Proceedings of the 2023 Winter Simulation Conference
C. G. Corlu, S. R. Hunter, H. Lam, B. S. Onggo, J. Shortle and B. Biller, eds.

A MATHEMATICAL THEORY TO QUANTIFY CYBER-RESILIENCE IN IT/OT NETWORKS

Ranjan Pal
Michael Siegel

Sloan School of Management
Massachusetts Institute of Technology
E94, 245 First Street
Cambridge, MA 02142, USA

Rohan Xavier Sequeira

Electrical and Computer Engineering
University of Southern California
3740 McClintock Avenue
Los Angeles, CA 90089, USA

ABSTRACT

Modern enterprise infrastructures (EIs) including those of industrial control systems (ICSs) are becoming increasingly crucial to businesses in a wide range of sectors spanning multiple end-user verticals (e.g., energy, chemical, manufacturing, biotechnology). These EIs improve the (real-time) decision support, productivity, and efficiency of business processes, but are necessarily reliant upon the cyber-resilience of complex infrastructures for sustainable business continuity. We are interested in the long-standing open question in the cyber-resilience domain: *how can managers formally quantify cyber-resilience for any complex networked EI (sub-)system in the event of a cyber-attack affecting its multiple (inter-dependent) components?* We propose a simulation-backed framework derived from probabilistic graph theory to answer this question. We pioneer the derivation and analysis of a quantifiable, closed-form *manager-friendly* expression exhibiting the degree of cyber-resilience (dependent upon individual EI component functionality quality and the varying extents of functional dependencies across networked components) within the (sub-)system post cyber-attack(s) affecting an EI.

1 INTRODUCTION

The modern IoT/CPS driven enterprise market - mostly spanned by industrial control system (ICS) driven enterprises, is currently valued at least around a few hundred billion dollars globally and growing at a CAGR of approximately 10% (according to *GlobeNewswire*). This market is crucial to businesses spanning a wide range of (public and private) sectors that include energy, chemical, power, manufacturing, transportation, biotechnology, and other end-user verticals. The physical machinery underlying the business supporting enterprise infrastructures (EIs), that traditionally used to be dumb, are often embedded today with software-programmable IoT/CPS devices such as sensors, actuators, programmable logic controllers (PLCs), programmable automation controllers (PACs), and intelligent electronic devices (IEDs). Furthermore, these devices can communicate with each other over a wireless network (e.g., WiFi, 5G) and/or the Internet through proprietary network protocols. This results in a smart and networked cyber-physical infrastructure with associated IT/software and OT controls supporting increasingly new forms of running enterprise business processes built upon software stacks. The steady growth of such cyber-physical EIs is primarily due to (a) rising cost of labor, (b) pressure on businesses to satisfy the two-fold constraint of meeting receding deadlines under increasing demand, (c) organizational push to improve quality control via real-time data driven decision making, and (d) mitigating human error in increasingly automated business processes. In summary, networked cyber-physical EIs will generate significant economic and societal benefits through improved efficiency, productivity, and reliability of a plethora of (critical) day-to-day business processes.

Despite the continual technical advancements in IoT/CPS technology, an EI can necessarily sustain business continuity (BC) both, for itself and for other external (ICS-driven EI reliant) businesses dependent

979-8-3503-6966-3/23/$31.00 ©2023 IEEE

on it, only if relevant (sub-)systems spanning the EI are cyber-resilient in the face of business-disrupting cyber-beach incidents. In this paper, we define 'cyber-resilience' as *the ability of any system (in this work, any (sub-)system at the physical and/or software spanned by an EI) to successfully absorb and adapt to such cyber-breach incidents [(Cutter et al. 2013)] by providing a minimum acceptable level of business functionality performance*. This ability is usually quantified in a metric that further drives enterprise C-suites to appropriately invest in resilience management and engineering.

As an example of non cyber-resilient system behavior, unauthorized access (e.g., via a spear phishing cyber-attack) into the supervised control and data acquisition (SCADA) system of an electric power grid can result in multiple software-controlled substations (representing ICS sub-systems) being disconnected for hours *(hence exhibiting cyber non-resilience)*, eventually leading to regional power blackouts that will not only disrupt consumer lifestyle and the local energy transmission business, but all other businesses (e.g., manufacturing, healthcare) that are (critically) dependent on power. Here, blackout events project the inability of the power grid to adapt or recover to a cyber-attack by providing enough electricity to certain (critical) corporations and/or households for a minimum amount of time (consequently satisfying a minimal BC threshold), even if the rest do not have power. The *Kyivoblenergo* regional electric distribution company in Ukraine faced a similar cyber-attack in the year 2015 when approximately 230,000 of their customers in the *Ivano-Frankivsk* region and inter-dependent businesses lost power (*https://www.globalsign.com/en/blog/cyber-autopsy-series-ukranian-power-grid-attack-makes-history*). Unfortunately, each EI built upon ICSs usually operates on a large cyber-risk terrain at its network, device, workstation, and perimeter layers that contributes to hundreds of thousands of cyber-vulnerabilities which adversaries can exploit - many of them capable of causing large-scale systemic business disruptions.

With (state-sponsored) cyber-attacks on (critical) EI infrastructure on the rise, it is mandatory for EI management to have a cyber-resilience plan in operation to sustain business continuity in the face of such cyber-attacks. The foundation elements of such a management plan often involve (but not limited to) (a) quantifying EI cyber-resilience via a metric and (b) subsequently deriving a constrained budget-allocation framework to enable an EI management to achieve a desired level of cyber-resilience. *We focus on the former foundational element in this paper.*

1.1 Research Contributions and Novelty

Motivated by the fact that there is a lack of (formally-backed) principles (in research or industry literature) among organizations (ICS-driven or otherwise) around the globe on how C-suites should metricize the degree of cyber-resilience for complex business processes in the event of cyber-attacks, *we take a first pass at proposing a general formal framework to* quantify *cyber-resilience in a complex IT/IoT driven EI system having inter-dependent networked (at either the physical, logical, informational, or geographical abstraction) components.* We make the following research contributions in this paper.

- We model an enterprise infrastructure (EI) as a general (physical, logical, informational, or geographical) weighted directed network of inter-dependent components, where the inter-component linkages, i.e., network edges, represent a measure of directional inter-dependency between components of the EI. In the event that a cyber-attack on any EI (sub-)system *directly* brings down multiple specific components (usually primary infrastructure targets by cyber-adversaries), we first derive an analytical and easily computable expression, using principles from the theory of fixed-point equations and lattice algebra, for the number of inter-dependent components that *indirectly* (via a spread effect) fail to function at their 'basic minimum' ability to (partially) support other components dependent on them for functioning. We term such components (both directly and indirectly affected) as 'dysfunctional'. The novelty of our approach rests in explicitly accounting for component inter-dependencies (apart from their logical network connectivity) while deriving such a metric that captures the total number of dysfunctional EI components post a cyber-attack event. *We identify this simple metric as a manager-friendly measure to quantify EI cyber-resilience* *given that the former is directly related and inversely proportional to an EI's ability to absorb and adapt from cyber-attack(s) - a standard definition of system resilience (Linkov et al. 2013).* From the perspective of enterprise cyber-resilience management, our proposed metric provides C-suites with an average estimate of the monetary impact of business disruption. This estimate is a determining factor for cyber-resilience budget planning (see Sections 2 and 3).

- We subsequently derive a closed form (quantifiable) expression for our proposed cyber-resilience measure for any general networked EI with interdependent components using probabilistic graph theory. We validate our theory with extensive Monte Carlo simulations that also output the statistical equivalent of our measure *apriori*, over multiple attack configurations. After all, managers cannot wait to assess enterprise cyber-resilience post a cyber-attack event as it moots the resilience planning and management process. *Apart from formally and uniquely accounting for system network topology, our metric formally and uniquely accounts for system network randomness, cyber-attack impact randomness, and the randomness in various components' ability to adapt and absorb the adverse impact of a cyber-attack.* This statistical, quantifiable, and computable measure of EI cyber-resilience provides enterprise management with an instantaneous and simple base estimate on how robust its (sub-)systems are post a cyber-attack, for existing (i.e., status quo) investments made towards ensuring cyber-resilience [(Alderson and Doyle 2010; Allspaw 2012)] (see Sections 4 and 5).

To the best of knowledge, we pioneer mathematical system resilience theory to quantify cyber-resilience for complex networked cyber infrastructures with functionally inter-dependent system components.

1.2 Related Work

Most well-known system cyber-resilience metrics introduced in the research literature are engineering focused, and either model cyber-resilience as (a) a rebound of the system from cyber-shock to reach the usual state of equilibrium level of performance at which the system usually performs, or (b) a synonym for robustness allowing the system to function at degraded but acceptable levels of performance post a rebound from a cyber-shock (Segovia et al. 2020; Francis and Bekera 2014; Linkov et al. 2013; Clark and Zonouz 2017; Woods 2015; Hosseini et al. 2016; Arghandeh et al. 2016; Gholami et al. 2018; Venkataramanan et al. 2019; Venkataramanan et al. 2019; Zuloaga et al. 2019; Hossain-McKenzie et al. 2018; DiMase et al. 2015; Sterbenz et al. 2011; Chaves et al. 2017; Haque et al. 2018). Despite a highly application-dependent overloading in the definition of cyber-resilience across these works, the common aspect among these metrics is that they are derived using mathematical frameworks that all account for the cyber-vulnerability dynamics of each (sub-)system component or a network (Haque et al. 2018), alongside some accounting for an adversarial input to model the cyber-vulnerability dynamics.

However, a common drawback to all these metrics is the fact that none of them account for the extent of liabilities between EI components - a salient complex system property, irrespective of whether the cyber-resilience measure is network dependent or not. More specifically, the degree of liability between (sub-)system components creates negative service degradation externalities that (non-linearly) percolate throughout an EI network when individual components experience a cyber-shock. These percolating externalities, that directly influence the ability of components to absorb and adapt, go unaccounted for in the calculation of existing cyber-resilience metrics. As an example, a water-cooling component within an ICS-type EI (e.g., a manufacturing plant) might heavily depend on component *A* for water. In the event of *A* failing, components *B* and *C* might partially satisfy the water demands of the cooling component which allow the latter to function with a degraded quality of service (QoS). Nonetheless, this degradation is not stand-alone, and would recursively percolate (hence the negative externality effect) within the component network affecting the QoS of all components that depend on the water-cooling component as the root service source. Such externalities need to be necessarily accounted for in metrics aiming to accurately model system cyber-resilience, and is missing, as a major drawback, from existing literature.

In line with the above-mentioned common cyber-resilience metric pitfall in existing literature, we in this paper, are interested in the long-standing open question (Musman et al. 2019; Cybenko 2019) in the cyber-resilience domain: *how can managers formally quantify cyber-resilience for any complex networked EI (sub-)system in the event of a cyber-attack affecting its multiple (inter-dependent) components?* To this end, we alleviate the aforementioned pitfall by the design and analysis of a formal amalgamated methodology rooted in probabilistic graph theory and lattice-theoretic fixed point algebra results (Topkis 1978), that accounts for the percolation of the negative externalities throughout a liability-driven EI network in determining a quantitative measure of cyber-resilience. This methodology importantly adds to the effectiveness and accuracy of the multiple existing and overloaded definitions of EI cyber-resilience that do not capture the said percolating externalities post cyber-shocks hitting multiple nodes of an EI network. With respect to modeling the aspect of externality percolation, we adopt the seminal works on *bootstrap percolation theory* (Holroyd 2003; Balogh and Bollobás 2006; Balogh and Pittel 2007) for un-directed networks and extend them to our EI setting of weighted directed graphs. The strong relevance of using bootstrap percolation theory in our work lies in the fact that (a) it is popular in fault tolerant distributed system models to analyze cascading-related failure probabilities in non-homogeneous systems - a defining characteristic of EIs in general, and (b) allows us to effectively analyze at scale networked systems of large sizes in the number of (sub-)system components (Kirkpatrick et al. 2002) - a property of societal EIs.

2 SYSTEM MODEL

We consider a general enterprise infrastructure setting reliant upon IT and/or IoT technology in our work. *However, without loss of generality and for the purpose of exposition, we present an industrial control system (ICS) as a representative example of an EI infrastructure in this paper.* We assume that an ICS comprises networked components that often exhibit inter-dependent relationships with each other. These inter-dependencies could be either at the physical, informational, geographical, or logical levels of abstraction. As pertinent examples of some of these inter-dependencies in the smart grid setting, we have (a) the supply of natural gas at a minimum pressure of 300 psig as a necessary functioning constraint for boilers; the supply of lube oil necessary for turbines and generators; and the supply of water for emissions control, as examples of physical inter-dependencies, (b) message-based e-recommendations from the energy management system (EMS) to turbines on optimal throttle settings; and networked transmissions of real-time operational conditions recorded by a power plant information system to EMS and plant engineers over a demilitarized zone (DMZ) router, as examples of informational dependencies, and (c) inter-dependencies among turbines, boilers, and chillers in different geographical locations, as examples of geographical dependencies. A figurative illustration of such functional dependencies in a real-world smart grid is shown in Figure 1, and borrowed from (Khan and Madnick 2021).

We model an ICS (or any of its sub-systems) by a weighted directed graph $G = (V, \mathbf{e})$. The vertex set $V = \{1, \ldots, n\} = [n]$ represent (sub-)system components. The *edge inter-dependency matrix* is given by $\mathbf{e} \in^{n \times n}$, where the ij-th entry $e(i, j)$ represents the amount of service liability (in tangible units) component i owes from component j for the normal functioning of i. As an example, i could be a cooling tower for a power plant that needs to consume approximately 2.4 gallons of water per minute (supplied from multiple sources, each representing a j and the sum of $e(i, j)$'s summing to 2.4) of operation per 100 tons of cooling required to always maintain a certain temperature range inside a power plant. The inability to do so will likely trigger overheating of machines inside the power plant and significantly increase the likelihood of their damage. The $e(i, j)$ values are usually known and obtained/estimated by site management administration by observing the traditional normal functioning of ICS operations over time. The inter-component service liability (inter-dependency) owed by any component i from other j's is given by $A(i) := \sum_j e(i, j)$. In a similar fashion, $\sum_j e(j, i)$ represents the inter-component liabilities i owes to other js in the ICS network. In addition to these inter-component liabilities, each component i may self-invest to 'generate' (including 'processing' efforts) D_i amounts of a relevant resource to serve its functionality. Figure 2 provides a

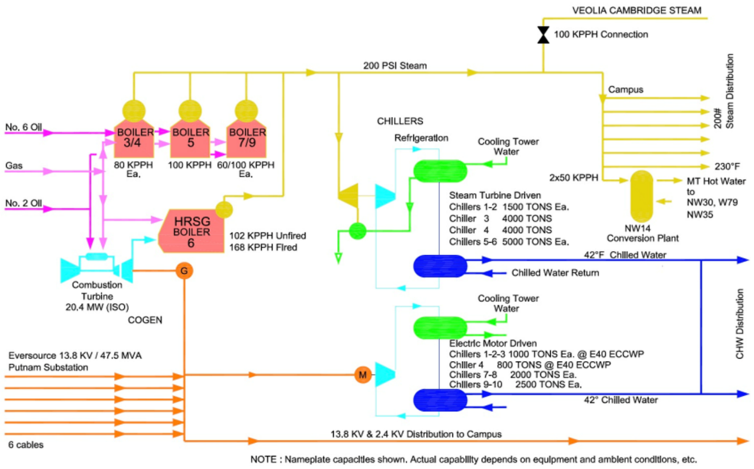


Figure 1: Illustrating functional dependencies among networked EI (i.e, a thermal plant ICS) components.

figurative illustration of our graph modeling ideas. Here, the purple arrows denote the $e(i,j)$ variables of our proposed graphical model.

Having modeled an ICS into a graph, we define a general ICS network, $(\mathbf{e},\gamma)$, to be one with the vertex set $V=[n]$ having a matrix of liability (inter-dependency) exposures $\{e(i,j)\}_{1\leq i,j\leq n}$, and a set of node independence quotient (NIQ) ratios $\{\gamma(i)\}_{1\leq i\leq n}$. Here, $\gamma(i):=\frac{c(i)}{A(i)}$ for each ICS component i is the ratio of the total amount of resources, $c(i)$, available to a component i to sustain functionality to the amount of resources i receives *only* from other components in the network via inter-dependent relationships to sustain the same functionality. Here, $c(i)=x(i)+\sum_{j\neq i}e(i,j)-\sum_{j\neq i}e(j,i)$ with $x(i)$ indicating self-reliant resources for component i. *In order words, $\gamma(i)$ for each component i represents how independent i is with respect to resources supporting its functionality in a resource inter-dependent network.* In this network, the *in-degree* of a node i is given by

$$d^{-}(i):=\#\{j\in V\mid\ e(j,i)>0\},$$

which represents the number of ICS components resource-dependent on i (i.e., the components i is liable to), while component i's *out-degree*

$$d^{+}(i):=\#\{j\in V\mid\ e(i,j)>0\}$$

represents the number of ICS components i is resource-dependent upon (i.e., nodes liable to i).

We assume that each EI node (e.g., an ICS component) i is subject to a non-negative pre-determined cyber-protection budget endorsed by the EI management that might allow it to sustainably function (albeit at a degraded performance) in the face of an adverse impact caused by a cyber-attack. We further assume that this budget is distributed across the EI components (nodes) following a statistical distribution that is usually (but not necessarily) a function of the strategic (with respect to inter-node liabilities) location of the nodes in the network. To rationalize this point, consider an example of an advanced persistent threat (APT) conducted through a botnet that spreads malware throughout an ICS network of IoT/CPS devices. Since the inter-dependent liability structure is heterogeneous across the nodes (with high in-degree nodes being increasingly critical and significantly liable), it makes management sense to invest in a cyber-protection budget that is proportional to (among other factors) the liability structure (investing higher in more critical nodes). Furthermore, we assume that this distribution induces a recovery probability R_i (attack-dependent among other factors) for each node i when it is compromised by the cyber-attack.

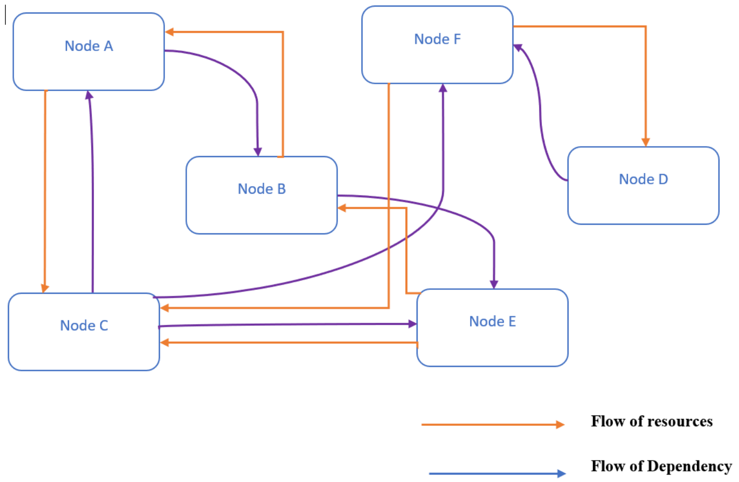


Figure 2: Graphical dependencies among networked EI components (nodes). The node dependencies are in purple arrows opposite to the (orange) arrows denoting resource flow characterizing the dependency.

3 HOW MANY EI COMPONENTS FAIL TO FUNCTION POST A CYBER-ATTACK?

An important metric to study is the number of components that fail to function in the event of a cyber-attack launched on an EI network (e.g., ICS network). *It is evident that this metric directly, but negatively, correlates with a measure of cyber-resilience - simply because a higher value of this metric is inversely proportional to the ability of any EI to absorb and adapt to cyber-attack events.* We will analyse this metric in this paper as a measure of cyber-resilience with respect to the definition in (Linkov et al. 2013).

We assume that a cyber-attack on an EI network induces *direct* (without the support of a network spread effect) performance hits to some of its (critical) components (e.g., as present in ICSs) that are the first to become dysfunctional in the EI network post attack. A practical example of such a setting is a traditional botnet induced cyber-attack (e.g., APT) on an ICS where a subset of critical nodes are initially targeted by adversaries who bring them down (e.g., via phishing or email spoofing attacks). We assume that this set of initial dysfunctional components (nodes) in network $(\mathbf{e},\gamma)$, denoted by $\mathbb{D}_0(\mathbf{e},\gamma)$, is given by

$$\mathbb{D}_0(e,\gamma) = \{i \in V \mid \gamma(i) = 0\},$$

where an NIQ value (γ_i) of 0 for any node i reflects its dysfunctional nature, or complete breakdown, to provide service (even at a degraded level of performance) to other ICS components dependent upon it. Now given that R_j is the recovery probability of any component j in the network, a dysfunctional j induces an expected loss (with respect to a given resource) amount of $(1-R_j))e(i,j)$ for component i that is dependent upon j as a resource supply. In the event that this loss exceeds $c(i) = \gamma(i)A(i)$, ICS component i becomes dysfunctional due to the loss amount of $(1-R_j))e(i,j)$ that acts as a negative externality, i.e., spillover effects, on the functioning ability (albeit at a degraded level) of components reliant upon j. The set of nodes (components) in $(\mathbf{e},\gamma)$ that subsequently become dysfunctional due to negative externality effects of $j \in \mathbb{D}_0(\mathbf{e},\gamma)$ becoming dysfunctional is then given by

$$\mathbb{D}_1(\mathbf{e},\gamma) = \{i \in V \mid \ \gamma(i)A(i) < \sum_{j \in \mathbb{D}_0} (1-R(j))e(i,j)\}.$$

This phenomenon is recursive in fashion and initiates a cascade of *indirect* (due to a spread process) EI component failures within the network. More generally, $\mathbb{D}_k(\mathbf{e},\gamma)$ represents the set of networked EI network components that are resource starved enough to be incapable of functioning due to failures of components in the set $\mathbb{D}_{k-1}(\mathbf{e},\gamma)$. It is self-evident that in an EI network of size n, the cascading process of generating EI component failures ends after at most $n-1$ iterations. Hence, $\mathbb{D}_{n-1}(\mathbf{e},\gamma)$ represents the set of *all* EI components which become dysfunctional post a cyber-attack, given the initial set of dysfunctional components, $\mathbb{D}_0(\mathbf{e},\gamma)$, generated due to a direct impact by the cyber-attack. Evidently, $\mathbb{D}_0(\mathbf{e},\gamma) \subseteq \mathbb{D}_1(e,\gamma) \subseteq \ldots \subseteq \mathbb{D}_{n-1}(\mathbf{e},\gamma)$, with $\alpha_n = \frac{|\mathbb{D}_{n-1}(\mathbf{e},\gamma)|}{n}$ denoting the final fraction of the nodes (components) in an EI network that fails to function (even at degraded levels of performance) post a cyber-attack hitting an EI. In reference to an APT launched on an EI, such a cascading event occurs when the botnet-induced malware propagates through cyber-protected EI components - potentially disabling them to such an extent that they are not independent enough to overcome the resource limitations posed by other dysfunctional components they rely upon for sustaining component functionality (albeit at a degraded performance level). Two questions of immense management interest that arises are: (i) *are α_n and $(\mathbb{D}_{n-1}(\mathbf{e},\gamma))$ fixed, i.e., converge, after n - 1 iterations?*, and (ii) *does there exist a closed form expression for α_n for general n?* In this section, we resort to lattice algebra to answer the first question. We have the following result as an answer.

Theorem 1 *For an EI with n components, the fraction of dysfunctional components $\alpha_n = \frac{|\mathbb{D}_{n-1}(\mathbf{e},\gamma)|}{n}$ and the associated recursive component set $\mathbb{D}_{n-1}(\mathbf{e},\gamma)$ post a cyber-attack converge after n - 1 iterations, given the knowledge of $(\mathbb{D}_0(\mathbf{e},\gamma))$ - the set of adversary targeted EI components directly getting dysfunctional due to the attack.*

Proof Insight - In order to answer the first question, the main crux is in realizing that the relation $\mathbb{D}_0(\mathbf{e},\gamma) \subseteq \mathbb{D}_1(\mathbf{e},\gamma) \subseteq \ldots \subseteq \mathbb{D}_{n-1}(\mathbf{e},\gamma)$ forms a lattice (Matoušek and Nešetřil 2008) as it is a partially ordered set (reflexive, anti-symmetric, and transitive) having both a least upper bound (the element $\mathbb{D}_{n-1}(\mathbf{e},\gamma)$)and a greatest lower bound (the element $\mathbb{D}_0(\mathbf{e},\gamma)$). What we need to look for is a vector comprising of $(1-R_j))e(i,j)$ values that results in $\mathbb{D}_{n-1}(\mathbf{e},\gamma)$ being a *fixed set* (one that does not get updated with iterations) such that

$$\mathbb{D}_n(\mathbf{e},\gamma) = \mathbb{D}_{n-1}(\mathbf{e},\gamma) = \{i \in V \mid \ \gamma(i)A(i) < \sum_{j \in \mathbb{D}_{n-2}} (1-R(j))e(i,j)\}. \tag{1}$$

We call such a vector a *clearing vector* as it clears the recursive $\mathbb{D}_i(\mathbf{e},\gamma)$ generation procedure from updating $\mathbb{D}_i(\mathbf{e},\gamma)$ at every iteration number greater than $n-1$. Evidently, the partially ordered set $\mathbb{D}_0(\mathbf{e},\gamma) \subseteq \mathbb{D}_1(\mathbf{e},\gamma) \subseteq \ldots \subseteq \mathbb{D}_{n-1}(\mathbf{e},\gamma)$ is a monotonic (increasing) sequence in the size of the sets. Then, according to the celebrated *Tarski Lattice Theorem* (Tarski 1955; Topkis 1978) (as applicable to this problem), there always exists a clearing vector of $(1-R_j))e(i,j)$ values being a fixed point in $\mathbb{R}^2$ that ensures (1) holds above, with the resulting partially ordered lattice having $\mathbb{D}_{n-1}(\mathbf{e},\gamma)$ as the greatest element and $\mathbb{D}_0(\mathbf{e},\gamma)$ as the least element. *Thus, α_n and $(\mathbb{D}_{n-1}(\mathbf{e},\gamma))$ are fixed after n - 1 iterations.*

Managerial Implications of the Theorem - The answer to the first question has significant implications for the EI management. It implies that if the latter has good knowledge (if not exact) about the set of main targets (components) behind a cyber-attack (represented by $\mathbb{D}_0(\mathbf{e},\gamma)$), they can tightly estimate in advance how many components (and necessarily which of them - characterized by $\mathbb{D}_{n-1}(\mathbf{e},\gamma)$) the cyber-attack majorly affect (result in their dysfunctionality) in the long-run, if the main targets, $\mathbb{D}_0(\mathbf{e},\gamma)$), become dysfunctional. The cyber-resilience metric α_n along with $\mathbb{D}_{n-1}(\mathbf{e},\gamma)$ enables an EI management to roughly estimate the amount of budget to reserve for system resilience boosting cyber-protection. The metric serves a handle to the famous saying *"if you can't measure it"* (e.g., cyber-resilience), *"you can't manage it"*.

4 A CLOSED FORM EXPRESSION FOR THE PROXY CYBER-RESILIENCE MEASURE

Thus far, we have shown that cyber-resilience in a networked EI with inter-dependent components is quantifiable via a measure, α_n. However, we are yet to express this measure in closed form as a function of the EI network topology and component inter-dependencies. In this section we answer in the affirmative: *does there exist a closed form quantifiable expression of α_n (general n) for arbitrary EI instances?*, via resorting to the use of probabilistic (random) graph theory.

In order to derive a closed form expression for α_n, we first need to formally capture the entire space of EI network structures possible. Using theoretical developments in (Amini et al. 2016), we do this by first letting $\mathscr{G}_n(\mathbf{e}_n)$ be the set of all n-node weighted directed graphs (networks) with degree sequence $\mathbf{d}_n^+, \mathbf{d}_n^-$. In other words, given an in-degree and out-degree sequence for each node in the EI network, $\mathscr{G}_n(\mathbf{e}_n)$ denotes the set of all possible networks that can be formed with this configuration. Given $\mathbf{d}_n^+, \mathbf{d}_n^-$, there is no reason to prefer any network over the other, as EI network structures with such a degree configuration are equally likely over the space of all EI networks. Let $(\Omega, \mathscr{A}, \mathbb{P})$ be a probability space, on which we define $\mathbf{E}_n : \Omega \to \mathscr{G}_n(\mathbf{e}_n)$ as a random directed graph uniformly distributed on $\mathscr{G}_n(\mathbf{e}_n)$.

Having formalized the space of EI networks, our next step to deriving a closed form expression for α_n is to formalize the degree statistics of graphs in this space. Subsequently, for any given $\mathbf{e}_n$, let

$$\mu_n(j,k) := \frac{1}{n}\#\{i \in [n] | d_n^+(i) = j, d_n^-(i) = k\},$$

be the empirical distribution of $\mathbf{d}_n^+, \mathbf{d}_n^-$. Then, we can assume a probability distribution μ on $\mathbb{N}^2$ such that for large n, $\mu_n(j,k) = \mu(j,k)$ as $n \to \infty$. This assumption is practically viable simply because with increasing network sizes, their empirical distribution of in and out-degrees (for all equiprobable networks with a given $\mathbf{d}_n^+, \mathbf{d}_n^-$ configuration) tends to become a constant distribution (this is easily verified through computer simulations even for a medium sized n). We can also assume that the number of components in any EI network will be finite and hence the average degree of any such network will be finite, i.e., $\sum_{j,k} j\mu(j,k) = \sum_{j,k} k\mu(j,k) = \lambda \in (0,\infty)$.

One must also note that, due to the service inter-dependencies between components, the order in which a sequence of components fail in an n-node EI network is also an important factor in eventually quantifying the number of components that will fail to function in the event of a cyber-attack. As a practical analogue, the order in which components such as a gas turbine, boiler, and chiller in an ICS electric power grid fail will lead to different α_n values for the grid (as the process spreading negative externalities within the network due to component failures differ with order). Hence, fail order sequence permutations are necessary to model en route quantifying α_n. In this regard, define $\Sigma_i^{\mathbf{e}}$ to be the set of permutations of the set $\{j \in [n] \mid \ e_{i,j} > 0\}$. For a node (component) i and permutation $\tau \in \Sigma_i^{\mathbf{e}}$ specifying the sequence in which the nodes that i depends upon fail to function, the threshold function determining the number of failed components i can withstand before it becomes dysfunctional is consequently given by

$$\Theta(i,\tau,\mathbf{e}) := \min\{k \geq 0 \mid \ \gamma_i \sum_{j=1}^{n} e_{i,j} < \sum_{j=1}^{k} (1-R) e_{i,\tau(j)}, \} \tag{2}$$

where it is assumed for analytical tractability that $R = R_i$, for all $i \in [n]$. We also define

$$p_n(j,k,\theta) := \frac{\#\{(i,\tau) \mid \ i \in [n], \ \tau \in \Sigma_i^{\mathbf{e}}, d_n^+(i) = j, d_n^- = k, \ \Theta(i,\tau,\mathbf{e}_n) = \theta\}}{n\mu_n(j,k)j!}, \tag{3}$$

where for large network sizes, n, $p_n(j,k,\theta)$ converges in probability to the constant, $p(j,k,\theta)$. Here, for $\theta = 1$, $n\mu_n(j,k)jp_n(j,k,1)$ represents the number of EI components on which nodes (components) with degree (j,k), with lower resource support than the former, are dependent upon for resources needed to function above a threshold level of performance. We have the following result adapted from the theory in (Amini et al. 2016) to characterize α_n for general enterprise infrastructure instances.

Theorem 2 *Let $\mathscr{G}_n(\mathbf{e}_n)$ be the set of all EI networks formally characterized by n-node weighted directed graphs (networks) with degree sequence $\mathbf{d}_n^+, \mathbf{d}_n^-$. Let π^* be the smallest fixed point of I in $[0,1]$, where we define the function $I : [0,1] \to [0,1]$ as*

$$I(\pi) := \sum_{j,k} \frac{\mu(j,k)k}{\lambda} \sum_{\theta=0}^{j} p(j,k,\theta)\beta(j,\pi,\theta), \tag{4}$$

where $\beta(j,\pi,\theta) := \mathbb{P}(Bin(j,\pi) \geq \theta) = \sum_{l\geq\theta}^{j} \binom{j}{l}\pi^{l}(1-\pi)^{j-l}$. Here, $I(\pi)$ represents (for large-enough ICS network sizes) the fact that if the end node of a randomly chosen inter-dependent edge becomes dysfunctional with probability π, $I(\pi)$ is the expected fraction of components dependent upon this randomly chosen node (component) that will fail (become dysfunctional) after one iteration of the cascade. Given $\mathbf{E}_n$ to be a random network uniformly sampled from $\mathscr{G}_n(\mathbf{e}_n)$, the following results consequently hold:

1. *The fraction of EI components that fail tends to one, i.e., all components fail, in the event of a cyber-attack if $\pi^* = 1$. In mathematical jargon, if $I(\pi) > \pi$ for all $\pi \in [0,1)$, then -*

$$\alpha_n(\mathbf{E}_n,\gamma_n) \xrightarrow{p} 1 \mid n \to \infty,$$

   signifying that almost all EI components fail in the event of a cyber-attack even if the number of components are large enough.
2. *The fraction of EI components that fail is less than 1 in the event of a cyber-attack if $\pi^* < 1$. In mathematical jargon, if $I'(\pi^*) < 1$, and furthermore π^* is a stable fixed point of I for all $\pi \in [0,1)$, then*

$$\alpha_n(\mathbf{E}_n,\gamma_n) \xrightarrow{p} \sum_{j,k}\mu(j,k)\sum_{\theta=0}^{j} p(j,k,\theta)\beta(j,\pi^*,\theta) \mid n \to \infty,$$

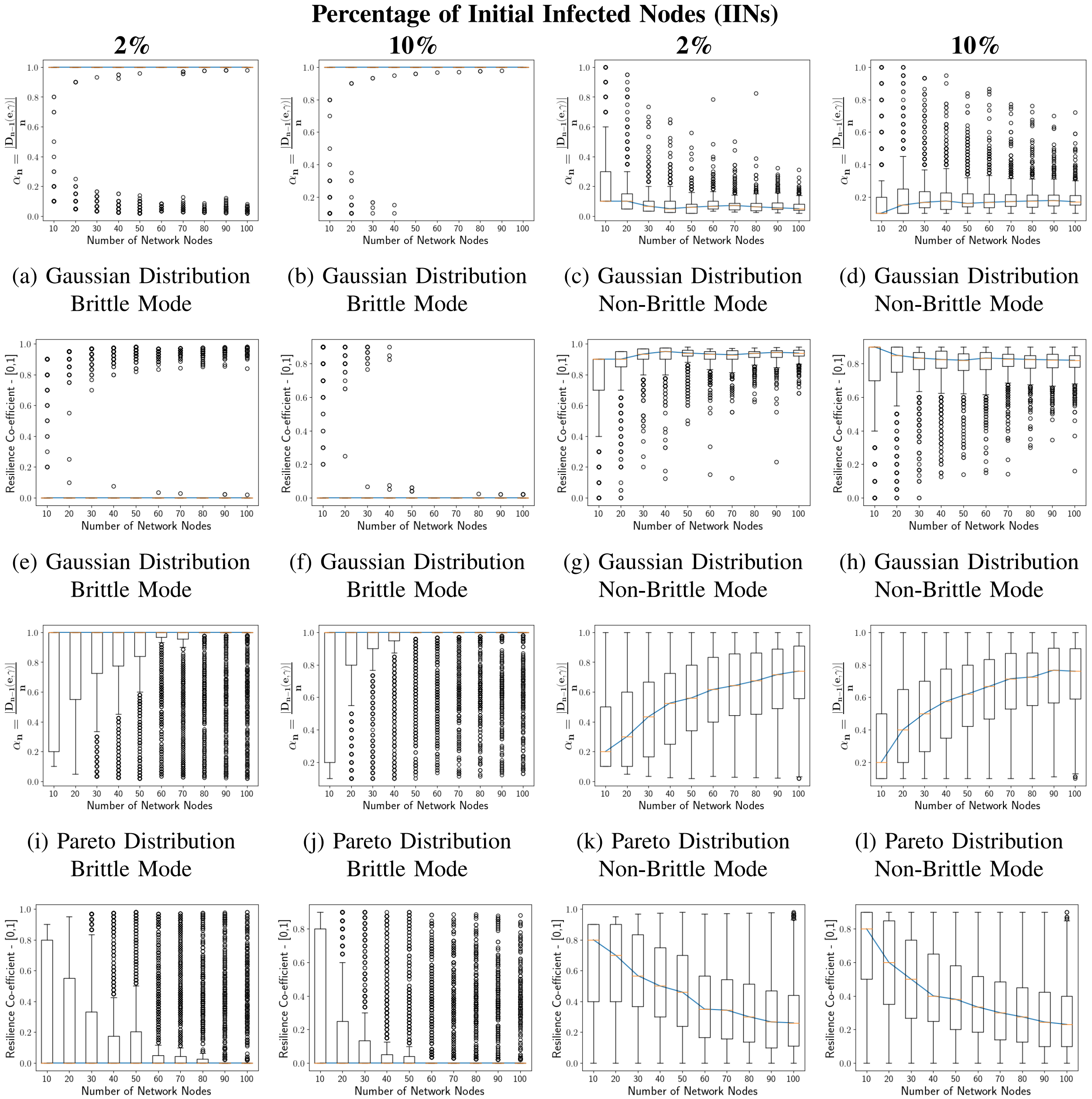
   signifying the strictly positive fraction (and strictly less than 1) of EI components that fail in the event of a cyber-attack even if the number of components are large enough.

Proof Insights - The proof follows directly from the application of Theorem 5.1 in (Wormald 1995) to stochastic processes on graphs - in our case the process generated by uniformly sampling $\mathbf{E}_n$ from $\mathscr{G}_n(\mathbf{e}_n)$.
Managerial Implications of the Theorem - The theorem first quantifies the number of EI components that will fail to function (above acceptable levels of performance) in the event of a cyber-attack as a cyber-resilience metric reflecting the ability of the EI with networked and interdependent components to absorb and adapt to a cyber-attack event. It then provides valuable insights for EI management on tradeoffs between the quality of cyber-protection deployed in its system and the degree to which the EI components can function at acceptable levels of performance. In the default case of π = 1, it is highly likely that a large enough number of components in the node are dysfunctional. This is a direct consequence of the fact that the probability, R, of component recovery is quite low. Hence, budget-conscious substantial investments need to be made (a topic of future work) to protect certain ‘critical’ components to ensure that the direct or indirect (spread) impact of a cyber-attack (e.g. spread-based APT malware cyber-attack) is not large enough to cause a cascade of systemic component dysfunctions - resulting in π^* values much lesser than 1.

5 NUMERICAL EVALUATION

In this section, we perform large scale Monte Carlo simulations (10K sample path runs per setting configuration) of $\alpha_n(\mathbf{E}_n,\gamma_n)$ for real world motivated random graph settings where each graph represents interconnected and interdependent components of an enterprise infrastructure. We simulate random graphs seeded upon a real world electricity microgrid network (see Figure 1) in Boston, USA (Khan and Madnick 2021). One of our goals is to validate the theoretical results we obtain in the paper, apart from studying other interesting results. We briefly describe our evaluation setup and followed by an analysis of the results.
Evaluation Setup - We study $\alpha_n(\mathbf{E}_n,\gamma_n)$ and a corresponding resilience coefficient $1-\alpha_n(\mathbf{E}_n,\gamma_n)$ by varying (a) the number of graph nodes, (b) the fraction of nodes initially dysfunctional via a direct infection mechanism, (c) the interconnection probability between random graph components, and (d) independence quotients of individual components. We sample the in-degrees and out-degrees of graph nodes, each, from both, a heavy-tailed distribution (Pareto) and a light-tailed (Normal) distribution for the sake of ensuring completeness in generating random non-tree graph topologies. As a plot-representative example, the power parameter of the Pareto distribution (for the plots shown in the paper) are taken from a Normal distribution

having a mean of 2 and a standard deviation of 5 to capture practical heavy-tailed topologies. Likewise, in the case of light-tailed topologies, the in and out degrees are sampled from a plot-representative Normal distribution with mean and standard deviation of 10 and 2, respectively. We simulate $\alpha_n(\mathbf{E}_n, \gamma_n)$ and corresponding resilience coefficients $1 - \alpha_n(\mathbf{E}_n, \gamma_n)$ for two contagion settings: one where each component is resilient (does not become dysfunctional with probability 1) post cyber-attack, and one where each component is brittle and fails immediately with probability 1 upon a cyber-attack. We ensure that the sum of the in-degrees of all the nodes in the graph is equal to the sum of the out-degrees of all the nodes in the



(a) Gaussian Distribution Brittle Mode

(b) Gaussian Distribution Brittle Mode

(c) Gaussian Distribution Non-Brittle Mode

(d) Gaussian Distribution Non-Brittle Mode

(e) Gaussian Distribution Brittle Mode

(f) Gaussian Distribution Brittle Mode

(g) Gaussian Distribution Non-Brittle Mode

(h) Gaussian Distribution Non-Brittle Mode

(i) Pareto Distribution Brittle Mode

(j) Pareto Distribution Brittle Mode

(k) Pareto Distribution Non-Brittle Mode

(l) Pareto Distribution Non-Brittle Mode

(m) Pareto Distribution Brittle Mode

(n) Pareto Distribution Brittle Mode

(o) Pareto Distribution Non-Brittle Mode

(p) Pareto Distribution Non-Brittle Mode

Figure 3: Illustrating the trends in the cyber-resilience measure α_n with variations in (i) # of network nodes (components/processes), (ii) node degree distribution, (iii) extent of node brittleness, and (iv) % of IINs.

graph to create a fully connected bi-directional graph with randomized in-degrees and out-degrees for each node. The recovery rate of any network node j, denoted by $R(j)$, is simulated based on a Beta distribution and a Uniform distribution. The representative plot setting in this paper is chosen to be Beta(5,1) and Uniform(0,1). The γ_n, or node independence quotient (NIQ) values are sampled from a Normal distribution with mean of 0.2 and variance of 0.1 to ensure that enterprise networks are not brittle to cyber-attacks.

Analysis of Plot Results - We broadly observe from Figures 4(a)-(p) that (i) in the brittle environments, with increasing network size and the percentage of initially dysfunctional nodes due to direct infection - the α_n values converge towards 1 (implying no cyber-resilience) at a fast rate (because there is no partial recovery) - thereby validating Theorem 2 (part 1), (ii) in the non-brittle environments, with increasing network size and the percentage of initially dysfunctional nodes due to direct infection - the α_n values steadily increase but does not usually converge to 1 (implying different degrees of cyber-resilience) but to a value relatively much lesser - thereby validating Theorem 2 (part 2). Both convergences validate Theorem 1. These results hold irrespective of whether the node degree distributions are statistically light or heavy-tailed. The difference being that non-brittle environments result in more outlier samples when compared to brittle environments because the former entails partial recovery for (sub-)system components to perform at varying degrees of cyber-resilience. Overall, we also observe balanced skewed interdependent topologies (characterized by Gaussian degree distribution) to be more cyber-resilient statistically than unbalanced skewed (characterized by Pareto degree distribution) topologies. Note that for a fixed network node size, the y-axis reflects the probability distribution of α_n taking a value between 0 and 1 - acting as a statistical measure of cyber-resilience over multiple cyber-attack configurations showcasing best to worst case likelihood of the degrees of cyber-resilience.

6 SUMMARY

We proposed the first formal probabilistic framework to quantify and analyze cyber-resilience in closed form within any complex IT/IoT driven enterprise infrastructure (EI) network prior to the occurrence of cyber-attack events. Consequently, we resolved the open problem of quantifying cyber-resilience in EI systems with networked and interdependent components. Our contributions will serve an EI management to advance estimate the amount of business disruption in the event of a cyber-attack, and in the planning of appropriate budget allocation to boost EI cyber-resilience. We ran extensive Monte Carlo simulations seeded upon a real world electricity microgrid EI network in Boston, USA to test and analyze our theory.

REFERENCES

Alderson, D. L., and J. C. Doyle. 2010. "Contrasting Views of Complexity and their Implications for Network-Centric Infrastructures". *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* 40(4):839–852.

Allspaw, J. 2012. "Fault Injection in Production". *Communications of the ACM* 55(10):48–52.

Amini, H., R. Cont, and A. Minca. 2016. "Resilience to Contagion in Financial Networks". *Mathematical finance* 26(2):329–365.

Arghandeh, R., A. Von Meier, L. Mehrmanesh, and L. Mili. 2016. "On the Definition of Cyber-Physical Resilience in Power Systems". *Renewable and Sustainable Energy Reviews* 58:1060–1069.

Balogh, J., and B. Bollobás. 2006. "Bootstrap Percolation on the Hypercube". *Probability Theory and Related Fields* 134(4):624–648.

Balogh, J., and B. G. Pittel. 2007. "Bootstrap Percolation on the Random Regular Graph". *Random Structures & Algorithms* 30(1-2):257–286.

Chaves, A., M. Rice, S. Dunlap, and J. Pecarina. 2017. "Improving the Cyber Resilience of Industrial Control Systems". *International Journal of Critical Infrastructure Protection* 17:30–48.

Clark, A., and S. Zonouz. 2017. "Cyber-Physical Resilience: Definition and Assessment Metric". *IEEE Transactions on Smart Grid* 10(2):1671–1684.

Cutter, S. L., J. A. Ahearn, B. Amadei, P. Crawford, E. A. Eide, G. E. Galloway, M. F. Goodchild, H. C. Kunreuther, M. Li-Vollmer, M. Schoch-Spana et al. 2013. "Disaster Resilience: A National Imperative". *Environment: Science and Policy for Sustainable Development* 55(2):25–29.

Cybenko, G. 2019. "Metrics Based on the System Performance Perspective". *Cyber Resilience of Systems and Networks*:29–40.

DiMase, D., Z. A. Collier, K. Heffner, and I. Linkov. 2015. "Systems Engineering Framework for Cyber Physical Security and Resilience". *Environment Systems and Decisions* 35(2):291–300.

Francis, R., and B. Bekera. 2014. "A Metric and Frameworks for Resilience Analysis of Engineered and Infrastructure Systems". *Reliability Engineering & System Safety* 121:90–103.

Gholami, A., T. Shekari, M. H. Amirioun, F. Aminifar, M. H. Amini, and A. Sargolzaei. 2018. "Toward a Consensus on The Definition and Taxonomy of Power System Resilience". *IEEE Access* 6:32035–32053.

Haque, M. A., G. K. De Teyou, S. Shetty, and B. Krishnappa. 2018. "Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights". In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 25–30. IEEE.

Holroyd, A. E. 2003. "Sharp Metastability Threshold for Two-Dimensional Bootstrap Percolation". *Probability Theory and Related Fields* 125(2):195–224.

Hossain-McKenzie, S., C. Lai, A. Chavez, and E. Vugrin. 2018. "Performance-Based Cyber Resilience Metrics: An Applied Demonstration Toward Moving Target Defense". In *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*, 766–773. IEEE.

Hosseini, S., K. Barker, and J. E. Ramirez-Marquez. 2016. "A Review of Definitions and Measures of System Resilience". *Reliability Engineering & System Safety* 145:47–61.

Khan, S., and S. Madnick. 2021. "Cybersafety: A System-Theoretic Approach to Identify Cyber-vulnerabilities & Mitigation Requirements in Industrial Control Systems". *IEEE Transactions on Dependable and Secure Computing* 19(5):3312–3328.

Kirkpatrick, S., W. W. Wilcke, R. B. Garner, and H. Huels. 2002. "Percolation in Dense Storage Arrays". *Physica A: Statistical Mechanics and its Applications* 314(1-4):220–229.

Linkov, I., D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott. 2013. "Resilience Metrics for Cyber Systems". *Environment Systems and Decisions* 33(4):471–476.

Matoušek, J., and J. Nešetřil. 2008. *Invitation to Discrete Mathematics*. 2 ed. OUP Oxford.

Musman, S., S. Agbolosu-Amison, and K. Crowther. 2019. "Metrics Based on the Mission Risk Perspective". *Cyber Resilience of Systems and Networks*:41–65.

Segovia, M., J. Rubio-Hernan, A. R. Cavalli, and J. Garcia-Alfaro. 2020. "Cyber-Resilience Evaluation of Cyber-Physical Systems". In *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, 1–8. IEEE.

Sterbenz, J. P., E. K. Cetinkaya, M. A. Hameed, A. Jabbar, and J. P. Rohrer. 2011. "Modelling and Analysis of Network Resilience". In *2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011)*, 1–10. IEEE.

Tarski, A. 1955. "A Lattice-Theoretical Fixpoint Theorem and its Applications.". *Pacific journal of Mathematics* 5(2):285–309.

Topkis, D. M. 1978. "Minimizing a Submodular Function on a Lattice". *Operations Research* 26(2):305–321.

Venkataramanan, V., A. Hahn, and A. Srivastava. 2019. "CP-SAM: Cyber-Physical Security Assessment Metric for Monitoring Microgrid Resiliency". *IEEE Transactions on Smart Grid* 11(2):1055–1065.

Venkataramanan, V., A. K. Srivastava, A. Hahn, and S. Zonouz. 2019. "Measuring and Enhancing Microgrid Resiliency Against Cyber Threats". *IEEE Transactions on Industry Applications* 55(6):6303–6312.

Woods, D. D. 2015. "Four Concepts for Resilience and the Implications for the Future of Resilience Engineering". *Reliability Engineering & System Safety* 141:5–9.

Wormald, N. C. 1995. "Differential Equations for Random Processes and Random Graphs". *The Annals of Applied Probability*:1217–1235.

Zuloaga, S., P. Khatavkar, L. Mays, and V. Vittal. 2019. "Resilience of Cyber-Enabled Electrical Energy and Water Distribution Systems Considering Infrastructural Robustness Under Conditions of Limited Water and/or Energy Availability". *IEEE Transactions on Engineering Management* 69(3):639–655.

AUTHOR BIOGRAPHIES

RANJAN PAL is a Research Scientist with the MIT Sloan School of Management. His primary research interest lies in developing interdisciplinary cyber risk/resilience management solutions based upon algorithmics, decision science, and applied probability. He serves as an Associate Editor of the ACM Transactions on MIS. His email address is ranjanp@mit.edu.

ROHAN XAVIER SEQUEIRA is a PhD student and Viterbi Fellow in the Electrical and Computer Engineering Department at the University of Southern California, USA. He has an M.S. in Electrical and Computer Engineering from the University of Michigan, USA. His research interest lies is cyber-risk management and computer networks. His email address is rsequeir@usc.edu.

MICHAEL SIEGEL is a Principal Research Scientist with the MIT Sloan School of Management. His primary research interest lies in cyber-security management of information systems. He is the founding co-Director of the Cybersecurity at MIT Sloan (CAMS) center within the MIT Sloan School of Management. His email is msiegel@mit.edu.