Toward Proactive Cyber-Physical-Human Risk Assessment in Power Systems

Amarachi Umunnakwe, *Member, IEEE,* Shining Sun, *Student Member, IEEE,* Katherine Davis, *Senior Member, IEEE*
Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843, USA
Email: amarachi@tamu.edu, sshh2@tamu.edu, katedavis@tamu.edu

***Abstract*—Energy delivery systems are the ultimate critical infrastructure. The urgency to develop and deploy automated techniques to identify and reduce risks is present. However, as adversarial actions in cyber-physical systems (CPS) continue to rise, it is increasingly important to understand and model the role of human behavior in affecting interactions within and between CPS. Hence, this paper proposes an asset-based risk assessment approach that integrates the common vulnerability scoring system to evaluate the impacts of adversary-exploitable paths. The approach models humans as nodes in a graph layer, which interfaces with both cyber and physical layers. Then, a risk analysis is performed to understand how human roles can leverage or mitigate vulnerabilities to actualize threats. A case study is presented on an 8-substation power system model. The results demonstrate the potential to develop new techniques for mitigating risk by including the human layer in the analysis of cyber-physical power systems.**

***Index Terms*—cyber-physical-human system, risk assessment, risk mitigation**

I. Introduction

Cyber-physical systems such as power systems integrate computing and communications technology, including both information (IT) and operational technology (OT). Such cyber technology underpins reliable grid operation and enables operational improvements. However, new technology is introduced at the risk of introducing more exploitable vulnerabilities [1], or weaknesses. The vulnerabilities of interest include those associated with the configurations/functions, or lack thereof, of physical controls, mechanisms, policies, and procedures. The vulnerabilities are latent properties of the system that may be activated to exploit assets. Exploitation of vulnerabilities can lead to a wide range of potential impacts including data breaches, asset damages, and outages. For instance, the Kaseya ransomware attack occurred in July 2021 that leveraged an authentication bypass vulnerability in the remote monitoring and management software against many managed service providers [2]. In the past 3 years, over 2500 organizations have fallen victim to ransomware attacks [3], , with organizations in the United States suffering more than 50% of these attacks including the infamous Colonial pipeline attacks of April 2021 which affected roughly 45% of the East Coast of United States supply of diesel, petrol, and jet fuel [4]. Although this attack was originally targeting the IT network, the realization remains that operators had to disrupt operations until they were certain on impacted components as well as their response strategy.

Hence, these attacks can directly impact or indirectly disrupt operations in critical CPSs. According to threat intelligence data [5] about 28% of attack vectors leveraged the system vulnerabilities. Attacks that leveraged phishing, the use of social engineering to coax victim to open a malicious attachment or link, as the initial attack vector were highest averaging 39%. At 28%, vulnerability exploitation targeted public-facing applications in exposed systems. Remote service login, trusted services, and supply chain attacks follow with 11% respectively.

The threat is exacerbated by the decreasing time necessary to exploit a new known vulnerability. This challenges critical systems with needing to patch identified vulnerable services in minimum time before access. Therefore, this paper proposes a proactive approach, where the defender aims to stay ahead of the adversary by avoiding, masking, or minimizing exploitable vulnerabilities.

II. Literature Review

The work in [6] motivates rigorously quantifying the effects of deception on the adversary. Specifically, researchers aim to discover how the adversary's emotional state can be classified, and how the observed cluster of behavioral data on the adversary can correlate with the adversary's ability to be successful. A model is proposed to capture adversary behavior patterns. In power systems, the method and results of [6] can offer recommendations to cyber-physical modeling, analysis, and response, by providing a direct link between the data collected (logs, alerts, sensors) and a mathematical model of human behavior. Such models can shed light on how to compose these states for a more complete portrayal of humans as both threat and defense actors, about whose behavior inferences can then be made. In particular, results using this model and data collected from cyber attack experts show a strong correlation between emotional state and the frequency an attacker performs reconnaissance and intrusion actions. Hence, the model provides a quantitative link showing the relevance of emotional state and the adversary's success or defeat. A temporal difference between the emotional state and the impact on adversary behavior is also seen [6]. If one can embed some of this information in the detection and response models, it can help improve mitigation results in the power system environment. In summary, such a model could be applied in power systems in the cyber-physical-human system model.

Assessing risk is essential in CPS. Cyber anomalies can have repercussions in the physical layer, and vice versa [7]. The adversary could gain access locally or via stepping stone attacks, e.g., a series of vulnerability exploitations. For instance, gaining Supervisory Control and Data Acquisition (SCADA) access by leveraging vulnerabilities to freeze management abilities, to limit the HMIs' ability to send and monitor commands, or to disable historian operations [8]. Vulnerability assessment aids risk assessment, leveraging tools like NMap, OpenVAS, Wireshark, and Snort. Vulnerability awareness can also be maintained through product vendor websites and third party resources such as the National Vulnerability Database (NVD) [9], Electricity Information Sharing and Analysis Center [10], SANS Internet Storm Center [11], and Exploit Database [12].

Stakeholders may need to assess their system risk to support policy and structure without total dependency on third party security which could be compromised [2]. Also, for smaller systems, third party security may be costly, requiring extensive labor to sift through and correlate logs, that may have high false alarms. Thus, propositions have been made using intelligent algorithms [13]–[15] which analyze data to support security software, as well as graph-based approaches for integrating topological attributes into risk assessment [16]–[18]. In [19], [20] a Markov-based approach is presented for cyber-physical contingency analysis that identifies high-risk assets and access paths toward high value targets [21]. Centrality features are shown able to be adapted to networks to identify critical components [22]–[24].

According to [25], ransomware threats on CPS are a growing concern based on ease of access of vulnerabilities, either internet connected or local. Ransomware attacks leveraging operational system vulnerabilities widely employ infection by email, USB, and URL-share by unawareness of employee [8].

Hence, this paper presents a framework for cyber-physical-human risk assessment of critical systems. The resulting information is used to make recommendations toward improving situational awareness and reducing exploitable attack vectors. The framework lays the grounds for risk management and consists of: 1) vulnerability assessment, 2) cyber-physical-human risk assessment, 3) proactive operator response strategy. Accordingly, the objective is to utilize vulnerability assessment, topological attributes, system-specific details such as locational security, and human/operator attributes to assess system risk, and thus prioritize the distribution of protection resources.

III. Modeling Risk and Vulnerability

It is judicious to develop approaches for assessing and mitigating system risk when compromise paths through the system inevitably occur. Risk is a function of a threat that leverages vulnerability, Eqn. (1). In this work, the threat is assumed to be intentional and adversarial. An assumption can be made that the analyst cannot control the threat or the impact; then, the optimal strategy to minimize risk becomes to minimize vulnerabilities.

$$\begin{aligned} \text{Risk} &= \mathit{Likelihood} \times \mathit{Impact} \\ \text{Likelihood} &= \mathit{Threat} \times \mathit{Vulnerability} \\ \text{Threat} &= \mathit{Capability} \times \mathit{Intent} \end{aligned} \qquad (1)$$

The modeling in this work is based on the goal to enable situational awareness for power system operators and analysts. The proposed framework considers a typical adversary intrusion process as follows: (i) identifying system access points, (ii) penetration via access points, (iii) determining optimal target, (iv) attack execution. Hence, the system analyst engages the framework of Fig. 1 by: (i) generating the system attack graph, (ii) identifying possible adversary access points, and (iii) calculating the optimal adversary targets to compromise which are critical components for the system to protect. Details of each step are described in the sections below.

A. Graph Model of System Interdependencies

In modeling CPS, crucial characteristics of the composed system originate from its detailed devices or assets and the interconnections between these assets that support information and control data exchange. The assets and dependencies can be represented in a graph by nodes and edges, respectively.

1) Cyber-physical graph: In this model, a node is an asset that is either *cyber* or *physical*. *Cyber* nodes are elements used for computation and communication tasks, such as data preprocessing, transfer, and/or storage as digital information or

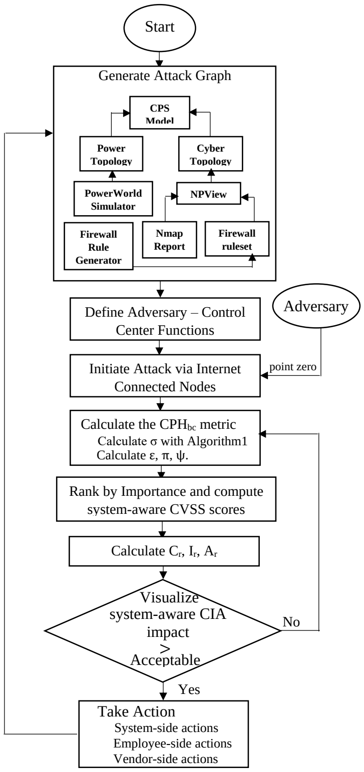
Start
Generate Attack Graph
CPS Model
Power Topology
Cyber Topology
PowerWorld Simulator
NPView
Firewall Rule Generator
Nmap Report
Firewall ruleset
Define Adversary – Control Center Functions
Adversary
point zero
Initiate Attack via Internet Connected Nodes
Calculate the CPH$_{bc}$ metric
Calculate σ with Algorithm1
Calculate ε, π, ψ.
Rank by Importance and compute system-aware CVSS scores
Calculate C$_r$, I$_r$, A$_r$
Visualize system-aware CIA impact > Acceptable
No
Yes
Take Action
System-side actions
Employee-side actions
Vendor-side actions

Fig. 1. The CPH_{bc} Risk Assessment Framework

commands. These nodes may be locally connected or may be networked. *Physical* nodes are field devices like sensors and circuit breakers, which can be manually operated or controlled by cyber nodes. The data originates from these nodes, or the control signals actuate these nodes. The cyber nodes are the intermediary steps that process the data into information for storage or into the commands sent back to the physical nodes. Cyber-physical edges are interconnections between the cyber and physical nodes.

It will also be defined in this model that both cyber and physical nodes are able to have some interaction with a human user or operator. That is, a human may be permitted access to it. More details on the human's roles and access permissions will be specified later. The cyber-physical interconnections include both autonomous and human-controlled communications and commands.

2) Cyber-physical-human graph: A human can be acting under a number of different roles. In our model, this means interacting with a cyber or physical node. The same human (modeled as a node) interacting with the cyber or physical node could have a diverse set of actual motivations and intentions, ranging from a power system operator (defender) to a well-funded adversary. This will be more fully considered and explained, on how to address and differentiate the human intentions in the context of this modeling approach, later.

For now, we simply consider the human to be any person that interacts with nodes and can influence cyber-physical edges: e.g., operators, SCADA engineers, and other personnel. In the proposed model, the human may be utilized or exploited by an adversary to leverage a vulnerability.

If a 'human is utilized or exploited,' what does it do in the model? The result is the human becomes a stepping stone and may connect nodes that were not previously connected. Hence, the interactions with humans can be modeled as another layer in our abstracted mathematical model, looking similar to the pathways enabled by firewalls, but instead are people.

The importance of this model is to better understand and model how the interactions of the cyber nodes with the humans/operators can alter the expected outcome of a given command. These interactions can create a new type of vulnerability surface, of latent or unexpected behavior in the CPS. Then, it is the actual outcome of this interaction, rather than the expected, that influences or controls the physical nodes. Hence, a better understanding and visibility into modeling these interactions is essential.

For example, an operator can cause a command to be sent from a cyber node to a physical node. However, an adversary can leverage a vulnerability of a device and influence the physical outcome, causing an operator's actual impact to deviate from his or her expected impact.

This motivates the cyber-physical interdependencies considered as follows:

- Between cyber vertices (communication) e.g., host-host, host-router link. This interdependency is the data flow or service between cyber vertices.

Metric from Base Score	**Indicator**	**Value Range**	**Interpretation**
Exploitability (exp.)	Attack complexity	0.44 - 0.77	Ease of exp.
	Attack vector	0.2 - 0.85	Context of exp.
	Authentication	0.27 - 0.85	Level of privilege
	User interaction	0.62 - 0.85	Level outside aid
Impact	On confidentiality	0 - 0.56	Table II
	On integrity	0 - 0.56	Table II
	On availabilty	0 - 0.56	Table II

TABLE I
CVSS COMPUTATION AS A VULNERABILITY INDICATOR: MAPPING FROM QUANTITATIVE SCORES, BASED ON [26].

	Confidentiality Impact	**Integrity Impact**	**Availability Impact**
High	Total information disclosure	Complete loss of veracity	Complete resource unavailability
Low	The loss is constrained	Consequence is constrained	Reduced Performance
None	No loss of confidentiality	No loss of integrity	No loss availability

TABLE II
SUB-SCORES, FROM HIGH TO NO IMPACT, RANGE INTEGRATED INTO THE METHODOLOGY, FROM [26].

- Cyber to physical vertex (control), used to send information/commands to physical nodes.

Hence, if data flows from object v_i to v_j, then object v_j is dependent on v_i, and the dependency is represented by the network edge $e_{ij} = v_i \rightarrow v_j$. We represent G as a pair of vertex and edge sets (V, E), with $V = \{v_1, v_2, v_3, ..., v_n\}$, and $E = \{e_1, e_2, e_3, ..., e_m\}$ with individual weights $CC(e)$ $\rightarrow \mathbf{R}^+$. Thus, connectivity characterization is stored in three elements: 1) a source object; 2) a sink object; and 3) their cyber cost (CC).

B. System Vulnerability Modeling

In this work, vulnerability is modeled by employing cyber costs (CC), computed based on the Common Vulnerability Scoring System (CVSS) obtained from the NVD [9], adopted as an international standard for scoring vulnerabilities. For instance, an attack source vertex may leverage knowledge of required username and password to remotely access another sink vertex with hard-coded SSH credentials by exploiting vulnerability `CVE-xxxx-xxxx`. More details of the methodology and examples are given in [27]. The score is computed as:

$$\text{CVSS(base)} = \begin{cases} 0, & \text{if Impact subscore} \leq 0. \\ (\text{roundup}(\min[(\text{Impact}+ & \\ \text{Exploitability}), 10])), & \text{otherwise.} \end{cases} \tag{2}$$

where the *Impact* and *Exploitability* sub-scores are calculated as (3) and (4) respectively.

$$\begin{aligned} \text{Impact} = 6.42 \times (1 - [(1 - \text{Confidentiality}_{\text{impact}}) \times \\ (1 - \text{Integrity}_{\text{impact}}) \times \\ (1 - \text{Availability}_{\text{impact}})]) \end{aligned} \tag{3}$$

$$\begin{aligned} \text{Exploitability} = 8.22 \times \text{AttackVector} \times \text{AttackComplexity} \\ \times \text{PrivilegeRequired} \times \text{UserInteraction} \end{aligned} \tag{4}$$

Specifically, Confidentiality (C) is the limitation of information access to authorized users and preventing disclosure to unauthorized users, Integrity (I) is the veracity of information, while Availability (A) is the accessibility of information resources or node functionality [26].

For example, if a node that communicates through ftp is compromised, it causes loss of integrity in the ftp service, and confidentiality of the node is in jeopardy. Then, the base score is obtained by analysis of the impact the vulnerability will have on confidentiality, availability and integrity, ranking these by high, medium or low, according to Table II, and then taking corresponding quantitative values according to Table I into calculation.

Then, once the vulnerability score is obtained, as described above, the cyber costs (CC) for each cyber-physical edge are calculated as follows:

$$CC(e) = \min V_e \quad \forall e \tag{5}$$

On paths where multiple vulnerabilities V_e exist, we assume the worst case, that is, we utilize the vulnerability with the lowest cost to the adversary and highest impact.

IV. Design of the Cyber-Physical-Human System Risk Assessment

The goal is to enable risk assessment using the above approach, with an additional calculation to dynamically seek the nodes that have a greater impact on the system. This allows the analyst to route resources to such critical nodes. This approach ensures that when vulnerabilities cannot be resolved in good time (e.g., patches are not yet available or will cause interruptions), the system can reduce its exposure by deferring to alternate risk management techniques, e.g., strengthened monitoring, firewalls, and resource allocation.

A. Cyber-Physical-Human Risk Assessment

The cyber-physical-human betweenness centrality CPH_{bc} metric is proposed to improve situational awareness by ranking nodes according to criticality. CPH_{bc} integrates human factors by assessing the likelihood of compromising the node's operator, as well the physical security of the system to assess the ease of intruder access, e.g., strategically placing compromised USB within operators' reach. The importance is highlighted in [28], given that 91% of cyber-attacks begin with phishing, which leverages the node's human operator. The cyberattack life cycle or cyber kill chain can be described in different ways but generally includes the stages of reconnaissance, to weaponization, to exploitation, to installation, to command and control, to achieve action objectives. The approach in this paper is focused on helping at the exploitation stage. Thus, by integrating the human aspect, the intention is to break the chain of attack life cycle early.

In particular, the risk posed by humans can be hard to model due to complex dynamic factors, hence, we identify important features that can quantify the level of human risk to social engineering. These features are based on awareness to different levels of social engineering-type attacks and are: 1.) Experience in recognizing anomalous behavior in the nodes/system. This feature is evaluated by the product of normalized time and consistency on the job. 2.) Test scores during test runs with a simulated/emulated cyber attack exercises. 3.) Education level which informs technical "know-how". For instance, a certified IT engineer vs. entry level operator. In essence, the ease of compromising a human operator is calculated using these features as follows:

$$\Pi(v) = (\omega_1 \times education) + (\omega_2 \times test\_scores) + (\omega_3 \times \Xi) \tag{6}$$

where ω_1, ω_2, and ω_3 are weights from expert opinion accorded to education, test_scores, and experience, Ξ which is calculated as:

$$\Xi = consistency \times \frac{No\ of\ work\ years}{Expected\ No\ of\ work\ years} \tag{7}$$

where consistency depicts the level of variability due to operator changes. For instance, if an operator has the same job description over time, there is a high consistency and lower chance the adversary will be able to exploit the operator. Human risk is high with little-to-no experience, medium with experience but low education, and lowest when well experienced and educated. Similarly, physical location security, Ψ, is also important, the more secure the physical location of a node, the less the risk. Given the above equations, the cyber-physical-human betweenness centrality CPH_{bc} index is then calculated

$$\text{as}: \ \text{CPH}_{bc}(v) = \sum_{s \neq v \neq t \in V} \sigma_{st}(v) + \left(\varepsilon \times \frac{1}{\Pi} \times \frac{1}{\Psi} \times \frac{1}{\left(\frac{1}{\sum^{e_v} CC(e)} \right)} \right),$$

where $\sigma_{st}(v)$ is the number of shortest paths from source vertex s to target (relay) node t that pass through the node v. The edges are weighted on the communication link cyber costs $CC(e)$, e_v is the set of all edges to/from v, with cardinality of ε which is proportional to vertex density in the network, and Ψ is the level of physical security of the location of v. In particular, $\sigma_{st}(v)$ informs the likelihood of the adversary reaching target relays from unique nodes v, and is computed based on the node v's betweenness centrality index. This topological index identifies nodes that play a central role in the network and in this paper is modified by considering the weighted shortest path based on the CC(e) calculated from the vulnerability assessment. The algorithm is based on the fact that the attack entry points will be internet connected nodes while the targets will be the relay nodes, according to Algorithm 1. Hence the CPH_{bc} ranks components according to criticality to system functionality assuming adversary access, and evaluation of ranked components is determined by the reduction in risk (i.e., the number of vulnerable paths exploitable by adversary) when the component is fully protected.

V. Study Results and Discussions

The proposed cyber-physical-human risk assessment is implemented on an 8-substation test case [29] with nodes such as

TABLE III
UNIQUE VULNERABILITIES IN THE TEST CASE

Denial Of Service	Obtain Information	Bypass a Restriction	Execute Code Directory	Cross-site Request Forgery	(Hard-coded) Credentials	Execute Code Overflow	Directory Traversal	Cross Site Scripting	Execute Code Sql Injection	Permission, Priviledge, Access control
CVE-2015-7845	CVE-2015-2897	CVE-2015-5352	CVE-2012-4716	CVE-2015-5999	CVE-2015-6476	CVE-2015-7674	CVE-2012-4716	CVE-2014-1902	CVE-2015-2866	CVE-2015-6563
CVE-2015-7752	CVE-2015-4216	CVE-2015-4216		CVE-2015-4108	CVE-2015-2907	CVE-2015-7673	CVE-2015-7603	CVE-2014-0337		CVE-2015-1330
CVE-2015-7760	CVE-2014-5406	CVE-2015-1126			CVE-2015-2906	CVE-2015-7768	CVE-2015-7601			CVE-2015-3459
CVE-2015-5600	CVE-2014-8329	CVE-2014-8006			CVE-2015-4196	CVE-2015-7767	CVE-2015-0984			CVE-2014-3019
CVE-2015-4236		CVE-2014-2350			CVE-2015-4217	CVE-2015-6750	CVE-2015-3939			CVE-2014-2321
CVE-2015-4195					CVE-2015-6316	CVE-2015-4022				CVE-2015-6333
CVE-2015-6300					CVE-2015-3968	CVE-2015-0014				
CVE-2015-7674					CVE-2013-7404					
CVE-2015-7673					CVE-2003-1603					
CVE-2015-7767					CVE-2001-1594					
CVE-2015-4051					CVE-2015-0924					
CVE-2015-0776					CVE-2014-0329					
CVE-2015-0775										
CVE-2014-3362										

Algorithm 1 Applying Betweenness Centrality

```
Select IP of targeted relays, Physical_vertices
Select IP of Internet vertices, Cyber_vertices
function $node\_importance$(vertices)
        ▷ vertices: Generated Attack graph unique vertices
    for relay in $Physical\_vertices$ do
        for host in $Cyber\_vertices$ do
            weighted shortest paths
        ▷ Get list of shortest paths $SPL$ unless host=relay
                                   ▷ Pass exception if no path
            for short_path $S$ in $SPL$ do
                for $node$ in $vertices$ do
                    if vertex in short_path then
                        $unique\_node\_importance$ += 1
                    end if
                end for
            end for
        end for
    end for
return $node\_importance$, $\sigma_{st}(v)$, (for the ranking index)
end function
```

hosts, routers, remote terminal units, and relays. Vulnerability scan on the test case detects 55 unique vulnerabilities as detailed in Table III, as shown in Fig. 2, approximately 48 of these vulnerabilities require no authentication, and as shown in Fig 3, approximately 18-20 of the unique vulnerability types partially or completely threaten the availability.

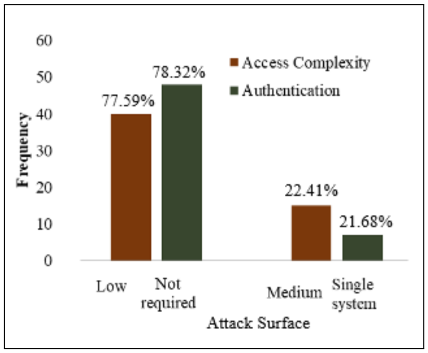

Fig. 2. Access complexity and authentication requirements of the test case.

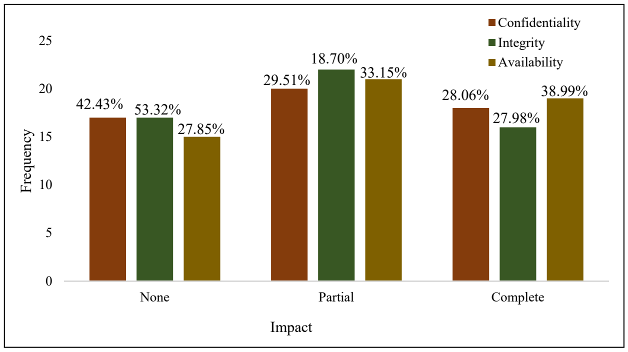

Fig. 3. Confidentiality, integrity and availability impact in the test case.

These vulnerabilities are combinatorially distributed among the system nodes giving rise to approximately 78000 potentially exploitable paths (edges). These exploitable paths are used to evaluate the CPH_{bc} ranking. The idea being that highly ranked nodes will reduce the number of exploitable attack paths more than lower ranked nodes when protected. To prevent bias in ranking, we assume the experience of human operators and physical locational security is the same for all nodes, however, in an actual system risk assessment, these parameters will vary by node. The time complexity of the CPH_{bc} algorithm is 7.7 secs. The ranking results are as presented in Table IV and detailed in Table V, the host PC with node ID 1896 ranked most critical. When completely protected, this node has the highest potential of reducing adversary exploitable paths, by 12.96%. A key component for the system analyst is to visualize how the system Confidentiality, Integrity and Availability change with system dynamics e.g.,

TABLE IV
COMPONENT RANKING: 8 SUBSTATION TEST CASE

Protecting any member of the first group by CPH$_{bc}$		
Protected vertex ID	Final No of Attack paths	% Decrease attack paths
1896	68398	12.960
[2018, 2020, 2004, 2006]	70469	10.324
[2014, 2016, 1998, 2000, 2002, 2008, 1996]	70860	9.827
2012	71256	9.323
1930	75097	4.435
[1920, 1922, 1924, 1926, 1928]	75063	4.478
2024	74991	4.570
[1938, 1940, 1942, 1934, 1936, 1932]	75267	4.219
2022	76080	3.184
[2010, 1894, 1875, 1892, 1877, 1870, 1871, 1916, 1910, ...]	78582	0.000

TABLE V
SECURITY GROUPS OF RANKED COMPONENTS

Rank	CPH$_{bc}$	Vertex ID	Component Type
1	0.0652	1896	Host PC
2	0.0583	[2018,2020,2004,2006]	[Overcurrent relay x2, Distance relay x2]
3	0.0528	[2014,2016,1998,2000,2002,2008,1996]	[Overcurrent relay x2, Distance relay x4, Host PC]
4	0.0476	2012	Overcurrent relay
5	0.0304	1930	Overcurrent relay
6	0.0282	[1920,1922,1924,1926,1928]	[Overcurrent relay x5]
7	0.0175	2024	Distance relay
8	0.0105	[1938,1940,1942,1934,1936,1932]	[Overcurrent relay x3, Distance relay x2, Host PC]
9	0.0067	2022	Host PC
10	0.0061	[2010,1877]	[Distance relay, Router/Switch]
11	0.0015	[1916,1918,1910,1912,1914,1870]	[Overcurrent relay x2, Distance relay x3, Router/Switch]
12	0.0013	1871	[Router/Switch]
13	0.0007	1878	[Router/Switch]
14	0.0005	1894	Host PC
15	0.0003	[1898,1900,1902,2030]	[Host PC x3, Router/Switch]

developing hot-fixes to patch vulnerabilities, assigning different operators to system nodes. The most critical node with ID 1896, when completely protected, generally reduces the attack surface and CIA impact more than lower ranked nodes. A higher percentage of impact and attack surface remain when lower ranked nodes are protected compared to higher ranked nodes. For instance, when node rank 1 node (ID: 1896) is protected, the vulnerabilities that leverage single system authentication are reduced to 19.91% and opposed to 20.27% and 20.54% of the rank 2 and rank 3 nodes, respectively. Same can be seen for CIA impact where the rank 1 node reduces the vulnerabilities that affect Availability to (26.08%, 30.67%, and 36.51%), more than a rank 2 node which will reduce these vulnerabilities to (26.44%, 31.17%, and 37.02%). The risk reduction attainable from ranked components keeps diminishing towards the least ranked nodes, and from Rank 10 nodes there is no substantial effect on risk reduction when the node is protected. Finally, the CPH_{bc} framework can guide analyst's actions to optimally route system resources while maintaining industry standards as follows.

ACKNOWLEDGMENTS

The authors would like to acknowledge the US Department of Energy under award numbers DE-CR0000018 and the National Science Foundation under award number 2220347.

VI. CONCLUSION

This paper presents a cyber-physical-human risk assessment framework for CPS based on the standard CVSS and identifying critical components, with a cyber-physical-human betweenness centrality metric introduced that can provide risk information to support about critical system defense. Finally, the framework provides a basis to optimize actions toward mitigating adversarial intrusions.

REFERENCES

[1] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security & Privacy*, vol. 4, no. 6, pp. 85–89, 2006.

[2] O. Analytica, "Kaseya ransomware attack underlines supply chain risks," *Emerald Expert Briefings*, no. oxan-es.

[3] "Darktracer: Darkweb criminal intelligence," [Online]. Available from: https://twitter.com/darktracer_int.

[4] B. Fung and G. Sands, "Ransomware attackers used compromised password to access colonial pipeline network," 2021. [Online]. Available: https://www.cnn.com/2021/06/04/politics/colonial-pipeline-ransomware-attack-password

[5] [Online]. Available: https://truesec.com/threat-intelligence-report-2021/

[6] R. Gabrys, A. Venkatesh, D. Silva, M. Bilinski, M. Major, J. Mauger, D. Muhleman, and K. Ferguson-Walter, "Emotional state classification and related behaviors among cyber attackers," 2023.

[7] S. M. Amin, "Electricity infrastructure security: Toward reliable, resilient and secure cyber-physical power and energy systems," in *IEEE PES General Meeting*. IEEE, 2010, pp. 1–5.

[8] U. J. Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal, and A. Kumar, "Ransomware threat and its impact on scada," in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*. IEEE, 2019, pp. 205–212.

[9] "National vulnerability database." [Online]. Available: https://nvd.nist.gov/

[10] [Online]. Available: https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx

[11] [Online]. Available: https://isc.sans.edu/

[12] [Online]. Available: https://www.exploit-db.com/

[13] A. Sahu, Z. Mao, P. Wlazlo, H. Huang, K. Davis, A. Goulart, and S. Zonouz, "Multi-source multi-domain data fusion for cyberattack detection in power systems," *IEEE Access*, vol. 9, pp. 119 118–119 138, 2021.

[14] N. Anjum, Z. Latif, C. Lee, I. A. Shoukat, and U. Iqbal, "Mind: A multi-source data fusion scheme for intrusion detection in networks," *Sensors*, vol. 21, no. 14, p. 4941, 2021.

[15] A. Sahu, Z. Mao, P. Wlazlo, H. Huang, K. Davis, A. Goulart, and S. Zonouz, "Multi-source data fusion for cyberattack detection in power systems," *arXiv preprint arXiv:2101.06897*, 2021.

[16] A. Umunnakwe, A. Sahu, M. R. Narimani, K. Davis, and S. Zonouz, "Cyber-physical component ranking for risk sensitivity analysis using betweenness centrality," *IET Cyber-Physical Systems: Theory & Applications*, 2021.

[17] S. Bi and Y. J. A. Zhang, "Graph-based cyber security analysis of state estimation in smart power grid," *IEEE Communications Magazine*, vol. 55, no. 4, pp. 176–183, 2017.

[18] A. Umunnakwe, A. Sahu, and D. Katherine, "Multi-component risk assessment usingcyber-physical betweenness centrality," *IEEE PowerTech Madrid 2021*, in press.

[19] 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, 2013.

[20] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Transactions on smart grid*, vol. 6, no. 5, pp. 2464–2475, 2015.

[21] K. Davis, R. Berthier, S. Zonouz, G. Weaver, R. Bobba, E. Rogers, P. Sauer, and D. Nicol, "Cyber-physical security assessment (cypsa) for electric power systems," *IEEE-HKN: THE BRIDGE*, 2016.

[22] B. Liu, Z. Li, X. Chen, Y. Huang, and X. Liu, "Recognition and vulnerability analysis of key nodes in power grid based on complex network centrality," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 3, pp. 346–350, 2017.

[23] M. R. Narimani, H. Huang, A. Umunnakwe, Z. Mao, A. Sahu, S. Zonouz, and K. Davis, "Generalized contingency analysis based on graph theory and line outage distribution factor," *arXiv preprint arXiv:2007.07009*, 2020.

[24] P.-Y. Chen, S. Choudhury, and A. O. Hero, "Multi-centrality graph spectral decompositions and their application to cyber intrusion detection," in *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2016, pp. 4553–4557.

[25] W. Schwab and M. Poujol, "The state of industrial cybersecurity 2018," *Trend Study Kaspersky Reports*, vol. 33, 2018.

[26] "Common vulnerability scoring system v3.0: Specification document."

[27] A. Sahu, K. Davis, H. Huang, A. Umunnakwe, S. Zonouz, and A. Goulart, "Design of next-generation cyber-physical energy management systems: Monitoring to mitigation," *IEEE Open Access Journal of Power and Energy*, vol. 10, pp. 151–163, 2023.

[28] MetaCompliance, "The Ultimate Guide to Phishing," https://www.metacompliance.com/lp/ultimate-guide-phishing/, 2021, [Online; accessed 27-October-2021].

[29] G. A. Weaver, K. Davis, C. M. Davis, E. J. Rogers, R. B. Bobba, S. Zonouz, R. Berthier, P. W. Sauer, and D. M. Nicol, "Cyber-physical models for power grid security analysis: 8-substation case," in *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2016, pp. 140–146.