagation dynamics in the interdependent infrastructure system over time. Considering the mean initial failure probabilities to be the same as the base case with (λ_{base}), $\Gamma = 0.5$, and the relative importance matrix as R_1, the failure probabilities of each node in time [0,24] considering both the intra- and inter-infrastructure vulnerabilities are estimated. First, the failure probabilities for every node of the infrastructures under the three different scenarios, namely, the worst case, the average case, and the best case, corresponding to the different number of iterations are estimated. Then, corresponding to each scenario and the number of iterations, the average probabilities of failure over the nodes of a particular infrastructure are obtained. That is, the average probability of failure of infrastructure I_i is $\frac{\sum_{j=1}^{N_i} P_{ij}^{fail}}{N_i}$, where N_i is the number of nodes in infrastructure I_i. In Figure 12a, the probabilities of failure in time [0,24] for the infrastructures are depicted for the best-case scenario as a function of the number of days (i.e., iterations). It is observed that as the number of iterations (days) increases, the probabilities of failure increase. However, the rate of increase decreases with the increase in the number of iterations. In Figure 12c and b, respectively, the failure probabilities of the infrastructures for the worst-case and average-case scenarios are depicted. Though there exist similar patterns for the different cases, the probabilities of failure for the

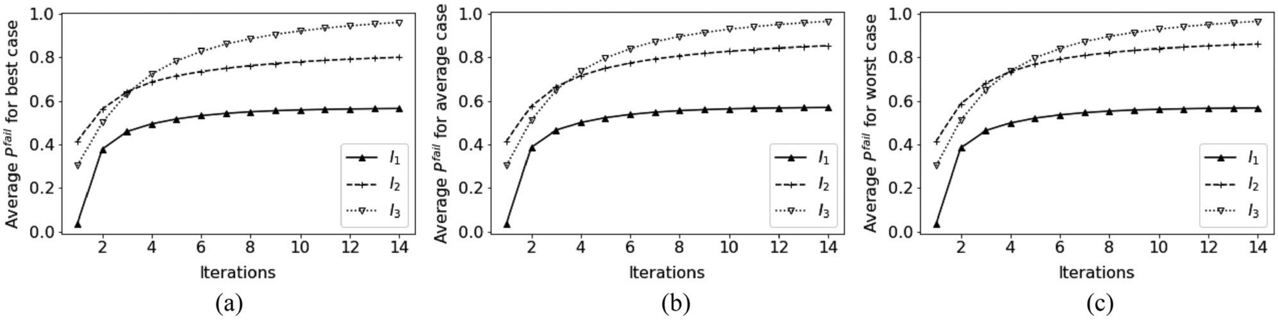


FIGURE 12 Number of iterations versus the average probability of failure of the nodes for each infrastructure in time $t \in [0, 24]$, for (a) best-case scenario, (b) average-case scenario, and (c) worst-case scenario where $\Gamma = .5$ and the relative importance matrix is $R1$, considering I_1 as the electricity infrastructure, I_2 as the water distribution infrastructure, and I_3 as the supply chain network.

worst-case scenario are the highest, followed by the probabilities of failure for the best case scenario. In fact, the probabilities of failure for the best case scenario are observed to be the lowest, as expected. Furthermore, it is observed that with increasing number of iterations (time), the vulnerability of I_3 surpasses the vulnerability of I_2 and I_1. This is because of the fact that, as I_3 is dependent on both I_1 and I_2, the inter-infrastructure vulnerability of I_3 is induced by both the parent infrastructures, as an alternative to I_1 or I_2, which is dependent on a single parent infrastructure.

The key findings from the results obtained using our framework are summarized as follows.

1. The intra-infrastructure vulnerability is observed to be inversely proportional to the number of redundancies inbuilt into the infrastructure system.
2. The infrastructure manager can simulate different values of the initial failure rates (λ) of the components and obtain the associated vulnerability of the infrastructure. It is observed that higher the failure rate of the components, higher is the vulnerability of the infrastructure due to intra-infrastructure cascading failure.
3. For the same value of Γ and the relative importance matrix, it is observed that the failure probabilities due to inter-infrastructure cascade under the worst-case scenario are more than that of the average-case scenario, which in turn is higher than the best-case scenario. The worst-case scenario is realized when there are more critical nodes (less redundant nodes), failure of which induces failure of nodes of the child infrastructure and is well suited for risk-averse conservative design. On the other hand, the best case is realized when there are redundant parent infrastructure nodes and depict the opportunistic or risk-seeking design of the system.
4. The parameter Γ is inversely proportional to the geographical proximity or neighborhood of the components of two infrastructure systems under consideration. As the threshold Γ increases, the neighborhood size decreases. Hence, for a particular infrastructure and particular relative importance matrix, the best-case scenario failure probability increases as Γ increases (geographical neighborhood decreases) due to a decrease in redundancy. On the other hand, for the worst-case scenario, the failure probability decreases as Γ increases (geographical neighborhood decreases), due to a decrease in the number of critical components of parent infrastructure, which may lead to failure of the child component.
5. The vulnerability of an infrastructure is dependent on the importance of each parent infrastructure system. If a particular infrastructure is critically dependent on another highly vulnerable infrastructure, then the vulnerability of the dependent infrastructure also increases.

5 | CONCLUSION

In this research, we present a novel simulation-based approach coupled with time-dependent Bayesian network (BN) analysis to model the vulnerabilities of multiple infrastructure systems arising from the cascading failure propagation within a single infrastructure network (intra-infrastructure) and across other infrastructure systems (inter-infrastructure) owing to the interdependencies. Unlike existing research studies, which unrealistically assume that all relevant information is available to the infrastructure managers for vulnerability estimation, our proposed approach does not assume that the information about the exact service–demand flow between different infrastructure networks is known beforehand, but effectively simulates such interdependencies for vulnerability assessment. Not only that, our proposed approach accounts for the physical, spatial, and informational uncertainties while estimating the multi-infrastructure vulnerability. Specifically, the constructed heuristic-based dynamic fault tree (DFT) accounts for the unavailability of exact information about the parent infrastructure's network topology to the manager of a child infrastructure. To account for the unavailability of exact supply–demand data, different user-defined simulated parameters considering the physical, logical, and geographical dependencies are used to construct the interdependent infrastructure network. Finally, the multi-infrastructure vulnerability is estimated using parameters for geographical proximity, the relative importance of one infrastructure on another, and the risk perception of the infrastructure manager. Leveraging synthetic data on electricity distribution, water distribution, and a supply chain network, our numerical experiments show how the time-based vulnerability of individual infrastructure and interdependent infrastructure changes with the amount of redundancies, the various risk scenarios under consideration, and the relative importance of infrastructure interdependencies.

One of the limitations of our study is that the parameters depicted in the case study are hypothetical. In the presence of real data, these parameters may be updated without any alteration of the overall framework. Another limitation of our study is that, in the presence of exact data, the deterministic supply–demand flow-based models may perform better compared to the proposed simulation-based approach. In this study, we did not analyze the computational complexity of the algorithms as it was out of the scope of the paper. In the future, a detailed computational complexity analysis of the algorithms can be carried out to understand the efficacy of the algorithms. Furthermore, in the presence of more accurate information, this work can be extended to leverage machine learning techniques for better estimation of interdependent infrastructure vulnerability.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

REFERENCES

Adachi, T., & Ellingwood, B. (2008). Serviceability of earthquake-damaged water systems: Effects of electrical power availability and power backup systems on system vulnerability. *Reliability Engineering & System Safety*, *93*, 78–88.

Aghababaei, M., & Koliou, M. (2022). Community resilience assessment via agent-based modeling approach. *Computer-Aided Civil and Infrastructure Engineering*, *38*(6), 1–20.

Alinizzi, M., Chen, S., Labi, S., & Kandil, A. (2018). A methodology to account for one-way infrastructure interdependency in preservation activity scheduling. *Computer-Aided Civil and Infrastructure Engineering*, *33*(11), 905–925.

Allen, E., Chamorro, A., Poulos, A., Castro, S., de la Llera, J. C., & Echaveguren, T. (2022). Sensitivity analysis and uncertainty quantification of a seismic risk model for road networks. *Computer-Aided Civil and Infrastructure Engineering*, *37*(4), 516–530.

Apostolakis, G. E., & Lemon, D. M. (2005). A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. *Risk Analysis*, *25*(2), 361–376.

Barker, K., & Haimes, Y. Y. (2009a). Assessing uncertainty in extreme events: Applications to risk-based decision making in interdependent infrastructure sectors. *Reliability Engineering & System Safety*, *94*(4), 819–829.

Barker, K., & Haimes, Y. Y. (2009b). Uncertainty analysis of interdependencies in dynamic infrastructure recovery: Applications in risk-based decision making. *Journal of Infrastructure Systems*, *15*(4), 394–405.

Bjerga, T., Aven, T., & Flage, R. (2018). Completeness uncertainty. In *Knowledge in risk assessment and management* (pp. 127–141) (eds. T. Aven and E. Zio). John Wiley & Sons, Ltd.

Boudali, H., Crouzen, P., & Stoelinga, M. (2010). A rigorous, compositional, and extensible framework for dynamic fault tree analysis. *IEEE Transactions on Dependable and Secure Computing*, *7*(2), 128–143.

Boudali, H., & Dugan, J. (2006). A continuous-time Bayesian network reliability modeling, and analysis framework. *IEEE Transactions on Reliability*, *55*, 86–97.

Brown, T., Beyeler, W., & Barton, D. (2004). Assessing infrastructure interdependencies: The challenge of risk analysis for complex adaptive systems. *IJCIS*, *1*, 108–117.

Casalicchio, E., Galli, E., & Ottaviani, V. (2009). MobileOnRealEnvironment-GIS: A federated mobile network simulator of mobile nodes on real geographic data. In *2009 13th IEEE/ACM international symposium on distributed simulation and real time applications, Singapore, October 25-28*, (pp. 255–258); The Institute of Electrical and Electronics Engineers (IEEE).

Casalicchio, E., Galli, E., & Tucci, S. (2007). Federated agent-based modeling and simulation approach to study interdependencies in IT critical infrastructures. In *Proceedings IEEE international symposium on distributed simulation and real-time applications* (pp. 182–189); The Institute of Electrical and Electronics Engineers (IEEE).

Cavallaro, M., Asprone, D., Latora, V., Manfredi, G., & Nicosia, V. (2014). Assessment of urban ecosystem resilience through hybrid social–physical complex networks. *Computer-Aided Civil and Infrastructure Engineering*, *29*, 608–625.

Cavdaroglu, B., Hammel, E., Mitchell, J., Sharkey, T., & Wallace, W. (2013). Integrating restoration and scheduling decisions for disrupted interdependent infrastructure systems. *Annals of Operations Research*, *203*, 1–16.

Chen, C. L., Zheng, Q. P., Veremyev, A., Pasiliao, E. L., & Boginski, V. (2021). Failure mitigation and restoration in interdependent networks via mixed-integer optimization. *IEEE Transactions on Network Science and Engineering*, *8*(2), 1293–1304.

Codetta-Raiteri, D., & Portinale, L. (2015). Dynamic Bayesian networks for fault detection, identification, and recovery in autonomous spacecraft. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *45*, 13–24.

Cormen, T., Leiserson, C., Rivest, R., & Stein, C. (2001). *Introduction to algorithms*. (Vol. 42); MIT Press.

Dong, S., Yu, T., Farahmand, H., & Mostafavi, A. (2020). Bayesian modeling of flood control networks for failure cascade characterization and vulnerability assessment. *Computer-Aided Civil and Infrastructure Engineering*, *35*(7), 668–684.

Dueñas-Osorio, L., Craig, J. I., & Goodno, B. J. (2007). Seismic response of critical interdependent networks. *Earthquake Engineering & Structural Dynamics*, *36*(2), 285–306.

Dueñas-Osorio, L., Craig, J. I., Goodno, B. J., & Bostrom, A. (2007). Interdependent response of networked systems. *Journal of Infrastructure Systems*, *13*(3), 185–194.

Dugan, J., Bavuso, S., & Boyd, M. (1992). Dynamic fault-tree models for fault-tolerant computer systems. *IEEE Transactions on Reliability*, *41*, 363–377.

Eusgeld, I., Nan, C., & Dietz, S. (2011). "System-of-systems" approach for interdependent critical infrastructures. *Reliability Engineering & System Safety*, *96*(6), 679–686.

Fang, Y., & Zio, E. (2019). An adaptive robust framework for the optimization of the resilience of interdependent infrastructures under natural hazards. *European Journal of Operational Research*, *276*(3), 1119–1136.

Faturechi, R., & Miller-Hooks, E. (2014). A mathematical framework for quantifying and optimizing protective actions for civil infrastructure systems. *Computer-Aided Civil and Infrastructure Engineering*, *29*(8), 572–589.

Franchin, P., & Cavalieri, F. (2022). Probabilistic assessment of civil infrastructure resilience to earthquakes. *Computer-Aided Civil and Infrastructure Engineering*, *30*(7), 583–600.

Fu, G., Wilkinson, S., & Dawson, R. J. (2016). A spatial network model for civil infrastructure system development. *Computer-Aided Civil and Infrastructure Engineering*, *31*(9), 661–680.

Galbusera, L., Giannopoulos, G., Argyroudis, S., & Kakderi, K. (2018). A Boolean networks approach to modeling and resilience analysis of interdependent critical infrastructures. *Computer-Aided Civil and Infrastructure Engineering*, *33*(12), 1041–1055.

Ganguly, P., & Mukherjee, S. (2021). A multifaceted risk assessment approach using statistical learning to evaluate socio-environmental factors associated with regional felony and misdemeanor rates. *Physica A: Statistical Mechanics and Its Applications*, *574*, 125984.

Gong, J., Mitchell, J. E., Krishnamurthy, A., & Wallace, W. A. (2014). An interdependent layered network model for a resilient supply chain. *Omega*, *46*, 104–116.

González, A. D., Chapman, A., Dueñas-Osorio, L., Mesbahi, M., & D'Souza, R. M. (2017). Efficient infrastructure restoration strategies using the recovery operator. *Computer-Aided Civil and Infrastructure Engineering*, *32*(12), 991–1006.

González, A. D., Dueñas-Osorio, L., Sánchez-Silva, M., & Medaglia, A. L. (2016). The interdependent network design problem for optimal infrastructure system restoration. *Computer-Aided Civil and Infrastructure Engineering*, *31*(5), 334–350.

Haimes, Y. Y., & Jiang, P. (2001). Leontief-based model of risk in complex interconnected infrastructures. *Journal of Infrastructure Systems*, *7*(1), 1–12.

Hernandez-Fajardo, I., & Dueñas-Osorio, L. (2013). Probabilistic study of cascading failures in complex interdependent lifeline systems. *Reliability Engineering & System Safety*, *111*, 260–272.

Krishnamurthy, V., Kwasinski, A., & Dueñas-Osorio, L. (2016). Comparison of power and telecommunications dependencies and interdependencies in the 2011 Tohoku and 2010 Maule earthquakes. *Journal of Infrastructure Systems*, *22*(3), 04016013.

Lee II, E. E., Mitchell, J. E., & Wallace, W. A. (2007). Restoration of services in interdependent infrastructure systems: A network flows approach. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *37*(6), 1303–1317.

Lu, L., Wang, X., Ouyang, Y., Roningen, J., Myers, N., & Calfas, G. (2018). Vulnerability of interdependent urban infrastructure networks: Equilibrium after failure propagation and cascading impacts. *Computer-Aided Civil and Infrastructure Engineering*, *33*(4), 300–315.

Mahmoud, H., & Chulahwat, A. (2018). Spatial and temporal quantification of community resilience: Gotham City under attack. *Computer-Aided Civil and Infrastructure Engineering*, *33*(5), 353–372.

Masoudvaziri, N., Ganguly, P., Mukherjee, S., & Sun, K. (2020). Integrated risk-informed decision framework to minimize wildfire-induced power outage risks: A county-level spatiotemporal analysis. In *Proceedings of the 30th European safety and reliability conference and the 15th probabilistic safety assessment and management conference (eds. Piero Baraldi, Francesco Di Maio and Enric Zio)*. Venice Italy, (pp. 4492–4500).

Mazumder, R. K., Salman, A., Li, Y., & Yu, X. (2018). Performance evaluation of water distribution systems and asset management. *Journal of Infrastructure Systems*, *24*, 03118001.

Mukherjee, S., Boamah, E. F., Ganguly, P., & Botchwey, N. (2021). A multi-level scenario-based predictive analytics framework to model community mental health—built environment nexus. *Scientific Reports*, *11*(1), 17548.

Mukherjee, S., & Nateghi, R. (2019). A data-driven approach to assessing supply inadequacy risks due to climate-induced shifts in electricity demand. *Risk Analysis*, *39*(3), 673–694.

Najafi, M. R., Zhang, Y., & Martyn, N. (2021). A flood risk assessment framework for interdependent infrastructure systems in coastal environments. *Sustainable Cities and Society*, *64*, 102516.

Nan, C., & Sansavini, G. (2017). A quantitative method for assessing resilience of interdependent infrastructures. *Reliability Engineering & System Safety*, *157*, 35–53.

Nocera, F., & Gardoni, P. (2022). Selection of the modeling resolution of infrastructure. *Computer-Aided Civil and Infrastructure Engineering*, *37*(11), 1352–1367.

Nurre, S. G., Cavdaroglu, B., Mitchell, J. E., Sharkey, T. C., & Wallace, W. A. (2012). Restoring infrastructure systems: An integrated network design and scheduling (INDS) problem. *European Journal of Operational Research*, *223*(3), 794–806.

O'Connor, P., & Kleyner, A. (2012). *Practical reliability engineering* (5th ed.), John Wiley & Sons.

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, *121*, 43–60.

Ouyang, M., & Fang, Y. (2017). A mathematical framework to optimize critical infrastructure resilience against intentional attacks. *Computer-Aided Civil and Infrastructure Engineering*, *32*(11), 909–929.

Ouyang, M., Hong, L., Mao, Z., Yu, M. H., & Qi, F. (2009). A methodological approach to analyze vulnerability of interdependent infrastructures. *Simulation Modelling Practice and Theory*, *17*, 817–828.

Pearson, K. (1900). On the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. *Philosophical Magazine and Journal of Science*, *50*(302), 157–175.

Quantum Geographic Information System Information (QGIS). (2021). *Qgis*. https://www.qgis.org/en/site/

Rausand, M., Barros, A., & Hoyland, A. (2020). *System reliability theory: Models, statistical methods, and applications, John Wiley & Sons*.

Reilly, A. C., Baroud, H., Flage, R., & Gerst, M. D. (2021). Sources of uncertainty in interdependent infrastructure and their implications. *Reliability Engineering & System Safety*, *213*, 107756.

Rinaldi, S., Peerenboom, J., & Kelly, T. (2002). Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE*, *21*, 11–25.

RTS-GMLC. (2021). *Reliability test system grid modernization lab consortium*. https://github.com/GridMod/RTS-GMLC

Sharkey, T. C., Cavdaroglu, B., Nguyen, H., Holman, J., Mitchell, J. E., & Wallace, W. A. (2015). Interdependent network restoration: On the value of information-sharing. *European Journal of Operational Research*, *244*(1), 309–321.

Sharma, N., Tabandeh, A., & Gardoni, P. (2020). Regional resilience analysis: A multiscale approach to optimize the resilience of interdependent infrastructure. *Computer-Aided Civil and Infrastructure Engineering*, *35*(12), 1315–1330.

Sincero, A. P., & Sincero, G. A. (1995). *Environmental engineering: A design approach*. Prentice Hall.

Song, G., Chen, H., & Guo, B. (2014). A layered fault tree model for reliability evaluation of smart grids. *Energies*, *7*(8), 4835–4857.

Talebiyan, H., & Duenas-Osorio, L. (2020). Decentralized decision making for the restoration of interdependent networks. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*, *6*(2), 04020012.

Tang, L., Jing, K., He, J., & Stanley, H. E. (2016). Complex interdependent supply chain networks: Cascading failure and robustness. *Physica A: Statistical Mechanics and Its Applications*, *443*, 58–69.

Utne, I., Hokstad, P., & Vatn, J. (2011, 06). A method for risk modeling of interdependencies in critical infrastructures. *Reliability Engineering & System Safety*, *96*, 671–678.

Veremyev, A., Sorokin, A., Boginski, V., & Pasiliao, E. (2014, 02). Minimum vertex cover problem for coupled interdependent networks with cascading failures. *European Journal of Operational Research*, *232*, 499–511.

Volkanovski, A., Čepin, M., & Mavko, B. (2009). Application of the fault tree analysis for assessment of power system reliability. *Reliability Engineering & System Safety*, *94*(6), 1116–1127.

Wallace, W., Mendonça, D., Lee, E., Mitchell, J., & Chow, J. (2003). Managing disruptions to critical interdependent infrastructures in the context of the 2001 world trade center attack. In *Beyond September 11th: An account of post-disaster research*, Special publication #39. Natural Hazards Research and Applications Applications Information Center, University of Colorado, (pp 165–198).

Wang, H., Abdin, A. F., Fang, Y. P., & Zio, E. (2022). Resilience assessment of electrified road networks subject to charging station failures. *Computer-Aided Civil and Infrastructure Engineering*, *37*(3), 300–316.

Wang, Y., Yu, J. Z., & Baroud, H. (2022). Generating synthetic systems of interdependent critical infrastructure networks. *IEEE Systems Journal*, *16*(2), 3191–3202.

Wang, Z., Wang, Q., Zukerman, M., Guo, J., Wang, Y., Wang, G., & Moran, B. (2017). Multiobjective path optimization for critical infrastructure links with consideration to seismic resilience. *Computer-Aided Civil and Infrastructure Engineering*, *32*(10), 836–855.

Watson, H. A. (1961). *Bell telephone laboratories, launch control saf. study*. Bell Teleph. Lab. Murray Hill, NJ USA.

Wood, A., & Wollenberg, B. (2012). *Power generation, operation, and control*. Wiley.

Xiong, C., Huang, J., & Lu, X. (2020). Framework for city-scale building seismic resilience simulation and repair scheduling with labor constraints driven by time–history analysis. *Computer-Aided Civil and Infrastructure Engineering*, *35*(4), 322–341.

Yagan, O., Qian, D., Zhang, J., & Cochran, D. (2012). Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness. *IEEE Transactions on Parallel and Distributed Systems*, *23*(9), 1708–1721.

Yang, Y., Ng, S. T., Zhou, S., Xu, F. J., & Li, H. (2020). Physics-based resilience assessment of interdependent civil infrastructure systems with condition-varying components: A case with stormwater drainage system and road transport system. *Sustainable Cities and Society*, *54*, 101886.

Zavadskas, E. K., Antucheviciene, J., Vilutiene, T., & Adeli, H. (2018). Sustainable decision-making in civil engineering, construction and building technology. *Sustainability*, *10*(1), 14.

Zhang, J., Li, G., & Zhang, M. (2022). Multi-objective optimization for community building group recovery scheduling and resilience evaluation under earthquake. *Computer-Aided Civil and Infrastructure Engineering*, *38*(6), 1–20.

Zhang, N., & Alipour, A. (2023). A stochastic programming approach to enhance the resilience of infrastructure under weather-related risk. *Computer-Aided Civil and Infrastructure Engineering*, *38*(4), 411–432.

Zhang, P., & Peeta, S. (2011). A generalized modeling framework to analyze interdependencies among infrastructure systems. *Transportation Research Part B: Methodological*, *45*(3), 553–579.

Zio, E., & Sansavini, G. (2011, 04). Modeling interdependent network systems for identifying cascade-safe operating margins. *IEEE Transactions on Reliability*, *60*, 94–101.

How to cite this article: Ganguly, P., & Mukherjee, S. (2023). A simulation-based generalized framework to model vulnerability of interdependent critical infrastructure systems under incomplete information. *Computer-Aided Civil and Infrastructure Engineering*, 1–23. https://doi.org/10.1111/mice.12999

APPENDIX: DERIVATION OF CLOSED-FORM SOLUTIONS

Using the unit step function defined by

$$u(t-\tau) = \begin{cases} 0, & \text{if } t < \tau \\ \frac{1}{2}, & \text{if } t = \tau \\ 1, & \text{if } t > \tau \end{cases}$$

and the impulse function or the Dirac delta function defined by

$$\delta(t-\tau) = 0, \quad \text{if } t \neq \tau \quad \text{and} \quad \int_{-\infty}^{\infty} \delta(t-\tau)dt = 1$$

we describe the probability density function (PDF) of the AND, OR, and the WSP gate of the DFT.

AND gate: If the nodes A and B with the marginal PDF $f_A(a)$ and $f_B(b)$, respectively, are connected by *AND* gate to produce the output X, then the conditional PDF of $f_{X|A,B}(x|a,b)$ is given by

$$f_{X|A,B}(x|a,b) = u(b-a)\delta(x-b) + u(a-b)\delta(x-a)$$

where the first term denotes when A fails before B, the state of X is same as the state of B, which failed later; and the second term denotes when B fails before A, then the state of X is the same as the state of A. The marginal probability density of X is obtained by marginalizing the joint distribution $f_{ABX}(a,b,x)$ as

$$\begin{aligned} f_X(x) &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_{ABX}(a,b,x)dbda \\ &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_{X|AB}(x|a,b)f_B(b)f_A(a)dbda \\ &= [F_B(b)F_A(a)]' \end{aligned}$$

Let us consider that the PDF of failure time of A follows an exponential distribution with rate λ_A and for B, the PDF of failure time is exponentially distributed with rate λ_B. Hence, the probability of failure of X in time $[0,t]$ is given by

$$\begin{aligned} F_X(t) = \int_0^t f_X(x)dx = F_B(t)F_A(t) = 1 - e^{-\lambda_A t} - e^{-\lambda_B t} \\ + e^{-(\lambda_A+\lambda_B)t} \end{aligned}$$

OR gate: If the nodes A and B with the marginal PDF $f_A(a)$ and $f_B(b)$, respectively, are connected by *OR* gate to produce the output X, then the conditional PDF of $f_{X|A,B}(x|a,b)$ is given by

$$f_{X|A,B}(x|a,b) = u(b-a)\delta(x-a) + u(a-b)\delta(x-b)$$

where the first term denotes if A fails before B, then the state of X is the same as the state of A, which fails first; on the other hand, if B fails before A, then the state of X is the same as the state of B. Using the similar procedure of the *AND* gate, we have

$$\begin{aligned} f_X(x) = \int_0^{\infty}\int_0^{\infty} f_{ABX}dbda = f_A(x) + f_B(x) \\ - [F_B(b)F_A(a)]' \end{aligned}$$

Finally, considering for A and B, the time of failure follows an exponential distribution with rates λ_A and λ_B, respectively, the probability of failure of X in time $[0,t]$ is given by

$$\begin{aligned} F_X(t) &= \int_0^t f_X(x)dx = F_A(t) + F_B(t) - F_B(t)F_A(t) \\ &= 1 - e^{-(\lambda_A+\lambda_B)t} \end{aligned}$$

WSP gate: In a two-input WSP gate, say, A is the primary unit and B is the spare unit. When the system starts, the component A starts working and the component B is in standby or dormant mode. In dormant mode, the failure rate is reduced by a factor α. First, to model the failure of the node B, we have

$$\begin{aligned} & f_{B|A}(b|a) \\ &\quad = u(a-b)\alpha f_{B_i}(b)[1-F_{B_i}(b)]^{\alpha-1} \\ &\qquad + u(b-a)f_{B_i}(b-a)[1-F_{B_i}(a)]^{\alpha} \end{aligned}$$

where f_{B_i} and F_{B_i} are the in isolation density and cumulative distributions. Considering the exponential time of failure for A and B_i in isolation with rates λ_A and λ_B, respectively, the PDF of node B is given as

$$\begin{aligned} f_B(b) = \int_0^{\infty} & f_{B|A}(b|a)f_A(a)da, \\ &= \alpha f_{B_i}(b)[1-F_{B_i}(b)]^{\alpha-1}[1-F_A(b)] \\ &\quad + \int_0^b f_{B_i}(b-a)[1-F_{B_i}(a)]^{\alpha} f_A(a)da \\ &= \alpha\lambda_B e^{-b(\lambda_A+\lambda_B\alpha)} + \frac{\lambda_A\lambda_B}{\lambda_B - \lambda_B\alpha - \lambda_A}[e^{-b\lambda_A - b\alpha\lambda_B} \\ &\quad - e^{-\lambda_B b}] \end{aligned}$$

Hence, the probability of failure of B in $[0,t]$ is given by

$$\begin{aligned} & F_B(t) \\ &= \int_0^t f_B(b)db, = \int_0^t \alpha\lambda_B e^{-b(\lambda_A+\lambda_B\alpha)}db \\ &\quad + \int_0^t \frac{\lambda_A\lambda_B}{\lambda_B - \lambda_B\alpha - \lambda_A}\left[e^{-b\lambda_A - b\alpha\lambda_B} - e^{-\lambda_B b}\right]db \\ &= \frac{\alpha\lambda_B\left(e^{-t(\lambda_A+\alpha\lambda_B)} - 1\right)}{-\lambda_A - \alpha\lambda_B} \\ &\quad - \frac{\lambda_A(-(e^{-\lambda_B t} - 1)(\lambda_A + \alpha\lambda_B) + \lambda_B e^{-t(\lambda_A+\alpha\lambda_B)} - \lambda_B)}{(\lambda_A + \alpha\lambda_B)(\lambda_B - \lambda_A - \alpha\lambda_B)} \end{aligned}$$

The output X of the WSP is an *AND* gate, that is, $X =$ *A AND B*.

Hence, the probability of failure of X in time $[0,t]$ is given by

$$\begin{aligned} F_X(t) = (1 - e^{-\lambda_A t})\Bigg(\frac{\alpha\lambda_B(e^{-t(\lambda_A+\alpha\lambda_B)} - 1)}{-\lambda_A - \alpha\lambda_B} \\ - \frac{\lambda_A(-(e^{-\lambda_B t} - 1)(\lambda_A + \alpha\lambda_B) + \lambda_B e^{-t(\lambda_A+\alpha\lambda_B)} - \lambda_B)}{(\lambda_A + \alpha\lambda_B)(\lambda_B - \lambda_A - \alpha\lambda_B)}\Bigg) \end{aligned}$$