ERDC/ITL MP-21-2

US Army Corps
of Engineers®
Engineer Research and
Development Center

A Framework for Modeling and Assessing System Resilience Using a Bayesian Network

A Case Study of an Interdependent Electrical Infrastructure System

Niamat Ullah Ibne Hossain, Raed Jaradat, Seyedmohsen Hosseini,
Mohammad Marufuzzaman, and Randy K. Buchanan

April 2021

Information Technology Laboratory

The U.S. Army Engineer Research and Development Center (ERDC) solves the nation's toughest engineering and environmental challenges. ERDC develops innovative solutions in civil and military engineering, geospatial sciences, water resources, and environmental sciences for the Army, the Department of Defense, civilian agencies, and our nation's public good. Find out more at www.erdc.usace.army.mil.

To search for other technical reports published by ERDC, visit the ERDC online library at https://erdclibrary.on.worldcat.org/discovery.

ERDC/ITL MP-21-2
April 2021

A Framework for Modeling and Assessing System Resilience Using a Bayesian Network

A Case Study of an Interdependent Electrical Infrastructure System

Randy K. Buchanan

Information Technology Laboratory
U.S. Army Engineer Research and Development Center
3909 Halls Ferry Road
Vicksburg, MS 39180

Niamat Ullah Ibne Hossai, Raed Jaradat, and Mohammad Marufuzzaman

Department of Industrial and Systems Engineering
Mississippi State University
75 B. S. Hood Road
Starkville, MS 39762

Seyedmohsen Hosseini

Industrial Engineering Technology
University of Southern Mississippi
3090 Halls Ferry Road
Long Beach, MS 39560

Final report

Prepared for U.S. Army Corps of Engineers
Washington, DC 20314-1000

Under Program Element 0603461A, Project Number DW5, Task Number 01

Preface

This study was conducted for the U.S. Army Corps of Engineers and funded under Army Direct Program Element Number 0603461A, Project Number DW5, Task Number 01. The technical monitors were Dr. Simon R. Goerger and Dr. Randy K. Buchanan.

The work was performed by the Institute for Systems Engineering Research (ISER) (CEERD-IER) of the Computational Science and Engineering Division, U.S. Army Engineer Research and Development Center, Information Technology Laboratory (ERDC-ITL). At the time of publication, Dr. Simon R. Goerger was Director, IER; and Dr. Jerrell R. Ballard Jr. was Chief, IE. The Technical Director was Dr. Robert Wallace. The Deputy Director of ERDC-ITL was Ms. Patti S. Duett, and the Director was Dr. David A. Horner.

This paper was originally published in the *International Journal of Critical Infrastructure Protection* on 13 February 2019.

The Commander of ERDC was COL Teresa A. Schlosser and the Director was Dr. David W. Pittman.

A Framework for Modeling and Assessing System Resilience Using a Bayesian Network:

A Case Study of an Interdependent Electrical Infrastructure System

Abstract

This research utilizes Bayesian network to address a range of possible risks to the electrical power system and its interdependent networks (EIN) and offers possible options to mitigate the consequences of a disruption. The interdependent electrical infrastructure system in Washington, D.C. is used as a case study to quantify the resilience using the Bayesian network. Quantification of resilience is further analyzed based on different types of analysis such as forward propagation, backward propagation, sensitivity analysis, and information theory. The general insight drawn from these analyses indicate that reliability, backup power source, and resource restoration are the prime factors contributed towards enhancing the resilience of an interdependent electrical infrastructure system.

1. Introduction

United States economic sectors are highly reliant on the electric power industry with generated energy being utilized to serve its people and conduct business in the global market [1]. This critical infrastructure system performs four fundamental functions: the *generation, transmission, distribution*, and *consumption of electricity*. The electric power system is linked with many other supporting infrastructures such as telecommunication, transportation, fuel distribution, and water supply [2].

The U.S. electrical systems are susceptible to diverse threats that can cause short-term power interruptions to long duration power outages. The Department of Energy (DOE) reports that the outages could be triggered by natural disasters and climate conditions such as tornados, hurricanes, blizzards, and earthquakes or man-made threats such as physical or cyber-attacks [3]. Such disruptions may affect the security, health and safety of residents and cause an annual estimated economic loss of $18-70 billion. For instance, the Northeast power blackout in 2003 caused financial losses in excess of $6 billion [3]. Needless to say, a *resilient and reliable*

electrical grid has been a central concern of national security for decades. A recent report by the National Academies of Sciences, Engineering, and Medicine (NASEM) entitled "Enhancing the Resilience of the Nations Electricity System" highlighted the potential threats including natural disaster, manmade attack, and cyber-attack of the power system and offered overarching recommendations to enhance the overall resilience of the U.S. electrical system [4].

The conditions of any disruptive event can be broadly characterized as intense, unsettling, and severe under both pre-and post-disaster applications. The complex nature and the dynamic interactions between the system components challenge the achievement of optimal operations for system infrastructure, and this causes economic loss [5]. For instance, statistics show that the economic losses caused by natural disasters from 2000 to 2017 were around $3,312 billion across the world [6]. In 2011, when Japan was devastated by the tsunami and the massive earthquake Tohoku, economic losses soared to $440 billion [7]. In the U.S. recent hurricanes Harvey, Irma, and Sandy caused immense damage to the economy. These three hurricanes caused an estimated $320 billion in financial losses [8]. Beyond financial losses and property damage, all these mentioned disasters have wreaked havoc on business, manufacturing and production industry, the job market, and devastation of human life. These examples would clearly highlight the importance of conducting research on systems resilience.

The term *resilience* comes from the Latin word "resiliere" which means "bounce back". Resilience is an intrinsic property of a system that describes the system's ability to absorb the shock of a disruptive event and recover to a pre-defined level of performance. The concept of resilience integrates four fundamental concepts, namely: robustness, resourcefulness, speed of recovery, and adaptability. These four concepts are addressed in risk management approaches during the different stages of the disruptive event [9]. The consequences of disruptions often lead to unanticipated system behaviour and reduced overall system resilience [10]. Several research studies have been conducted to reduce the likelihood of the occurrence of the catastrophic event by applying security management tools, known as *pre-disaster* or *contingency strategy*. Beyond the contingency strategy, a fast response, a high level of preparedness, and a quick recover are of paramount importance in minimizing the disruption caused by the event. The combined approach of response and recovery are often referred to as *post-disaster strategy* or *mitigation strategy*.

The purpose of this research paper is to quantify the resilience of interdependent electrical systems by building an effective Bayesian network model. The model is specifically developed to deal with risks and uncertainties associated with the complex network of electrical infrastructure systems under disruption. The underlying factors related to the resilience of electrical infrastructure systems are identified, and the model is developed based on expert judgement and historical data. Washington, D.C. is used as a case study to illustrate the quantification of the resilience of an electrical system and its interdependent network.

The following subsection discusses the literature pertaining to the quantification of resilience and the state-of-the-art Bayesian approach in risk and resilience engineering. Section 2 discusses various factors related to design in the resilience of EIN. Section 3 provides background information about the Bayesian structure. Quantification of resilience factors associated with the Bayesian network for EIN is presented in Section 4. Various kinds of analysis such as forward propagation, backward propagation, sensitivity analysis and information theory are described in Section 5. Finally, Section 6 ends the paper with concluding remarks and future recommendations.

1.1. *Related research*

This section has two primary purposes. The first is to show some of the related methods used in quantifying system resilience and to present the general thread running through these methods. The different methods are then mathematically presented. The second is to discuss the existing literature related to the use of the Bayesian network in risk and resilience engineering and to present current gaps in the literature. To address these gaps, this research identifies the basic factors of resilience associated with the interdependent electrical infrastructure system in Washington, D.C. and then proposes a conceptual framework to quantify the resilience based on the Bayesian network.

1.1.1. *Quantification of resilience*

In recent years, research pertaining to system resilience in critical infrastructure has significantly increased and quantification of resilience has become a central factor. Despite an increased importance on system resilience in various sectors over the past few years, substantial differences exist among the definitions and descriptions of resilience. Different researchers attempted to quantify resilience in different manners. For instance, Youn et al. [11] developed a metric for measuring engineering resilience in terms of passive survival rate and proactive survival rate where resilience is the summation of *passive survival rate* and *proactive survival rate*. Passive survival rate refers to the reliability of the system and proactive survival rate represents the restoration of the system (see Eq. (1)). Although this approach is most applicable for earthquakes, it still can be utilized to quantify resilience for other systems.

$$Resilience(\Psi) = Reliability(R) + Restoration(\rho) \tag{1}$$

Bruneau et al. [9] designed a resilience triangle model for civil infrastructure by incorporating four dimensions of resilience: robustness, resourcefulness, rapid recovery, and adaptability. The authors proposed a deterministic static metric for measuring the resilience loss in terms of quality of degraded infrastructure. In this approach, resilience loss is calculated by the quality of the infrastructure before disruption, which is assumed to be 100, minus the quality of the disrupted infrastructure after recovery over time period t_0 to t_1 where t_0 represents the time when the disruption occurred and t_1 refers the time when the infrastructure returns to its normal pre-disruption state. This approach is presented as a mathematical expression in Eq. (2). Let *RL* is defined as the *resilience loss* and the average disrupted scenario is exhibited

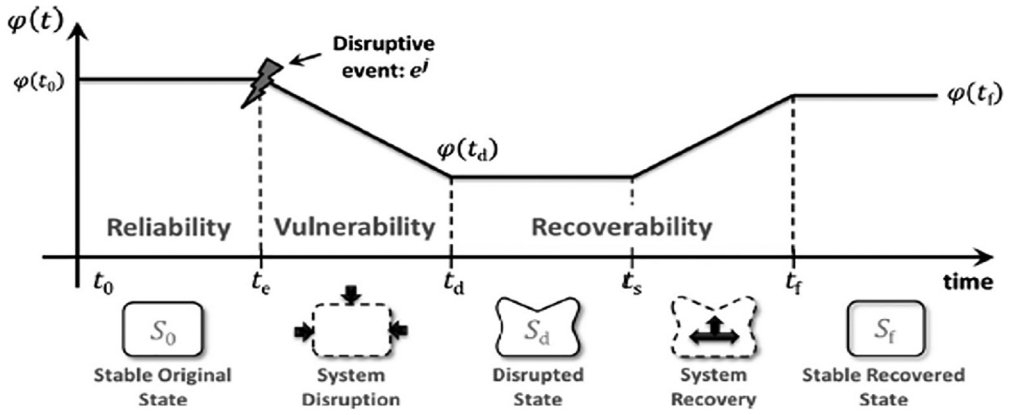


Fig. 1 – System performance and state transition to describe resilience (adapted from [13]).

as a function of Q(t).

$$RL = \int_{t_0}^{t_1} (100 - Q(t))dt \tag{2}$$

Rose [12] provided a definition of *dynamic resilience* (*DR*) which incorporated the concept of time-dependent characteristics of recovery. The author further computed dynamic resilience in terms of output of the system under hastened recovery (SO_{HR}) and without hastened recovery (SO_{WR}) where *N* is the number of time steps and t_i is the ith time step during recovery (see Eq. (3)).

$$DR = \sum_{i=1}^{N} SO_{HR}(t_i) - SO_{WR}(t_i) \tag{3}$$

Another time-dependent resilience approach was proposed by Henry and Ramirez-Marquez [13]. This approach simply computed the resilience as a ratio of recovery to loss. In this approach, the performance of the system at a point in time is measured through performance function $\phi(t)$, and three different transition states are considered: (i) the baseline stable state (S_0) functions under normal conditions before any disruption e^j occurs at time t_e, (ii) the disruptive state (S_d) at time t_d due to disruptive event e^j, and (iii) the recovered state (S_f) that represents the new state after the recovery action started at time t_s. The resilience equation ($\Re(t|e^j)$) is the ratio of recovery to loss and is presented in Eq. (4) and illustrated in Fig. 1.

$$\Re(t|e^j) = \frac{\phi(t|e^j) - \phi(t_d|e^j)}{\phi(t_0) - \phi(t_d|e^j)} \tag{4}$$

There are several other approaches such as graph theory, simulation, and optimization techniques that have been conducted to quantify resilience in different ways. For instance, Omer et al. [14] propose a resilience metric for infrastructure system resilience where resilience is computed as the ratio of the closeness centrality of the network for pre-and post-disruptive scenarios. Soni et al. [15] use graph theory to determine the supply chain resilience in terms of the deterministic modeling approach. Carvalho et al. [16] apply discrete event simulation to compare different scenarios to enhance the resilience of a supply chain network. In another research, Faturechi et al. [17] develop a mathematical model in order to maximize the resilience of an airport's taxiway and runway system. An optimization model and heuristic solution approach is proposed by Khaled et al. [18] and Vulgrin et al. [19] to maximize the resilience of the U.S. transportation system. Interested readers can refer to the works of Chang and Shinozuka [20], Cimellaro et al. [21], Murray-Tuite [22], Berche et al. [23], Heaslip et al. [24], Dorbritz [25], Miller-Hooks et al. [26], and Hosenni et al. [27] to understand different techniques applied to quantifying and assessing resilience. The different techniques used in quantifying and modeling resilience are summarized in Table 1.

1.1.2. *Existing literature related to Bayesian network in risk and resilience engineering*

The Bayesian network (BN) has a wide range of usage in the field of reliability, resilience engineering, and decision support systems. Hosseni and Barker [47] develop a resilient supplier selection method based on the Bayesian approach which modeled a Bayesian framework that can assess and select the best supplier based on primary and green criteria. Constantinou et al. [48] develop a robust Bayesian structure to select the optimal decision for a complex medical support system. The authors develop a realistic BN model that can handle both expert knowledge and data-driven interviews with patients in order to provide decision support for a forensic medical system. Khan et al. [49] examine the risk associated with marine transportation in arctic waters by conducting a quantitative risk assessment via BN. The authors predict the risk of collision between oil tankers and ice floes in the waters of the Northern Sea Route. Perez-Minana et al. [50] conduct an environmental risk assessment using the BN to illustrate the underlying risk associated with biodiversity. The authors initially develop mind-maps and the information obtained through the minds-map is fed into the BN to better manage the uncertainty associated with functions of biodiverse ecosystems. In another study, Amunddson et al. [51] demonstrate a Bayesian quantitative approach to handle the risk in the development of sustainable biomass supply chain networks. The authors identify risk drivers related to a biomass supply chain network and translated these factors into the Bayesian framework to assess how risk factors influence each other and how they impact the overall resilience of the biomass feedstock

Table 1 – Different techniques for quantifying and modelling resilience.

Approach	References	Application areas
Conceptual framework	Vlacheas et al. [28]	Telecommunication
	Labaka et al. [29]	Nuclear plant
	Sterbenz et al. [30]	Communication network
Semi quantitative	Shirali et al. [31]	Community
	Bruyelle et al. [32]	Process industry
Probabilistic approach (Quantitative)	Barker et al. [33]	Networks
	Pant et al. [34]	Transportation
	Ouyang et al. [35]	Urban infrastructure
Deterministic approach (Quantitative)	Enjalbert et al. [36]	Transportation
	Orwin and Wardle [37]	Soil system
	Ouedraogo et al. [38]	Human-machine system
	Brown et al. [39]	Organization
Fuzzy	Tadic et al. [40]	Organization
	Azadeh et al. [41]	Chemical industry
Simulation	Jain and Bhunya [42]	Water system
	Spiegler et al. [43]	Supply chain
	Landegren et al. [44]	IT network
Optimization	Alderson et al. [45]	Infrastructures
	Baroud et al. [46]	Water system

supply network. Some other applications of BN available in the literature are traffic accidents [52], customer service management [53], manufacturing systems [54], data classification [55], software development projects [56], and safety management [57]. All the results drawn from this research indicate that the BN model can effectively address mutual interdependency of incidents in risk analysis and provide recommendations to mitigate risk.

Although BN has been applied in different research, two significant gaps are identified and need to be addressed. These gaps are:

- The need for a Bayesian framework to design an interdependent electrical infrastructure system that takes into consideration the complex interactions that exist among different entities of the entire network.
- The lack of research assessing the resilience of EIN with respect to the concept of absorptive, adaptive and restorative capacities.

To address these gaps, this research paper proposes a new decision making approach based on Bayesian network theory that addresses the risk and uncertainty associated with EIN. A Bayesian network is an analytical tool that demonstrates all the causal relationships among the different qualitative and quantitative variables and allows practitioners to understand the interdependencies among the variables and how the change in one variable affects the others. The main contributions of the research are summarized below:

- Proposing a new conceptual framework for designing electrical system and its interdependent network.
- Classifying the underlying factors of EIN with respect to the concept of absorptive, adaptive, and restorative capacities.
- Developing a probabilistic graphical model, known as Bayesian network, for assessing the resilience of EIN.
- Conducting different types of analysis such as forward propagation, backward propagation, sensitivity analysis and information theory to provide a better insight regarding the result of the model.

2. Problem description and model formulation

This section discusses the problem description and model formulation using a case study and quantifying the resilience of EIN with respect to the concept of absorptive, adaptive, and restorative capacities.

2.1. *Interdependent electrical infrastructure system case study*

The main objective of the research is to build a Bayesian network for assessing and quantifying the resilience of an interdependent electrical infrastructure system. For this objective, the interdependent electrical infrastructure of Washington, D.C. is chosen to serve as a case study. Washington, D.C. is selected because (i) it is the capital of the U.S., (ii) the electrical infrastructure of Washington, D.C. plays a crucial role in the U.S. economy because it promotes an opportunity to trade electricity and is correlated to the U.S. gross domestic product (GDP) [58], and (iii) the electrical infrastructure is connected to the adjacent states of Maryland and Virginia which makes it a complex network to study. Washington, D.C. has a population around 65 million and the annual electric power generation is 0.1 TWh which is less than 1% of total U.S power generation [59]. The electricity is mainly generated from natural gas. The electrical infrastructure of Washington, D.C. is subjected to several disruptions mainly caused by natural disaster and human error such as executing a wrong computer command to control the equipment. The most common natural hazards

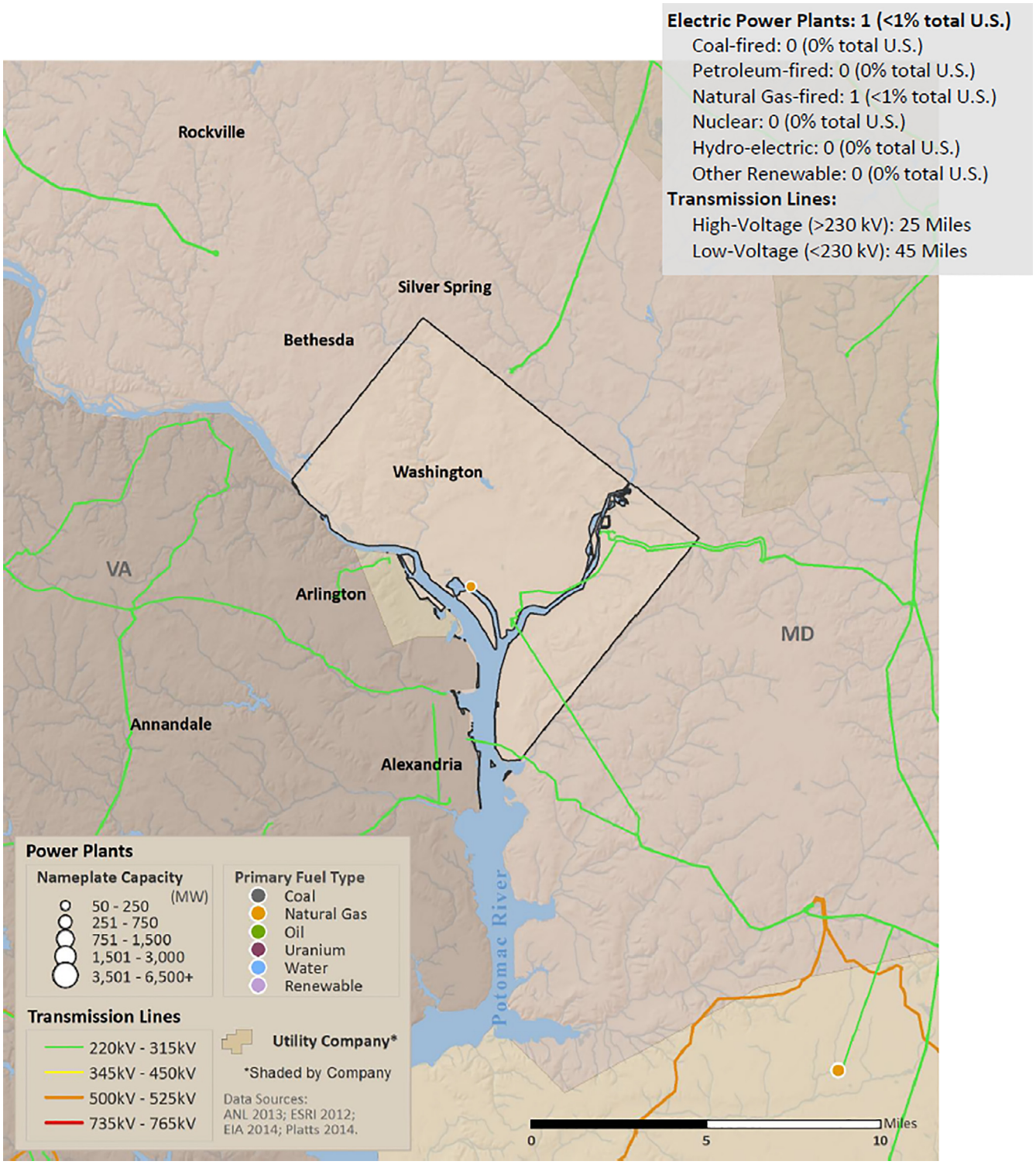


Fig. 2 – Energy sector profile of Washington, D.C (Adapted from [59]).

in Washington, D.C. are thunderstorms, lightning and winter storms [60]. This study covers all possible aspects related to quantifying the resilience of the interdependent electrical infrastructure system of Washington, D.C. Energy sector profile of Washington, D.C is shown in Fig. 2.

2.2. *Resilience capacity (RC)*

Capacity is the property of a system to achieve its objectives. *Resilience capacity* enhances the capability of a system to absorb, adapt, and recover from any shock or disruption.

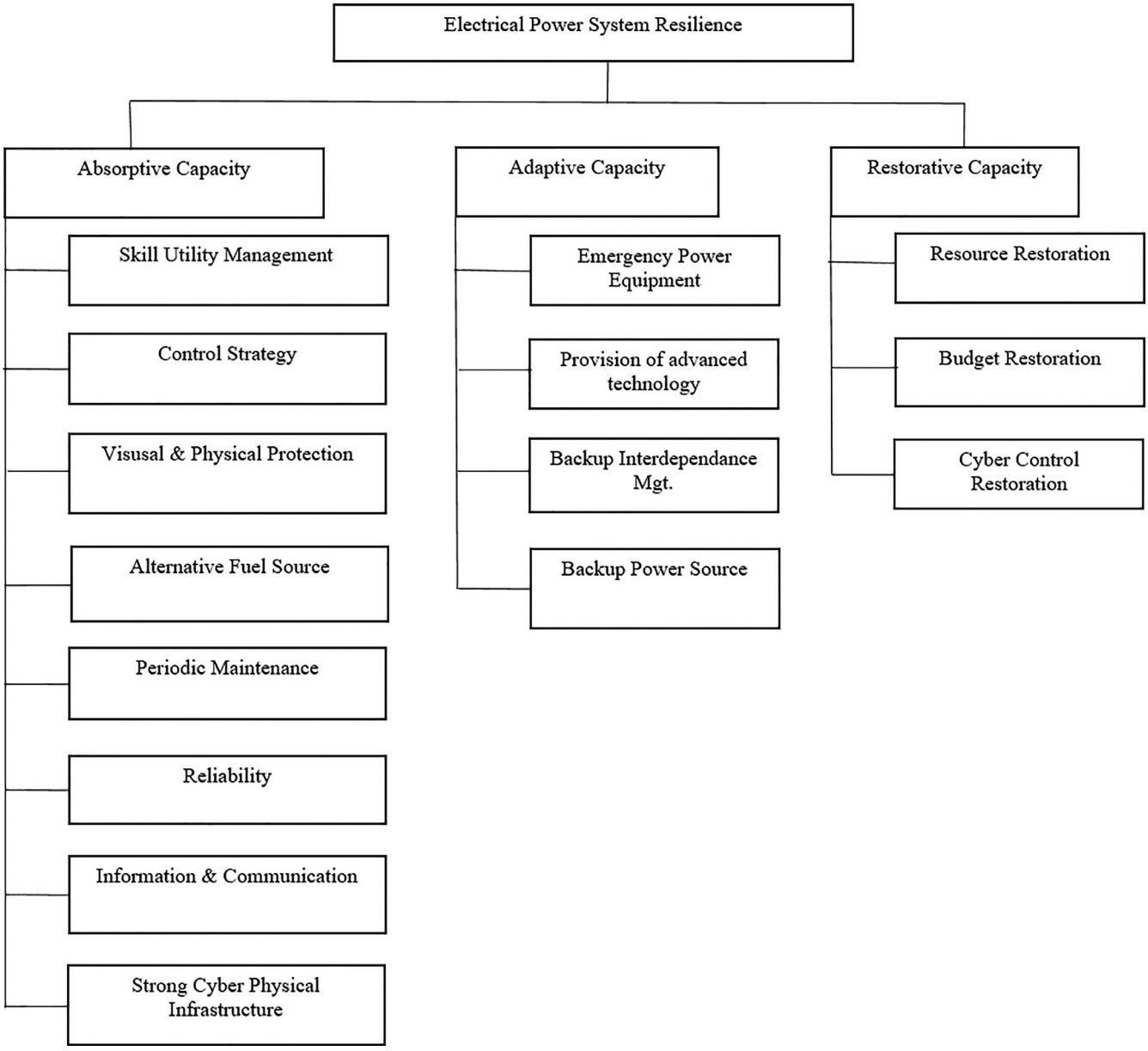


Fig. 3 – Fundamental structure of the resilience capacity for EIN.

Resilience capacity can take the form of resources such as the aptitude and skills of people, assets including intelligence systems, and/or actions [61]. Biringer et al. [62] proposed that the resilience paradigm can be described by using a set of resilience capacities, namely, absorptive capacity, adaptive capacity, and restorative capacity based on the different stages before, during, and after a disruption. After review of the literature, we have identified some underlying factors pertaining to these three capacities for the interdependent electrical infrastructure system of Washington, D.C. The underlying factors, which appear in Fig. 3, will be included and quantified in the developed BN framework to measure the resiliency of the interdependent electrical infrastructure system (Fig. 4).

2.2.1. *Absorptive capacity*

Absorptive capacity, an endogenous feature of a system, is the ability of a system to automatically absorb the impact of a disruption in order to minimize exposure or sensitivity to the shock. Absorptive capacity is also considered to be the *first line of defense* to withstand and absorb the shock due to a disruptive event. The absorptive capacity of a system involves a set of preventive measures and a course of strategies that must be developed before a disruption occurs in order to circumvent permanent undesirable consequences. The literature identifies the following eight aspects of absorptive capacity that are key factors related to the absorptive capacity of the electrical power system and its interdependent network.

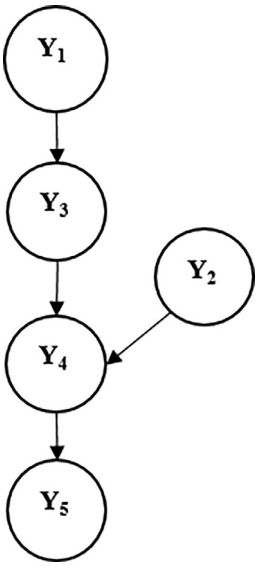


Fig. 4 – An example of a Bayesian network with five nodes.

- *Skilled Labour Management*, an efficient response team, and strong utility management are key features of absorptive capacity. Well-trained operators and efficient resources can react quickly to the disruption and maintain operation of the electrical power system [63]. A competent response team can quickly arrive at the repair yards and take less time to repair the fault.
- *A Control Strategy* is a substantial factor in absorptive capacity. Advanced automatic control and different kinds of control strategies such as Distributed Energy Resources (DER) help to prevent the severity of the outage [2]. The self-adapting and self-repairing feature of the advanced automatic control increases the reliability of fault-tolerant systems and maintains the power quality.
- The deployment of *Visual and Physical Protection* such as tall opaque fencing, grills, protective walls, and roadblocks serve as protection from physical attack, help to prevent from unauthorized visual data collection, and ultimately maintain privacy. Vegetation management and selective undergrounding also help mitigate the potential threat of local distribution outage [64].
- Because over-reliance on a single fuel source might lead to vulnerability in an energy supply network, it is prudent to have *Alternative Fuel Sources*. Incorporating diverse fuels such as renewable fuels, coal, and nuclear power enhances the robustness of the fuel supply network and ensures continued power service [63]. Redundancy of supply options due to multiple fuel sources also strengthens system reliability.
- Routine preventive maintenance activities including on-time repair scheduling of electrical components and ready availability of spare parts limit the probability of a major failure and the resulting massive financial loses. For the electrical system, *Periodic Maintenance* consists of a set of elementary tasks such as data collection, visual inspection, replacing old motors, lubrication, and bolt tightening. All of these activities must be completed in accordance with periodic maintenance guides and up-to-date safety standards.
- In terms of *Reliability*, the pieces of equipment used in electrical systems are highly sensitive and interrelated so that failure in one component may ripple through the entire system and affect the whole facility. Reliability of an electrical system is defined as the probability that electrical components continue to operate normally for a given amount of time under normal operating conditions. Redundancy of critical components, a standby power source, and a current risk analysis enhance the reliability of the electrical system. Lessening the probability of failure would greatly decrease the interruption of power generation and distribution.
- Having in place an effective plan for *Information and Communication* can reduce the impact of a disruption. Deployment of sensors, advanced data analytics, development of the Internet of Things (IoT) enable seamless communication among the generation, distribution and transformation networks [63]. Detailed pre-register information and register checklist related to the emergency power must be stored in a centralized, accessible database to ensure immediate action during the power interruption.
- A strong *Physical Cyber Critical Infrastructure* can reduce the consequences of a disruption. For an electrical system, a cyber-attack can be classified as inadvertent or deliberate. Implementing the Supervisory Control and Data Acquisition (SCADA), a Distributed Control System (DCS), smart meter, corporate network communication, strong password control, and secure software updates can all reduce the likelihood of an individual or group attack [2].

2.2.2. *Adaptive capacity*

Adaptive capacity adjusts the perturbations due to the shock brought on by a disruptive event. Adaptive capacity, which is considered to be the *second line of defense*, is defined as the capability of a system to adapt itself and attempt to cope with the adverse consequences or moderate potential damage without any recovery activity. It is considered to be part of a post-disaster strategy also known as "capacity of response" [65]. Following is a list of four key factors related to the adaptive capacity of the electrical power system and its interdependent network

- Stockpiling regular equipment and contracts for the provision of *emergency power equipment* reduces the severity of adverse consequences during power outages [63].
- *Provision of advanced technology* such as advanced metering infrastructure and smart inverter can improve the robustness of the entire electrical system and limit the consequences of any disruption [66].
- *Mode flexibility* (substitution) is one of the key factors to maintaining continuity of an electrical system operation. Backup interdependence management such as electric vehicles, locomotives, and other non-standard power sources can be connected to the grid to provide limited electric service during outages. Advanced technologies such as smart grid can serve as a strong media to connect and regulate the operation between vehicle to grid (V2G) to ensure

interoperability (two-way flow of electricity) between two systems [66].
- *A backup power source* is regarded as an adaptive measure. When the grid is down due to any disruption, backup generators can serve as an emergency measure during crisis management [63]. Backup power sources are an affordable option and can be permanent, standby or portable with ease of use.

2.2.3. *Restorative capacity*

Restorative capacity is the degree of ease with which a system can recover permanently from a disruption. Restorative capacity is considered as the *last line of defense*. Restorative capacity is highly dependent on the restoration of the budget and restoration of technical resources. Restorative capacity might not be fully achieved if the stakeholders fail to provide adequate financial and technical support. Within restorative capacity, three factors are identified.

- *Resource restoration*, which involves the repair or recovery of damaged equipment or facilities through post-disaster strategy. Resource restoration can be done through either human-based assistance such as trained engineers and a repair task force or non-human based support such as repair equipment and repair vehicles.
- In order to restore or repair the disrupted electrical infrastructure, *budget restoration* or monetary capital is one of the primary factors of resilience-enhancing investments [67]. For an electrical system, the damaged equipment can be repaired or restored depending on the severity of disruption and budget availability.
- The last factor, *restoration of cyber control* is expected to go faster compared to physical attacks. Cybersecurity staff and resource services often struggle to predict all vulnerabilities and threats related to cybersecurity. For instance, if the entire system is affected by the malicious virus, reinstallation might take more time than expected [68].

3. Background of the Bayesian network

This section provides background information on the Bayesian Network (BN), which is a powerful tool for risk assessment, reliability prediction, and decision making under the stochastic conditions of a complex system. The BN makes statistical inference in a rational way by updating the prior beliefs of an elementary event. Prior beliefs or probabilities are set based on *subjective judgement* (e.g., expert knowledge, historical data) or through a *frequentist approach*. BN is a Directed Acyclic Graph (DAG), developed based on the Bayes theorem [69], that helps in addressing the cause and effect relationship (edges) among the set of interacting variables (nodes). The complete network represents a full joint probability distribution where the cause to effect and effect to cause relationships are mathematically equivalent, even though the direction of the underlying network depicts a unidirectional impact [69].

3.1. *Bayes theorem*

Bayes theorem, proposed by Thomas Bayes [70], is a mathematical expression that enables us to reason about belief under the condition of uncertainty. According to Bayes rule, the probability that A and B both would occur is the product of the probability of A and probability of B given A and this can be presented using the following equation.

$$P(A \cap B) = P(A) \times P(B|A) \tag{5}$$

where, $P(A \cap B)$ = probability of A and B both would occur (joint probability); $P(A)$ = initial probability of A (prior probability); and $P(B|A)$ = probability of B given that A already occurred (posterior probability). Eq. (5) can be modified by symmetry and written as follows:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \tag{6}$$

The common terminology associated with BN is described below, followed by a detailed mathematical expression.

- *Node*: Node is also known as *vertices*, represents a random variable.
- *Edge*: Edge is also known as an *arc*, represents the conditional interdependencies between the variables.
- *Directed graph*: The underlying topology of the BN structure consisting of a set of variables and a set of arcs.
- *Parent node*: Parent nodes are without root nodes.
- *Intermediate nodes*: Intermediate nodes are node with parent and child node.
- *Child node*: Child nodes are without leaf nodes.
- *Node Probability Table (NPT)*: Every node possesses probability tables, known as *node probability table* (NPT). NPT can be developed manually or achieved by eliciting the distribution or related expression. For a node without its parent node, the NPT would be simply the probability distribution of that specific node.

3.2. *Mathematical expression for Bayesian network*

Suppose a BN consists of n variables $Y_1, Y_2, Y_3, \ldots, Y_n$. The full joint probability distribution of BN can be written as follows:

$$\begin{aligned} P(Y_1, Y_2, Y_3, \ldots, Y_n) &= P(Y_1|Y_2, Y_3, \ldots, Y_n)P(Y_2|Y_3, \ldots, Y_n) \\ &\quad \ldots P(Y_{n-1}|P_n)P(Y_n) \end{aligned} \tag{7}$$

The above equation can be further simplified and streamlined as follows:

$$\begin{aligned} P(Y_1, Y_2, Y_3, \ldots, Y_n) &= \prod_{i=1}^{n} P(Y_i|Y_{i+1}, Y_{i+2}, \ldots, Y_n) \\ &= \prod_{i=1}^{n} P(Y_i|Parents(Y_i)) \end{aligned} \tag{8}$$

The above concepts can be represented with a simple example in Fig. 7 where a BN consists of a set of variables $S = \{Y_1, Y_2, Y_3, Y_4, Y_5\}$ and a set of edges to show the interdependencies among the variables. An outgoing edge from Y_i to Y_j signifies a relationship where the value of Y_j is conditioned on the value of Y_i and Y_i is the parent of Y_j and Y_j is the child of

Y_i. Based on this definition, Y_1 and Y_2 are the parent nodes, Y_5 is the child node, and Y_3 and Y_4 are the intermediate nodes. Then, according to Eq. (8) the full *joint probability distribution* can be written as follows:

$$P(Y_1, Y_2, Y_3, Y_4, Y_5) = P(Y_1)P(Y_2)P(Y_3|Y_1)P(Y_4|Y_2, Y_3)P(Y_5|Y_4) \quad (9)$$

Once we compute the full joint probability, then the marginal distribution of each node can be calculated by the process of *marginalization*. Marginal distribution provides the probabilities of different values of the random variables in the subset without explicitly referring to the values of the other variables. For instance, we are interested in calculating $P(Y_3)$ by the marginalization approach. Marginalization of variable Y_3 can be calculated as follows:

$$P(Y_3) = \sum_{Y_1, Y_2, Y_4, Y_5} P(Y_1)P(Y_2)P(Y_3|Y_1)P(Y_4|Y_2, Y_3)P(Y_5|Y_4) \quad (10)$$

Marginalization in belief function theory corresponds to a distributive operation over combinations which specifies that we can marginalize the global joint probability by marginalizing local NPTs [69]. From Fig. 7, $P(Y_3)$ can be calculated as follows:

$$P(Y_3) = \Bigg(\sum_{Y_1} P(Y_1)P(Y_3|Y_1) \Bigg(\sum_{Y_4} \Bigg(\sum_{Y_2} P(Y_4|Y_2, Y_3)P(Y_2) \Bigg(\sum_{Y_5} P(Y_5|Y_4) \Bigg) \Bigg) \Bigg) \Bigg) \quad (11)$$

It is important to note that Eqs. (9)–(11) are considered to be *true* when all the variables in the BN structure have two possible binary outcomes: *true* or *false*. However, in many cases, such as the Washington, D.C. case study, different types of variables including *continuous* and *fixed* variables must be taken into consideration during the computation.

4. Quantifying resilience capacity

The following subsections demonstrate the quantification of the resilience of the system as a function of the various elements of the BN through the interdependent electrical infrastructure of our Washington, D.C. case study. AgenaRisk software [69] is used to show the different states of the variables to quantify the resilience. Various kinds of nodes such as discrete, continuous, rank node, label node can be designed through AgenaRisk.

4.1. *Types of variables used*

- *Boolean variables* (BV): A Boolean variable is expressed in forms of exactly two states, *true* and *false*, to present *positive* and *negative* outcomes, respectively. For instance, in Fig. 5, the node for periodic maintenance (bottom of the figure) shows True = 0.71453 and False = 0.28547, meaning that the periodic maintenance of the electrical system is successful 71.453% and fails 28.547% of the time, respectively. In other words, the chance of being a successful periodic maintenance (*true* state) is 71.453% while the probability of being a failed state is 28.547%. Similarly, the prior distribution of the management variable with two states of True = 0.82 and False = 0.18 means that there is a 82% chance that a strong management policy, administered by authorities, can effectively thwart the adverse impacts of disruptive events according to expert opinion; on the other hand, there is a 18% chance that it may fail. In another example, while 92% of the time a strong cyber critical infrastructure may positively contribute towards adaptive capacity, there is an 8% chance that it might fail.
- *Continuous variables* (CV): Continuous variables can take continuous realizations via a probability distribution of random variables. An example of a continuous variable is the availability of spare parts (see Fig. 5). The node of the continuous variable, "availability of spare parts" is modeled using a truncated normal distribution (TNORM) with a mean (μ) of 87%, variance (σ^2) of 2%, and a lower bound (*LB*) and upper bound (*UB*) set as 70% and 100%, respectively. This is represented in Eq. (12).

$$\text{Availability of spare parts} \sim TNORM \left(\mu = 0.87, \sigma^2 = 0.02, LB = 0.70, UB = 1.0\right) \quad (12)$$

The above equation represents that in the worst possible scenario, the availability of spare parts is not lower than 70% and in the best possible scenario all the spare parts (100%) are available to conduct the periodic maintenance work. Since truncated normal distribution is a simple modification of a normal distribution that confines the mean values between lower and upper bounds, it is one of the best possible ways to represent the continuous variables related to the electrical system and its interdependent network. All the parameters for continuous normal distribution are generated through collecting and analyzing the historical data.

- *Qualitative variables*: Qualitative variables, which are also known as *categorical variables*, capture ordinal categories used for the weight of different factors pertaining to absorptive, adaptive, and restorative capacity.
- *Labelled variables*: These variables possess a number of discrete states. *Weighted value* node is an example of Labelled variables.

4.2. *Quantifying absorptive capacity*

As discussed earlier, eight important factors were identified as contributing to the absorptive capacity of EIN (Fig. 3). The prior probability distribution for six of the variables i.e., skill utility management, control strategy, visual and physical protection, alternative fuel source, information and communication, and strong cyber-physical infrastructure are represented by two states through Boolean expression. In other words, these six variables follow the same rules of Boolean variables as discussed in Section 4.1. The posterior probability distribution for the reliability and periodic maintenance variables are computed based on Boolean logic.

To calculate the reliability of EIN, *mean time to failure* (MTTF) is computed in terms of operating hours. MTTF can be simply obtained from historical data and is an example of a continuous variable. If the MTTF is greater than or equal to the expected MTTF of EIN, then the electrical system and its related

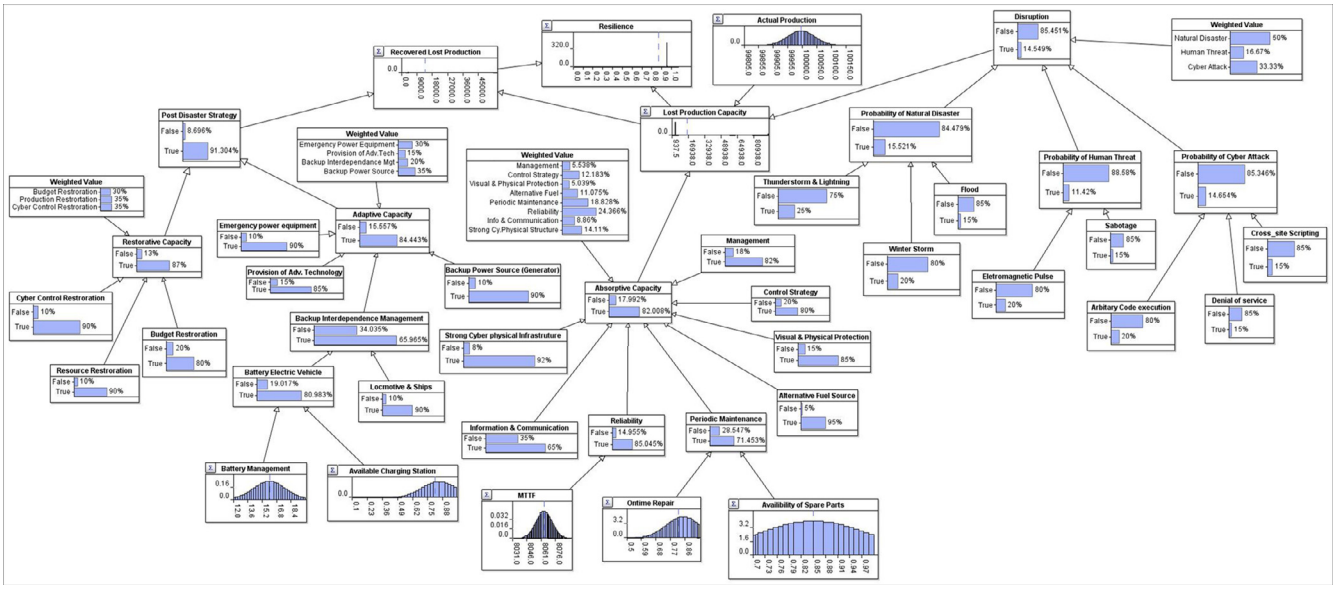


Fig. 5 – Base model of the Bayesian network for measuring the resilience of EIN.

Table 2 – Boolean expression used to define the posterior probability distribution of reliability and periodic.

Variable name	Prior distribution	Boolean expression	Significance of boolean expression
Reliability	MMTF $\sim$ TNORM($\mu = 8,064$, $\sigma^2 = 75$, $LB = 0$, $UB = 8,400$)	IF (MTTF $\geq$ 8,016, "On", "Fail")	If the MTTF is greater than or equal to 8,016 hr of EIN, then EIN is reliable (On state); otherwise, it fails (Fail state)
Maintenance	On time repair $\sim$ TNORM (μ= 0.85, $\sigma^2 = 0.01$, $LB = 0.50$, $UB = 0.95$) Availability of spare parts $\sim$ TNORM (μ= 0.87, $\sigma^2 = 0.02$, $LB = 0.70, UB = 1.0$)	IF (Ontime repair $\geq$ 0.85 || Availability of spare parts $\geq$ 0.85, "True", "False")	If the probability of on time repair scheduling is greater than or equal to 85% AND the the probability of availability of spare equipment is greater than 85%, then the maintenance mission will succeed (True state); otherwise not (False state)

networks are reliable (*on* state); otherwise, they are failures (*fail* state). The same logic is applied to determine the posterior probability value for the continuous variable on time repair scheduling and spare parts availability. The Boolean expressions for these "reliability" and "periodic maintenance" nodes are summarized in Table 2.

The posterior probability distribution of absorptive capacity of EIN is computed by the weighted sum of probabilities of its parent nodes. In order to calculate the absorptive capacity of EIN, a labelled node named "weighted value" is created to show the weight of each variable contributing to the absorptive capacity of EIN. Such weights can be obtained through different decision-making processes such as Analytical Hierarchy Process (AHP) [71], swing weights, or from survey data. The general equation associated with a *weighted mean* (WMEAN) is presented in equation (13), where i is the number of variables connected (eight in this case) to the weighted average node of absorptive capacity (see Fig. 5) and W_i is the weight associated with the ith variable. This same weighted average approach has been applied to the weighted value of adaptive capacity and restorative capacity as well.

$$\text{WMEAN} = \sum W_i X_i = 1, 2, \ldots, n, \forall i = 1; 0 < W_i < 1; \sum_i W_i = 1 \tag{13}$$

4.3. *Quantifying adaptive and restorative capacity*

To set the prior probability of four nodes under adaptive capacity and three nodes under restorative capacity, the same Boolean logic will be applied. Adaptive capacity and restorative capacity contribute to *post-disaster* strategy; however, their significance might be different. Adaptive capacity is the second line of defense in recovering the lost capacity whereas restorative capacity is the last line of defense. If adaptive capacity is not able to withstand the shock due to the disruption, restorative capacity restored the damage, but it takes a longer time compared to adaptive capacity. The fundamental structure of Bayesian networks depicts the causal relationship between the nodes. The causal relationships between

the nodes are shown by drawing a connection between them through arcs. The posterior probability of post-disaster strategy can be calculated through Boolean logic. However, other than adaptive and restorative capacity, there might be some other hidden factors contributing toward post-disaster strategy. This can be better described by *NoisyOR* function. These hidden or missing parameters are known as "leak parameters" in *NoisyOR* function. For instance, if there are n causal factors such as $Y_1, Y_2, \ldots, Y_n$ are conditioned on Z, with a probability value for Z being *true* when one and only one Y_1 is *true*, and all causes other than Y_1 are *false*. The *NoisyOR* function is presented in Eq. (14) where for each $i, S_i = P(Z = true|Y_i = true, Y_j = false; \forall j \neq i)$ is the probability of the conditional being *true* if and only if that causal factor is *true* [69].

$$NoisyOR(Y_1, S_1, Y_2, S_2, \ldots, Y_n, S_n, l) \tag{14}$$

Leak factor l can be defined as the extent to which there are missing factors from the model that can contribute to the consequence being *true*. It is the probability that Z will be *true* when all of its causal factors are *false*. The conditional probability of Z obtained with the *NoisyOR* function is presented below in Eq. (15).

$$P(Z = True|Y_1, Y_2, \ldots, Y_n) = 1 - \prod_{i=1}^{n} [(1 - P(Z = True|Y_i = True)(1 - P(l))] \tag{15}$$

As discussed in the proposed BN model, in order to calculate the posterior probability of the "post-disaster strategy", we have used *NoisyOR* function, represented in Eq. (14). This equation means that the chance of successful achievement of a post-disaster strategy is 70% if only adaptive capacity is met, while this value increases to 95% when only restorative capacity is met and the leak parameters are set as 0.02 (shown below in Eq. (16)). This approach is supported by Vugrin et al. [72] where the authors stated that during a disruption, restorative capacity is needed to attain a higher level of recovery compared to adaptive capacity.

$$NoisyOR(\text{Adaptive capacity}, 0.7, \text{Restorative capacity}, 0.95, 0.02) \tag{16}$$

4.4. *Disruption modeling*

An electrical system and its interdependent network (EIN) are subject to different types of disasters. The three most common types of disasters are natural disasters, human threats, and cyber-attacks. The most common natural disasters are hurricanes, tornados, and snow storms. Human threats can be intentional (sabotage) or electromagnetic while cyber-attacks are often in the form of denial of service, cross-site scripting, and arbitrary code generation. In Fig. 5, the likelihood of occurrence of these threats is represented through True state based on historical data. We have used NoisyOR function to compute the posterior probability of natural disaster, human threat, and cyber-attack (see equations (17)–(19)). Finally, the probability of disruption is calculated based on the weight value of each individual disaster.

Table 3 – NPT for lost production capacity.

Absorptive capacity	False	True
Expression	PDO × APC	0

Table 4 – NPT for recovered production capacity.

Post disaster strategy	False	True
Expression	0	LPC × 0.95

$$P(\text{Natural disaster}) = NoisyOR(\text{Hurricane}, 0.15, \text{Snow storm}, 0.10, \text{Tornados}, 0.05, 0.1) \tag{17}$$

$$P(\text{Human threat}) = NoisyOR(\text{Electromagnetic}, 0.12, \text{Sabotage}, 0.09, 0.08) \tag{18}$$

$$P(\text{Cyber-attack}) = NoisyOR(\text{Arbitrary code}, 0.15, \text{Denial of services}, 0.1, \text{Cross site scripting}, 0.05, 0.1) \tag{19}$$

4.5. *Actual production capacity and lost production capacity*

Based on the available data source for the city of Washington, D.C., yearly production capacity is considered as 0.1TWh [59]. The production capacity of the electrical facility may hamper due to either man-made attacks or natural disasters, such as natural disaster, human attack, or cyber-attack. The lost production capacity is highly dependent on whether the absorptive capacity is capable of absorbing shocks (the probability of being a True state) or not (the probability of being False). In our model, the lost production capacity variable is conditioned on three variables including the probability of disruption occurrence, the absorptive capacity, and the actual production. Lost production capacity is computed as the product of the likelihood of disaster occurrence and actual production. The electrical facility does not lose its production if the shock of disruption can be absorbed (True-state). Thereby, the lost production capacity is set to zero. NPT for lost production capacity is shown in Table 3.

4.6. *Recovered lost production capacity*

Recovered lost production capacity is a function of two variables: *post-disaster strategy* and *lost production capacity* (LPC). We assume that an electrical facility will recover 95% of its lost production capacity, if the post-disaster strategy is successful (*True*-state); zero otherwise (*False*-state). NPT for recovered production capacity is represented in Table 4.

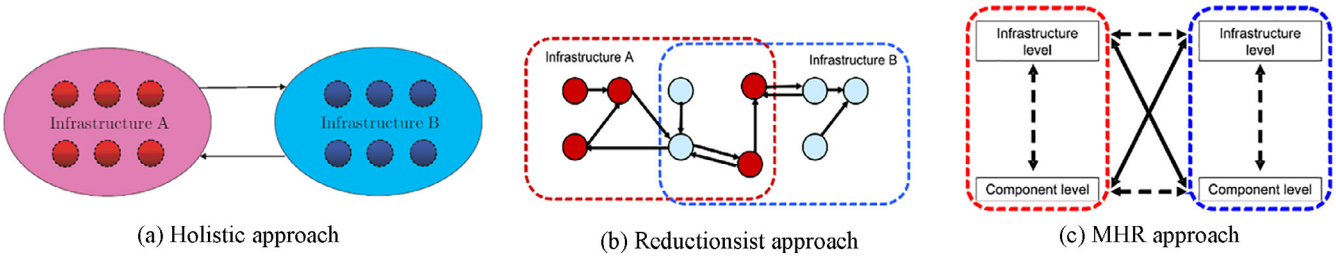


Fig. 6 – Different approaches to model interdependencies [74].

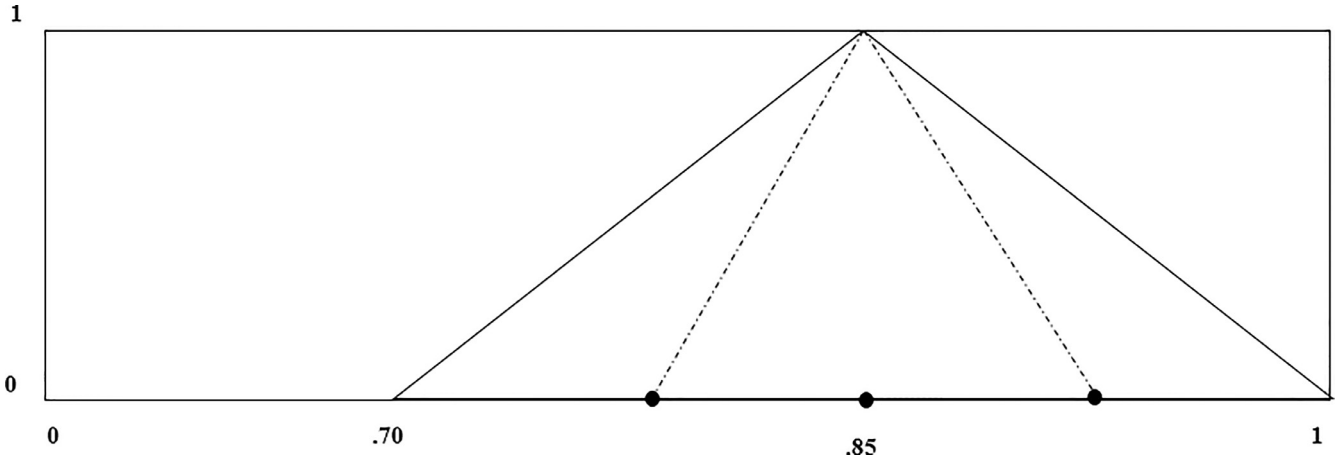


Fig. 7 – Triangular Fuzzy Numbers representation of ASP [75].

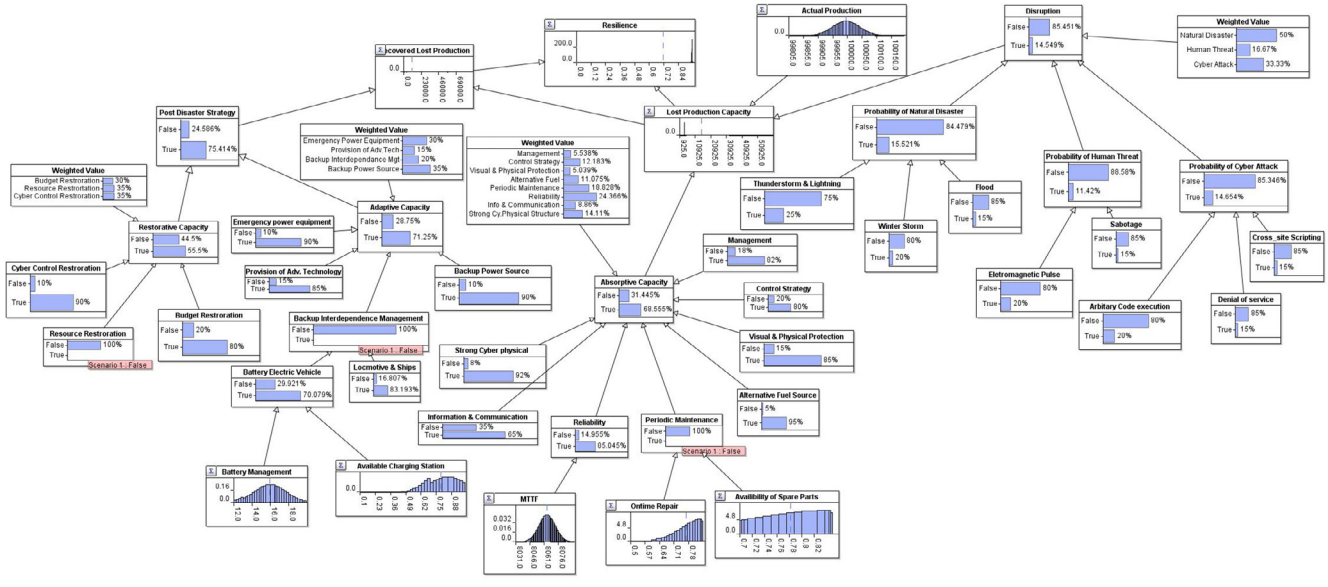


Fig. 8 – Forward propagation analysis of Bayesian network for measuring resilience of EIN.

4.7. *Resilience*

Resilience is the ratio of recovery (recovered production capacity) to loss (lost production capacity). Based on this calculation, the expected resilience is 0.87 as depicted in Fig. 5.

4.8. *Other modeling and quantification techniques*

Holistic and reductionist approaches, mixed holistic-reductionist paradigm, and multiple formalism are some techniques that can be used to model infrastructure in-

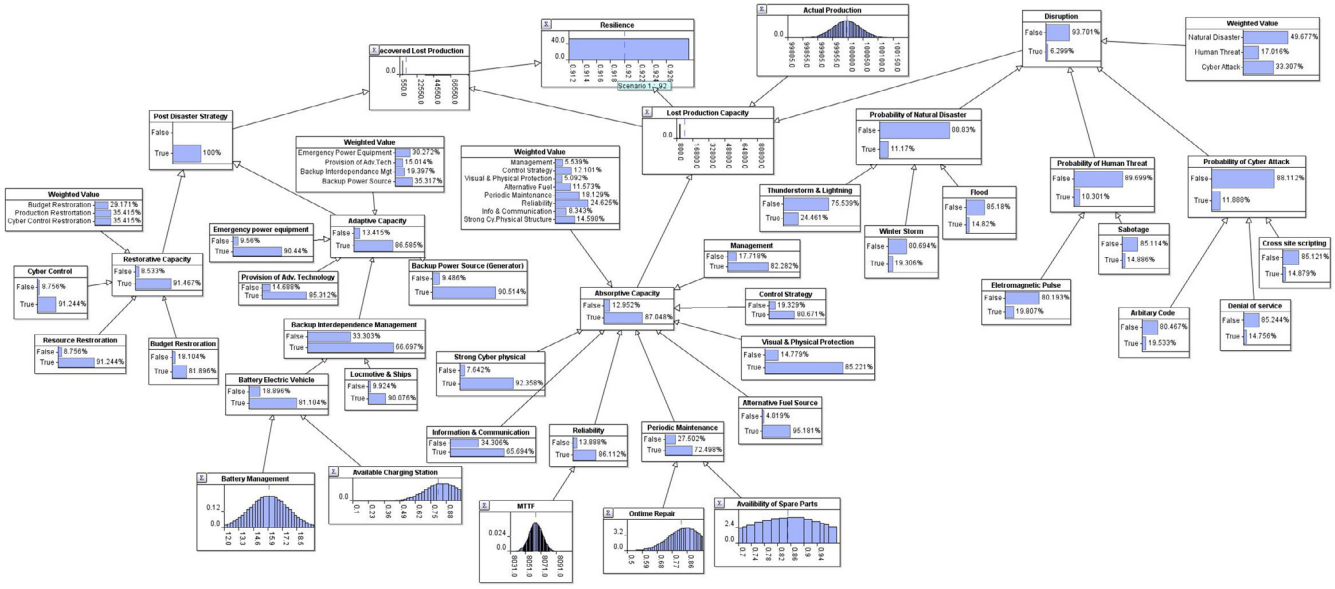


Fig. 9 – Backward propagation analysis of Bayesian network for measuring the resilience of EIN.

Table 5 – Comparative scenarios among different capacities.

Scenario	periodic maintenance	Backup interdependence management	Restoration resource	Absorptive capacity (%)	Adaptive capacity (%)	Restorative capacity (%)	Expected resilience (%)
Base Case	–	–	–	82.00	84.44	87.00	86.70
1	*false*	–	–	68.55(↓)	84.44	87.00	85.70(↓)
2	*false*	*false*	–	68.55	71.25(↓)	87.00	84.80(↓)
3	*false*	*false*	*false*	68.55	71.25	55.50(↓)	71.64(↓)

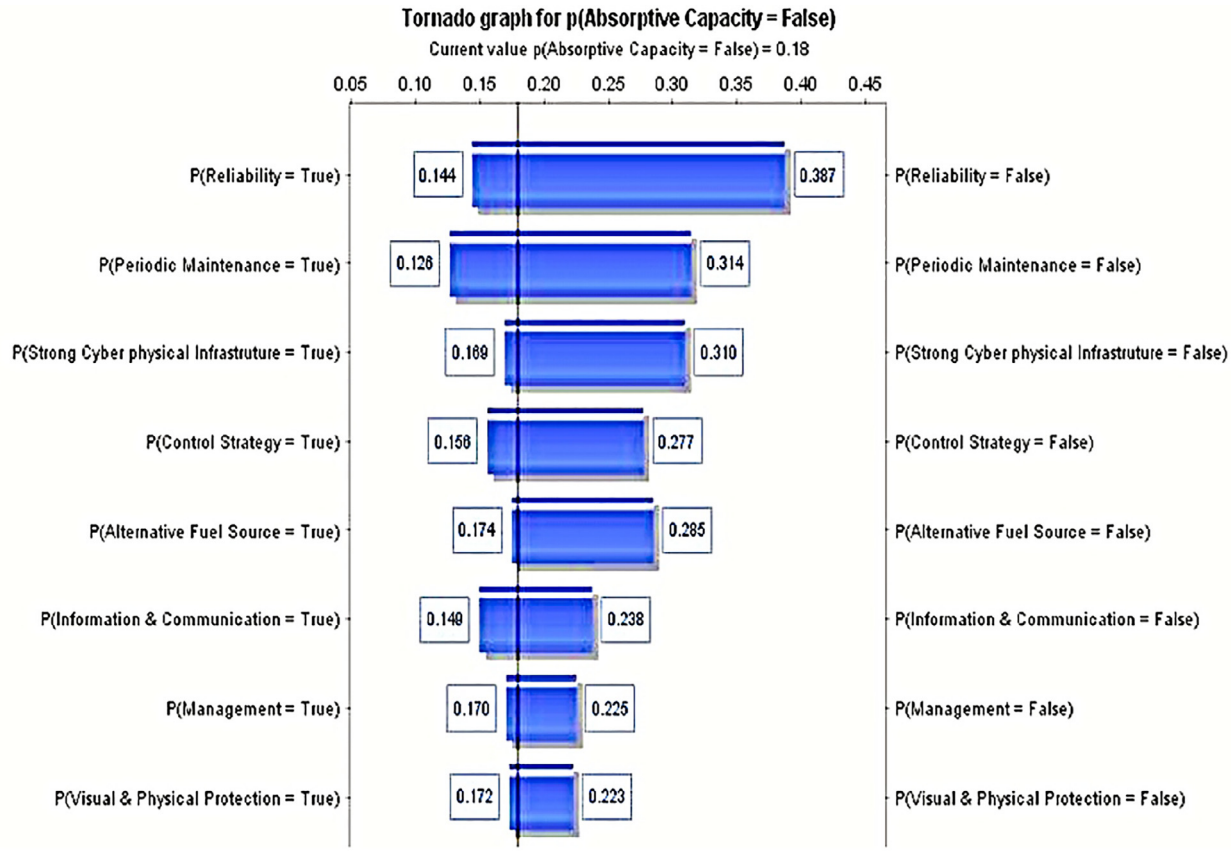
↓ indicates that the value of the corresponding variable reduces compare to the value of the base case.

terdependencies [73,74]. Holistic approaches treat critical infrastructures as a whole unit by simplifying the appearance of infrastructure interdependencies(see Fig. 6a). Reductionist approaches on the other hand identify different fundamental systems components of the complex infrastructures, and then describe the evolutionary development of the entire system based on the aggregate behavior of the identified system's components(see Fig. 6b). In the mixed holistic-reductionist (MHR) approach, modeling of infrastructure interdependencies is performed through reductionist approaches and the logical and functional dependencies between the heterogeneous infrastructures are performed through holistic approaches. Fig. 6(c) shows the MHR modelling approach.

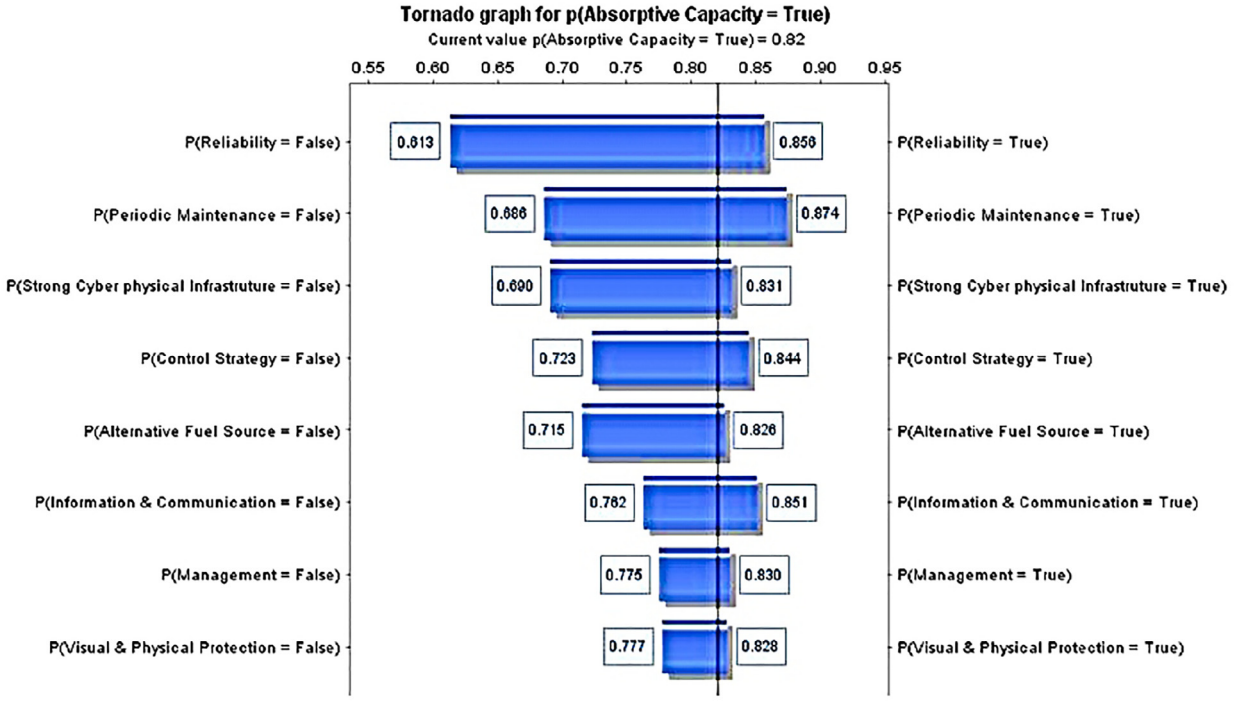
With regards to the quantification of different variables, the extension of this work can be performed using triangular fuzzy approach. For example, the conditional probability table of variables using expert knowledge can be expressed in terms of triangular fuzzy numbers. Fuzzy approach is one of the easiest ways to handle data uncertainty and a more flexible technique to define a prior probability [75]. Let us define a fuzzy number M on Z to be a triangular fuzzy number and let $\mu_M(y)$: $Z \rightarrow [0, 1]$ be its elemental functions as represented in following Eq. (20) where, $l \leq m \leq u$, l and u denote lower and upper value of of the support for M, respectively, and m represents the mid value of the fuzzy triangular number. This triangular fuzzy number can be donated by (l,m,u) [76].

$$\mu_M(y) = \begin{cases} \dfrac{y}{m-l} - \dfrac{l}{m-l}, & y \in [l, m], \\ \dfrac{y}{m-u} - \dfrac{u}{m-u}, & y \in [m, u], \\ 0, & otherwise \end{cases} \tag{20}$$

For our base model as depicted in Fig. 5, the NPT of availability of spare parts (ASP) for the periodic maintenance of EIN can be defined in terms of triangular fuzzy number. For example, the expert opinions suggest that in order to successfully conduct the periodic maintenance, the probability of spare parts availability should range from a minimum of 70% to a maximum of up to 100% while most likely may fall into 85%. This can be represented by a triangular fuzzy number where 0.70 is the minimum value (lower bound, l), 0.85 is the most likely value (m), and 1.0 is the maximum value (upper bound, u). The mathematical representation of this statement is depicted in Fig. 7.



(a) absorptive capacity =“False” state



(b) absorptive capacity =“True” state

Fig. 10 – Sensitivity analysis of absorptive capacity.

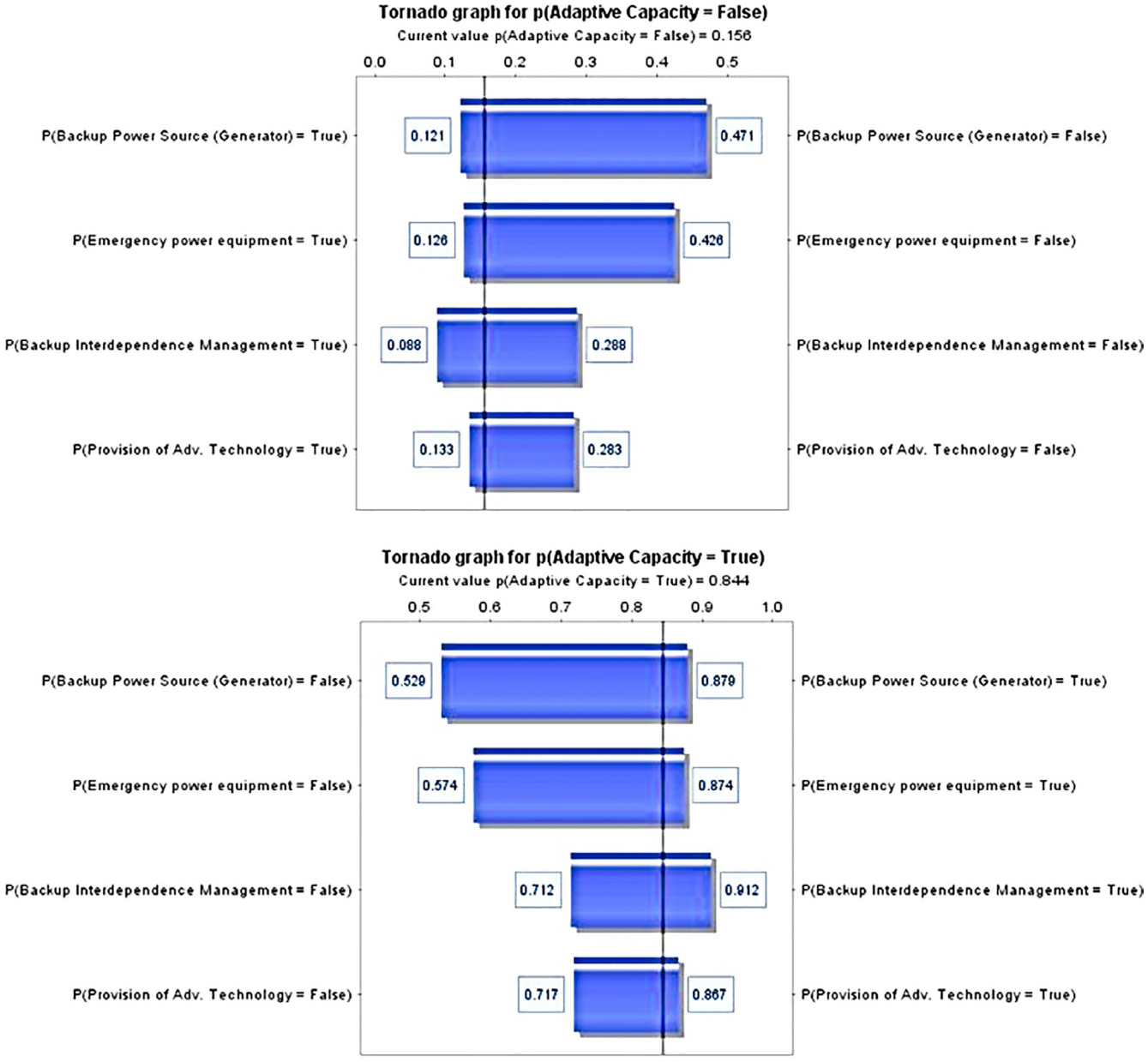


Fig. 11 – Sensitivity analysis of adaptive capacity.

5. Results and analysis

This section analyzed results based on forward propagation, backward propagation, sensitivity analysis, and information theory. During the analysis of probabilistic inference of multiconnected BN, the posterior probability of a set of variables is computed such that $\mathbf{Y}_1 \subset \mathbf{S}$ at given evidence e. The feature of the BN to disseminate the effect of evidence through the network is defined as "propagation analysis", and the related probability is represented by $P(Y_i|e); \forall Y_i \in \mathbf{Y}_1$ [69]. BN offers a robust framework to compute *posterior propagation probabilities* from the experimental data. There is no strict direction of information flow; thus, queries can be made at any node in the underlying structure. *Forward propagation* refers to the propagation of an individual or set of observed variables and measures their impact on the target node. Forward propagation is a type of reasoning that refers the cause to effect analysis. In the forward propagation analysis, *predictive calculations* are computed by successively passing the resulting marginal distributions from one node to one of its connected child nodes.

In order to conduct the forward propagation analysis, three different types of scenarios are designed by setting the *false* state to three different variables types. Three decision variables are chosen that contribute significantly toward the overall resilience of the electrical system and its independent network. The three variables are: (i) *maintenance*, which belongs to absorptive capacity, (ii) *backup interdependence management* as a part of adaptive capacity, and (iii) *restoration resource* which

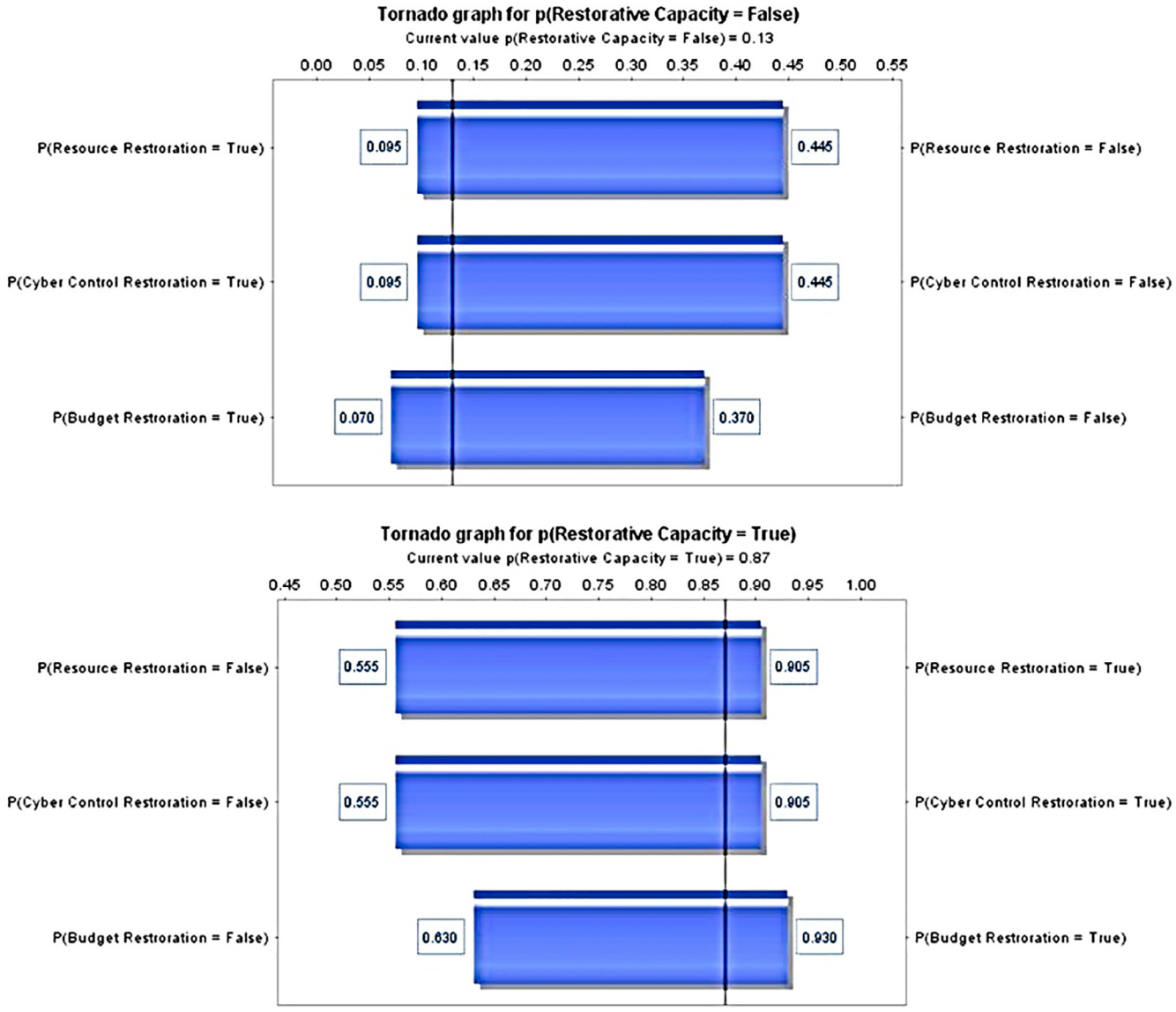


Fig. 12 – Sensitivity analysis of restorative capacity.

falls into restorative capacity. Scenario 1 accounts for the failure of periodic maintenance which if not successful (*false* state) eventually increases the lost production capacity. Scenario 2 refers to the case when observation is made for failure of two events: *periodic maintenance* and *backup interdependence*, which ultimately drops the resiliency from 86.70% to 84.80%. Scenario 3 simulates the impact of failures of all three variables: *periodic maintenance*, *backup interdependence management*, and *restoration resource*. Results indicate that failure of all three variables generates a larger adverse impact on the resilience which drops the resilience of EIN to 71.64%. The observations generated by these three scenarios are reported in Table 5. Forward propagation analysis for scenarios 1, 2, and 3 is illustrated in Fig. 8.

On the other hand, *backward propagation* is the opposite approach to the forward propagation analysis. Backward propagation enables us to conduct what-if analysis; an observation is set for a specific (descendant/target) variable and then the BN calculates the marginal probabilities of ancestor variables by propagating the impact of the successor variable in a backward tactic through the entire network. In the case study, if the resilience value is set to 92%, as shown in Fig. 9, then the absorptive, adaptive, and restorative capacities should be enhanced from 82.00% to 87.04%, 84.44% to 86.58%, and 87.00% to 91.46%, respectively. Several analyses could also be performed for different desired outcomes as well.

Remark 1. We realized that in the real-world BN models, where different number of states exist for each variable, it becomes a daunting task to perform all the calculations manually. Therefore, there is a need to develop computationally-efficient algorithms which are capable of assessing fast and efficient propagation for a large class of BN models. Among the existing ones, Junction Tree (JT) is commonly used to feature factorization of the distribution for efficient inference with faster calculation [77]. This inference algorithm runs based on

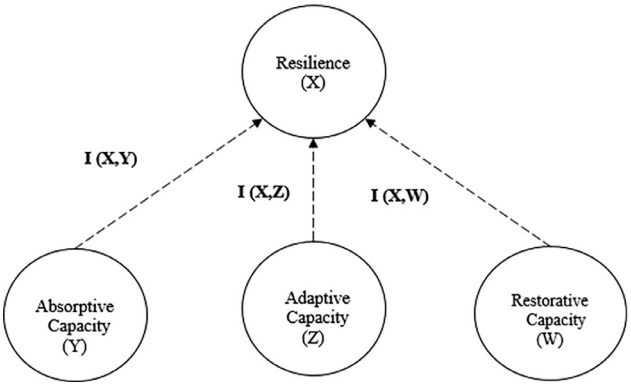


Fig. 13 – Mutual information between resilience and three individual capacities.

the distributive property of marginalization and conduct local computation on the different part of the tree and propagate this calculation to other parts of the tree. Future extension of this work can delve more into this research direction.

Sensitivity analysis is a useful means to check the validity of the expert-built simulation model. Sensitivity analysis provides a visual representation to understand the greatest impact of a set of variable nodes on a selected node (target node) in the BN. Sensitivity analysis is highly applicable in the field of analysis, quantification, and propagation of uncertainty in a complex system. In order to gain more insight and a better understanding of the simulation model, we have used AgenaRisk software to examine the extent to which the input parameters affect the output (target) of the underlying model. To examine the impact of the causal factors of the absorptive capacity, absorptive capacity is set as a target node and the impact of its causal factors is measured in terms of conditional probability. The sensitivity analysis of the absorptive capacity is illustrated in Fig. 10, in the form of a tornado graph. The length of the bar in the tornado chart represents the impact of that corresponding variable on absorptive capacity. Fig. 10(a) illustrates the impact of a set of selected nodes including reliability, maintenance, visual and physical protection, control strategy, alternative fuel source, information and communication, management and strong cyber-physical infrastructure on the absorptive capacity when absorptive capacity is *false*. Fig. 10(b) shows the impacts of those variables when the absorptive capacity is *true*. It is evident from both figures that reliability has the highest impact and visual and physical protection has the lowest impact on absorptive capacity. Fig. 10(b) further shows that the probability of absorptive capacity changes from 0.613 (when reliability is *false* = *fail*) to 0.856 (when reliability is *true* = *on*). Compared to the widely impacted range of reliability, the impact of visual and physical protection is limited to a narrow range which varies from 0.777 to 0.828. This implies that improvement in electrical system reliability will have the highest impact on improving the absorptive capacity of EIN, whereas improvement in visual and physical protection will have a negligible impact on enhancing the absorptive capacity of the EIN. The sensitivity analysis of adaptive and restorative capacities are shown in the Figs. 11 and 12, respectively. It is evident from Fig. 11 that a backup power source has the highest impact and provision of advanced technology has the lowest impact on improving adaptive capacity. Further, Fig. 12 shows that resource restoration has the highest impact and budget restoration has the lowest impact on improving restorative capacity.

In order to improve the quality of communication, we utilize *information theory* as proposed by Shannon and Weaver [78]. In information theory, *entropy* is one of the critical factors in calculating the mutual information between the parent node and its child nodes. The entropy is measured by the

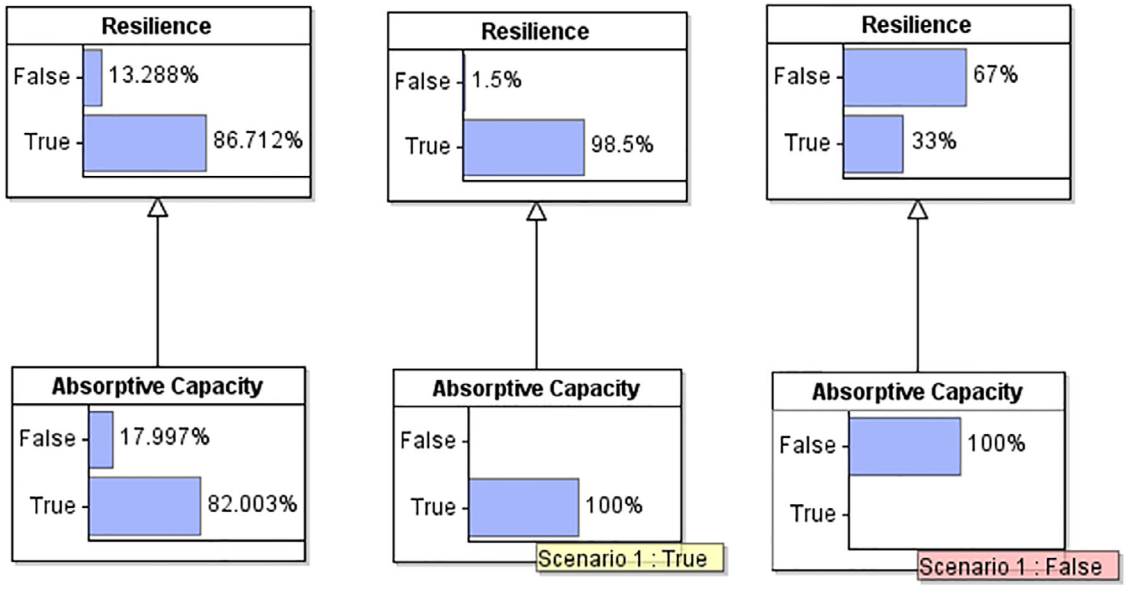


Fig. 14 – Different states of mutual information between resilience and absorptive capacity.

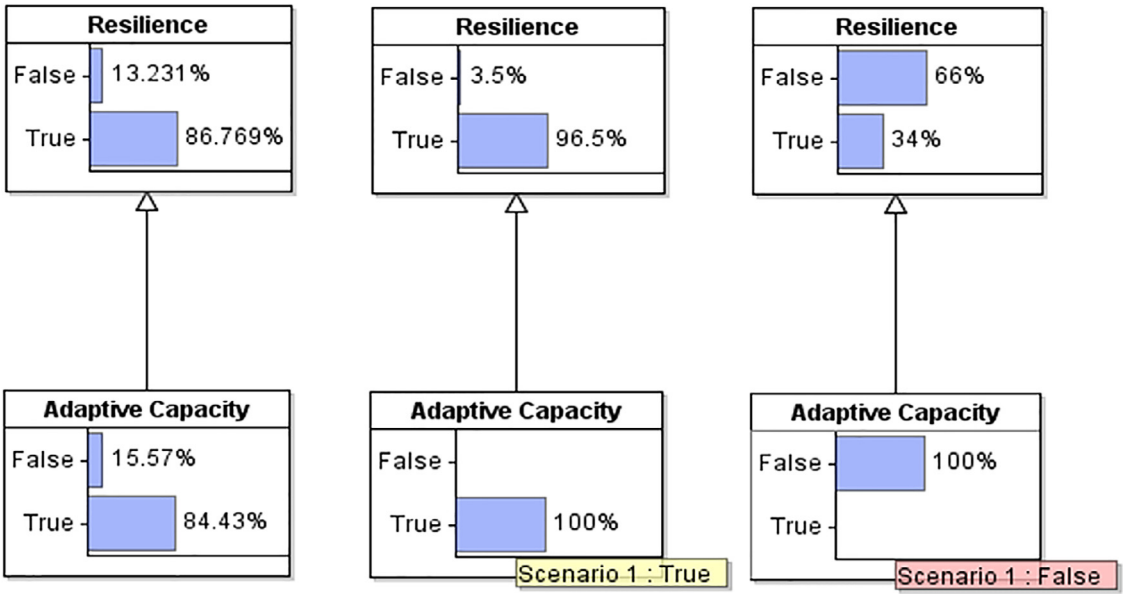


Fig. 15 – Different states of mutual information between resilience and adaptive capacity.

"mess" inherent in the variable X. Let $P(X)$ and $H(X)$ be the probability and entropy of a random variable X. In terms of risk analysis, entropy is a measure of uncertainty which can be computed using Eq. (21) as shown below:

$$H(X) = -\sum_{x \in X} P_X(x) log_2 P_X(x) \tag{21}$$

Suppose, the entropy of the target node X is conditional on its dependent variables Y, then Eq. (22) can be used to represent such relationships:

$$H(Y|X) = \sum_i P(Y_i) H(Y_i|X_i) \tag{22}$$

where i refers the number of states. The mutual information between the target node and its conditional node can be represented by Eq. (23) as shown below:

$$I(X, Y) = H(X) - H(Y|X) \tag{23}$$

where $I(X, Y)$ refers to the mutual information between the target node and its dependent node; $H(X)$ signifies the marginal entropy of the target node; and $H(Y|X)$ refers to the conditional entropy of target node on its dependent node.

In the proposed model, resilience is conditional on absorptive, adaptive, and restorative capacities. These capacities are connected through the dotted line with the resilience node as illustrated in Fig. 13. We have used dotted lines since in our model these capacities are not directly connected to resilience. We are interested in calculating the mutual information between resilience and all of these individual capacities. A different state of mutual information between resilience and absorptive capacity $I(X, Y)$ is shown in Fig. 14. The detailed calculation for mutual information between resilience and absorptive capacity $I(X, Y)$ is shown below. Note that H(Resilience), H(Resilience|Absorptive capacity), and I(Resilience, Absorptive capacity) are calculated using Eqs. (21), (22), and (23), respectively.

From Fig. 14, we find out that the prior probability of nodes (Resilience = Yes) = 0.867 and (Resilience = No) = 0.132. H(Resilience) and H(Resilience|Absorptive capacity) can be cmputed as follows:

$$\begin{aligned} H(\text{Resilience}) &= \sum_{x \in X} P_x(\text{Resilience}) log_2 P_x(\text{Resilience}) \\ &= 0.867 log_2(0.867) + 0.132 log_2(0.132) \\ &= 0.5656 \end{aligned}$$

$$\begin{aligned} &H(\text{Resilience}|\text{Absorptive capacity}) \\ &= \sum_{i=1}^{2} P(\text{Resilience}) \times H((\text{Resilience}|\text{Absorptive capacity}) \\ &= P(\text{Resilience} = \text{Yes}) H(\text{Resilience} = \text{Yes}|\text{Absorptive} \\ &\quad \text{capacity} = \text{Yes}) + P(\text{Resilience} = \text{No}) H(\text{ResilienceNo}| = \\ &\quad \text{Absorptive capacity} = \text{No}) \end{aligned} \tag{24}$$

In order to calculate H(Resilience = Yes|Absorptive capacity = Yes) and H(Resilience = No|Absorptive capacity = No) in equation (24), we set the absorptive capacity at *True* and *False* state, respectively, and simulate the model. The resulting outputs are reported below:

$$\begin{aligned} &H(\text{Resilience} = \text{Yes}|\text{Absorptive capacity} = \text{Yes}) \\ &= -\{0.985 log_2(0.985) + 0.015 log_2(0.015)\} \\ &= 0.1123 \\ &H(\text{Resilience} = \text{No}|\text{Absorptive capacity} = \text{No}) \\ &= -\{0.33 log_2(0.33) + 0.67 log_2(0.67)\} \\ &= 0.9149 \end{aligned}$$

Plugging the above values into Eq. (24) yields the following:

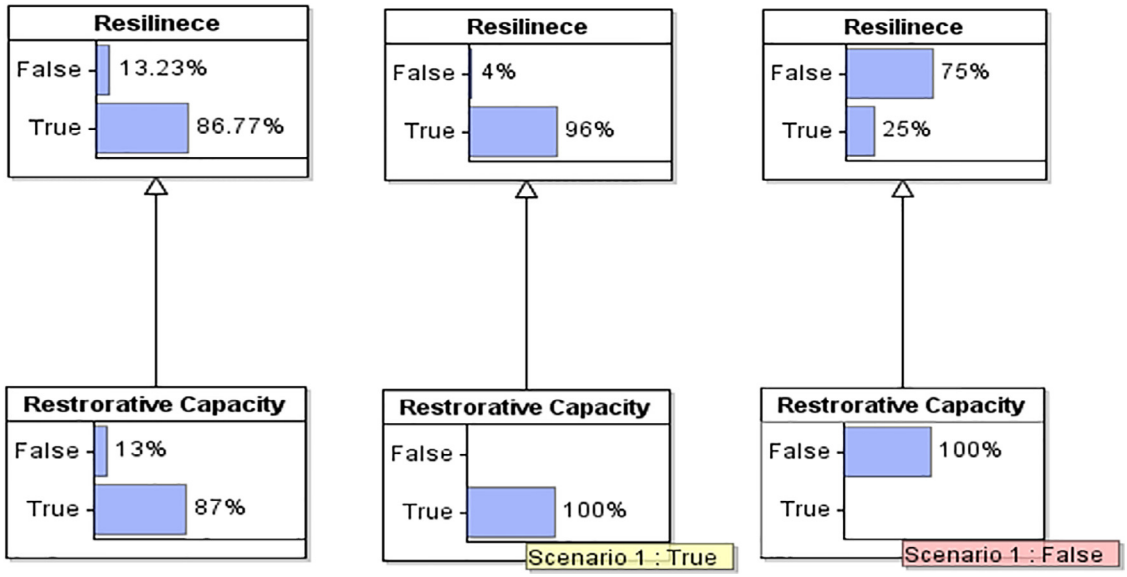


Fig. 16 – Different states of mutual information between resilience and restorative capacity.

Table 6 – Summary of information theory results.

H(Resilience|Types of capacity)	Mutual information	Significance of mutual information
H(Resilience|Absorptive capacity) = 21.81%	I(Resilience|Absorptive capacity) = 34.75%	If we have proper knowledge about absorptive capacity, we can reduce the uncertainty about resilience by 34.75%
H(Resilience|Adaptive capacity) = 31.27%	I(Resilience|Adaptive capacity) = 25.29%	If we have proper knowledge about adaptive capacity, we can reduce the uncertainty about resilience by 25.29%
H(Resilience|Restorative capacity) = 31.70%	I(Resilience|Restorative capacity) = 24.78%	If we have proper knowledge about restorative capacity, we can reduce the uncertainty about resilience by 24.78%
Concluding Remarks: I(Resilience, Absorptive capacity) > I(Resilience, Adaptive capacity) > I(Resilience, Restorative capacity). This implies that *absorptive capacity*, the first line of defense, has more influence in terms of uncertainty for the resilience of EIN.		

$$H(\text{Resilience}|\text{Absorptive capacity}) = (0.867 \times 0.11236) + (0.132 \times 0.91493) = 21.87\%$$

$$I(\text{Resilience}|\text{Absorptive capacity}) = H(X) - H(Y|X) = 0.5656 - 0.2181 = 34.75\%$$

This implies that if we have proper knowledge about absorptive capacity, we can reduce the uncertainty about resilience by 34.75%. Similarly, for adaptive capacity

$$H(\text{Resilience}) = \sum_{x \in X} P_x(\text{Resilience}) log_2 P_x(\text{Resilience}) = 0.5656$$

$$H(\text{Resilience}|\text{adaptive capacity}) = 0.3127 = 31.27\%$$

$$I(\text{Resilience, adaptive capacity}) = H(X) - H(Y|X) = 0.5656 - 0.3127 = 25.29\%$$

Likewise, it implies that if we have proper knowledge about adaptive capacity, we can reduce the uncertainty about resilience by 25.29%. Different states of mutual information between resilience and adaptive capacity is shown in Fig. 15.

Finally, for restorative capacity we can compute H(Resilience), H(Resilience|Restorative capacity), and I(Resilience, Restorative capacity) as follows:

$$H(\text{Resilience}) = \sum_{x \in X} P_x(\text{Resilience}) log_2 P_x(\text{Resilience}) = 0.5656$$

$$H(\text{Resilience}|\text{Restorative capacity}) = 0.3178 = 31.78\%$$

$$I(\text{Resilience, Restorative capacity}) = H(X) - H(Y|X) = 0.5656 - 0.3178 = 24.78\%$$

This implies that if we have proper knowledge about restorative capacity, we can reduce the uncertainty about resilience by 24.78%. Different states of mutual information between resilience and restorative capacity is shown in Fig. 16. The summary of results obtained from information theory are reported in Table 6.

6. Conclusion

A general framework for the resilience of electrical systems and their interdependents (EIN) is proposed in this research paper. The prime objective is to quantify the resilience of electrical systems during disruptive events. We developed a BN model for assessing resilience with respect to the concept of absorptive capacity, adaptive capacity, and restorative capacity. BN is a rigorous tool that provides a better insight into the uncertainty pertaining to complex models and allows the creation of future scenarios where assumptions and alterations in conditions or states can be tested and verified.

The proposed framework has been demonstrated through a case study of the interdependent electrical infrastructure system of Washington, D.C. The BN framework facilitates the identification of the different underlying factors that could potentially impact the resilience of the electrical system and its interdependent network. The information obtained from the historical data and the subjective judgment of experts is translated into BNs to provide a better understanding of the complex interaction among the different variables. The BN model is then validated through sensitivity analysis. We found that the key elements of the EIN are reliability, a backup power source, and resource restoration. The belief preparation further reveals how the failing of any variable impacts the other variables. The information theory analysis was also conducted to better understand the mutual information between resilience and different capacities. The contribution of this paper to the existing body of knowledge in interdependent electrical infrastructure system can be summarized as follows:

- A model for designing an electrical system and its interdependent network was developed.
- The underlying factors pertaining to interdependent electrical infrastructure system were identified and classified with respect to the concept of absorptive, adaptive and restorative capacities using Bayesian structure.
- A real-world case study of the model is presented and different kinds of analysis are performed to validate the effectiveness of the proposed model. Although this framework is specifically developed for the electrical infrastructure network, it can be modified based on the structure and nature of complex systems and utilized to quantify the resilience for any other system as well. This framework can also be used as a decision support tool in assessing risk and uncertainties in a complex environment and providing better insight when designing and developing strategies to offset the severity of a disruptive event.

This work can be extended in several directions. For instance, decision-theoretic troubleshooting for interdependent electrical infrastructure systems and corresponding improvement activities can be designed and executed in order to achieve higher resiliency.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.ijcip.2019.02.002.

REFERENCES

[1] U.S. Department of Energy, United States Electricity Industry Primer, 2015. Available from: https://www.energy.gov/sites/prod/files/2015/12/f28/united-states-electricity-industry-primer.pdf.

[2] B.L. Preston, S.N. Backhaus, M. Ewers, J.A. Phillips, J.E. Dagle, C.A. Silva-Monroy, A.G. Tarditi, J. Looney, T.J. King Jr., Resilience of the US Electricity System: A Multi-Hazard Perspective, Department of Energy. Washington DC, 2016.

[3] Presidents Council of Economic Advisers and the U.S. Department of Energys Office of Electricity Delivery and Energy Reliability, Economic Benefits of Increasing Electric Grid Resilience to Weather Outages, 2013. Available from: https://www.energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.

[4] National Academies of Sciences, Engineering, and Medicine, Enhancing the Resilience of the Nation's Electricity System, 2017. Available from: https://www.naesb.org/misc/nas_report.pdf.

[5] P. Tamvakis, Y. Xenidis, Comparative evaluation of resilience quantification methods for infrastructure systems, Procedia-Social and Behavioral Sciences, vol. 74, pp. 339–348, 2013.

[6] Statista, Economic loss from natural disasters worldwide 2000 to 2017., 2018. Available from: https://www.statista.com/statistics/510894/natural-disasters-globally-and-economic-losses.

[7] N. McCarthy, Economic Losses From Global Disasters Soared To $306 Billion In 2017, 2018. Available from: https://www.forbes.com/sites/niallmccarthy/2017/12/21/economic-losses-from-global-disasters-soared-to-306-billion-in-2017-infographic/#766cd2983fbf.

[8] A. Kimberly, Natural Disasters Effect on the Economy, 2018. Available from: https://www.thebalance.com/cost-of-natural-disasters-3306214.

[9] M. Bruneau, S.E. Chang, R.T. Eguchi, G.C. Lee, O T.D. Rourke, A.M. Reinhorn, M. Shinozuka, K. Tierney, W.A. Wallace, D. Von-Winterfeldt, A framework to quantitatively assess and enhance the seismic resilience of communities, Earthquake spectra, vol. 19(4), pp. 733–752, 2003.

[10] B. Buma, Disturbance interactions: characterization, prediction, and the potential for cascading effects, Ecosphere, vol. 6(4), pp. 1–15, 2015.

[11] B.D. Youn, C. Hu, P. Wang, Resilience-driven system design of complex engineered systems, Journal of Mechanical Design, vol. 133(10), 2011.

[12] A. Rose, Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions, Environmental Hazards, vol. 7(4), pp. 383–398, 2007.

[13] D. Henry, J.E. Ramirez-Marquez, Generic metrics and quantitative approaches for system resilience as a function of time, Reliability Engineering & System Safety vol. 99, pp. 114–122, 2012.

[14] M. Omer, Ali. Mostashari, U. Lindemann, Resilience analysis of soft infrastructure systems, Procedia Computer Science, vol. 28, pp, 565–574, 2014.

[15] U. Soni, Jain, Vipul., S. Kumar., Measuring supply chain resilience using a deterministic modeling approach, Computers & Industrial Engineering, vol. 74, pp. 11–25, 2014.

[16] H. Carvalho, A.P. Barroso, V.H. Machado, S. Azevedo, V. Cruz-Machado, Supply chain redesign for resilience using simulation, Computers & Industrial Engineering, vol. 62(1), pp. 329–341, 2012.

[17] R. Faturechi, E. Levenberg, E. Miller-Hooks, Evaluating and optimizing resilience of airport pavement networks, Computers & Operations Research, vol. 43, pp. 335–348, 2014.

[18] A.A. Khaled, M. Jin, D.B. Clarke, M.A. Hoque, Train design and routing optimization for evaluating criticality of freight railroad infrastructures, Transportation Research Part B: Methodological, vol. 71, pp. 71–84, 2015.

[19] E.D. Vugrin, M.A. Turnquist, N.J. Brown, Optimal recovery sequencing for enhanced resilience and service restoration in transportation networks, International Journal of Critical Infrastructures 10(3-4) (2014) 218–246.

[20] S.E. Chang, M. Shinozuka, Measuring improvements in the disaster resilience of communities, Earthquake spectra, vol. 20(3), pp. 739–755, 2004.

[21] G.P. Cimellaro, A.M. Reinhorn, M. Bruneau, Framework for analytical quantification of disaster resilience, Engineering Structures, vol. 32(11), pp. 3639–3649, 2010.

[22] Murray-Tuite P.M, A comparison of transportation network resilience under simulated system optimum and user equilibrium conditions., in: Winter Simulation Conference, pp. 1398–1405, 2006.

[23] B. Berche, C. Von-Ferber, T. Holovatch, Y. Holovatch, Resilience of public transport networks against attacks, The European Physical Journal B, vol. 71(1), pp. 125–137, 2009.

[24] K. Heaslip, W. Louisell, J. Collura, S.N. Urena, A sketch level method for assessing transportation network resiliency to natural disasters and man-made events, in: Transportation Research Board Annual Meeting, 2010.

[25] R. Dorbritz, Assessing the resilience of transportation systems in case of large-scale disastrous events., in: International Conference on Environmental Engineering, pp. 1070–1076, 2011.

[26] E. Miller-Hooks, X. Zhang, R. Faturechi, Measuring and maximizing resilience of freight transportation networks, Computers & Operations Research, vol. 39(7), pp. 1633–1643, 2012.

[27] S. Hosseini, K. Barker, J.E. Ramirez-Marquez, A review of definitions and measures of system resilience, Reliability Engineering & System Safety, vol. 145, pp. 47–61, 2016.

[28] P. Vlacheas, V. Stavroulaki, P. Demestichas, S. Cadzow, D. Ikonomou, S. Gorniak, Towards end-to-end network resilience, International Journal of Critical Infrastructure Protection, vol. 6(3-4), pp. 159–178, 2013.

[29] L. Labaka, J. Hernantes, J.M. Sarriegi, Resilience framework for critical infrastructures: An empirical study in a nuclear plant, Reliability Engineering & System Safety, vol. 141, pp. 92–105, 2015.

[30] J.P. Sterbenz, D. Hutchison, E.K. Cetinkaya, K. Egemen, A. Jabbar, J.P. Rohrer, M. Scholler, P. Smith, Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines, Computer Networks, vol. 54(8), pp. 1245–1265, 2010.

[31] G.H.A. Shirali, M. Motamedzade, I. Mohammadfam, V. Ebrahimipour, A. Moghimbeigi, Challenges in building resilience engineering (RE) and adaptive capacity: a field study in a chemical plant, Process safety and environmental protection, vol. 90(2), pp. 83–90, 2012.

[32] J.L. Bruyelle, C. ONeill, E.M. El-Koursi, F. Hamelin, N. Sartori, L. Khoudour, Improving the resilience of metro vehicle and passengers for an effective emergency response to terrorist attacks, Safety science, vol. 62, pp. 37–45, 2014.

[33] K. Barker, J.E. Ramirez-Marquez, C.M. Rocco, Resilience-based network component importance measures, Reliability Engineering & System Safety, vol. 117, pp. 89–97, 2013.

[34] R. Pant, K. Barker, J.E. Ramirez-Marquez, C.M. Rocco, Stochastic measures of resilience and their application to container terminals, Computers & Industrial Engineering, vol. 70, pp. 183–194, 2014.

[35] M. Ouyang, L. Dueñas-Osorio, X. Min, A three-stage resilience analysis framework for urban infrastructure systems, Structural safety, vol. 36, pp. 23–31, 2012.

[36] S. Enjalbert, F. Vanderhaegen, M. Pichon, K.A. Ouedraogo, P. Millot, Assessment of transportation system resilience, Human modelling in assisted transportation, 2011.

[37] K.H. Orwin, D.A. Wardle, New indices for quantifying the resistance and resilience of soil biota to exogenous disturbances, Soil Biology and Biochemistry, vol. 36(11), pp. 1907–1912, 2004.

[38] K.A. Ouedraogo, S. Enjalbert, F. Vanderhaegen, How to learn from the resilience of Human–Machine Systems?, Engineering Applications of Artificial Intelligence, vol. 26(1), pp. 24–34, 2013.

[39] C. Brown, E. Seville, J. Vargo, Measuring the organizational resilience of critical infrastructure providers: A New Zealand case study, International Journal of Critical Infrastructure Protection, vol. 18, pp. 37–49, 2017.

[40] D. Tadić,A. Aleksić, M. Stefanović, S. Arsovski, Evaluation and ranking of organizational resilience factors by using a two-step fuzzy AHP and fuzzy TOPSIS, Mathematical Problems in Engineering, 2014.

[41] A. Azadeh, V. Salehi, M. Arvan, M. Dolatkhah, Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps: A petrochemical plant, Safety Science, vol. 68, pp. 99–107, 2014.

[42] S.K. Jain, P.K. Bhunya, Reliability, resilience and vulnerability of a multipurpose storage reservoir/Confiance, résilience et vulnérabilité d'un barrage multi-objectifs, Hydrological sciences journal, vol. 53(2), pp. 434–447, 2008.

[43] V.L. Spiegler, M.M. Naim, J. Wikner, A control engineering approach to the assessment of supply chain resilience, International Journal of Production Research, vol. 50(21), pp. 6162–6187, 2012.

[44] F. Landegren, M. Host, P. Muller, Simulation based assessment of resilience of two large-scale socio-technical IT networks, International Journal of Critical Infrastructure Protection, 2018.

[45] D.L. Alderson, G.G. Brown, W.M. Carlyle, A. Newman, J. Leung, Assessing and improving operational resilience of critical infrastructures and other systems. Stat, vol. 745, p. 70, 2014.

[46] H. Baroud, K. Barker, J.E. Ramirez-Marquez, Importance measures for inland waterway network resilience, Transportation research part E: logistics and transportation review, vol. 62, pp. 55–67, 2014.

[47] S. Hosseini, K. Barker, A Bayesian network model for resilience-based supplier selection, International Journal of Production Economics, vol. 180, pp. 68–87, 2016.

[48] A.C. Constantinou, N. Fenton, W. Marsh, L. Radlinski, From complex questionnaire and interviewing data to intelligent Bayesian network models for medical decision support, Artificial intelligence in medicine, vol. 67, pp. 75–93, 2016.

[49] B. Khan, F. Khan, B. Veitch, M. Yang, An operational risk analysis tool to analyze marine transportation in Arctic waters, Reliability Engineering & System Safety, vol. 169, pp. 485–502, 2018.

[50] E. Pérez-Miñana, Improving ecosystem services modelling: Insights from a Bayesian network tools review, Environmental modelling & software, vol. 85, pp. 184–201, 2016.

[51] J. Amundson, W. Faulkner, S. Sukumara, J. Seay, F. Badurdeen, A bayesian network based approach for risk modeling to aid in development of sustainable biomass supply chains, Computer Aided Chemical Engineering, vol. 30, pp. 152–156, 2012.

[52] M. Hänninen, Bayesian networks for maritime traffic accident prevention: benefits and challenges, Accident Analysis & Prevention, vol. 73, pp. 305–312, 2014.

[53] B. Song, C. Lee, Y. Park, Assessing the risks of service failures based on ripple effects: a Bayesian network approach, International Journal of Production Economics, vol. 141(2), pp. 493–504, 2013.

[54] S. Hosseini, A. Al Khaled, M.D. Sarder, A general framework for assessing system resilience using Bayesian networks: A case study of sulfuric acid manufacturer, Journal of Manufacturing Systems, vol. 41, pp. 211–227, 2016.

[55] C. Arizmendi, D.A. Sierra, A. Vellido, E. Romero, Automated classification of brain tumours from short echo time in vivo MRS data using Gaussian Decomposition and Bayesian Neural Networks, Expert systems with applications, vol. 41(11), pp. 5296–5307, 2014.

[56] M. Perkusich, G. Soares, H. Almeida, A. Perkusich, A procedure to detect problems of processes in software development projects using Bayesian networks, Expert Systems with Applications, vol. 42(1), pp. 437–450, 2015.

[57] M. Hänninen, O.A.V. Banda, P. Kujala, Bayesian network model of maritime safety management, Expert Systems with Applications, vol. 41(17), pp. 7837–7846, 2014.

[58] Energy Information Administration (EIA), District of Columbia - State Energy Profile Overview - U.S. Energy Information Administration (EIA), 2018. Available from: https://www.eia.gov/state/?sid=DC.

[59] U.S. Department of Energy, Washington D.C. Energy Sector Risk Profile, 2018. Available from: https://www.energy.gov/sites/prod/files/2016/09/f33/DC_Energy%20Sector%20Risk%20Profile.pdf.

[60] National Centers for Environmental Information, Storms Events Database, 2014. Available from: https://www.ncdc.noaa.gov/data-access/severe-weather.

[61] A. Sharma, Resilience capacities assessment for critical infrastructure disruption., 2017. Master's [Thesis]. Italy: Politecnico di Milano.

[62] B. Biringer, E. Vugrin, D. Warren, Critical infrastructure system security and resiliency, CRC Press, 2016.

[63] B.A. Wender, M.G. Morgan, K.J. Holmes, Enhancing the Resilience of Electricity Systems, Engineering, vol. 3(5), pp. 580–582, 2017.

[64] Electric Power Research Institute, Electric Power System Resiliency Challenges and Opportunities, 2018. Available from: https://www.naseo.org/Data/Sites/1/resiliency-white-paper.pdf.

[65] G.C. Gallopín, S. Funtowicz, M. O'Connor, J. Ravetz, Science for the Twenty-First century: From social contract to the scientific core, International Social Science Journal, vol. 53(168), pp. 219–229, 2001.

[66] National Renewable Energy Laboratory, The Role of Smart Grid in Integrating Renewable Energy, 2018. Available from: https://www.nrel.gov/docs/fy15osti/63919.pdf.

[67] Y.Y. Haimes, On the definition of resilience in systems, Risk Analysis, vol. 29(4), pp. 498–501, 2009.

[68] Mission Support Center:Idaho National Laboratory, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, 2018. Available from: https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

[69] N. Fenton, M. Neil, Risk assessment and decision analysis with Bayesian networks, CRC Press, 2012.

[70] W.C. Salmon, Bayes's Theorum and the history of science, 1970. Available from: https://conservancy.umn.edu/bitstream/handle/11299/184663/5-03_Salmon.pdf?sequence=1.

[71] T.L. Saaty, Decision making with the analytic hierarchy process, International journal of services sciences, vol. 1(1), pp. 83–98, 2008.

[72] E.D. Vugrin, D.E. Warren, M.A. Ehlen, A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane, Process Safety Progress, vol. 30(3), pp. 280–290, 2011.

[73] D. Porcellinis, G. Olivia, S. Panzieri, R. Setola, A holistic-reductionistic approach for modeling interdependencies, in: International Conference on Critical Infrastructure Protection, pp. 215–227, 2009.

[74] D. Porcellinis, S. Panzieri, R. Setola, Modelling critical infrastructure via a mixed holistic reductionistic approach, International Journal of Critical Infrastructure, vol. 5(1–2), pp. 86–99, 2009.

[75] D. Porcellinis, R. Setola, S. Panzieri, G. Ulivi, Simulation of heterogeneous and interdependent critical infrastructures, International Journal of Critical Infrastructure, vol. 4(1–2), pp. 110–128, 2008.

[76] D.Y. Chang, Applications of the extent analysis method on fuzzy AHP, European journal of operational research, vol. 95(3), pp. 649–655, 1996.

[77] M. Borsotto, W. Zhang, E. Kapanci, A. Pfeffer, C. Crick, A junction tree propagation algorithm for bayesian networks with second-order uncertainties, in: IEEE Tools with Artificial Intelligence, pp. 455–464, 2006.

[78] R.M. Gray, Entropy and information theory, Springer Science & Business Media, 2011.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
April 2021	Final	

4. TITLE AND SUBTITLE

A Framework for Modeling and Assessing System Resilience Using a Bayesian Network: A Case Study of an Interdependent Electrical Infrastructure Systems

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
0603461A

6. AUTHOR(S)

Niamat Ullah Ibne Hossain, Raed Jaradat, Seyedmohsen Hosseini, Mohammad Marufuzzaman, and Randy K. Buchanan

5d. PROJECT NUMBER
DW5

5e. TASK NUMBER
01

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Engineer Research and Development Center
Information Technology Laboratory
3909 Halls Ferry Road
Vicksburg, MS 39180

8. PERFORMING ORGANIZATION REPORT NUMBER

ERDC/ITL MP-21-2

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army Corps of Engineers
Washington, DC 20314

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

This paper was originally published in the *International Journal of Critical Infrastructure Protection* on 13 February 2019.

14. ABSTRACT

This research utilizes Bayesian network to address a range of possible risks to the electrical power system and its interdependent networks (EIN) and offers possible options to mitigate the consequences of a disruption. The interdependent electrical infrastructure system in Washington, D.C. is used as a case study to quantify the resilience using the Bayesian net- work. Quantification of resilience is further analyzed based on different types of analysis such as forward propagation, backward propagation, sensitivity analysis, and information theory. The general insight drawn from these analyses indicate that reliability, backup power source, and resource restoration are the prime factors contributed towards enhancing the resilience of an interdependent electrical infrastructure system.

15. SUBJECT TERMS

Bayesian network, Electrical infrastructure system, System resilience, Resilience capacity

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
Unclassified	Unclassified	Unclassified	SAR	25	