Attack Impact Quantification Prioritizing Security Operation Center Alerts in Energy Distribution

Romain Dagnas* , Anthony Bonnard* , 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*—Critical infrastructure systems, such as water treatment facilities and electrical substations, are getting enhanced with smart features. This addition increases their competitiveness for mission-completion purposes, but renders them more vulnerable to cyber attacks. Under this context, Security Operation Center (SOC) analysts are in charge of monitoring and prioritizing alerts related to those potential new threats. Their task is challenging, due to the large volume of alerts they must handle. We propose to tackle the problem with a novel impact quantification approach based on multi-layered models augmented with knowledge graphs. Knowledge graphs have the ability to model various components and relationships between those components within a single formalism, hence offering an efficient and practical solution to the large panel of topics involving the cybersecurity field. We applied graph analytics metrics to highlight critical points. We validate the approach under a realistic use case involving a representative electricity transmission system operator in France (RTE, Réseau de Transport d'Électricité).**

***Index Terms*—Alert Prioritization; Attack Impact Quantification; Attack Propagation; Cyber Resilience; Energy Distribution; Impact Metric; Multi-layered Model; Knowledge Graph; Graph Analytics; Security Operation Center.**

I. Introduction

Due to the increase in competitiveness, critical infrastructure systems have become highly digitized and connected to the cyber world. This renders such systems vulnerable to cyber attacks. An alarming amount of cyber attacks are being perpetrated against these complex systems due to the increase of the attack surface resulting from digitization. Adversarial events associated to ransomware attacks affecting the energy sector, such as the US Colonial Pipeline breach in May 2021 [1], or Romania's Oltenia Energy Complex intrusion in December 2025 [2], illustrate the damaging consequences generated by cyber attacks against critical infrastructure systems.

Complex systems associated to critical infrastructure are made of a large number of elements in strong interaction and with diverse characteristics. The overall system, connected to internal as well as external actors, rely on each element to be functioning properly. Thus, a cyber attack affecting a part of the system could lead to cascading effects and therefore serious damages on the numerous layers that composes the system, known as systemic impacts. The detection of such situations is of paramount importance. Organizations associated to the protection of critical infrastructure rely on Security Operation Center (SOC) operators, to monitor and handle alerts associated to potential cybersecurity incidents. The criticality levels of cyber attack alerts is later integrated and processed with respect to interoperable classification systems, such as the European Network of Transmission System Operators for Electricity (ENTSO-E) standard for incident classification, which comprises four main levels: low, medium, high, critical.

While attack impact quantification is usually used after an incident occurred, to get a clear insight of the incident and the consequences that resulted of it, it can also be used in a predictive manner to assess the probable consequences of an attack, thus supporting governance and decision making. In this paper, we propose an attack impact quantification strategy for augmented SOC operators. The objective is to help cyber operators prioritize alerts following their identification as true positives, according to the potential damaging effects of cyber attacks, allowing thus their quick and adequate processing.

Motivation of our work. Considering attack impact quantification for augmented cyber operators can help in prioritizing alerts. In fact, the *symptoms* of an attack associated with a quantification methodology can improve the ability of SOC operators to avoid critical failure caused by cyber attacks.

Contributions. Our contributions are threefold: (i) We propose a new version of our multilayered model introduced in [3] that takes advantage of knowledge graphs for building complex systems. In this new version, we include an Information Technology (IT) and a human dimension for modeling complex Cyber-Physical Systems (CPSs); (ii) We propose a methodology for quantifying the impact of cyber attacks of augmented SOC operators; and (iii) We apply our methodology to an example of critical infrastructure which is an electrical distribution system of the Réseau de transport d'électricité (RTE) company.

The remaining sections are organized as follows. Section II presents our formalism and metric. Section III validates our approach for a representative stakeholder. Section IV surveys related work. Section V concludes the work and provides further perspectives of research for future work.

II. Quantifying the Impact of Cyber Attacks

We consider an intentional, negative event that aims to inflict damages to a complex system. Being of a cyber nature, it implies consequences on complex CPSs. However, when dealing with complex systems, the high connectivity between

components and the interaction of components from different layers force to broaden the subjects of impacts and consider other families and types of losses, as discussed by Leveson [4]. Different losses are defined: material, meaning physical damage to components; mission, meaning a loss in a mission completion; financial, which is especially true in the case of a ransomware attack, or when the attack generates damages to components; reputation, when the system cannot be trusted anymore or when an attack generates negative repercussions for its reliability; regulation, when there is a loss of compliance; human lives, when an attack generates injury to or death of people. Agrafiotis *et al*. [5] defined the notion of cyber harm, as the damages that arise as a direct result of an attack conducted wholly or partially through digital infrastructures. He then built a taxonomy of cyber harm that can be encountered by organizations, composed of five themes: physical/digital harm, economic harm, psychological harm, reputational harm, and social or societal harm.

The impact of an attack depends on the loss under consideration. For example, let us consider a manufacturing machine dropping a package on a human employee following a cyber attack aimed at compromising it. In this situation, there is no damage to the material. However, the attack caused an important injury to the employee. Quantifying the impact of an attack implies understanding the subjects of impact, meaning the elements who suffer from the attack, and the types of impact that are the consequences on those subjects arising from it. Our quantification approach relies on the understanding of the criticality of the subjects of impacts in the complex system, based on the relations and interaction between the components from different dimensions.

A. Multilayered Model Based on Knowledge Graphs

Knowledge graphs have the ability to model various components and relationships between those components. Their use in the cybersecurity field can be applied to a large panel of topics, e.g., attack propagation analysis, resilience quantification methodologies or vulnerability detection.

We build upon previous work [3], [6] relying on a multilayered model based on knowledge graphs for resilience quantification and critical point identification purposes. The extension is confronted to the assessment of resilience associated to a specific critical infrastructure. We expand the approach and include two new layers: IT , Service and Stakeholder, to broaden the model and consider alternative new dimensions related to IT or human beings, associated to our problem domain. The updated multilayered model is presented in Fig. 1.This model allows us to study the complex system and the interactions between it's components in three groups of layers. The service and stakeholders layer is made up of the entities that gravitate around the complex infrastructure. Whereas the end users benefit from the service offered by the infrastructure, the users in contact with the IT layer,and the operators operating in the OT layer are together responsible for the well-functioning of the infrastructure. The OT layer describes the operational components, such as actuators, sensors, or physical elements, connected to the cyber world to analyze the status of the components in their objective of carrying out their mission. The IT layer is composed of all the computer and communication systems used in the digitization process of the infrastructure, made of software, hardware components linked to the cyber world, allowing the IT components to fulfill their purpose.

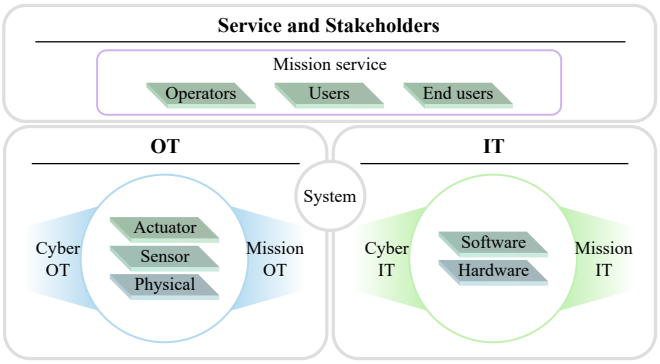

Fig. 1: Extended multilayered model

B. Graph Analytics for Attack Impact Quantification

We present two graph-based metrics and explain their relevance for attack impact quantification.

1) Eigenvector Centrality: The use of the eigenvector centrality in a resilience context has already been validated in the literature [3]. The eigenvector centrality can also be used to find critical points in a complex CPS modeled with knowledge graphs [6]. Identifying critical points is an important step for building an attack impact quantification strategy. When critical points are identified in a system, we can analyze the possible propagation of an attack according to a starting point. In a graph, the eigenvector centrality metric measures neighbors' influence on a node [7], [8]. Neighbors with high eigenvector centrality carry more weight in the measure than neighbors with low-value. A node with high eigenvector centrality is in relationships with several neighbors having high eigenvector centrality.

Let $G = (V, E)$ be a graph with $|V|$ vertices. Let $A = (a_{v,t})$ be the adjacency matrix of G, such that we have $a_{v,t} = 1$ if the vertex v is linked to the vertex t (or $a_{v,t} = 0$, otherwise). The eigenvector centrality measurement of v is:

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

where $M(v)$ is the set of neighbors of v, and λ a constant.

Following Newman reasoning [7], Eq. (1) can be rewritten as follows: $AX = \lambda X \cdot X$ is an eigenvector of the adjacency matrix A with the eigenvalue λ, where λ must be the largest eigenvalue of the adjacency matrix A.

2) Harmonic Centrality: It measures the ability for a given node in the graph to spread information very efficiently [9]. It represents a notion of proximity between nodes. This is very relevant for analyzing propagation effects.

This metric is robust, and solves the issue of unreachable nodes that lead to infinite distances in weakly connected directed graphs. Furthermore, the use of the inverse of the distance emphasizes short distances compared to long ones which is relevant to depict more accurately the proximity of nodes. Our approach takes advantage of this metric to analyze if a node is critically located, meaning a location where an attack could quickly propagate to other nodes. We measure the proximity of nodes to the layers we defined, to be able to quantify how close a node is to be able to propagate to other layers, to group of nodes that we specifically target.

For a node u, the targeted and normalized harmonic centrality we consider is defined by:

$$H(n) = \frac{1}{|T|} \sum_{\substack{t \in T \\ t \neq n}} \frac{1}{d(n,t)} \tag{2}$$

where $d(n,t)$ is the shortest distance between node n and a target node t, T is the set of target nodes, and $|T|$ its cardinality.

C. Quantitication Approach

Let us consider a graph $G_S = (V, E)$ representing a system architecture, such that V is the set of vertices and E the set of nodes. The nodes are used to model the components of the system and the links between those nodes are used to model the relationships between the components. We denote by $\mathcal{M}_{Eig}$ the table containing the eigenvector centrality measurement (for each layer) of the nodes in the G_S. Similarly we denote by $\mathcal{M}_{Har}$ the table containing the harmonic centrality values of the nodes in G_S for each layer.

Definition 1 (Attack): Let $\alpha = (\ell, A)$ be the tuple representing an attack α, being ℓ a node in G_S representing the component targeted by the adversary, i.e., ℓ is the starting point of the attack, and A, the corresponding alert in the SOC.

For a starting point ℓ in G_S given by the alert A following an attack α, we identify the critical points in the graph G_S. These critical points are identified as the nodes having the maximum eigenvector centrality measurement and the maximum harmonic centrality measurement.

Definition 2 (Critical point): A node in the graph G_S is said to be critical in a layer L if its eigenvector centrality measurement is maximum in L.

In the context of critical systems, the notion of critical point may differ according to the system under consideration. The companies responsible for these critical systems are the only ones who can choose which critical point to protect in a specific attack scenario. Our methodology allows us to identify these critical points. Starting from a critical point identified as the most important one, it is possible to build a path from the starting point of the attack to this node. This gives us the attack graph that a SOC operator wants to avoid.

Let E_α be the set of compromised components until the final step of the attack, i.e., until the attack reaches the prioritized critical point, and V_α be the set of links between the compromised components.

Definition 3 (Attack graph): We denote by $G_{S,\alpha} = (v_\alpha, E_\alpha)$ the attack graph corresponding to an attack α for an architecture graph G_S.

Property 1: Let us consider an architecture graph G_S and an attack graph $G_{S,\alpha}$ corresponding to an attack α. $G_{S,\alpha}$ is a subgraph of G_S.

Definition 4 ($\mathcal{C}$ – criticity): Let $\mathcal{M}_{Eig,\alpha} = (x_{i,j})$ be a table containing the eigenvector centrality measurements (in each layers) of the nodes compromised during an attack α, with $i = \{1, \dots m\}$ and $j = \{1, \dots n\}$, being m the number of components compromised by α, and n the total number of layers in our model. We have $\mathcal{M}_{Eig,\alpha} \in \mathcal{M}_{Eig}$. We define the criticity $\mathcal{C}$ as a vector containing the maximum eigenvector centrality value across the different layers for each node compromised by the attack α:

$$\mathcal{C}_i = \max_{1 \leq j \leq n} (x_{i,j}) \tag{3}$$

Definition 5 ($\mathcal{P}$ – proximity): Let $\mathcal{M}_{Har,\alpha} = (y_{i,j})$ be a table containing the harmonic centrality measurements of the nodes compromised during an attack α for each layers, with $i = \{1, \dots m\}$ and $j = \{1, \dots n\}$, being m the number of components compromised by Attack α, and n the total number of layers in our model. We have $\mathcal{M}_{Har,\alpha} \in \mathcal{M}_{Har}$. The proximity $\mathcal{P}$ is defined by the number of layers having a high proximity with the node compromised by Attack α:

$$\mathcal{P} = \sum_{j=1}^{n} \mathbf{1} \left(\exists i \in \{1, \dots, m\} \text{ such that } y_{i,j} = \max_{1 \leq j \leq n} (y_{i,j}) \right) \tag{4}$$

Definition 6 (IQA metric): For an attack α perpetrated on a CPS modeled by the graph G_S, the IQA metric is defined by $IQA = \{\mathcal{C}, \mathcal{P}, \mathcal{N}_\mathcal{C}, \mathcal{N}_\mathcal{P}\}$. $\mathcal{N}_\mathcal{C}$ is the number of nodes compromised by α identified as having a maximum eigenvector centrality in the tables of Section III, and $\mathcal{N}_\mathcal{P}$ is the number of layers having a high proximity with the compromised nodes.

III. An Electrical Distribution System Analysis

We consider an electrical distribution system inspired from RTE. Fig. 2 presents a functional view of this complex system.

This complex system allows electricity transportation and distribution from Electric productions centers (nuclear plant, hydraulic dam, etc.) to the consumers. This process is supported by several physical installations, called substations, with different goals: some distribute electricity on several lines, others change the voltage of the current before transportation and distribution depending on the needs. This process is done thanks to electrical components inside the stations such as busbars, transformers which are directly on the power lines. To protect the systems and the operators working in the stations, some components like Inteligent Electronical Device (IED), circuit breaker, are used. All those systems are remotely monitored from a control center, thanks to sensors, communication devices and an IT system allowing the operators from the center to analyze the status of the process and send instructions to operate on it thanks to a Supervisory Control and Data Acquisition (SCADA).

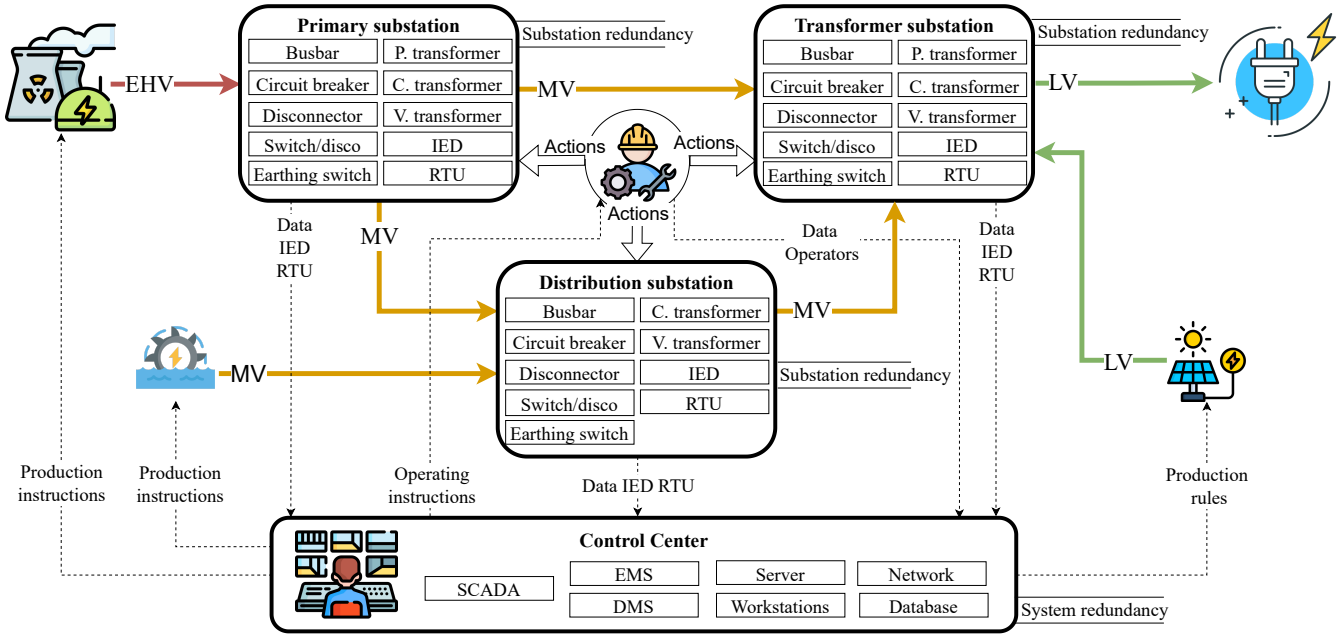

Fig. 2: Functionnal model of the complex electricity system.

Following our methodology, we compute the eigenvector centrality of each node in the graph to identify the critical points. The results are available in our Github repository [10]. We present the most critical points, i.e., the nodes having a maximum eigenvector centrality value for each layer of our model. These critical points are listed in Table I for the Operational Technology (OT) part, Table II for the IT part and Table III for services. In Fig. 3 we present a graphical view of these critical points.

TABLE I: RTE system - OT Influence points

Layer	Physical	Sensor	Actuator	Cyber	Mission
Component	All	All	Disconnector	NetworkOT	RTU
EigenV	0.45	0.5	0.57	0.61	0.56

TABLE II: RTE system - IT Influence points

Layer	Hardware	Software	Cyber	Mission
Component	All	WanRTE	NetworkIT	NetworkOT
EigenV	0.22	0.70	0.49	0.58

TABLE III: RTE system - Service Influence points

Layer	User	EndUser	Operator	Mission
Component	All	EndUsers	Operators	WorkstationIT
EigenV	0.5	1	1	0.33

We also compute the harmonic centrality of each node. The results are available in our Github repository [10]. The components having the highest proximity are listed in Table IV for the OT part, Table V for the IT part and Table VI for services. In Fig. 4 we present a graphical view of the points identified as those having a high proximity with other layers.

TABLE IV: RTE system - OT Proximity points

Layer	Physical	Sensor	Actuator
Component	Disconnector	Operators	Operators
Value	0.41	0.81	0.87

TABLE V: RTE system - IT Proximity points

Layer	Software	Hardware
Component	WanRTE	NetworkOT
Value	0.37	0.40

TABLE VI: RTE system - Service Proximity points

Layer	User	EndUser	Operator
Component	Workstations	LineConsumer	Electrical Components
Value	0.35	1	1

TABLE VII: SOC alert A

Time	Alert type	Source	Impacted asset
12:20:34	Unexpected communication	Endpoint detect. resp.	SCADA Server

Our approach identify critical points and components having a proximity with other layers in our multilayered model. Thus, industrial entities can use this methodology to support their usual business or financial quantification methods done with knowledge they hold, to find critical points that must never be attacked in order to preserve the system and quantify how critical they are.

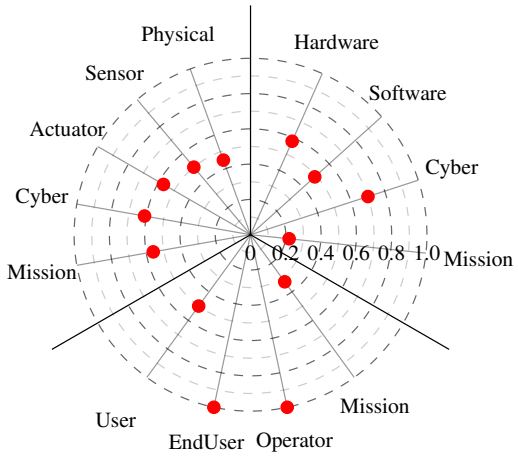

Fig. 3: Highest criticity value per layer

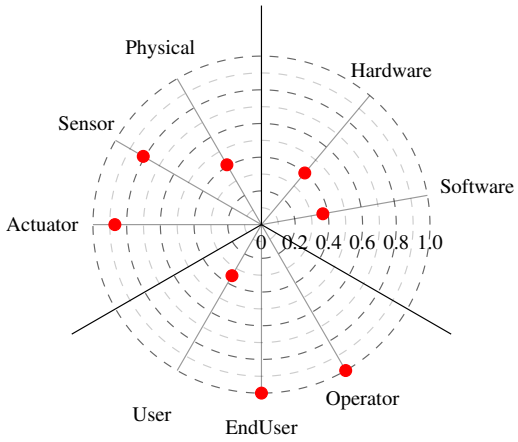

Fig. 4: Highest proximity value per layer

Let us now consider a scenario where an alert A come to the SOC. The details of this alert are represented in Table VII. An attacker who compromised an OT server can perform reconnaissance, exploit vulnerabilities to pivot through firewalls and routers, and move laterally to reach and compromise other components of the system. The first step of the attack α, on one of the SCADAs servers, is noticed through the processing of Alert A. Let us assume that the point identified as critical by our methodology and the usual quantification methods of the system holders identifies the Remote Terminal Unit as critical for the OT missions. Having the starting point and the final destination that we want to avoid, it is possible to build one possible path between these two points, i.e., a list of components potentially compromised by the adversary before reaching the critical point. According to our model, this path is as follows: *Server OT (Scada), Network OT, Firewall OT, Router North, Router West, Router South, Firewall Station, Remote Terminal Unit*.

We compute the $\mathcal{C} - criticity$ and the $\mathcal{P} - proximity$ associated to α. We obtain: $IQA = \{\mathcal{C}, \mathcal{P}, 7, 6\}$. With $\mathcal{C}_\alpha = [0, 0, 0, 0, 0.6, 0.56, 0, 0.22, 0, 0, 0, 0]$, i.e., critical components with their maximum value per layer, $\mathcal{P} = [0.27, 0.28, 0.56, 0.33, 0.4, 0, 0, 0.33]$, i.e., the number of layers close to the scenario, $\mathcal{N}_\mathcal{C} = 7$ and $\mathcal{N}_\mathcal{P} = 6$.

IV. Related Work

A. Mathematical Models

Originally, cyber attack impact quantification works use mathematical models and metrics. Orojloo and Azgomi used a methodology based on analyzing the dynamic behavior of systems in a normal situation and under attacks to estimate the direct and indirect impacts of attacks on CPSs [11]. Milošević *et al*. present a framework based on a state-space model to estimate the impact of cyber attacks against a dynamic control system including an anomaly detector [12]. In a more recent work, Milošević *et al*. studied the problem of estimating the impact of cyber attacks in stochastic linear Networked-Control Systems (NCSs) [13]. Lanotte *et al*. provide a formal compositional metric that estimates the impact of cyber-physical attacks targeting sensor devices in Internet of Things (IoT) systems [14]. In a more recent work, Lanotte *et al*. used two probabilistic metrics to study the physical impact of attacks considering the severity of damage inflicted in a given time and the probability that these attacks can be perpetrated [15]. We understand from these works that mathematical modeling and models based on control theory are relevant for CPSs modeling. However, it is difficult to model critical infrastructures that include a wide range of components because of their complexity.

B. Quantification Frameworks

According to the literature, quantification frameworks gained interest in the field of attack impact processing. Especially for methodologies that use risk analysis or Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS) scoring. Park and Lee [16] introduced a quantitative assessment framework that evaluates the risk of cyber attack considering the difficulty and consequences of an attack. Amro *et al*. presented a contribution based on a risk assessment approach. Their work uses a Failure Modes Effects and Criticality Analysis (FMECA) enriched with selected semantics and components of the MITRE ATT&CK framework [17]. In their work, Stellios *et al*. used an attack tree topology associated to CVE, CVSS and threat modeling for attack path analysis [18]. Model-based engineering (MBE) approaches can be used to evaluate the risk and impact of an attack on a CPS by evaluating its likelihood. Hutzler *et al*. proposed a method to automate the discovery of cyber attacks in a distributed system [19]. Their work showcases the possibilities in eliciting the most efficient attack vectors an attacker can exploit by evaluating all possible attack paths in a CPS topology using visibility graphs and cost graphs.

C. Graph-based Methodologies

More recently, methodologies that use graph modeling to quantify the impact of the attack have gained interest within the community. Indeed, such models allow one to study attack propagation and attack paths in complex architectures.

Krautsevich *et al*. provide a formal approach to model cyber attacks and evaluate the security of complex systems. Thus, the attacks surface and attack graph approaches are combined in order to establish an explicit link between the assessment of security risks and the two previous approaches [20]. In their work, Maiti *et al*. present a solution based on causal graphs to identify the exact set of Design Parameters (DPs) affected by a cyber attack launched on another set of DPs in a CPS [21]. Rosso *et al*. presented a methodology considering the required attack knowledge about a CPS to perpetrate an attack and used context factors to estimate the cost of an attack [22].

D. Discussion

Various methodologies have been proposed in the literature for attack impact quantification purposes, e.g., mathematical-model-based methodologies, quantification frameworks, and graph-based methodologies. The novelty of our approach lies in its ability to leverage the advantages of knowledge graphs for modeling complex components. The methodologies available in the literature are highly related to the system under consideration and may not be transposable to other families of complex systems. The use of knowledge graph allow to model various families of critical architectures. Most of the existing approaches start from assumptions to quantify losses with qualitative measurements. Our approach is based on numerical quantification with a material introduced for resilience purposes and extended to be applied in the attack impact quantification field.

V. Conclusion

We have presented an extended methodology based on a multi-layered model using knowledge graphs for attack impact quantification purposes. From an alert received in a SOC, we identify critical points with the eigenvector centrality and the harmonic centrality metrics. The path from the component having triggered the alert to a specific critical point gives the steps of a probable attack. We use the harmonic centrality to understand which layers of the model can be crossed by the different steps, reflecting damaging consequences. This knowledge enables SOC teams to prioritize proactively, targeting damaging threats well before they hit the point of no return. We foresee the following research perspectives for future work. First, the temporal dimension is not considered in our approach. It is important to consider dynamic graphs in the case of an architecture with components that can be connected at time t, but not connected anymore at time $t + 1$. Second, considering a duration aspect of the attack quantification can help in understanding, from past attacks, which symptoms can highlight damaging consequences if an attack succeeds.

Acknowledgments — This work has been supported by the French government under the "France 2030" program, as part of the SystemX Technological Research Institute within the Cybelia Program.

References

[1] J. Beerman, D. Berent, Z. Falter, and S. Bhunia, "A review of colonial pipeline ransomware attack," in *2023 IEEE/ACM 23rd international symposium on cluster, cloud and internet computing workshops (CCGridW)*, pp. 8–15, IEEE, 2023.

[2] ShieldWorkz and I. Cyber, "The Holiday Siege: Unpacking the Ransomware Attack on Oltenia Energy Complex," January 2026. Details the December 26, 2025, 'Gentlemen' ransomware attack on Romania's largest coal-based energy producer, including attack vectors, impact on IT/ERP systems, and broader context of coordinated holiday cyber campaigns.

[3] R. Dagnas, M. Barbeau, J. Garcia-Alfaro, and R. Yaich, "Resilience Assessment of Multi-Layered Cyber-Physical Systems," in *2024 IFIP Networking Conference (IFIP Networking)*, pp. 1–6, 2024.

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

[5] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity*, vol. 4, p. tyy006, 10 2018.

[6] R. Dagnas, M. Barbeau, J. Garcia-Alfaro, and R. Yaich, "Graph Analytics for Cyber-Physical System Resilience Quantification," 2025. https://doi.org/10.48550/arXiv.2504.02120,underreview.

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

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

[9] Neo4j, "Harmonic Centrality." https://neo4j.com/docs/graph-data-science/current/algorithms/harmonic-centrality/, 2024.

[10] "Cybelia — Attack Impact Quantification." https://github.com/romaindgns/cybelia_attack_impact_quantification, 2026. GitHub repository, created: 2026-03-16.

[11] H. Orojloo and M. A. Azgomi, "A method for evaluating the consequence propagation of security attacks in cyber–physical systems," *Future Generation Computer Systems*, vol. 67, pp. 57–71, 2017.

[12] J. Milošević, D. Umsonst, H. Sandberg, and K. H. Johansson, "Quantifying the impact of cyber-attack strategies for control systems equipped with an anomaly detector," in *2018 European Control Conference (ECC)*, pp. 331–337, IEEE, 2018.

[13] J. Milošević, H. Sandberg, and K. H. Johansson, "Estimating the impact of cyber-attack strategies for stochastic networked control systems," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 2, pp. 747–757, 2019.

[14] R. Lanotte, M. Merro, and S. Tini, "Towards a formal notion of impact metric for cyber-physical attacks," in *International Conference on Integrated Formal Methods*, pp. 296–315, Springer, 2018.

[15] R. Lanotte, M. Merro, A. Munteanu, and S. Tini, "Formal impact metrics for cyber-physical attacks," in *2021 IEEE 34th Computer Security Foundations Symposium (CSF)*, pp. 1–16, IEEE, 2021.

[16] J. W. Park and S. J. Lee, "A quantitative assessment framework for cyber-attack scenarios on nuclear power plants using relative difficulty and consequence," *Annals of Nuclear Energy*, vol. 142, p. 107432, 2020.

[17] A. Amro, V. Gkioulos, and S. Katsikas, "Assessing cyber risk in cyber-physical systems using the ATT&CK framework," *ACM Transactions on Privacy and Security*, vol. 26, no. 2, pp. 1–33, 2023.

[18] I. Stellios, P. Kotzanikolaou, and C. Grigoriadis, "Assessing IoT enabled cyber-physical attack paths against critical systems," *Computers & Security*, vol. 107, p. 102316, 2021.

[19] G. Hutzler, H. Klaudel, W. Klaudel, F. Pommereau, and A. Rataj, "Automatic Discovery of Cyberattacks," in *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 1–8, 2024.

[20] L. Krautsevich, F. Martinelli, and A. Yautsiukhin, "Evaluation of Risk for Complex Systems Using Attack Surface," in *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, pp. 275–280, IEEE, 2014.

[21] R. R. Maiti, S. Adepu, and E. Lupu, "ICCPS: Impact discovery using causal inference for cyber attacks in CPSs," *arXiv preprint arXiv:2307.14161*, 2023.

[22] M. Rosso, L. Allodi, E. Zambon, and J. den Hartog, "A Methodology to Measure the "Cost" of CPS Attacks: Not all CPS Networks are Created Equal," in *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 112–129, IEEE, 2024.