Resilience assessment of multi-layered cyber-physical systems

Romain Dagnas, Michel Barbeau, Joaquin Garcia-alfaro, Reda Yaich

Resilience Assessment of Multi-Layered Cyber-Physical Systems

Romain Dagnas* , Michel Barbeau† , Joaquin Garcia-Alfaro‡ , Reda Yaich*
*Institut de Recherche Techologique SystemX, Palaiseau, France
†School of Computer Science, Carleton University, Ottawa, Canada
‡SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris, Palaiseau, France

***Abstract*—Thanks to technological advancements, critical infrastructures integrate many smart technologies and become highly connected to the cyber world. This is especially true for Cyber-Physical Systems (CPSs), which combine hardware and software components. Despite the advantages of smart infrastructures, e.g., sustainable energy usage, security, safety enhancement, and predictive algorithms using machine learning, they remain vulnerable to cyber threats and adversarial events such as cyber-attacks. This work focuses on the cyber resilience of CPSs. We propose a methodology leveraging knowledge graph modeling to increase the remediation potential of CPSs and to avoid critical failures that can occur due to cascading effects in complex architectures. We propose an approach based on multi-layered modeling applied to complex systems to achieve this objective. Indeed, a complex system can be considered an overlay of several layers. We use knowledge graphs to model a Secure Water Treatment System (SWaT) test bed subsystem. We conduct a resilience assessment analysis of several designs with a quantitative metric. This resilience analysis, applied to each layer of our models, is also used to highlight critical points, e.g., the key functions or components that are significant for completing a mission.**

***Index Terms*—Attack Path, Attack Propagation, Cascading Effect, Complex System, Cyber-Physical System, Cyber Resilience, Cyber Threat, Knowledge Graph, Remediation Path, Resilience Enhancement, Resilience Quantification, Semantic Network**

I. Introduction

During the past years, many adversarial attacks such as StuxNet in 2010 [1], CryptoLocker in 2013 [2], and WannaCry in 2017 [3] have highlighted the vulnerabilities of Critical Infrastructures facing cyber adversaries. These cyber attacks impact every strategic sector, e.g., health, transport, and maritime. Statistics produced by governmental entities show an increase each year of perpetrated attacks and costs resulting from such attacks [4]. Protecting critical infrastructures is paramount, especially in our era where cyber adversaries can perpetrate powerful attacks that can disrupt and put a system in an unstable state. The resilience concept has gained interest in the research community, and industrial entities have gradually understood the importance of increasing the resilience potential of a system. Resilience refers to the ability of a system to continue to operate and complete a mission, even if an adversarial event (natural of intentional) occurs. A definition provided by Kott and Linkov describes resilience as *the system's ability to recover or regenerate its performance after an unexpected impact produces a degradation of its performance* [5]. The resilience notion was initially applied in ecology by Holling [6] to quantify a population's ability to recover from changes. Resilience is used in many other fields [7] such as psychology, economy, engineering, computer sciences, and cyber security. As mentioned by Kott and Linkov: *to improve the cyber resilience of a system, you have to measure it* [8]. Measuring the resilience of a Cyber-Physical System (CPS) implies using metrics based on certain system properties, such as performance indicators. We must use architecture models to apply these metrics to an architecture, e.g., mathematical modeling or simulation models. However, in our digitization era, CPSs and especially critical infrastructures increasingly connect and include many components. Their architectures become increasingly complex (e.g., architecture design, human workflows, and operating environment). Due to this complexity, building accurate models of such systems is not easy. Inevitably, the lower the model accuracy, the lower the assessment accuracy resulting from a metric's evaluation.

Motivation. The underlying challenge of making complex systems and CPSs more resilient boils down to building barriers that make attacking difficult for adversaries. From a resilience point of view, we consider that risk zero does not exist. Thus, we seek appropriate countermeasures that increase the resilience potential of an architecture. Ideally, metrics must be available to quantify the resilience of a CPS. Knowledge graph modeling is well suited to representing various links and elements in a system architecture.

Contribution. The contribution of this work is threefold: (i) We model several designs of the Secure Water Treatment System (SWaT) pumping stage as knowledge graphs; (ii) We conduct a resilience assessment analysis of these designs modeled as multi-layered systems by using an eigenvector centrality metric. We also identify the critical points of each layer; (iii) We compare the obtained results with two other metrics presented in our previous works: the (k, ℓ)-resilience property [9], [10] and spectral radius [11].

Section II presents works related to the knowledge graph concept. Section III presents our approach to assessing multi-layered systems' resilience. Section IV conducts a resilience assessment of a SWaT subsystem. We discuss our results in Section V. Section VI concludes and provides some future research axes.

II. Related Work

This section presents several works related to graph techniques and graph analysis in cyber security.

A. Graph Techniques in Cyber Security

1) Graph Analytics: Graph analytics is a data analysis used to understand complex relationships between data entities represented in a graph. It consists of evaluating pieces of information and their connections to know how pieces of information relate to each other or how they could be related.

Noel reviews graph-based methods for assessing and improving operational computer network security, maintaining situational awareness, and ensuring organizational missions [12].

2) Graph Mining: Securing cyberspace and exchanging sensitive data become paramount for organizations, governments, and industrial firms. Graph Mining is a set of techniques used for different purposes: (i) conduct analysis about the properties of real-world graphs; (ii) understand and establish predictions about how a graph can affect some application, and (iii) build models to generate realistic graphs matching real-world graph patterns. Building on graph mining techniques created by the scientific community, researchers are trying to capture correlations between cyber entities. The work by Yan *et al*. [13] presents a review of graph mining techniques used for cyber security.

B. Attack Graphs for Resilience Purposes

In their work, Al Ghazo and Kumar proposed a methodology to identify the critical attacks that could compromise a system's behavior and, when blocked, to guarantee the system security [14]. Zonouz *et al*. work on a different axis. Indeed, their work is based on contingency analysis, which provides guidelines to achieve resilience goals and enable a system to continue to operate even if a failure occurs. In addition to this methodology, they propose using a cyber-physical security evaluation technique that plans remediation measures for accidental and intentional adversarial events [15]. Such a methodology can be used to help operators to choose prevention solutions in case of proactive intrusions. However, such a technique works before an adversarial event occurs and does not increase a system's resilience potential because a human operator's action is required. Furthermore, when an adversary can bypass these measures, the system cannot return to a stable state.

III. Graph Analytics

This section presents the necessary material for establishing our multi-layered approach based on knowledge graph modeling. We also present a metric for quantifying the resilience of a system modeled by such graphs.

A. Knowledge Graph

Ehrlinger and Woess [16] review several definitions of *knowledge graph* found in the literature. One of the definitions highlights that knowledge graphs use ontologies to acquire information and then apply reasoning mechanisms to derive new knowledge about this information. Google introduced a general definition of a knowledge graph in 2012. Other definitions go further and differ across fields. For developers, knowledge graphs are similar to a database with which we interact by the bias of Application Programming Interfaces (APIs). For data scientists, it corresponds to an augmented feature store for connected data, where we can compute and access structural features for Machine Learning (ML). For data engineers, it is similar to a data store where we can integrate data from different sources. It is a database linked to a front-end interface for other fields, with which we can communicate with [17].

In the cyber resilience field, we consider knowledge graphs for their ability to model various entities and relationships between them. Knowledge graphs can be used to model the knowledge acquired by an adversary to perpetrate high-impact attacks. Defenders can also use knowledge graphs to anticipate cascading effects from attacks perpetrated on critical points. We must highlight that knowledge graphs are also interesting for building remediation graphs to provide specific actions for avoiding cascading effects and major losses.

B. Eigenvector Centrality

Modeling complex systems with knowledge graphs implies representing Information Technology (IT)/Operational Technology (OT) components by the bias of nodes. These nodes interact with each other via a set of links, representing physical, wireless, and logical relationships. These knowledge graph models allow us to find critical points, i.e., components or functions that can have a major impact on the performance of systems in case of a failure or when an attack occurs. An adversary attempting to target a critical point can damage a system significantly. Thus, identifying and protecting these critical points is paramount for ensuring the resilience of CPSs.

Eigenvector centrality measures neighbors' influence on a node [18], [19]. Neighbors with high eigenvector centrality carry more weight in the measure than neighbors with low-value neighbors. A node with high eigenvector centrality is in relationships with several neighbors having high eigenvector centrality.

For a given graph $G = (V, E)$ with $|V|$ vertices, let $A = (a_{v,t})$ be the adjacency matrix, i.e., we have $a_{v,t} = 1$ if the vertex v is linked to the vertex t, and $a_{v,t} = 0$ otherwise. The eigenvector centrality score of v is:

$$x_v = \frac{1}{\lambda} \sum_{t \in M(v)} x_t = \frac{1}{\lambda} \sum_{t \in G} a_{v,t} x_t \tag{1}$$

with $M(v)$ the set of neighbors of v and λ a constant. Following the Newman reasoning [18], Eq. (1) can be rewritten as follows:

$$AX = \lambda X \tag{2}$$

X is an eigenvector of the adjacency matrix A with the eigenvalue λ. λ must be the largest eigenvalue of the adjacency matrix A. According to the Perron-Frobenius theorem, this choice guarantees that if A is irreducible, i.e., if the considered graph is (strongly) connected, then the eigenvector solution X is unique and positive. Such a metric is interesting for catching the influence of neighbor nodes, which is related to the notion of critical point. A critical point or node in a graph model is an important function, component, or subsystem for completing a mission. On the other hand, a critical point could also generate cascading effects when an adversary attempts to attack it. This notion of critical point is important in multi-layered models. A layer's overall resilience is insufficient to ensure a good resilience potential. We must ensure that an adversary cannot target critical points to generate cascading effects.

C. Multi-layered Approaches

Modeling systems as multi-layered architectures is not a new topic in the literature. In 1977, Gardner [20] introduced two multi-level approaches for modeling systems with the SARA design, considering *relatively abstract submodels*.

Before this work, in 1968, Zurcher [21] highlighted the importance of considering the levels of abstraction in modeling strategies. Zurcher's work introduces a technique for modeling a multi-processing system's hardware and software components. More recently, Carreras *et al*. have presented an approach to consider the key features of CPSs by the bias of a multi-layered representation for safety and security analysis purposes [22].

Multi-layered representations are also pyramidal representations to model a system's architectural, logical, or regulation-related levels.

There are frameworks, i.e., the Industrial Internet Reference Architecture (IIRA) [23] and Reference Architectural Model Industrie 4.0 (RAMI 4.0) [24] suitable for modeling Industry 4.0 architectures as multi-layered systems. RAMI 4.0 uses a 3-D model by representing an architecture with the following layers: asset, integration, communication, information, functional and business. In our previous work [25], we have applied the RAMI 4.0 model to a water treatment architecture.

D. Multi-layered Architectures for Resilience Purposes

Multi-layered strategies allow one to consider the different levels of a system independently and analyze each of these layers. Our objective is to conduct a resilience analysis on each layer of a multi-layered model to ensure that the resilience potential of all these layers is consistent with the others. Critical infrastructures are complex systems. Conducting a resilience analysis on such an architecture is a difficult task. In our previous work, we have presented a way to quantify the resilience potential of a system with the (k, ℓ)-resilience property (giving an estimation of the controllability degree k and the monitorability degree ℓ of a CPS) [9], [10]. Indeed, increasing a system's resilience implies monitoring it (by the bias of sensors) and controlling it (by the bias of actuators) to bring it back to its original state in case of an attack. We have also presented an approach using the spectral radius metric to quantify the resilience of a system modeled by the bias of a graph [11]. We must highlight that we consider Networked-Control Systems (NCSs). In other fields, such as biology, self-healing systems can restore themselves. Resilience of CPS is similar from the point of view of the recoverability aspect.

However, how can we ensure that a resilience countermeasure that is proven effective does not negatively impact the resilience of another layer? We must remember that increasing a system's resilience potential can also increase the attack surface. Indeed, in previous work [10], we have shown that increasing the monitorability and steerability of a CPS increases its resilience. This implies diverse architecture with monitorability, i.e., sensors, and steerability components, i.e., pumps and valves for water treatment purposes. However, our analysis also shows that having more components connected to cyberspace can increase the attack surface. Thus, a fine balance must be achieved between increasing the resilience potential and mitigating the security risk. Resilience analysis and risk analysis must be conducted in concert.

The objective of our approach is twofold: (i) A first step to achieving this goal is to ensure that the resilience potential of each layer of a given architecture is *consistent*, i.e., ensuring that a layer is not resilient at the expense of the other ones. (ii) The second step consists in protecting critical points. A critical point is an architecture's component, function, or subsystem. It is called *critical* because an adversary attempting to attack a critical point can cause cascading effects that could generate important losses. According to Leveson [26], a loss can be related to life or injury to people, damage to the material, mission completion, regulation conformity, reputation, or finances. We consider the multi-layered representation shown in Fig. 1 to achieve this goal.

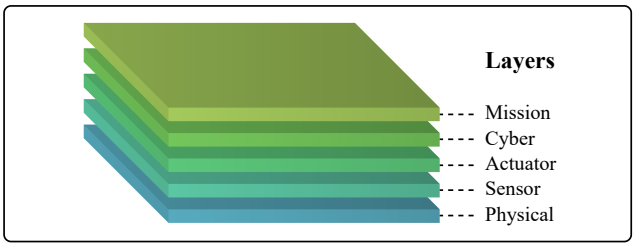


Fig. 1. Multi-layered model of a CPS.

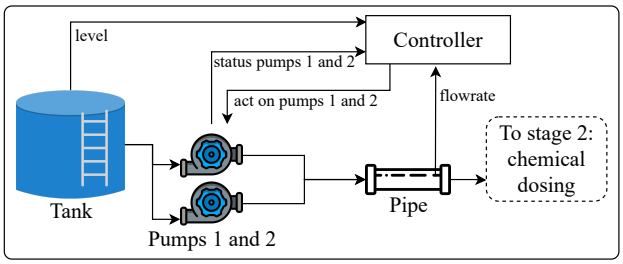
The first level is the physical layer. This layer includes the physical components not playing a role in a system's steerability or monitorability potential, e.g., a tank or a pipe. The second layer is the sensor one. Indeed, the monitorability potential is the first pillar of resilience. To assess the resilience of a system, we must be able to measure it [8]. The third layer is the actuator one, referring to the steerability potential (the second pillar of resilience), including pumps and valves. Then, the cyber layer includes the components connected to cyberspace, i.e., sensors sending readings to a controller through a network. These connected components are visible to an adversary spying on them from cyberspace. It includes all the components sending data through a network. The mission layer corresponds to the components used to complete a system mission. We must highlight that the links connecting the nodes differ in the five identified layers. For example, a sensor link can be: *Flowrate sensor sends data to the controller*. A mission link can be: *Controller must check the water level in the tank according to the readings made by the level sensor*.

This layered model is based on the fact that we mapped components according to the resilience potential they can bring to an architecture. The two last layers (cyber and mission) are transversal layers covering the whole architecture.

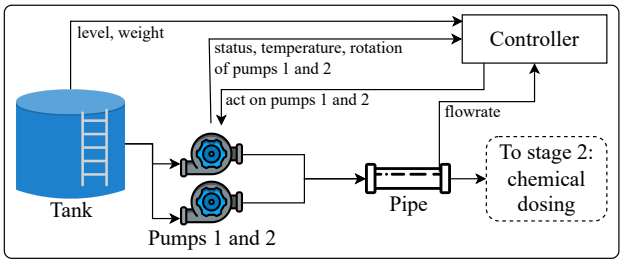
IV. SWaT Pumping Stage Resilience Assessment

Our approach is based on knowledge graph modeling. In such models, nodes represent the components of an architecture. The links are used to model the relationships between each component. The relationships differ across the layers. We apply the eigenvector centrality metric presented in Section III-B to the knowledge graphs to get a measure for each node. Then, following our multi-layered strategy, we map the components according to the layers to which they belong. Each node representing a component has an eigenvector centrality value. We compute a mean eigenvector centrality value for each layer with the eigenvector centrality of the nodes in these layers. These values estimate the resilience potential of each layer. We also conduct a critical point analysis by considering each layer's components with the maximum eigenvector centrality. We consider three designs of the SWaT

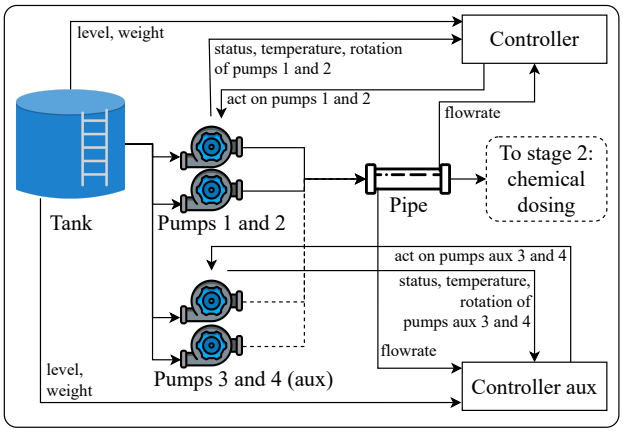
pumping stage to conduct our resilience assessment. SWaT is a test bed built by the Singapore University of Technology and Design (SUTD). This system mimics the real behavior of the Singapore water treatment facility. SWaT is divided into six stages: *Pumping*, *Chemical Dosing*, *Ultrafiltration (UF)*, *Dechlorination*, *Reverse Osmosis (RO)*, *Final stage and Backwash of the UF membrane* [27]. As a use-case, we consider the first stage of SWaT, in which raw water must be cleaned and pumped into the system.



(a) A_0: Original design.



(b) A_1: Design with additional sensors.



(c) A_2: Design with an auxiliary controller and pumps, plus additional sensors.

Fig. 2. Designs of the SWaT pumping stage.

Fig. 2(a) illustrates the original design of the SWaT first stage, which is a sub-system of the overall water treatment station. This subsystem is in charge of pumping the water to be purified. The water is pumped in a tank and sent to the chemical dosing station in stage 2 by two redundant pumps. Fig. 2(b) presents the same design as in Fig. 2(a), with additional sensors, i.e., the weight of the tank and temperature and rotation speed of the two pumps. These additional sensors increase the system's monitorability potential. Fig. 2(c) presents an architecture comprising an auxiliary controller and two pumps. These extra components increase the steerability potential of the system. This architecture consists of the same diversified family of sensors as in Fig. 2(b). Our objective is to conduct a resilience analysis on each layer in order be sure that all layers are mutually resilient. To achieve this goal, we compare these three designs of the pumping stage of SWaT.

Knowledge graphs model the three architectures. Each node represents a component, and different families of links model the interactions between these components. These interactions are related to the layers of the model presented in Fig. 1. Indeed, each layer we consider is a subgraph that includes the related relationships between the nodes. For example, we have a physical connection between the water tank and its level sensor in the physical layer. We use the Neo4j browser and Bloom tools to build the knowledge graphs of the three architectures of the SWaT pumping stage. Via Neo4j Bloom, we apply the eigenvector centrality metric to the graph of the three considered designs. We obtain an eigenvector centrality measure of each node. The obtained results are available in the Excel file of our repository [28]. We map each component of the graph according to the layer it belongs, and we compute a mean eigenvector centrality value for each layer of the three designs.

Figs. 3(a) to 3(e) present the resilience assessment of the physical, sensor, actuator, cyber, and mission layers of the three designs of the SWaT pumping stage. The blue squares present the mean eigenvector centrality computed for each layer of the architectures A_0, A_1, and A_2. In addition to the eigenvector centrality evolving according to the resilience degrees of each design, the Standard Deviation (STD) is depicted with yellow areas. As the eigenvector centrality value of the blue square is a mean, we compute the STD of each layer of the considered designs. Red points indicate the critical points having the highest eigenvector centrality for each layer.

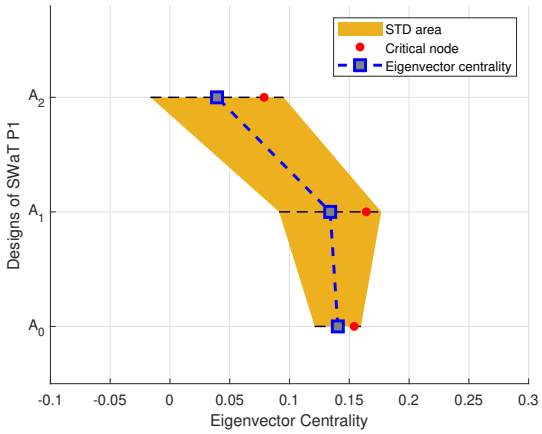
V. Discussion

We must highlight that the eigenvector centrality computation methods differ across the layers (see Table I). This choice reflects that each component in the architectures can be related to one of these three layers (physical, sensor, actuator). Thus, we consider all the links and compute each layer's mean eigenvector centrality measures on a subset of nodes to obtain independent results related to each layer. However, the cyber and mission layers cover all the components of the graphs. Thus, to catch independent results across these two last layers, the granularity resulting from applying the metric lies in selecting specific links when using the eigenvector centrality metric.

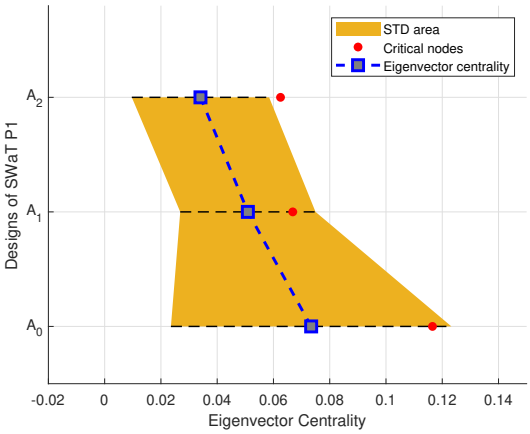
TABLE I
Metric application and computation across the layers.

Layer	*Metric application*	*Metric computation*
Physical	Full graph with all relationships	Mean eigenvector centrality for physical component nodes
Sensor	Full graph with all relationships	Mean eigenvector centrality for sensor nodes
Actuator	Full graph with all relationships	Mean eigenvector centrality for actuators nodes
Cyber	Full graph with cyber relationships	Mean eigenvector centrality for all the nodes
Mission	Full graph with mission relationships	Mean eigenvector centrality for all the nodes

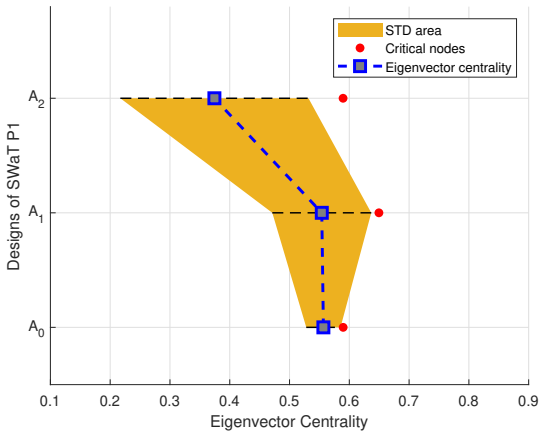
Two important observations can be made by inspecting the results presented in Fig. 3. Firstly, each layer's mean



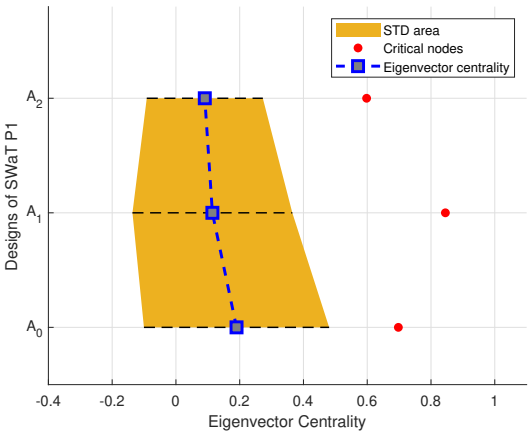
(a) Physical layer of SWaT pumping stage designs.



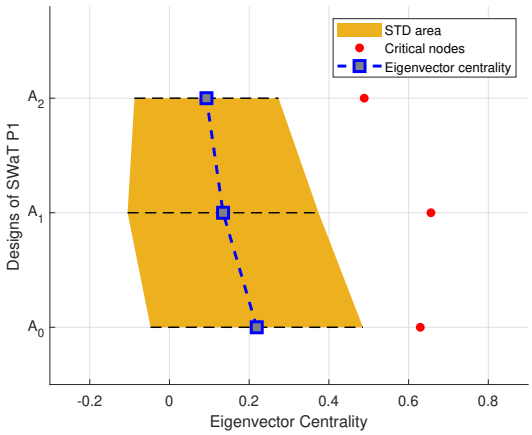
(b) Sensor layer of SWaT pumping stage designs.



(c) Actuator layer of SWaT pumping stage designs.



(d) Cyber layer of SWaT pumping stage designs.



(e) Mission layer of SWaT pumping stage designs.

Fig. 3. Resilience assessment of SWaT pumping stage designs modeled with a multi-layered approach.

eigenvector centrality decreases as the system's resilience potential increases. This could be explained by the fact that the eigenvector centrality measures a node's impact according to the importance of its neighbors in the graph. Thus, making a system more resilient by adding steerability and monitorability components makes a graph more complex, decreasing each node's individual importance. In addition, the more complex a graph modeling an architecture, the more paths there are to recover in case of an attack or in case of a malfunction of a component. This explains why the eigenvector centrality decreases in the architectures A_0, A_1, and A_2. Thus, a decrease in the eigenvector centrality measurements corresponds to an increase in a system's resilience potential.

Secondly, we must consider the critical points in red in each figure. We aim to have the critical points in the yellow areas. Indeed, the yellow areas can be considered safe

zones where an adversary cannot distinguish critical points in an architecture. These results show that A_0 has the best placement of critical points, while A_1 has the worst. We also learn that each architecture's cyber and mission layers have their critical points misplaced outside the yellow areas.

Table II presents a comparative analysis of the results obtained with the (k, ℓ)-resilience [9], [10] and spectral radius [11]. These results are consistent with an increase in the resilience potential in A_0, A_1, and A_2. However, our multi-layered analysis shows the importance of considering critical points in architectures that appear to be resilient.

TABLE II
(k, ℓ)-RESILIENCE AND SPECTRAL RADIUS EVALUATION.

Architecture (A)	***(k,ℓ)-resilience***	***Spectral radius*** $(\rho(A))$
A_0	$(2, 4)$	4.64
A_1	$(2, 8)$	7.75
A_2	$(4, 8)$	10.27

VI. CONCLUSION

This work presents a multi-layered approach to modeling complex systems using five layers: physical, sensor, actuator, cyber, and mission. We have conducted a resilience assessment of each layer of the SWaT pumping stage. We have also built several designs with different degrees of resilience to compare our results. The eigenvector centrality metric shows a decrease in its value when the resilience capabilities of the system are increasing. We have compared our results with the (k, ℓ)-resilience and spectral radius metrics. The results are consistent with an increase in the resilience potential. However, the architecture with the best critical point placement is not necessarily the most resilient one. The critical nodes, i.e., those with higher eigenvector centrality values, must be protected. To achieve this goal, each critical node of each layer must be brought into the yellow areas, considered safe zones. To achieve this goal, designing architectures where the amount of data transmitted through critical nodes is lower is possible. Indeed, a high eigenvector centrality measure means that a node plays an important role in transmitting information across the graph according to the importance of its neighbors. Decentralizing information that flows through critical nodes can be a solution to bring them into safe zones.

We foresee the following research axes for considering cyber resilience applied to complex systems modeled by multi-layered representations. Firstly, there is a need to be able to build remediation graphs. The objective is to ensure that specific countermeasures can absorb the impact of an attack. Secondly, we must ensure the adversary never acquires perfect knowledge about the system to perpetrate an attack with high-impact cascading effects. To achieve this goal, the cyber layer of a system can use decoy mechanisms to fool the adversary and avoid the attack on critical points, leading to moving-target defense strategies.

REFERENCES

[1] D. Kushner, "The Real Story of Stuxnet." https://spectrum.ieee.org/the-real-story-of-stuxnet, Feb 2013.

[2] M. Buckbee, "Cryptolocker: Everything you need to know." https://www.varonis.com/blog/cryptolocker, May 2023.

[3] A. S. Gillis, "WannaCry Ransomware." https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware, Jul 2023.

[4] I. Health, "Cybersecurity Nightmares: The Cost of Healthcare Cyberattacks in 2023." https://intraprisehealth.com/the-cost-of-cyberattacks-in-healthcare/, April 2023.

[5] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, "Resilience metrics for cyber systems," *Environment Systems and Decisions*, vol. 33, pp. 471–476, 2013.

[6] C. S. Holling, "Resilience and stability of ecological systems," *Annual Review of Ecology, Evolution, and Systematics*, vol. 4, pp. 1–23, 1973.

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

[8] A. Kott and I. Linkov, "To improve cyber resilience, measure it," *Computer*, vol. 54, no. 2, pp. 80–85, 2021.

[9] M. Barbeau, F. Cuppens, N. Cuppens, R. Dagnas, and J. Garcia-Alfaro, "Metrics to enhance the resilience of cyber-physical systems," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1167–1172, 2020.

[10] M. Barbeau, F. Cuppens, N. Cuppens, R. Dagnas, and J. Garcia-Alfaro, "Resilience estimation of cyber-physical systems via quantitative metrics," *IEEE Access*, vol. 9, pp. 46462–46475, 2021.

[11] R. Dagnas, M. Barbeau, M. Boutin, J. Garcia-Alfaro, and R. Yaich, "Exploring the quantitative resilience analysis of cyber-physical systems," in *2023 IFIP Networking Conference (IFIP Networking)*, pp. 1–6, 2023.

[12] S. Noel, *A Review of Graph Approaches to Network Security Analytics*, pp. 300–323. Cham: Springer International Publishing, 2018.

[13] B. Yan, C. Yang, C. Shi, Y. Fang, Q. Li, Y. Ye, and J. Du, "Graph mining for cybersecurity: A survey," *ACM Transactions on Knowledge Discovery from Data*, vol. 18, p. 1–52, nov 2023.

[14] A. T. Al Ghazo and R. Kumar, "Identification of critical-attacks set in an attack-graph," in *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 0716–0722, 2019.

[15] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "Socca: A security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 3–13, 2014.

[16] L. Ehrlinger and W. Wöß, "Towards a definition of knowledge graphs.," *SEMANTiCS (Posters, Demos, SuCCESS)*, vol. 48, no. 1-4, p. 2, 2016.

[17] J. Barrasa, "What is a knowledge graph?." https://neo4j.com/blog/what-is-knowledge-graph/, Jul 2023.

[18] M. E. Newman, "The mathematics of networks," *The new palgrave encyclopedia of economics*, vol. 2, no. 2008, pp. 1–12, 2008.

[19] Neo4j, "Eigenvector centrality." https://neo4j.com/docs/graph-data-science/current/algorithms/eigenvector-centrality/, 2024.

[20] R. I. Gardner, "Multi-level modeling in sara," in *Proceedings of the Symposium on Design Automation and Microprocessors*, p. 63–66, IEEE Press, 1977.

[21] F. W. Zurcher and B. Randell, "Iterative multi-level modelling. a methodology for computer system design.," in *IFIP Congress (2)*, pp. 867–871, Citeseer, 1968.

[22] N. H. Carreras Guzman, M. Wied, I. Kozine, and M. A. Lundteigen, "Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis," *Systems Engineering*, vol. 23, no. 2, pp. 189–210, 2020.

[23] S.-W. Lin, B. Miller, J. Durand, R. Joshi, P. Didier, A. Chigani, R. Torenbeek, D. Duggal, R. Martin, G. Bleakley, *et al.*, "Industrial internet reference architecture," *Industrial Internet Consortium (IIC), Tech. Rep*, 2015.

[24] M. Hankel and B. Rexroth, "The reference architectural model industrie 4.0 (rami 4.0)," *Zvei*, vol. 2, no. 2, pp. 4–9, 2015.

[25] R. Dagnas, M. Barbeau, M. Boutin, J. Garcia-Alfaro, and R. Yaich, "Methodological Resilience Assessment of Smart Cyber Infrastructures," in *Security and Privacy in Smart Environments (SPSE)* (S. Katsikas and N. Pitropakis, eds.), Springer, 2024. To appear.

[26] N. G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. The MIT Press, 01 2012.

[27] J. Goh, S. Adepu, K. N. Junejo, and A. Mathur, "A dataset to support research in the design of secure water treatment systems," in *Critical Information Infrastructures Security: 11th International Conference, CRITIS 2016, Paris, France, October 10–12, 2016, Revised Selected Papers 11*, pp. 88–99, Springer, 2017.

[28] "Resilience Multi Layer." https://github.com/IRT-SystemX/resilience_multi_layer. GitHub repository, created: 2024-03-27.