Received 1 November 2022; revised 15 April 2023 and 5 December 2023; accepted 6 February 2024. Date of publication 22 February 2024; date of current version 27 March 2024. The review of this article was arranged by Associate Editor Michael W. Sievers.

Digital Object Identifier 10.1109/OJSE.2024.3368921

Extending Ecological Network Analysis to Design Resilient Cyber-Physical System of Systems

ABHEEK CHATTERJEE [1], HAO HUANG [2] (Member, IEEE), RICHARD MALAK [1], KATHERINE R. DAVIS [3] (Senior Member, IEEE), AND ASTRID LAYTON [1] (Member, IEEE)

[1] J. Mike Walker '66 Department of Mechanical Engineering, Texas A&M University, College Station, TX 77843 USA
[2] Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ 08544 USA
[3] Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843 USA

CORRESPONDING AUTHOR: ASTRID LAYTON (e-mail: alayton@tamu.edu.)

This work was supported by Systems Engineering Research Center under Grant WRT-1027.

ABSTRACT The design of resilient infrastructure is a critical engineering challenge for the smooth functioning of society. These networks are best described as cyber-physical systems of systems (CPSoS): integration of independent constituent systems, connected by physical and cyber interactions, to achieve novel capabilities. Bioinspired design, using a framework called the ecological network analysis (ENA), has been shown to be a promising solution for improving the resilience of engineering networks. However, the existing ENA framework can only account for one type of flow in a network. Thus, it is not yet applicable for the evaluation of CPSoS. This article addresses this limitation by proposing a novel multigraph model of CPSoS, along with guidelines and modified metrics that enable ENA evaluation of the overall (cyber and physical) network organization of the CPSoS. The application of the extended framework is demonstrated using an energy infrastructure case study. This research lays the critical groundwork for investigating the design of resilient CPSoS using biological ecosystems inspiration.

INDEX TERMS Bioinspired design, cyber-physical systems, ecological network analysis (ENA), resilience, system of systems (SoS).

I. INTRODUCTION

Infrastructure networks, such as power grids, water distribution networks, and supply chains, are essential to the functioning of modern society. Resilience to catastrophic events, including extreme weather and cyberattacks, is a critical requirement for the successful operation of such networks. Infrastructure networks are made up of a set of *physical systems* that accomplish the sourcing, processing, and distribution of physical flows (such as energy or water). This networked integration of *heterogeneous* and *independent* constituent systems that together produce capabilities that cannot be obtained by using any of the constituent systems alone [1], [2], [3] makes them systems of systems (SoS). The constituent systems in SoS networks have operational and/or managerial independence and are usually developed independently. The behavior of the overall SoS depends largely on how the constituent systems interact with each other and cannot be determined only by knowing the behaviors of the systems in isolation, a property called *emergence* [2], [4]. These characteristics make design and evaluation extremely challenging.

Infrastructure networks also more recently include a set of *cyber systems* that monitor and regulate the operations of the physical systems through "computation, communication, sensing, and actuation" [5], making them *cyber-physical system of systems* (CPSoS). Recent work by Guariniello et al. [6] recognized the overlap between SoS engineering and complex cyber-physical systems, including dynamic interactions between components, the possible presence of multiple stakeholders, and emergent behavior in the operational domain. These areas of overlap are part of what makes design for SoS resilience extremely challenging. Quantifying resilience in the early design stages for complex, large-scale, and (often) geographically dispersed CPSoS with a large number of possible disruption scenarios is extremely difficult. Because of this, early-stage design decisions for resilience are based on *qualitative* guidelines (heuristics) such as physical and functional redundancy, localized capacity, internode communications, and human-in-the-loop [7], [8]. While such guidelines are useful, they cannot be used to assess tradeoffs with other attributes of interest because of their qualitative nature.

The inclusion of cyber elements in the CPSoS only increases the complexity of evaluating and designing for resilience. Disruptions in the cyber domain, such as false data injection or denial of service attacks, can lead to cascading failures in the physical domain. Physical disruptions, which can stop or reduce the operation of constituent systems, are typically easy to detect compared to cyber disruptions, which can *negatively modify* the operation of constituent systems, instead of stopping them, making timely detection difficult. For example, during a false data injection attack, all constituent systems *appear* to be operating normally despite potentially sending doctored inputs that would lead to inappropriate regulation decisions and subsequent failures in the physical operations [9]. Evaluating the resilience of CPSoS to such attacks also requires the ability to *cosimulate* the cyber and physical systems operations under disrupted conditions, which is a formidable task in the early/conceptual design stages [10].

Recent work has presented promising evidence that the architecting principles of biological ecosystems (Nature's resilient SoS) can be used to design resilient engineering SoSs. Ecologists have found that biological ecosystems achieve a simultaneously resilient and sustainable (efficient) design through a unique balance of constraints and redundancies in their network architectures. This architectural feature is evaluated using an approach called ecological network analysis (ENA, detailed in Section II-B). Investigation of the resilience versus affordability trade spaces of ($> 38\,000$) notional SoS architectures under various disruption scenarios indicated that ecologically similar SoS architectures had more desirable resilience and affordability attributes [11], [12]. A recent study found promising correlations between SoS resilience and ENA-based metrics (and other graph-theoretic metrics) [13]. Bioinspired designs of electric power grids (and microgrids), using a similar approach, were also found to have significantly fewer violations (better resilience) in various disruption scenarios compared to traditional configurations [14], [15], [16], [17]. The ENA framework as used in ecology and those studies, however, is only applicable to networks with *one type* of flow/interaction. In addition, ecological modeling guidelines for ENA are focused on flows of *physically conserved* quantities, such as energy and nutrients. The CPSoS have multiple types of interactions, physical material flows and monitoring and regulation interactions (information flows), and information flows are not bound by the same conservation laws. Because of this mismatch, the traditional ecology-based ENA framework is not suitable for CPSoS, hindering research into the application of ecological principles for designing resilient CPSoS.

This work addresses this limitation by proposing a novel *multigraph model* of the CPSoS, along with *guidelines* and *modified metrics* that enable ENA evaluation of the overall (cyber *and* physical) network organization of the CPSoS. The modeling decisions for the proposed multigraph model are discussed in detail and compared to previously studied ENA models of engineering networks and conventional topological analyses of cyber-physical systems. The application of the extended framework is shown using an eight-substation power grid case study. This lays the critical groundwork for future research investigating the design of resilient CPSoS using biological ecosystem inspiration. A preliminary version of this research was presented at IEEE SmartGridComm 2021 [18]. This work approaches the resilience of the CPSoS from a *proactive* standpoint: it investigates how to take actions better at the design-phase, or ahead-of-time of the disruptive events. Hence, the proposed approach differs from the usual *reactive* approach of "sense-plan-act" after disruptions. The reactive approaches to resilience are outside the scope of this work. In addition, the modified ENA models and metrics presented in this work are not meant to assess the resilience of the CPSoS to specific cyber threats. Rather, this work aims to present a complementary decision-support tool that can be used in the early/conceptual stages of CPSoS architecture development, which are nondata intensive and threat agnostic.

II. BACKGROUND AND MOTIVATION

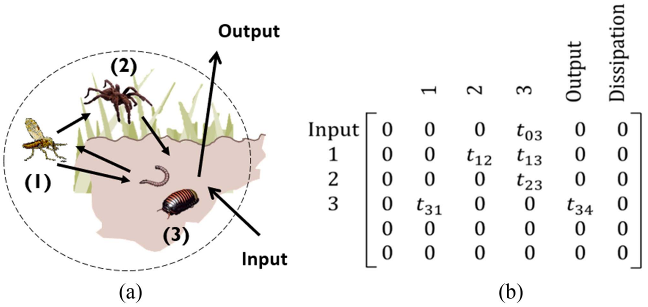
A. CYBER PHYSICAL SYSTEMS AND SYSTEM OF SYSTEMS MODELING AND ANALYSIS FOR RESILIENCE

Resilience describes a system's ability to securely operate during and recover from adverse situations to resume normal operations. As a cyber-physical system, resilience is a multidimensional property that requires managing disturbances originating from physical component failures, cyber component malfunctions, and human attacks [19]. Modeling the cyber-physical system holistically is essential to analyzing and investigating its resilience. Conventionally, cyber-physical systems are modeled graphically by classifying the nodes (constituent systems) into cyber and physical layers: interactions between the cyber nodes form the *cyber network* and interactions between the physical nodes form the *physical network*. Interlayer links then capture the interdependence on functions, topologies, and facilities between the cyber and physical networks [20], [21].

Taking power systems as an example, resilience has been quantified through the resilience trapezoid, to capture temporal properties of the power system's performance during an extreme event [22]. The resilience trapezoid is a portrayal of the preparation, duration, and recovery from a severe disturbance in electric power systems. This portrayal can quantitatively show an aggregate resilience property of the system: for power systems, this is its ability to meet the load. As commonly used, the resilience trapezoid hence depicts a system-wide property's evolution over time, subject to disturbance.

Modeling to quantify resilience in real, complex, and nonlinear systems is more complicated than the resilience trapezoid. The resilience of a system depends on both how the network is designed and how the system is operated, recognized as infrastructural resilience and operational resilience. As discussed in [23], infrastructural resilience lays the foundation for operational resilience, which provides more resources that operators and stakeholders can utilize. Recent work has shown that more robust power networks have an improved tolerance of disturbances while maintaining systems' security and resilience against hazards [16]. Likewise, a more robust communication network exhibits more paths to deliver critical information through different routes [24]. A further limitation of the resilience trapezoid is that it is specific to each particular threat. Infrastructural resilience, the focus of this work, enables further reliable and sustainable operations. Hence, the proposed holistic design-based solution would benefit future operators under different cyber and physical threats.

Power network design involves economic aspects such as [25], [26], and [27]; investment portfolios and contingency scenarios must be included, where tracking of power system constraints using detailed models under these variable investments and events must occur in practice, to inform network expansion for better resilience against unexpected contingencies. With the integration of cyber networks, different definitions and quantification of cyber-physical power system resilience are proposed. Clark and Zonouz [28] proposed a resilience metric to quantify the ability of the system to recover from a given attack using discrete stochastic models and dynamical linear system models to capture the interdependencies of the cyber network and the underlying physical processes. Venkataramanan et al. [29] proposed a framework to quantify cyber-physical transmission resiliency where a graphical analysis was applied along with a measure of critical network parameters in both the cyber and physical systems. Huang et al. [24] built the interconnections between cyber and physical networks through the amount of critical data transferred among physical and cyber networks for control and observability to capture the resilience of cyber-physical power systems. To ensure cyber-physical resiliency, a resilient communication network is essential for the smart control of the different resources against threats. Lin et al. [30] proposed a self-healing phasor measurement unit network using the software-defined networking (SDN) infrastructure to achieve resiliency against cyberattacks. A mixed-integer nonlinear optimization model was formulated to capture the self-healing process in a communication network while considering constraints on the physical network. Al et al. [31] proposed an SDN platform using Industrial Internet of Things technology to support power systems' resiliency by reacting immediately whenever a failure occurs to recover smart grid networks using real-time monitoring techniques. Jin et al. [32] presented an SDN-based communication network architecture for microgrid operations with the applications of self-healing communication network management, real-time and uncertainty-aware communication network verification, and specification-based intrusion detection for cyber-physical systems' resilience.



$$\begin{array}{c|cccccc} & & 1 & 2 & 3 & \text{Output} & \text{Dissipation} \\ \hline \text{Input} & 0 & 0 & 0 & t_{03} & 0 & 0 \\ 1 & 0 & 0 & t_{12} & t_{13} & 0 & 0 \\ 2 & 0 & 0 & 0 & t_{23} & 0 & 0 \\ 3 & 0 & t_{31} & 0 & 0 & t_{34} & 0 \\ & 0 & 0 & 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

FIGURE 1. Schematic of the modeling procedure used in ENA, describing the (a) hypothetical food web as a (b) flow matrix. Figure based on [35].

Existing methodologies on cyber-physical systems' resilience focus on the interactions between the cyber and physical systems as well as the functionalities of both the cyber and physical networks. With the specified threat vector and objectives, they can then optimize and analyze the system through cyber and/or physical development and actions. These methodologies, however, are not feasible in the early design stages when specific threat vectors are not yet known.

B. EXISTING ENA AND CHALLENGES

ENA is a tool used by ecologists to study the complex interactions among species in ecosystems. ENA provides a set of metrics to study structural and functional characteristics of ecological networks [33]. The nodes in the digraph represent the species and the directed arcs represent the transfer of energy or nutrients between them and their immediate environment. The flows between the actors (or nodes) within the system boundaries and the system inputs, outputs, and dissipation exchanged with the environment are stored in the $(N+3) \times (N+3)$ flow matrix $\mathbf{T}$, where N is the number of actors within the network (see Fig. 1). The nodes 1 to N in the flow matrix represent the actors within the specified network boundary. The nodes 0, $N+1$, and $N+2$ are the imports, exports, and dissipations, respectively. Any matrix element T_{ij} represents the magnitude of flow from node i (producers/prey) to node j (consumers/predators). The hypothetical food web of Fig. 1, for example, shows that midges (node 1) are consumed by predators (node 2) and predators are consumed by detritivores (node 3). ENA models these food web interactions as caloric (energy) transfers between the nodes and the flow information are saved in the elements T_{12} and T_{23} of the flow matrix, respectively. The entries T_{03} and T_{34} represent the input and output flows between the detritivores (node 3) and their environment, respectively. Readers interested in a more detailed description may refer to [34]. ENA includes multiple metrics that quantify different architectural characteristics of flow networks such as cyclicity, nestedness, and synergism. Such analyses have been applied to industrial networks showing promising improvements in resilience and sustainability [35], [36], [37], [38].

The ENA metric of interest in this work is *degree of system order* (DoSO), which quantifies the relative pathway constraints/organization in a flow network [39]. The level of network pathway organization or constraints is measured using the metric average mutual information [AMI; see (1)]. The upper limit of AMI is quantified by the metric Shannon Index [H, see (2)]. DoSO is evaluated as the ratio of AMI to H (3) and takes values from 0 to 1. In (1)–(3), TST_p is the sum of all flows in the network, $T_{i.}$ is the sum of flows leaving node i, and $T_{.j}$ is the sum of flows leaving node j [see (4)].

Highly pathway-constrained networks will have more static routes for flows between nodes to improve the efficiency of transporting material from one point to another. These networks will have DoSO values close to 1. Highly pathway-flexible networks will have multiple (but not the most efficient) options to route flows between nodes. These networks will have DoSO values close to 0. A DoSO analysis of biological ecosystems showed that they have evolved to exist within a narrow range of DoSO $\in [0.213, 0.589]$, called the window of vitality [40], [41]. This study provided evidence for the hypothesis that a balance between constraints and redundancies in network organization is crucial to ecosystems' resilience and sustainable growth [39]. The DoSO evaluation has also been applied to engineering networks such as supply chains [42], industrial water networks [43], and power grids [14], [15].

$$\text{AMI} = \sum_i \sum_j \frac{T_{ij}}{\text{TST}_p} \log_2 \left[\frac{T_{ij} \cdot \text{TST}_p}{T_{i.} \cdot T_{.j}} \right] \tag{1}$$

$$H = -\sum_i \sum_j \frac{T_{ij}}{\text{TST}_p} \log_2 \left[\frac{T_{ij}}{\text{TST}_p} \right] \tag{2}$$

$$\text{DoSO} = \frac{\text{AMI}}{H} \tag{3}$$

where

$$\text{TST}_p = \sum_i \sum_j T_{ij}; \quad T_{i.} = \sum_j T_{ij}; \quad T_{.j} = \sum_i T_{ij}. \tag{4}$$

The existing ENA framework and DoSO formulation are only applicable to networks with one type of flow and are unsuitable for the evaluation of CPSoS architectures. Ulanowicz [33] provided generalizations of the AMI and H metrics across multiple dimensions (including time, flow types, and spatial location). However, the authors identified the following two issues regarding the application of this modified formulation for CPSoS analysis:

1) the formulation uses sums of the flows of different types leading to dimensional inconsistencies in CPSoS with physical and information flows;
2) a trivial change in the unit/scale of any one flow can lead to a different DoSO evaluation of the same CPSoS.

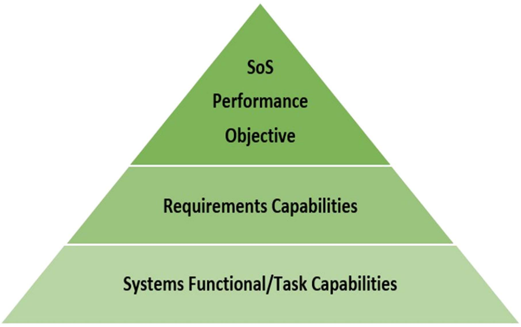

SoS
Performance
Objective
Requirements Capabilities
Systems Functional/Task Capabilities

FIGURE 2. Hierarchical description of SoS, based on [44].

The observation is that earlier work had an undesirable sensitivity to the scale/unit for measuring flows. This is not an acceptable characteristic for a CPSoS architecture assessment technique. Therefore, we assert that a new formulation is required to evaluate DoSO of CPSoS architectures with multiple flow types.

III. PROPOSED CPSOS MODELING FRAMEWORK

The authors propose that CPSoS architectures should be modeled as directed multigraphs. A multigraph is a graph that is permitted to have multiple edges/links between the nodes. The nodes represent the constituent systems and the directed edges represent the different types of interactions. This section proposes a set of guidelines to model CPSoS architectures as directed multigraphs for ENA and provides a modified formulation for DoSO evaluation that addresses the issues identified in Section II-B.

A. IDENTIFYING CONSTITUENT SYSTEMS AND INTERACTIONS

The first step in developing the multigraph model of CPSoS is to identify the constituent systems (nodes) and distinct interactions (edges). Han et al. [44] presented a hierarchical description of SoS, as illustrated in Fig. 2. The SoS has a main *operational objective*. The main objective is met by accomplishing a set of *requirement capabilities*, and each requirement capability is met by completing fundamental tasks/functions in a meaningful order by the constituent systems. Following this hierarchical description of SoSs, constituent systems in a CPSoS (unique nodes in the ENA model) are identified using the following rules:

1) the system operation can be changed (at least to some degree) independently;
2) the system performs one or more of the fundamental tasks for the SoS;
3) the system ownership/management/development process is different from other systems.

Contrary to some previous applications of ENA to engineering networks (see [14] and [43]), the authors propose that systems like pipeline segments and transmission branches should be modeled as unique nodes and not simply as graph edges/interactions. This is because these systems fulfill a unique and essential role in the SoS and have a certain level of operational independence. For instance, transmission branches in power grids can be shut down to protect from power surges, and flow through pipeline segments can be controlled using valves. In addition, these systems have their own cyber interactions (for monitoring and/or regulation) with the supervisory control and data acquisition (SCADA) systems. These unique functional flows require that they be modeled as nodes because edges in a directed graph/multigraph can only exist between two nodes and not between a node and an edge. This was not considered in prior work using ENA on engineering networks because they were only considering the physical flows.

In this model, human operators are considered to be a part of the system that they work on. For example, human operators working at the physical systems (such as generators in power grids) are lumped into the physical system node. Human operators are also included in the cyber system nodes if they are involved in processing the data received to ascertain the state of the monitored physical systems and make regulatory decisions. The human operators give the physical systems their ability for independent operation and/or decision making.

Physical systems' operations are measured using sensors/meters attached to them. These sensors/meters are not considered separate nodes in the proposed model because they are components built into the physical systems and are not independent constituent systems themselves. A physical system could have multiple (redundant) sensor/meter components. However, when analyzing the overall SoS, the focus is on the higher level network architecture, and not on the minute component-level details.

The different types of interactions are identified based on the *requirement capabilities* of the SoS. Each type of interaction represents the interdependencies and task flows to achieve a specific requirement capability. The authors identify the following three types of common interactions (requirement capabilities) in CPSoS.

1) *Physical interactions:* The sourcing, processing, and distribution of physical flows, such as energy and water.
2) *Monitoring interactions:* Collecting, communicating, or processing the state information of the physical operations.
3) *Regulatory interactions:* Generating, communicating, or processing information for regulating physical operations.

This classification does not imply that the proposed ENA modeling framework can only be used on SoS with three types of flows. Instead, this is intended to provide a detailed procedure that allows for a consistent analysis of many critical CPSoS such as energy/gas/water distribution infrastructure.

B. ASSIGNING INTERACTION MAGNITUDES

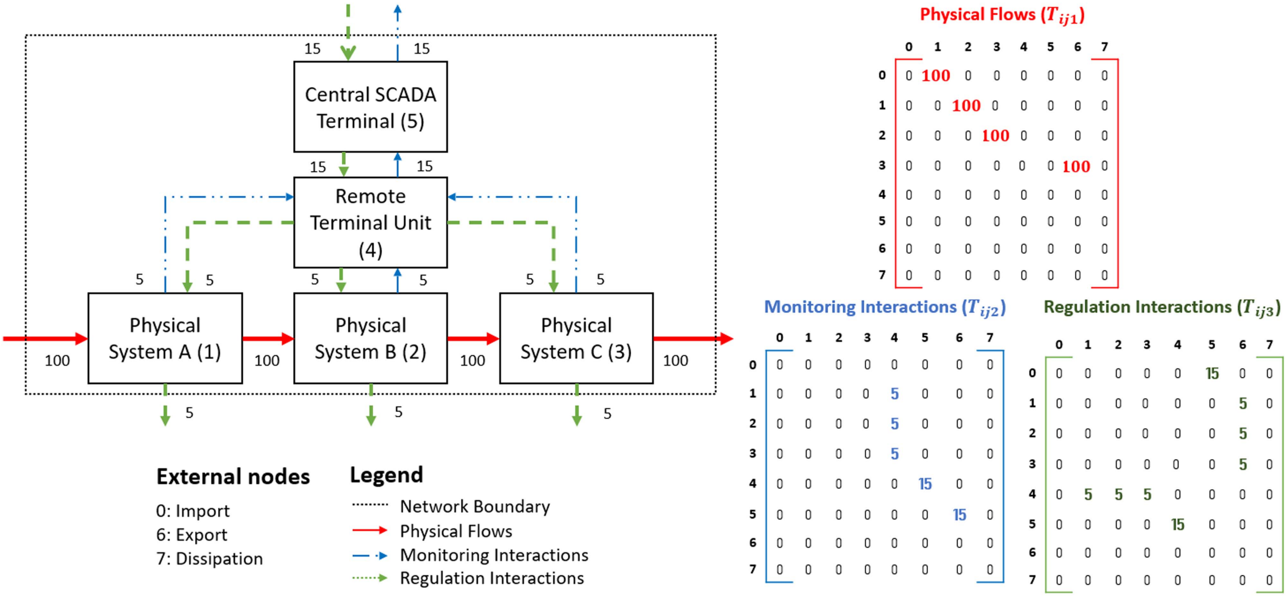
The next step is to identify the interactions between the constituent systems, as well as the constituent systems and the SoS operating environment. Once all interactions (of each type identified in step 1) are known, it is required to assign a magnitude to each of these interactions for the DoSO analysis. The amount (or fraction) of a task accomplished by a system (referred to as the task load in this article) should be used to determine the strength/magnitude of interactions from a node. The interaction magnitudes assigned in this step are meant to create a generalized representation of how the architecture is designed to work during its operation period, to evaluate pathway constraints and redundancies. This step (or the whole framework) is not being proposed as a simulation of the CPSoS at any given time. This step is explained in more detail for physical interactions and cyber interactions as follows.

1) *Physical flows*: In the case of physical interactions, the strength of interactions can be assigned as equal or proportional to the amount of planned material or energy transfers between the constituent systems, and the systems and the environment. For example, in supply chains, the magnitude of flow between a supplier and an assembler would be equal (or proportional) to the amount of material supplied by the supplier to the assembler under normal operating conditions [42]. In an energy distribution network, the flows between any two systems would be equal (or proportional) to the planned transfer of energy between the systems under normal operating conditions [16], [45].

   It should be noted that the exact amounts of the flows are not required for ENA modeling. When designing an architecture, designers make decisions regarding what amount of material/energy flows will be routed through different channels in the network. These planned proportions can be used to create an ENA model instead of needing to know the exact amount of flow. This is especially important where the flows may vary over the period of operation.
2) *Cyber interactions*: The guidelines for assigning the cyber interaction magnitudes (monitoring and regulation) are described later for a typical SCADA-based architecture that has local cyber systems and a central terminal. In this work, local cyber systems are referred to as remote terminal units (RTUs). The RTUs receive information from physical devices, process them, and communicate them with other RTUs or the central SCADA terminal (CST). A notional CPSoS of this type is shown in Fig. 3(left).

The process to assign task-load magnitudes to the *monitoring interactions* is outlined as follows.

1) *Physical operation systems to RTUs:* Sensor or meter components on the physical systems measure the operating parameters of interest and communicate that information with RTUs connected with those systems. To assign magnitudes to the monitoring interactions, first, it needs to be identified whether the monitoring of each system is equally important or if there are some systems whose monitoring is more important to the SoS operation. If the monitoring of each system is equally important, then a fixed quantum of monitoring task load



Physical Flows (T_{ij1})

	0	1	2	3	4	5	6	7
0	0	100	0	0	0	0	0	0
1	0	0	100	0	0	0	0	0
2	0	0	0	100	0	0	0	0
3	0	0	0	0	0	0	100	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0

Monitoring Interactions (T_{ij2})

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	0	0	0	5	0	0	0
2	0	0	0	0	5	0	0	0
3	0	0	0	0	5	0	0	0
4	0	0	0	0	0	15	0	0
5	0	0	0	0	0	0	15	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0

Regulation Interactions (T_{ij3})

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	15	0	0
1	0	0	0	0	0	0	5	0
2	0	0	0	0	0	0	5	0
3	0	0	0	0	0	0	5	0
4	0	5	5	5	0	0	0	0
5	0	0	0	0	15	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0

FIGURE 3. Notional CPSoS modeled using the proposed multigraph approach and its corresponding 3-D flow matrix.

(say five units) is assigned to each interaction from a physical system to its RTU. However, if some of the systems' monitoring is more important/critical, the link between those systems and their RTUs can be assigned a proportionally higher task-load magnitude.

2) *Inter-RTU interactions:* If the architecture allows communication between RTUs (for example, a mesh communication topology), there are bidirectional links between each RTU. The magnitude of these interactions is equal to the amount of monitoring information that was received by the sender RTU from its associated physical systems and that is useful to the receiver RTU.

3) *Export and dissipation at RTUs:* If an RTU has received redundant monitoring information for one or more physical systems, the monitoring task-flow dissipation from that RTU is equal to the amount of the redundant input. In case the RTU has been given certain local regulatory authority in the architecture design, a fraction of the nonredundant input is assigned as the magnitude of the monitoring task-flow export at the RTU. This fraction depends on the level of regulatory authority granted to local systems in the architecture.

4) *RTU to CST interactions:* A fraction of the nonredundant input to RTUs is assigned as the magnitude for the monitoring interactions from the RTUs to the CST. This fraction depends on the level of regulatory authority granted to the CST in the architecture.

5) *Export and dissipation at CST:* If the CST has received redundant monitoring information streams for one or more physical systems, the monitoring task-load dissipation from the CST is equal to the amount of redundant input. The nonredundant input to the CST is assigned as the magnitude of the monitoring task-load export.

A similar process is followed to assign task-load magnitudes to the *regulation interactions*, outlined as follows.

1) *Import at CST:* The import at the CST represents the transformation of monitoring information to regulation information since the SCADA terminal uses the monitoring information to make regulatory decisions. The magnitude of the import flow depends on the number of systems being regulated by the CST and the level of regulatory authority granted to the CST in the architecture. First, a task load is assigned to the regulation task of each system, similar to the monitoring task-load assignment. If the regulation of each system is equally important, then a fixed quantum of task load (say five units) is assigned to all systems. However, if some of the systems' regulation is more important/critical, then the task loads for these systems are assigned a proportionately greater amount. The magnitude of the import flow of regulation interaction into the CST is set equal to the sum of the assigned regulation task loads for all systems regulated by the CST.

2) *CST to RTU interactions:* The CST provides input of regulation information to each RTU equal to the sum of regulation task loads of systems that they can communicate with directly or (indirectly) through inter-RTU communication links.

3) *Inter-RTU interactions:* The magnitude of regulation interaction from RTU A to RTU B (if connected) is equal to the sum of the regulation task loads of systems directly connected to RTU B and whose regulation information was received by RTU A from the CST.

4) *Import at RTUs:* The magnitude of the regulation task-load import at any RTU is set equal to the sum of the

assigned regulation task loads for all systems regulated by that RTU if the RTU has local regulatory authority.

5) *Dissipation at RTUs:* The magnitude of the dissipation flow of regulation interaction into any RTU is set equal to the sum of the redundant input streams of regulation information.
6) *RTUs to physical systems interactions:* The magnitude of regulation interaction from an RTU to a physical system is equal to the assigned task load of that system's regulation.
7) *Export and dissipation at physical systems:* The magnitude of the export flow of regulation task load at a physical system is equal to the assigned task load of that system's regulation. The magnitude of the dissipation flow of regulation at any physical system is set equal to the sum of the redundant streams of regulation task load into that physical system.

C. PREPARING FLOW MATRIX AND CONDUCTING DOSO ANALYSIS

Once the multigraph is modeled, as described in the aforementioned steps, a 3-D flow matrix is prepared to represent the model and evaluate the DoSO. In this 3-D flow matrix $\mathbf{T}$, any element T_{ijl} represents the interaction/transfer of type l from node i to node j. An example of the multigraph model and flow matrix, for a notional CPSoS, is shown in Fig. 3.

To facilitate the DoSO evaluation of the overall network, the modified AMI and H metrics, shown in (5) and (6), are proposed. The symbols in the metrics have the same meanings as described in Section II-B and the new subscript l represents the different flow types. These flow values required to use (5) and (6) can be obtained from the 3-D flow matrix $\mathbf{T}$. In (5) and (6), T_l is the sum of all flows of types l in the network, $T_{i.l}$ is the sum of flows of type l leaving node i, and $T_{.jl}$ is the sum of flows of type l leaving node j [see (7)]. Once AMI and H are calculated using the modified metrics, DoSO can be calculated using (3). The formulation of these modified metrics is described in detail in [46]. The modified metrics do not use the sum of flows of different types and have been used to analyze supply chains with multiple physical flows [47] and surveillance networks with multiple information flows [48].

$$\mathrm{AMI} = \sum_i \sum_j \left[\prod_l \left(\frac{T_{ijl}}{T_l} \right) \right] \cdot \log_2 \left[\prod_l \left(\frac{T_{ijl} \cdot T_l}{T_{i.l} \cdot T_{.jl}} \right) \right] \tag{5}$$

$$H = - \sum_i \sum_j \left[\prod_l \left(\frac{T_{ijl}}{T_l} \right) \right] \cdot \log_2 \left[\prod_l \left(\frac{T_{ijl}}{T_l} \right) \right] \tag{6}$$

where

$$T_l = \sum_{ij} T_{ijl}; \, T_{i.l} = \sum_j T_{ijl}; \, T_{.jl} = \sum_i T_{ijl}. \tag{7}$$

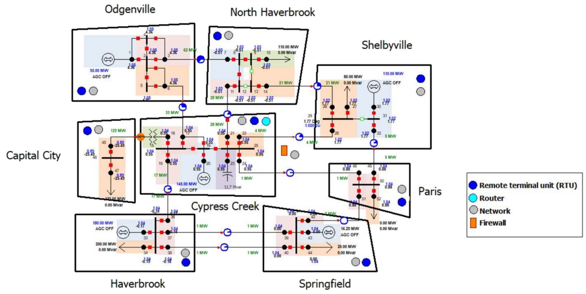


FIGURE 4. Eight-substation power grid case study from [49].

IV. CASE STUDY

A. CASE STUDY DESCRIPTION

The proposed ENA modeling guidelines are tested on a synthetic eight-substation cyber-physical power networks (CPPN) case study from [49]. There are five generators, six loads, and 12 branches/transmission systems in this case study. The monitoring and regulation of the physical systems are accomplished using a SCADA network. Each substation has its own RTU and every generator or load is assigned to a specific substation (see Fig. 4). The RTUs communicate with a central SCADA terminal.

In this case study, the physical systems (buses, generators, loads, and branches/transmission systems) generate and distribute energy to the end users. The cyber systems include communication devices, such as routers, firewalls, etc. For simplification, an RTU system is used to model all local communication devices at a substation for ENA. The cyber systems (RTUs and the CST) communicate and process the data received from the physical systems to ensure that the system operates securely, reliably, and economically. The following interaction types are identified for the CPPN case study: energy flows, monitoring interactions, and regulatory interactions.

Various architectures of the eight-substation CPPN were evaluated using the proposed ENA framework for CPSoS. The physical infrastructure was unchanged in the tested architectures. The design variations explored in the cyber infrastructure are explained as follows.

1) How is the regulatory/control authority distributed?
   a) *Central:* Only the CST has regulatory authority. The RTUs communicate data to and from the CST.
   b) *Local:* The substation RTUs make regulation decisions for the systems in their substation.
2) What is the communication network topology?
   a) *Star topology:* RTUs only communicate to the CST.
   b) *Mesh topology:* RTUs communicate to the CST and amongst themselves.

B. DOSO ANALYSIS

The DoSO evaluations for the three interactions (energy, monitoring, and regulation) and the overall CPPN are shown for

TABLE 1. DoSO Values for the Synthetic Eight-Substation Power Grid Architectures

#	Regulation Authority	Communication Topology	Overall $DoSO$	Power flows $DoSO$	Monitoring $DoSO$	Regulation $DoSO$
1	Centralized	Star	0.601	0.764	0.561	0.476
2	Centralized	Mesh	0.477	0.764	0.233	0.132
3	Decentralized	Star	0.532	0.764	0.444	0.407
4	Decentralized	Mesh	0.532	0.764	0.444	0.407

TABLE 2. Topological Analysis of the Cyber Networks in the Synthetic Eight-Substation Power Grid Architectures

#	Regulation Authority	Communication Topology	Average Node Degree ($\bar{d}$)	Average Clustering Coefficient ($\bar{c}$)	Average Shortest Path ($\bar{l}$)	Average Betweenness Centrality ($\bar{b}$)
1	Centralized	Star	1.778	0	1.778	0.111
2	Centralized	Mesh	8	1	1	0
3	Decentralized	Star	1.778	0	1.778	0.111
4	Decentralized	Mesh	8	1	1	0

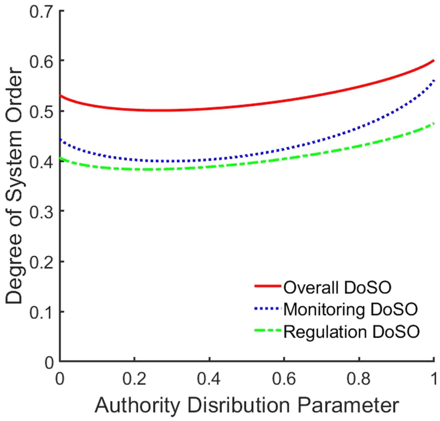


FIGURE 5. DoSO trends with changing authority distribution for the star communication topology-based eight-substation CPPN.

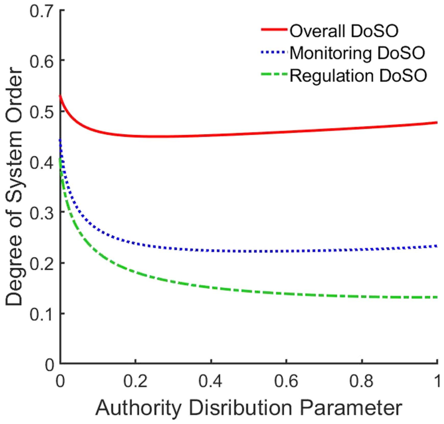


FIGURE 6. DoSO trends with changing authority distribution for the mesh communication topology-based eight-substation CPPN.

the four architectures in Table 1. The communication topology selection was a discrete design variable: either a star or a mesh topology. However, the authority distribution is a continuous design variable. The central versus local designs described in the aforementioned list are the two extreme cases. In regular operation, the regulation authority is usually distributed between the local and central systems. For example, the primary regulatory authority may be assigned to the CST but the local RTUs would have a certain level of decision-making authority for emergency response. The trend of DoSO across the spectrum from central to local regulation is also studied and the results are shown in Fig. 5 for architectures with a star communication topology and in Fig. 6 for architectures with a mesh communication topology. In these figures, an authority distribution parameter value of 1 indicates completely centralized monitoring and regulation, and a value of 0 indicates completely local monitoring and regulation.

C. CONVENTIONAL TOPOLOGICAL ANALYSIS

A conventional topological analysis of the cyber network architectures, consisting of the RTUs and CST in the eight-substation CPPN, was also conducted. The results of this topological analysis are shown in Table 2. The following four topological metrics [50] were used in this analysis.

1) *Average node degree* ($\bar{d}$): Measures the average number of links connected to each node in the network.
2) *Average clustering coefficient* ($\bar{c}$): Measures the average degree to which nodes in a graph tend to cluster together.
3) *Average shortest path* ($\bar{l}$): Measures the average minimum distance between any two pairs of nodes in the network.
4) *Average betweenness centrality* ($\bar{b}$): Measure of the average centrality of nodes in a graph based on shortest paths that represent the degree to which nodes form connections between each other.

V. DISCUSSION

A. NOTABLE FEATURES OF THE MODEL

1) UNBALANCED FLOWS

ENA applied to biological ecosystems typically requires that all physical flows are balanced at all nodes: flow entering a node equals flow exiting a node. This is because the flows of interest for ecologists, such as energy and nutrients, obey the laws of conservation. Unlike physically conserved flows,

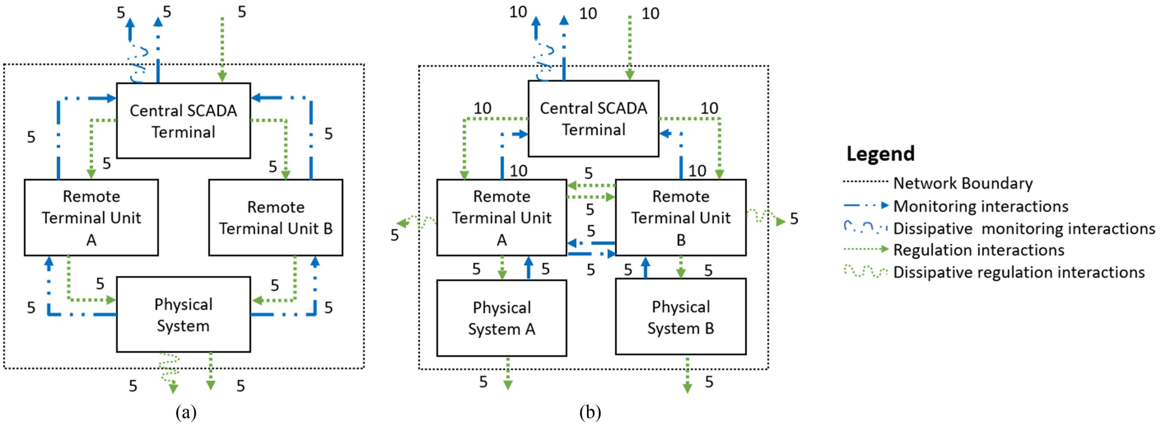


FIGURE 7. **Examples of modeling redundancy in CPSoS architectures. (a) Physical redundancy (use of multiple RTUs). (b) Redundancy via flexible communication pathways.**

information flows are not bound by conservation laws as new information can be generated at any time and existing information can be copied to multiple receivers.

For instance, a metering device outputs information about the operation of its physical system. An information import flow that would "balance" this information output is not meaningful because the information is not received from the external environment, rather it is generated in the system. This can be seen in the examples in Figs. 3 and 7. Examples of unbalanced information flows due to the copying of information at the physical system and at the RTU can be seen in Fig. 7(a) and (b), respectively.

The DoSO evaluation does not mathematically require flow balance at all nodes. Therefore, unbalanced flows are theoretically acceptable in the model as long as they do not violate any physical laws of the network under consideration. It should be noted that physically conserved flows are still balanced in the proposed model.

2) TRANSFORMATION OF FLOWS

Flows can be transformed from one type to another after processing. For example, the CST uses the state information (received through the monitoring interactions) to make decisions regarding altering the operations of physical systems (communicated using regulation interactions). This functionality is represented using export–import flow pairs in the proposed model. For example, the CST in Figs. 3 and 7 exports the useful monitoring interactions and imports and an equivalent amount of regulatory interactions.

Transformation can also be observed at the physical system nodes. While the monitoring interactions received by the physical systems are not converted to another type of information flow, they are transformed into productive actuation operations. This is modeled as the export of monitoring interactions from the physical system nodes (as shown in Figs. 3 and 7).

Finally, redundant information streams are modeled as dissipation leaving the nodes, in this model. Examples of dissipation flows to model redundancy can be seen in the two designs in Fig. 7. The first design Fig. 7(a), employs physical redundancy by using two RTUs for one physical system. The redundancy is modeled by the dissipation flows at the CST and the physical system. The second design, shown in Fig. 7(b), adds redundancy to the CPSoS architecture using multiple communication pathways. This redundancy is modeled by the dissipation flows at the CST and the RTUs.

3) SCALE INVARIANCE

The proposed model and the modified metrics presented in Section III are scale-invariant. Changing the scale/unit of any subset of flows will *not* affect the DoSO evaluation of the CPSoS architecture. This is an essential feature of the model because a meaningful overall evaluation of the network should not be affected by trivial matters such as the selection of measurement units/scales. In this proposed approach, modelers are free to use any unit/scale for the flows as long as the same convention is used for all other flows of the same type. This feature also makes it easier to assign magnitudes to the information flows. For example, when assigning interaction magnitudes to the cyber interactions (see Section III), a modeler can assume any arbitrary value for monitoring or regulation task loads for each system as long as it is consistent throughout the model and proportional to the importance of each system's monitoring and regulation.

B. KEY OBSERVATIONS FROM THE EIGHT-SUBSTATION POWER GRID CASE STUDY

Consider architecture 1 (in Table 1), with the star communication topology and centralized regulation authority, as the base architecture. By changing the communication network from a star topology to a mesh topology (architecture 1 to 2), the DoSO evaluations shift toward a high level of pathway redundancy. This is consistent with the fact that the mesh-type communication topology provides a greater level of flexibility to maintain normal communication between cyber systems with regulatory authority and the physical systems. This difference between the architectures is also captured by the topological analysis (as shown in Table 2).

Next, consider the effect of changing the control authority from centralized to decentralized (architecture 1 to 3). The architectures have the same nodes and use the same communication pathways but they function in different ways because of the differences in regulatory authority. In architecture 1, all monitoring information is sent to the CST for processing and to make regulatory decisions. In architecture 3, the CST is not performing any function in the CPSoS because the regulation authority is completely localized. The architectures 1 and 3 are *topologically equivalent*, as shown by their identical topological analysis metric values (see Table 2). However, the proposed ENA modeling and DoSO analysis framework can capture these *functional/behavioral* differences, as shown by the different DoSO values of the two architectures in Table 1.

Figs. 5 and 6 provide an insight into the variation of the architectures DoSO values with the distribution of regulatory authority. These results indicate that authority decentralization does not always lead to higher pathway redundancy/flexibility. For the star topology architectures (see Fig. 5), the pathway redundancy increases (DoSO decreases) up to a certain level of authority decentralization. Beyond that, greater decentralization of regulatory authority makes the system more pathway constrained. In the case of the mesh topology architectures (see Fig. 6), the communication between the RTUs provides a high level of pathway flexibility. Decentralizing the authority distribution in architectures with the mesh communication topology is observed to have little effect on the CPSoS pathway organization, at first. However, extreme authority decentralization makes the architecture more pathway constrained.

These results are surprising at the first glance. However, it should be noted that decentralization of the regulatory authority has two unique (and opposing) effects on the pathway organization of the CPSoS. While regulatory authority decentralization does add flexibility by adding to the functionality of the RTUs, it also reduces the amount of information shared between RTUs and between the RTUs and the CST. The flexibility provided by the inter-RTU communications is the primary contributor to the pathway redundancy in mesh topology-based architectures. Therefore, reducing the communication between RTUs reduces the flexibility provided by the mesh communication topology, explaining why these architectures are observed to become more pathway constrained with the increase in regulation decentralization.

Finally, the DoSO evaluations of architectures 3 and 4 are identical. This is surprising because the architectures are different from a topological perspective (note the different values of the topological metrics in Table 2). However, upon scrutiny, it is noted that when the regulation authority is completely decentralized/local, the CST is not functional and the RTUs are only interested in the information about the physical systems that they are connected to directly. Therefore, there is no information sharing from RTUs to the CST or between RTUs. This leads to both architectures behaving identically—as eight separate subnetworks for the two cyber interactions, and only connected by the power flows between them. The fact that the DoSO evaluation can identify such subtle functional features is a promising indication of its value as a CPSoS architecture evaluation tool.

C. POTENTIAL IMPACT, CHALLENGES, AND FUTURE RESEARCH DIRECTIONS

This work showed that the ENA approach can be extended for the evaluation of CPSoS. The results also indicate that the proposed framework and the DoSO analysis can capture subtle functional/behavioral characteristics of CPSoS architectures, which makes it unique compared to existing graphical analyses that only consider their topological features. Section III has detailed the procedures of applying this multigraph ENA modeling techniques and DoSO evaluation for CPSoS. It is also worth pointing out that the proposed multigraph-based ENA modeling framework does not get more complex with the increasing network size, and is therefore applicable to large-scale CPSoS too. The DoSO evaluation does not require the knowledge of any detailed disruption scenarios or the ability to evaluate CPSoS under disruptions using complex co-simulation techniques. Therefore, the proposed framework can provide much-needed architecture evaluation feedback to engineers in the early stages of CPSoS design.

CPSoS can be designed for significantly different types of operation over a range of time horizons. For example, the task loads for data collection may increase during peak operating periods, compared to regular operations. The regulatory authorities in a CPSoS could also change based on the operating condition. CPSoS stakeholders who are interested in evaluating the pathway organization state of the CPSoS (using the DoSO metric) during different operational situations can develop multiple instances of the CPSoS ENA model for each of those operational situations, and then, use the same steps outlined in this article to compare them. The approach can be extended to include information about ownership of CPSoS assets and data, a capability that could be useful in quantifying the impact of data corruption scenarios against normal day-to-day operations.

The proposed framework is developed to assess the design of CPSoS considering the heterogeneous flows and network topologies. It has the capability to provide an early-stage assessment of the resilience capabilities of the CPSoS given the condition that all inputs are correctly collected. This approach takes the flows into consideration, not the quality of the cyber data or information used for operation. The data flow integrity check would come from (and here it is assumed that it is done externally) an organization's external security event monitoring and intrusion detection systems.

This work has not yet tested whether the DoSO analysis of CPSoS architectures can "predict" their ability to handle cyber disruptions. Toward prediction, this work has developed an extended ENA framework that makes such an investigation possible. In addition, recent research has shown promising indications that the DoSO analysis can guide resilience improvements in complex systems and SoSs. This motivates future research comparing the DoSO analysis of

CPSoS against their resilience evaluation (to cyber threats) using state-of-the-art cyber physical cosimulation testbeds such as those developed in [9], [51], and [52].

Past research has found that ecologically similar DoSO values can lead to desirable resilience in engineering networks with physically conserved flows (see [15], [43], and [47]). However, the cyber interactions in CPSoS have unique behavioral properties, including the ability to generate new information and copy information. Cyber-physical disruption scenarios can also involve the unique aspect of deception. Based on these considerations, it is possible that the favorable DoSO range for resilience from cyber threats may be different from the ecologically identified *Window of Vitality* (discussed in Section II-B). This is in line with prior work that suggests certain engineering networks and SoS may have specialized *Windows of Vitality*, especially in cases where the severity of potential threats is known [11], [12]. Future research should also investigate different CPSoS applications such as oil and gas infrastructure, and water distribution infrastructure to test if the favorable DoSO ranges vary based on the application. The approach presented here paves the way to uncover the existence and qualities of unique CPSoS' *Windows of Vitality*.

VI. CONCLUSION

This article presented a novel multigraph model of CPSoS, along with guidelines and modified metrics that enable ENA evaluation of the overall (cyber and physical) network organization of the CPSoS. The proposed model can accommodate unbalanced flows (as long as they are consistent with the operating principles of the network), accounts for the transformation of flows, and is scale invariant. This article also demonstrated the practical application of the extended ENA framework and DoSO formulation using a realistic energy infrastructure case study. It is shown that the proposed model evaluates both topological and functional (flow-based) characteristics of SoS architectures, which makes it unique compared to existing graphical analyses that only consider the topological features of SoS architectures. The approach presented here paves the way to discover ecology-inspired design principles for resilient CPSoS.

REFERENCES

[1] M. Jamshidi, "Introduction to system of systems," in *System of Systems Engineering Innovations for the 21st Century*, Boca Raton, FL, USA: CRC Press, 2009, pp. 1–43, .

[2] M. W. Maier, "Architecting principles for systems-of-systems," *Syst. Eng.*, vol. 1, no. 4, pp. 267–284, 1998.

[3] B. E. White, "Fostering intra-organizational communication of enterprise systems engineering practices," in *Proc. Nat. Defense Ind. Assoc. 9th Annu. Syst. Eng. Conf.*, San Diego, CA, USA, 2006, pp. 23–26.

[4] A. P. Sage and C. D. Cuppan, "On the systems engineering and management of systems of systems and federations of systems," *Inf. Knowl. Syst. Manage.*, vol. 2, no. 4, pp. 325–345, 2001.

[5] C. McCarthy and K. Harnett, "National Institute of Standards and Technology (NIST) cyber-security risk management framework applied to modern vehicles," United States National Highway Traffic Safety, Tech. Rep. DOT HS 812 073, 2014.

[6] C. Guariniello, A. K. Raz, Z. Fang, and D. DeLaurentis, "System-of-systems tools and techniques for the analysis of cyber-physical systems," *Syst. Eng.*, vol. 23, no. 4, pp. 480–491, 2020.

[7] S. Jackson and T. L. J. Ferris, "Resilience principles for engineered systems," *Syst. Eng.*, vol. 16, no. 2, pp. 152–164, 2013.

[8] P. Uday and K. Marais, "Designing resilient systems-of-systems: A survey of metrics, methods, and challenges," *Syst. Eng.*, vol. 18, no. 5, pp. 491–510, 2015.

[9] A. Sahu et al., "Design and evaluation of a cyber-physical testbed for improving attack resilience of power systems," *IET Cyber-Physical Syst. Theory Appl.*, vol. 6, no. 4, pp. 208–227, 2021.

[10] P. Palensky, E. Widl, and A. Elsheikh, "Simulating cyber-physical energy systems: Challenges, tools and methods," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 44, no. 3, pp. 318–326, Mar. 2014.

[11] A. Chatterjee, R. Malak, and A. Layton, "Exploring system of systems resilience versus affordability trade-space using a bio-inspired metric," *J. Comput. Inf. Sci. Eng.*, vol. 21, no. 5, 2021, Art. no. 050905.

[12] A. Chatterjee, R. Malak, and A. Layton, "Ecology-inspired resilient and affordable system of systems using degree of system order," *Syst. Eng.*, vol. 25, no. 1, pp. 3–18, 2022.

[13] A. Chatterjee, C. Helbig, R. Malak, and A. Layton, "A comparison of graph-theoretic approaches for resilient system of systems design," *J. Comput. Inf. Sci. Eng.*, vol. 23, pp. 1–13, 2023.

[14] V. Panyam, H. Huang, K. Davis, and A. Layton, "Bio-inspired design for robust power grid networks," *Appl. Energy*, vol. 251, 2019, Art. no. 113349.

[15] H. Huang, Z. Mao, A. Layton, and K. R. Davis, "An ecological robustness oriented optimal power flow for power systems' survivability," *IEEE Trans. Power Syst.*, vol. 38, no. 1, pp. 447–462, Jan. 2023.

[16] H. Huang, Z. Mao, V. Panyam, A. Layton, and K. R. Davis, "Ecological robustness-oriented grid network design for resilience against multiple hazard," *IEEE Trans. Power Syst.*, vol. 39, no. 1, pp. 416–428, Jan. 2024.

[17] A. Chatterjee, A. Bushagour, and A. Layton, "Resilient microgrid design using ecological network analysis," in *Proc. Conf. Syst. Eng. Res.*, Hoboken, NJ, USA, Mar. 2023.

[18] A. Chatterjee, H. Huang, K. R. Davis, and A. Layton, "A multigraph modeling approach to enable ecological network analysis of cyber physical power networks," in *Proc. IEEE Int. Conf. Commun. Control Comput. Technol. Smart Grids*, Aachen, Germany, 2021, pp. 239–244.

[19] R. Arghandeh, A. Von Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," *Renewable Sustain. Energy Rev.*, vol. 58, pp. 1060–1069, 2016.

[20] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151019–151064, 2020.

[21] L. Xu, Q. Guo, Y. Sheng, S. Muyeen, and H. Sun, "On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective," *Renewable Sustain. Energy Rev.*, vol. 152, 2021, Art. no. 111642.

[22] M. Panteli, P. Mancarella, D. N. Trakas, E. Kyriakides, and N. D. Hatziargyriou, "Metrics and quantification of operational and infrastructure resilience in power systems," *IEEE Trans. Power Syst.*, vol. 32, no. 6, pp. 4732–4742, Nov. 2017.

[23] A. Gholami, T. Shekari, M. H. Amirioun, F. Aminifar, M. H. Amini, and A. Sargolzaei, "Toward a consensus on the definition and taxonomy of power system resilience," *IEEE Access*, vol. 6, pp. 32035–32053, 2018.

[24] H. Huang, A. Chatterjee, A. Layton, and K. Davis, "An investigation into ecological network analysis for cyber-physical power systems," in *Proc. IEEE Int. Conf. Commun. Control Comput. Technol. Smart Grids*, Aachen, Germany, 2021, pp. 252–257.

[25] H. Nagarajan, E. Yamangil, R. Bent, P. Van Hentenryck, and S. Backhaus, "Optimal resilient transmission grid design," in *Proc. Power Syst. Comput. Conf.*, 2016, pp. 1–7.

[26] N. Nezamoddini, S. Mousavian, and M. Erol-Kantarci, "A risk optimization model for enhanced power grid resilience against physical attacks," *Electric Power Syst. Res.*, vol. 143, pp. 329–338, 2017.

[27] T. Lagos et al., "Identifying optimal portfolios of resilient network investments against natural hazards, with applications to earthquakes," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1411–1421, Mar. 2020.

[28] A. Clark and S. Zonouz, "Cyber-physical resilience: Definition and assessment metric," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1671–1684, Mar. 2019.

[29] Tushar, V. Venkataramanan, A. Srivastava, and A. Hahn, "CP-TRAM: Cyber-physical transmission resiliency assessment metric," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5114–5123, Nov. 2020.

[30] H. Lin et al., “Self-healing attack-resilient PMU network for power system operation,” *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1551–1565, May 2018.

[31] S. Al-Rubaye, E. Kadhum, Q. Ni, and A. Anpalagan, “Industrial Internet of Things driven by SDN platform for smart grid resiliency,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 267–277, Feb. 2019.

[32] D. Jin et al., “Toward a cyber resilient and secure microgrid using software-defined networking,” *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2494–2504, Sep. 2017.

[33] R. E. Ulanowicz, “Quantitative methods for ecological network analysis,” *Comput. Biol. Chem.*, vol. 28, no. 5, pp. 321–339, 2004.

[34] B. D. Fath, U. M. Scharler, R. E. Ulanowicz, and B. Hannon, “Ecological network analysis: Network construction,” *Ecological Model.*, vol. 208, no. 1, pp. 49–55, 2007.

[35] A. Layton, B. Bras, and M. Weissburg, “Ecological principles and metrics for improving material cycling structures in manufacturing networks,” *J. Manuf. Sci. Eng.*, vol. 138, no. 10, 2016, Art. no. 101002. [Online]. Available: https://doi.org/10.1115/1.4033689

[36] A. Layton, B. Bras, and M. Weissburg, “Improving performance of ECO-industrial parks,” *Int. J. Sustain. Eng.*, vol. 10, no. 4/5, pp. 250–259, 2017. [Online]. Available: https://doi.org/10.1080/19397038.2017.1317874

[37] A. Chatterjee, C. Brehm, and A. Layton, “Evaluating benefits of ecologically-inspired nested architectures for industrial symbiosis,” *Resources, Conservation Recycling*, vol. 167, 2021, Art. no. 105423.

[38] B. C. Watson, S. Malone, M. Weissburg, and B. Bras, “Adding a detrital actor to increase system of system resilience: A case study test of a biologically inspired design heuristic to guide sociotechnical network evolution,” *J. Mech. Des.*, vol. 142, no. 12, 2020, Art. no. 121705.

[39] R. E. Ulanowicz, S. J. Goerner, B. Lietaer, and R. Gomez, “Quantifying sustainability: Resilience, efficiency and the return of information theory,” *Ecological Complexity*, vol. 6, no. 1, pp. 27–36, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1476945X08000561

[40] B. D. Fath, “Quantifying economic and ecological sustainability,” *Ocean Coastal Manage.*, vol. 108, pp. 13–19, 2015.

[41] A. C. Zorach and R. E. Ulanowicz, “Quantifying the complexity of flow networks: How many roles are there?,” *Complexity*, vol. 8, no. 3, pp. 68–76, 2003.

[42] T. Wilson, A. Chatterjee, and A. Layton, “Exploring the effects of partnership and inventory for supply chain resilience using an ecological network analysis,” in *Proc. ASME Int. Des. Eng. Tech. Conf. Comput. Inf. Eng. Conf.*, St. Louis, MI, USA, Aug. 2022, Art. no. V005T05A011, doi: 10.1115/DETC2022-89936.

[43] T. Dave and A. Layton, “Designing ecologically-inspired robustness into a water distribution network,” *J. Cleaner Prod.*, vol. 254, 2020, Art. no. 120057.

[44] S. Y. Han, K. Marais, and D. DeLaurentis, “Evaluating system of systems resilience using interdependency analysis,” in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, Seoul, Korea, 2012, pp. 1251–1256.

[45] H. Huang, K. R. Davis, and H. V. Poor, “An extended model for ecological robustness to capture power system resilience,” in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2023, pp. 1–5.

[46] A. Chatterjee and A. Layton, “Bio-inspired human network design: A multi-currency robustness metric inspired by ecological network analysis,” in *Proc. ASME Int. Des. Eng. Tech. Conf. Comput. Inf. Eng. Conf.*, Anaheim, CA, USA, Aug. 2019, Art. no. V007T06A023, doi: 10.1115/DETC2019-98235.

[47] A. Chatterjee and A. Layton, “Mimicking nature for resilient resource and infrastructure network design,” *Rel. Eng. Syst. Saf.*, vol. 204, 2020, Art. no. 107142.

[48] A. Chatterjee, R. Malak, and A. Layton, “A bioinspired framework for analyzing and predicting the trade-off between system of systems attributes,” in *Recent Trends and Advances in Model Based Systems Engineering*. Cham, Switzerland: Springer, 2022, pp. 503–513.

[49] G. A. Weaver et al., “Cyber-physical models for power grid security analysis: 8-substation case,” in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2016, pp. 140–146.

[50] B. Bollobás, *Modern Graph Theory*, vol. 184. Berlin, Germany: Springer, 2013.

[51] C. Davis, J. Tate, H. Okhravi, C. Grier, T. Overbye, and D. Nicol, “SCADA cyber security testbed development,” in *Proc. 38th North Amer. Power Symp.*, 2006, pp. 483–488.

[52] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, “EPOCHS: A platform for agent-based electric power and communication simulation built from commercial off-the-shelf components,” *IEEE Trans. Power Syst.*, vol. 21, no. 2, pp. 548–558, May 2006.

ABHEEK CHATTERJEE received the B.Tech. degree in mechanical engineering from the National Institute of Technology, Warangal, India, in 2018. He is currently working toward the Ph.D. degree in mechanical engineering from Texas A&M University, College Station, TX, USA, in 2022.

He is currently a Postdoctoral Associate with the University of Maryland, College Park, MD, USA. His research interests include the use of complex systems modeling and analysis approaches to support early-stage design and scenario analysis for resilient and sustainable infrastructure development.

HAO HUANG (Member, IEEE) received the B.S. degree in electrical engineering (power system and its automation) from the Harbin Institute of Technology, Harbin, China, in 2014, the M.S. degree in electrical engineering (electric power) from the University of Southern California, Los Angeles, CA, USA, in 2016, and the Ph.D. degree in electrical engineering from Texas A&M University, College Station, TX, USA, in 2022.

He is a Postdoctoral Research Associate with the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ, USA. His research interests include power system resilience, data-driven approaches for power systems, graph theory, cyber-physical security, etc.

RICHARD MALAK received the B.S. degree in electrical engineering from Stony Brook University, Stony Brook, NY, USA, in 1998, the M.S. degree in electrical and computer engineering from Carnegie Mellon University, Pittsburgh, PA, USA, in 2000, and the M.S. and Ph.D. degrees in mechanical engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2005 and 2008, respectively.

He is currently an Associate Professor and Gulf Oil/Thomas A. Dietz Career Development Professor I with the J. Mike Walker'66 Department of Mechanical Engineering, Texas A&M University, College Station, TX, USA. His research interests include the fundamentals of engineering decision making and the application of computational techniques (optimization, machine learning, and artificial intelligence) to improve engineering decision making.

KATHERINE R. DAVIS (Senior Member, IEEE) received the B.S. degree in electrical engineering from the University of Texas at Austin, Austin, TX, USA, in 2007, and the M.S. and Ph.D. degrees in electrical engineering from the University of Illinois at Urbana-Champaign, Champaign, IL, USA, in 2009 and 2011, respectively.

She is currently an Associate Professor of electrical and computer engineering with Texas A&M University, College Station, TX, USA.

ASTRID LAYTON (Member, IEEE) received the B.S. degree in mechanical engineering from the University of Pittsburgh, Pittsburgh, PA, USA, in 2009, and the Ph.D. degree in mechanical engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2014.

She is currently an Assistant Professor and Donna Walker Faculty Fellow with the J. Mike Walker '66 Department of Mechanical Engineering, Texas A&M University, College Station, TX, USA. Her research interests include bioinspired system design problems, focusing on the use of biological ecosystems as inspiration for resilience and sustainability.