Towards the Characterization of Cyber-Physical System Interdependencies in the Electric Grid

Shamina Hossain-McKenzie*, Nicholas Jacobs, Adam Summers, Ryan Adams, Chris Goes
Sandia National Laboratories
*shossai@sandia.gov

Abheek Chatterjee, Astrid Layton, Katherine Davis
Texas A&M University

Hao Huang
Princeton University

***Abstract*—As the electric grid becomes increasingly cyber-physical, it is important to characterize its inherent cyber-physical interdepedencies and explore how that characterization can be leveraged to improve grid operation. It is crucial to investigate what data features are transferred at the system boundaries, how disturbances cascade between the systems, and how planning and/or mitigation measures can leverage that information to increase grid resilience. In this paper, we explore several numerical analysis and graph decomposition techniques that may be suitable for modeling these cyber-physical system interdependencies and for understanding their significance. An augmented WSCC 9-bus cyber-physical system model is used as a small use-case to assess these techniques and their ability in characterizing different events within the cyber-physical system. These initial results are then analyzed to formulate a high-level approach for characterizing cyber-physical interdependencies.**

***Index Terms*—cyber-physical systems, electric grid, interdependencies, biological system modeling, k-shell decomposition, principal component analysis, coupled oscillators**

I. Introduction

The electric grid is increasingly cyber-physical, rapidly evolving with smart grid technologies, wide-area monitoring capabilities, and advanced automation. However, these modernization efforts also broaden the grid's vulnerability surface and increase cyber-physical mutuality. Multi-hazard events such as cyber attacks and climate change-driven extreme weather can cause detrimental, cascading impacts [1], [2]. The cyber-physical nature of the grid does not limit cyber disturbances to the cyber system and physical disturbances to the physical system – disturbances can propagate between systems [3]. Similarly, operational system changes can affect both cyber and physical domains; observability is needed for both normal operation and during disturbances.

Obtaining cross-domain observability into the cyber-physical system (CPS), including connected critical infrastructure, is an important requirement to informing grid operation and response. It no longer suffices to only monitor the physical system to achieve full observability of the grid. Conversely, network monitors that only process cyber data are not enough to thwart adversaries that aim to disrupt the physical system. Therefore, *cyber-physical observability* (CPO), the ability to determine both cyber and physical system states with input and output system measurements in finite time, is crucial for characterizing the grid's intricate cyber-physical interactions and enabling detailed feature extraction.

Prior work developed an approach to define CPO by combining physical observability algorithms with graph-theoretic network methods to study the CPS as a single combined graph [4]. However, the interdependencies between cyber and physical graph-nodes and the structure of these connections were not investigated. The graph model of the CPS must be revised and extended with techniques to gain understanding of interdependencies within the system, especially those that cross the cyber and physical boundaries, before a comprehensive understanding of the system is achieved. We hypothesize that by applying numerical analysis and decomposition techniques on the combined cyber-physical graph we can define a systematic approach to understand how the interactions of cyber and physical components affect the behavior of the CPS overall. The proposed approach can then be used to study the alignment of terms and quantities in a mixed system model and how information flows change across system boundaries. It is crucial to assess how seemingly disparate cyber and physical data sets can be combined in a rigorous and useful manner for improving grid operation and response.

In this paper, we focus on identifying potential numerical analysis and decomposition techniques for characterizing cyber-physical interdependencies. A literature review is performed on several different methods and an augmented WSCC 9-bus cyber-physical use-case is leveraged to assess each technique and inform next steps for the characterization approach.

A. Background

In existing CPS analysis and interdependency research, the focus is on characterizing general, nodal architecture of cyber-physical systems that are not specific to the electric grid dynamic parameters and/or only addressing the more direct relationship between controllers and power system impact. In the research conducted by Marashi, the quantification of dependability and interdependency models for large-scale cyber-physical systems is explored [5]. Dependency is defined as the linkage between two components where the state of

This article has been authored by an employee of National Technology & Engineering Solutions of Sandia, LLC under Contract No. DE-NA0003525 with the U.S. Department of Energy (DOE). The employee owns all right, title and interest in and to the article and is solely responsible for its contents. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this article or allow others to do so, for United States Government purposes. The DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan https://www.energy.gov/downloads/doe-public-access-plan. This material is based upon work supported by the Sandia Laboratory Directed Research and Development Project # 229324; SAND2023-11682C.

2023 IEEE Power and Energy Conference at Illinois (PECI) | 979-8-3503-9940-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/PECI57361.2023.10197709

one component influences or is correlated with the state of the other; therefore, the two types of relationships proposed are causation and correlation. Causation is a direct impact between two states, such as a controller providing a control command, and correlation is a statistical relationship between two states computed using metrics such as Pearson's correlation coefficient. This research is a foundational start to understanding how cyber and physical states could influence each other; it remains focused on cyber components such as Flexible AC Transmission System (FACTS) controllers and phasor measurement units (PMUs). In this paper, we would like to extend past considering only cyber components within the physical topology but also consider the interconnected cyber network that could include network gateways, protocol translators, switches, and other such devices.

In the paper by Torngren and Grogan, the challenge of addressing complexity of future CPSs is discussed. Particularly, they describe how current limitations of describing highly varying environments and dealing with uncertainty and composability (of cyber and physical components) must be overcome [6]. They identify 3 main requirements to tackle these future CPS design and control challenges: 1) Increased awareness of complexity and impact of CPSs as well as establishing best practices for design and operation, 2) Research into new knowledge, methods, and tools for CPS engineering, and 3) Research into organizational approaches and processes to adopt the newly developed methodologies and permit effective collaboration between all stakeholders and provide deeper insights into human-in-the-loop systems.

Thus, in this research, we aim to dive into requirements 1) and 2) by developing an approach to systematically expose how seemingly disparate cyber and physical components depend on one another and how their relationship evolves, quantitatively, when certain changes or disturbances occur in the overall system. In the next section, we present a few different techniques that we plan to explore for suitability in characterizing cyber-physical interdependencies.

II. Techniques of Interest

For characterizing cyber-physical interdependencies, several numerical analysis and decomposition techniques have been identified. By analyzing and comparing these techniques for a cyber-physical power system use-case, we seek to add to the knowledge gained from our prior CPO work that utilized a graph-theoretic observability approach; specifically, we would like to dive deeper into the CPS interdependencies, not just their nodal linkages. As such, different numerical analysis and decomposition techniques may be beneficial to explore, to both understand what types of interdependencies may be present and the limits to these types of analyses. The knowledge gained from this research can be effective for use in algorithms that help stakeholders achieve or maintain cyber-physical resilience; this includes prevention, detection, and response. The WSCC 9-bus system, described next, will be used to perform the initial assessment of the different techniques.

A. Case Study: WSCC 9-Bus Cyber-Physical System

The WSCC 9-bus system is a simple approximation of the Western System Coordinating Council (WSCC) to an equivalent system with 9 buses and 3 generators [7]; the oneline diagram is pictured in Fig. 1. A corresponding synthetic cyber network was created for the WSCC 9-bus system, described in detail in [8]. A combined, directed graph is generated of the WSCC 9-bus cyber-physical model using graph-theoretic, power system and network observability techniques, pictured in Fig. 2. It includes physical components (Fig. 4), such as bus (**B**), load (**L**), and generator (**G**), and cyber components (Fig. 3), such as relay (**R**), switch (**SW**), human machine interface (**HMI**), and control center (**CC**). The graphs of cyber and physical networks are based on their configurations and power flow direction; while the integration of cyber and physical networks depends on digital protective relays.

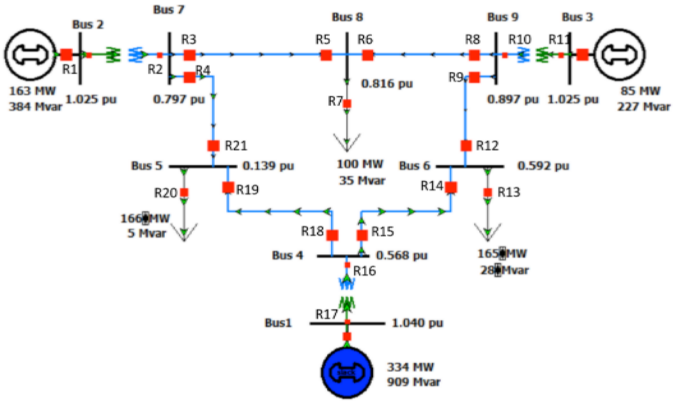

Fig. 1. Oneline diagram of WSCC 9-bus physical power system with labeled relay placement.

Digital protective relays have both communication and control capability to deliver data among cyber network and control physical devices to maintain the stability of physical network, respectively. This unique feature makes them the bridge between cyber and physical networks. For each substation in WSCC 9-bus case, there are relays protecting nearby components, and thus there is a directed connection from **R** to **B** or **L** to integrate cyber and physical networks. The relay locations are shown in Fig. 1. Details for this approach are provided in our prior work [4]. This results in a model that can be readily applied to perform the CPO analysis, as well as the additional techniques described in this work.

B. K-Shell Network Decomposition

K-Shell (or K-Core) network decomposition is a method to divide nodes on the basis of the number of degree like nodes within buckets or cores. This is a method for analyzing large-scale graphs that is useful for identifying network rankings [9]. These network rankings can infer a node's importance within the system. The graph in Fig. 2 is utilized to demonstrate the use of the method for the WSCC 9-bus cyber-physical system combined graph. The K-Shell method can quantitatively capture decomposed networks of interest to help evaluate the impact to a system during a cyber and/or physical events.

Using K-Shell analysis, the cyber graph shown in Fig. 3 provides insight into the cyber nodal linkages. For example, in the cyber network all switches are connected to the a control switch and two switches provide a redundant path to

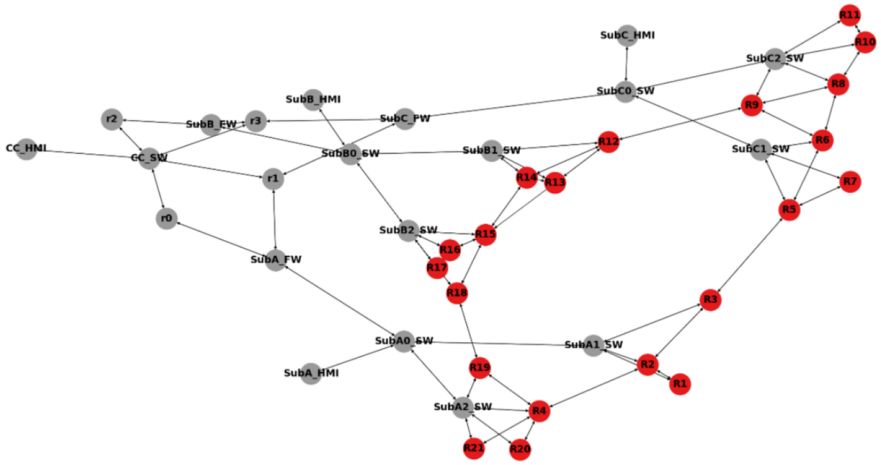

Fig. 2. Combined, directed cyber-physical graph of WSCC 9-bus system.

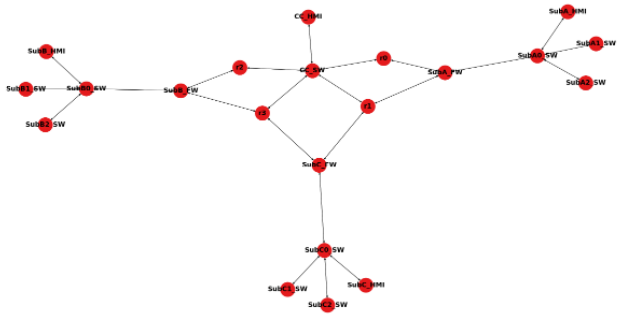

Fig. 3. A directed cyber graph of the WSCC 9-bus system communication network.

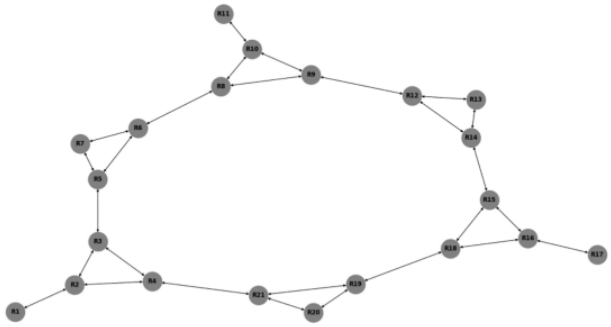

Fig. 4. A directed physical graph of the WSCC 9-bus system power system topology.

a substation switch. With the K-Shell network decomposition, we can see that that each substation forms its own core as well as which nodes have redundant paths and which do not. As seen in Fig. 5, this is a cyber-physical example of using the K-Shell method to reduce Fig. 2 to a graph of which nodes form a core and which nodes may need to be included in a core for resilience such as the HMI.

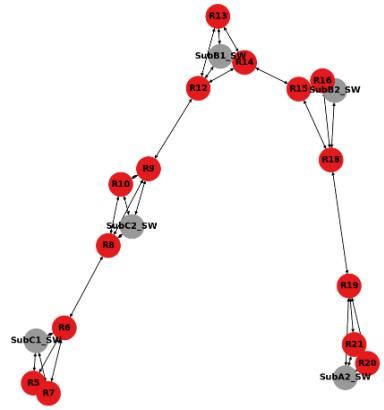

Fig. 5. Example of decomposed K-Shell cyber-physical directed graph that highlights specific nodes that form a core.

C. Ecological Network Analysis

A major motivation for using Ecological Network Analysis (ENA) is that it has shown to be a beneficial, novel approach to translate the long-term resilient trait of ecosystems, ecological robustness (R_{ECO}), to electric power systems. The potential for ENA methods to be applied toward cyber-physical resilience of power systems is initially considered in [10], [11]. However, understanding how to best chararacterize and exploit bio-inspired network resilience properties through modeling and optimizing the interdependencies of the realistic electric power grid network as a comprehensive cyber-physical system has remained largely unexplored prior to this work.

ENA requires the creation of a Food Web Matrix [F] that captures the predator-prey based interactions inside the ecosystem boundaries [12], [13]. A food web matrix is a square matrix ($N \times N$, where N is the number of actors inside the chosen set of system boundaries) that contains ones for connections from row-actor to column-actor (F_{ij}) and zeros for no connections. The food web matrix only depicts the presence and direction of interactions inside the system

To Process # - Consumer

From Process # - Producer		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Generator 1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Generator 2	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Generator 3	3	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
Bus 1	4	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
Bus 2	5	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
Bus 3	6	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
Bus 4	7	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0
Bus 5	8	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Bus 6	9	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Bus 7	10	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0
Bus 8	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Bus 9	12	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
Load 5	13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Load 6	14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Load 8	15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Fig. 6. Food web matrices for the WSCC 9-bus physical network.

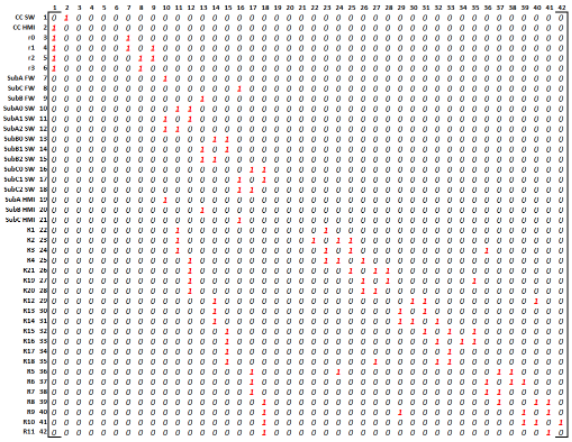

Fig. 7. Food web matrices for the WSCC 9-bus cyber network.

boundaries. The WSCC 9-Bus case study used here produces food web matrices for the physical network (Fig. 4 and Fig. 6), the cyber network (Fig. 3 and Fig. 7), and the cyber-physical network (Fig. 2).

ENA is a promising solution to quantitatively translate architecting principles of naturally resilient and sustainable biological ecosystems to engineering networks such as supply chains [14], [15], industrial symbiosis [16]–[18], and System of Systems (SoSs) [19]–[22]. More specifically, the resilience of CPS and power grids have been investigated using ENA-based approaches, specifically ecological resilience, in prior works [10], [11], [23], [24]. The metrics that ENA uses for quantitatively describing characteristics of food web architectures are used here to quantify different resilience-related characteristics of the cyber-physical WSCC 9-bus system. The results of these metrics, alongside the food web means, are listed in Table I.

A brief description of each tested metric is provided in this section. Readers interested in a more detailed description of these metrics are directed to refs. [16], [25]. *Cyclicity* measures the presence and complexity of structural cycles in a network's architecture and is calculated as the magnitude of the maximum real eigenvalue of the inverse of the food web matrix [F] (λ_{max}, see Eq. 1). *Specialized Predator Ratio* measures the fraction of predators (consumers) that only consume from one prey (producer) (P_s, see Eq. 2). The metrics *Generalization* and *Vulnerability* indicate the average number of prey (producers) for each predator (consumer) (G, see Eq. 3), and the average number of predators (consumers) for each prey (producer) (V, see Eq. 4), respectively. *Modularity* is a value between zero and one, with higher values indicating that there are groupings of actors whose interactions are almost exclusively within their group. A popular algorithm for evaluating network modularity was proposed by Newman [26], [27] (Q_N, see Eq. 5). This work uses an implementation of Newman's algorithms provided by Zuo [28]. Finally, *Connectance* (or density) is a measure of how many links (edges) exist in a network compared to the maximum possible number of links (Eq. 6).

$$0 = det(F - \lambda I) \tag{1}$$

$$P_s = \frac{N_{S-predator}}{N_{predator}} \tag{2}$$

$$G = \frac{L}{N_{predator}} \tag{3}$$

$$V = \frac{L}{N_{prey}} \tag{4}$$

$$Q_N = max(\sum_{i=1}^{k}(e_{ii} - a_i^2)) \tag{5}$$

$$C = \frac{L}{N(N-1)} \tag{6}$$

Where, L is the number of links/interactions in the food web matrix (F) with N number of nodes. λ represents the eigenvalues of F. In Eq. 5, e_{ii} is the percentage of edges in module i, and a_i is the percentage of edges with at least one end in module i.

Using the ENA approach and the collection of metrics to assess the WSCC 9-bus cyber-physical system, it allows us to further study how different cyber and physical nodes depend on one another and their predator/prey relationships. For example, we can see that the WSCC 9-bus cyber-physical network is less cyclical than the biological food webs, since the real power flows at any time are not cyclical. The Specialized Predator Ratio is also seen to be high for the physical network, which indicates that the power system nodes have relatively higher dependency on each other, with less redundancy. By comparison, for the cyber communication network with bidirectional traffic, it is observed that the ratio is lower due to the existing redundancy. High values of the Specialized Predator Ratio metric have recently been shown to be correlated with lower resilience of resource distribution SoSs [29]. Thus, we see the network structure of the cyber and physical systems impact each of the metrics in Table I. A next step in this work will examine how different disturbances (removal of nodes) and addition of network flows affect these metrics and our understanding of the cyber-physical system's inherent characteristics.

TABLE I
ENA RESULTS FOR WSCC 9-BUS SYSTEM

Metrics	Physical Network	Cyber Network	Cyber-Physical Network	Biological Food Webs (mean)
Cyclicity	0	2.776	2.776	5.293
Specialized Predator Ratio	0.75	0.114	0.085	0.178
Generalization	1.25	3.171	3.127	6.764
Vulnerability	1.25	2.643	2.722	6.109
Modularity	0.462	0.647	0.633	0.231
Connectance (Density)	0.071	0.064	0.046	0.217

D. Principal Component Analysis

Principal Component Analysis (PCA) provides the best approximation of a linear model between a set of variables that may or may not be dependent on each other; PCA can be used to perform dimensionality reduction and project the original data in a much smaller space while preserving important attributes of the data [30], [31]. For example, in power system analysis, PCA is often applied to perform transient stability assessment, phase identification, and fault classification. PCA has also been explored for communication networks for anomaly detection and performance monitoring [32], [33].

Due to PCA's suitability for sparse data sets, it is a promising technique to explore for characterizing cyber-physical interdependencies. For this initial investigation, we leverage disturbance data sets from a real-time, cyber-physical emulation environment modeling the WSCC 9-bus CPS described in [34], with three substations (A, B, C), and represented in the combined, directed graph in Fig. 2. We implemented two different scenarios within this environment:

- Cyber disturbance: Denial of Service (DoS) against a protective relay in Substation A
- Physical disturbance: Line and generator outage in the power system (generator 1, line 6-9)

The emulation is composed of a real-time digital simulator (RTDS) that enables streaming C37.118 data from PMUs in the RTDS WSCC 9-bus model and SCEPTRE^{TM}, a Sandia industrial control system (ICS) emulation tool that enables modeling of ICS cyber/control networks and implementation of actual communication protocols such as Modbus and DNP3. The details of this emulation, scenarios, and implementation method are described in more detail in [34]. The physical disturbance data sets, bus frequencies, are collected from 8 different PMUs in the WSCC 9-bus model and the cyber disturbance data sets, roundtrip times (RTTs), are collected from 3 different relays in each Substation A, Substation B, and Substation C.

For the physical disturbance, we can see that it in Fig. 8 that in normal operation, the weaker components mapped to the two principal components (PCs) (PC 1 and PC 2) very similarly with positive PC 1 coefficients and positive and negative coefficients for PC 2. Additionally, the scores (red dots) are dispersed across the axes. However, when the disturbance occurs, the weaker components coefficients change slightly (though with similar positive and negative coefficient range) and the scores are mostly zero for the PC 2 axis. Table II shows the explained metric that is the percentage of total variance explained by each PC. We can see that when the disturbance occurs, the percentage of total variance increases for PC 1 from 91.177% to 99.914%.

TABLE II
VARIATION IN EXPLAINED PCA METRIC WITH AND WITHOUT PHYSICAL DISTURBANCE FOR FREQUENCY DATA

PC	Explained % (Normal Operation)	Explained % (Physical Disturbance)
1	91.177	99.914
2	8.704	0.084
3	0.119	0.001
4	2.911e-10	8.007e-04
5	2.656e-28	3.082e-04
6	4.802e-31	1.496e-05
7	1.008e-31	9.115e-36
8	1.853e-33	1.836e-36

TABLE III
VARIATION IN EXPLAINED PCA METRIC WITH AND WITHOUT CYBER DISTURBANCE FOR RTT DATA

PC	Explained % (Normal Operation)	Explained % (Cyber Disturbance)
1	43.543	99.808
2	38.907	0.103
3	17.550	0.089

For the cyber disturbance, Fig. 9 shows that the weaker components map to PC 1 and PC 2 with positive components for PC 2 and both positive and negative for PC 1. However, when the disturbance occurs (DoS against relay in Substation A, corresponding to PC 1) we see that the PCA results change significantly and shift towards PC 1 almost completely. This shift is captured by Table III where the PC 1 explained metric changes from 43.543% to 99.808%.

These initial PCA results for cyber and physical disturbances provide interesting ideas to be explored in future work. For example, due to more significant shift of PCs during the cyber disturbance than physical disturbances, it could interesting to study how system (or synthetic) inertia can be defined for the cyber and physical systems. We can also study a cyber-physical event (affecting both systems) and assess if both cyber and physical data PCs shift similarly or not.

E. Coupling: Oscillators and Interactions

Many dynamical systems can be appropriately modeled as networks of oscillatory components and are studied in a field of research dedicated to understanding coupled oscillators. This is a useful model for many systems that include both local dynamics and coupling interactions, such as synchronous gen-

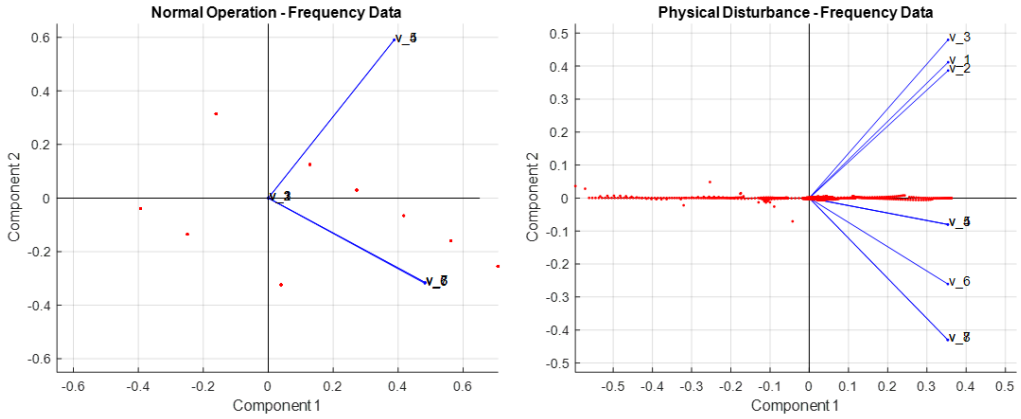

Fig. 8. Shift in PC mapping between normal operation and physical disturbance scenarios.

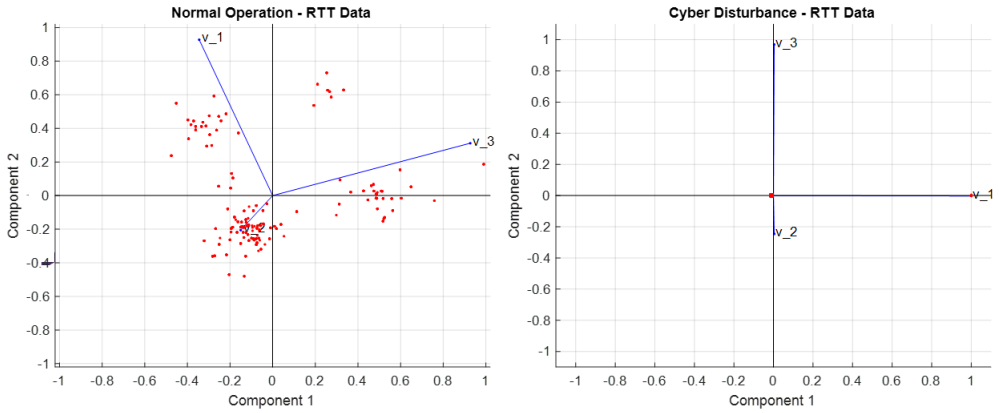

Fig. 9. Shift in PC component mapping between normal operation and cyber disturbance scenarios.

erators, cardiorespiratory synchronization, biological rhythms, and many more [35]–[37]. These methods have been applied to better understand interdependence and competition in multilayer networks in [38], which can provide a framework for understanding dynamical interactions and abrupt system transitions in networked complex systems.

While modeling CPS as networks of coupled oscillators may only be appropriate in cases where the behavior is governed by oscillatory behavior; this type of system is fairly common. Related work has shown that similar techniques and structures can be used to understand the interactions between non-oscillatory components as well [39]. This provides insight into how networked components are coupled and the mechanisms for modeling those interactions. The use of coupling functions for modeling physical interactions of components, as discussed in [40], can be used to examine how different elements in the CPS interact. One such application uses coupling functions as part of a secure communications scheme along with Bayesian inference, where the form and parameters of the coupling functions that model the interaction between transmitter and receiver acts as part of the key mechanism for the scheme [41].

The general form for modeling coupling interactions is as follows. Consider two isolated systems with dynamics that follow the isolated dynamics shown in (7).

$$\begin{aligned} \dot{x} &= f_1(x) \\ \dot{y} &= f_2(y) \end{aligned} \tag{7}$$

These equations show a general relationship where the dynamics of $\{x, y\}$ are described by the form of the functions $\{f_1, f_2\}$. To model coupling interactions between these two systems we add a new term as shown in (8).

$$\begin{aligned} \dot{x} &= f_1(x) + g_1(x, y) \\ \dot{y} &= f_2(y) + g_2(x, y) \end{aligned} \tag{8}$$

In (8), the terms $\{g_1, g_2\}$ describe the coupling behavior of these two systems and how they interact. These can take any form to appropriately model those interactions, although there are a few common ones such as direct coupling, diffusive coupling, reactive coupling, and other such forms. These differ in the structure of the coupling itself, such as direct coupling being reliant solely on the $(g_1(x, y) = g_1(y))$ while diffusive coupling would use the difference between the two systems $(g_1(x, y) = g_1(y - x))$. As can be seen in these equations, there is an inherent direction in these interactions. Estimation

techniques can be applied to identify the correct direction and estimate parameters, such as shown in [42].

The main hurdle to using coupling functions to describe interdependencies in CPS is that while the form and structure needed to do so is given by (8), the equations for those interactions still needs to be derived. This needs to be done for each component in the CPS, and so would add new information to the graph shown in Fig. 2. For each node in the system, the storage and use of information is included as the local dynamics, while each edge would require one or more functions describing the interactions of the nodes.

Additionally, the form these coupling functions would take differs greatly depending on which node in the system we are examining, and whether the interaction is a physical connection, such as a mechanical or electrical link, or an information flow in the communications network. For that purpose the coupling function method needs to be adapted and applied to model interactions between variables that may differ in their format, which requires insight into how information is passed between the cyber and physical domains and how that logical connection of information flow causes the interacting system to respond.

III. Cyber-Physical Interdependency Characterization Approach

Four different techniques were studied to assess their ability to model cyber-physical interdependencies. This is not a comprehensive set of techniques, but analyzing this initial set helped define the different levels of the approach needed. These levels can be described as:

- Decomposing CPS structure
- Analyze CPS nodal relationships
- Capture CPS data structures and relationships
- Analyze CPS data interdependence

Thus, the techniques assessed can be mapped to the different approach levels as shown in Fig. 10. The K-Shell, ENA, and PCA techniques and their application to the WSCC 9-bus system use-case showed promising results for characterizing CPS interdependencies and will continue to be tested with more complex scenarios and use-cases. Additionally, we seek to dive deeper into the coupling functions to determine what type of component interactions we can capture. We will revise the proposed techniques and add additional techniques as we iterate on this approach but the overall levels will help progress our characterization goals.

IV. Conclusions and Next Steps

In this paper, we have presented and discussed the need for characterizing cyber-physical interdependencies. To begin formulating an approach to perform this characterization, several numerical analysis and decomposition techniques are presented. It is important to note that we are not limited to these numerical analysis and decomposition techniques, but are using them as a basis to inform next steps on what types of analyses will be most useful for characterizing cyber-physical interdependencies. The analysis of these techniques with the WSCC 9-bus use-case helped formulate the approach framework and the levels necessary for our characterization goal.

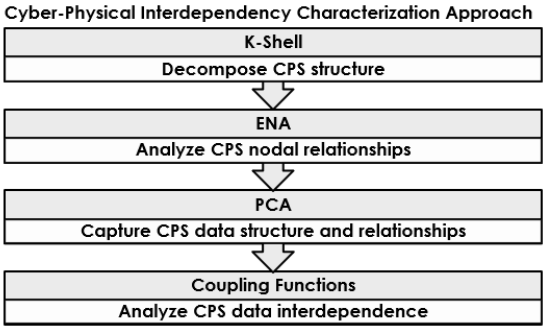

Fig. 10. Approach for characterizing CPS interdependencies with different analysis levels and technique mapping.

By applying the K-Shell network decomposition technique, we learned the primary cores of the WSCC 9-bus cyber network and inferred nodal importance within the network. Using ENA, we were able to study how the cyber and physical network structures influenced the cyclicity, specialized predator ratio, generalization, vulnerability, modularity, and connectance metrics. Using PCA, we can assess how the cyber and physical systems react similarly or dissimilarly for different disturbances.In studying coupling functions, potential for assessing how different cyber-physical variables influence one another is apparent.

For future work, we plan on running additional real-time emulation experiments with the WSCC 9-bus and larger cases to explore diverse and more complex disturbance scenarios. We will study how techniques such as ENA and K-Shell reflect the disturbance impact in the combined, cyber-physical graph and also study how time-series data from the emulation can be utilized. We will also further study the suitability of techniques such as PCA with time-series data and if other, related techniques such as t-distributed stochastic neighbor embedding (t-SNE) provide similar results in terms of CPS data structures and relationships. The emulation datasets will also be leveraged to quantitatively assess the coupling function approach and if it is more suited for low-level or high-level system/component interactions. In summary, next steps will include using emulation experiments to understand challenges with comparing cyber and physical data streams, assessing data format requirements and analysis burden of different techniques, and what additional techniques can be added to the approach framework.

Acknowledgements

We would like to thank the remainder of the InterGraph-CPS project team for their discussions and review of this work: Michael Livesay, Erin DeCarlo, Jack Flicker, and Daniel Bauer. Additionally, we are very grateful to the Sandia Energy and Homeland Security Investment Area for funding and supporting this research.

References

[1] J. W. Busby, K. Baker, M. D. Bazilian, A. Q. Gilbert, E. Grubert, V. Rai, J. D. Rhodes, S. Shidore, C. A. Smith, and M. E. Webber,

"Cascading risks: Understanding the 2021 winter blackout in texas," *Energy Research & Social Science*, vol. 77, p. 102106, 2021.
[2] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.
[3] O. Boyaci, M. R. Narimani, K. Davis, and E. Serpedin, "Spatio-temporal failure propagation in cyber-physical power systems," in *2022 3rd International Conference on Smart Grid and Renewable Energy (SGRE)*, 2022, pp. 1–6.
[4] N. Jacobs, S. Hossain-McKenzie, A. Summers, C. B. Jones, B. Wright, and A. Chavez, "Cyber-Physical Observability for the Electric Grid," in *2020 IEEE Texas Power and Energy Conference (TPEC)*, Feb. 2020, pp. 1–6.
[5] K. Marashi, "Quantitative Dependability and Interdependency Models for Large-Scale Cyber-Physical Systems - ProQuest."
[6] M. Törngren and P. T. Grogan, "How to Deal with the Complexity of Future Cyber-Physical Systems?" *Designs*, vol. 2, no. 4, p. 40, Dec. 2018, number: 4 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/2411-9660/2/4/40
[7] A. S. Al-Hinai, *Voltage collapse prediction for interconnected power systems*. West Virginia University, 2000.
[8] S. Hossain-McKenzie, D. Calzada, N. Jacobs, C. Goes, A. Summers, K. Davis, H. Li, Z. Mao, T. Overbye, and K. Shetye, "Adaptive, cyber-physical special protection schemes to defend the electric grid against predictable and unpredictable disturbances," in *2021 Resilience Week (RWS)*. IEEE, 2021, pp. 1–9.
[9] S. Carmi, S. Havlin, S. Kirkpatrick, Y. Shavitt, and E. Shir, "A model of internet topology using *k*-shell decomposition," *Proceedings of the National Academy of Sciences*, vol. 104, no. 27, pp. 11 150–11 154, 2007. [Online]. Available: https://www.pnas.org/doi/abs/10.1073/pnas.0701175104
[10] 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 *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2021, pp. 239–244.
[11] H. Huang, A. Chatterjee, A. Layton, and K. Davis, "An investigation into ecological network analysis for cyber-physical power systems," in *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2021, pp. 252–257.
[12] S. R. Borrett, B. D. Fath, and B. C. Patten, "Functional integration of ecological networks through pathway proliferation," *Journal of theoretical biology*, vol. 245, no. 1, pp. 98–111, 2007.
[13] B. D. Fath, "Structural food web regimes," *Ecological Modelling*, vol. 208, no. 2-4, pp. 391–394, 2007.
[14] A. Chatterjee and A. Layton, "Mimicking nature for resilient resource and infrastructure network design," *Reliability Engineering & System Safety*, vol. 204, p. 107142, 2020.
[15] T. Wilson, A. Chatterjee, and A. Layton, "Exploring the effects of partnership and inventory for supply chain resilience using an ecological network analysis," in *ASME 2022 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, vol. Volume 5: 27th Design for Manufacturing and the Life Cycle Conference (DFMLC), V005T05A011, 2022, Conference Proceedings.
[16] A. Layton, B. Bras, and M. Weissburg, "Designing industrial networks using ecological food web metrics," *Environmental Science & Technology*, vol. 50, no. 20, pp. 11 243–11 252, 2016.
[17] C. Brehm and A. Layton, "Nestedness of eco-industrial networks: Exploring linkage distribution to promote sustainable industrial growth," *Journal of Industrial Ecology*, vol. 25, no. 1, pp. 205–218, 2021.
[18] A. Chatterjee, C. Brehm, and A. Layton, "Evaluating benefits of ecologically-inspired nested architectures for industrial symbiosis," *Resources, Conservation and Recycling*, vol. 167, p. 105423, 2021.
[19] A. Chatterjee, R. Malak, and A. Layton, "Exploring system of systems resilience versus affordability trade-space using a bio-inspired metric," *Journal of Computing and Information Science in Engineering*, vol. 21, no. 5, 2021.
[20] ——, "Ecology-inspired resilient and affordable system of systems using degree of system order," *Systems Engineering*, vol. 25, no. 1, pp. 3–18, 2022.
[21] Y. Liu, Z. Fang, X. Qin, and W. Jin, "Exploring functional dependency network based order-degree analysis for resilient system-of-systems architecture design," in *2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2022, pp. 2319–2325.
[22] 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," *Journal of Mechanical Design*, vol. 142, no. 12, 2020.
[23] V. Panyam, H. Huang, K. Davis, and A. Layton, "Bio-inspired design for robust power grid networks," *Applied Energy*, vol. 251, p. 113349, 2019.
[24] H. Huang, Z. Mao, A. Layton, and K. R. Davis, "An ecological robustness oriented optimal power flow for power systems' survivability," *IEEE Transactions on Power Systems*, 2022.
[25] R. E. Ulanowicz, "Quantitative methods for ecological network analysis," *Computational Biology and Chemistry*, vol. 28, no. 5, pp. 321–339, 2004.
[26] M. E. J. Newman, "Modularity and community structure in networks," *Proceedings of the National Academy of Sciences*, vol. 103, no. 23, pp. 8577–8582, 2006.
[27] E. A. Leicht and M. E. J. Newman, "Community structure in directed networks," *Physical Review Letters*, vol. 100, no. 11, p. 118703, 2008.
[28] Z. Zhuo, "Community detection by maximizing modularity - python implementaion of newman spectral method," https://github.com/zhiyzuo/python-modularity-maximization, Python Library, 2018.
[29] A. Chatterjee, C. Helbig, R. Malak, and A. Layton, "A comparison of graph-theoretic approaches for resilient system of systems design," in *ASME 2022 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, vol. Volume 2: 42nd Computers and Information in Engineering Conference (CIE), V002T02A076, 2022, Conference Proceedings.
[30] J. Han, M. Kamber, and J. Pei, "Data Mining: Concepts and Techniques, 3rd Edition [Book]," iSBN: 9780123814807. [Online]. Available: https://www.oreilly.com/library/view/data-mining-concepts/9780123814791/
[31] S. P. Jayadev, A. Rajeswaran, N. P. Bhatt, and R. Pasumarthy, "A novel approach for phase identification in smart grids using graph theory and principal component analysis," in *2016 American Control Conference (ACC)*, 2016, pp. 5026–5031.
[32] K. J. Chabathula, C. Jaidhar, and M. Ajay Kumara, "Comparative study of principal component analysis based intrusion detection approach using machine learning algorithms," in *2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN)*, 2015, pp. 1–6.
[33] L. Wu, D. He, B. Ai, J. Wang, H. Qi, K. Guan, and Z. Zhong, "Artificial neural network based path loss prediction for wireless communication network," *IEEE Access*, vol. 8, pp. 199 523–199 538, 2020.
[34] S. Hossain-McKenzie, N. Jacobs, A. Summers, B. Kolaczkowski, C. Goes, R. Fasano, Z. Mao, L. Al Homoud, K. Davis, and T. Overbye, "Harmonized automatic relay mitigation of nefarious intentional events (harmonie) - special protection scheme (sps)." 9 2022. [Online]. Available: https://www.osti.gov/biblio/1890265
[35] T. Nishikawa and A. E. Motter, "Comparative analysis of existing models for power-grid synchronization," *New Journal of Physics*, vol. 17, no. 1, p. 015012, jan 2015. [Online]. Available: https://dx.doi.org/10.1088/1367-2630/17/1/015012
[36] D. Iatsenko, A. Bernjak, T. Stankovski, Y. Shiogai, P. J. Owen-Lynch, P. B. M. Clarkson, P. V. E. McClintock, and A. Stefanovska, "Evolution of cardiorespiratory interactions with age." *Philosophical transactions. Series A, Mathematical, physical, and engineering sciences*, vol. 371, no. 1997, p. 20110622, Aug. 2013, place: England.
[37] A. T. Winfree, "Biological rhythms and the behavior of populations of coupled oscillators," *Journal of Theoretical Biology*, vol. 16, no. 1, pp. 15–42, 1967. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0022519367900513
[38] M. M. Danziger, I. Bonamassa, S. Boccaletti, and S. Havlin, "Dynamic interdependence and competition in multilayer networks," *Nature Physics*, vol. 15, no. 2, pp. 178–185, Feb. 2019. [Online]. Available: https://doi.org/10.1038/s41567-018-0343-1
[39] T. Stankovski, T. Pereira, P. McClintock, and A. Stefanovska, "Coupling functions: Universal insights into dynamical interaction mechanisms," *Reviews of Modern Physics*, vol. 89, no. 4, Nov. 2017, publisher: American Physical Society (APS). [Online]. Available: https://doi.org/10.48550/arXiv.1706.01810
[40] T. Stankovski, T. Pereira, P. V. E. McClintock, and A. Stefanovska, "Coupling functions: dynamical interaction mechanisms in the physical, biological and social sciences," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 377, no. 2160, 2019. [Online]. Available: https://royalsocietypublishing.org/doi/abs/10.1098/rsta.2019.0039
[41] T. Stankovski, P. V. E. McClintock, and A. Stefanovska, "Coupling functions enable secure communications," *Phys. Rev. X*, vol. 4, p. 011026, Feb 2014. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevX.4.011026
[42] M. G. Rosenblum and A. S. Pikovsky, "Detecting direction of coupling in interacting oscillators." *Physical review. E, Statistical, nonlinear, and soft matter physics*, vol. 64, Oct. 2001.