Power System Equipment Cyber-Physical Risk Assessment Based on Architecture and Critical Clearing Time

Hao Huang, *Student Member, IEEE,* Katherine Davis, *Senior Member, IEEE*
Department of Electrical and Computer Engineering
Texas A&M University
College Station, TX, USA
Email: hao_huang@tamu.edu, katedavis@tamu.edu

***Abstract*—With the trend of constructing Internet protocol (IP)-based systems, modern power grids are involving into integrated networks made up of cyber and physical infrastructure with the goal of improving stability, reliability, and efficiency. Cyber technology is the backbone of modern power grid operation, yet vulnerabilities in the cyber network can introduce cyber-enabled disruption of physical components, which may lead catastrophic outcomes. Thus, cyber-physical equipment assessment is needed for modern power grids to better prepare against unexpected contingencies. In this paper, the digital relay is representative of cyber-physical equipment in power grids since it is a connector between the cyber network and the physical infrastructure. This paper presents two methods to evaluate cyber-physical risk of all digital relays in a power system. These methods are based on cyber-physical architecture and critical clearing time respectively. The analysis is conducted on an 8-substation model with its cyber network and cyber-physical architecture. The ranks of each digital relay provide useful information for situational awareness in modern power grids. An online framework that evaluates cyber-physical assets in power systems from these two perspectives is presented.**

I. Introduction

With increased integration of cyber technology, power systems are undergoing a transition toward automated cyber-physical systems. Recent innovations for hardware and software of cyber networks in power systems are emerging. On the hardware side, the upgraded power grids are equipped with intelligent electronic devices (IEDs) [1] which can support various communication protocols in both serial-based and IP-based system, to achieve supervisory control and data acquisition (SCADA), remote control, peer-to-peer communication, etc. [2]. On the software side, energy management systems (EMS), communication architectures, and cyber security algorithms have been applied to ensure the reliability, integrity and security of modern power grids [3].

As a critical infrastructure, modern power grids deserve attention more than before, not only due to their importance for daily and industrial life, but also because of increased potential vulnerabilities within the system in both physical and cyber domains. Several major blackouts happened in 2003, including the U.S-Canadian blackout, the Southern Sweden and Eastern Denmark blackout, and the Italian blackout [4]. All these major blackouts started from a small problem in the physical infrastructure; then, another failure in the EMS software or substation equipment left operators unaware of conditions in the system, leading to a wrong decision. Millions of lives have been affected, and great economic loss occurred in those incidents. In 2015, the Ukraine power grid cyber attack caught public attention [5]. A third party illegally hacked into the SCADA systems and disconnected seven substations, causing large area power outages for three hours. To avoid those incidents from happening again and to protect the power systems, security analysis and situational awareness studies for systems are necessary.

In this paper, digital relays are treated as a representative of cyber-physical equipment, and a new cyber-physical assessment method based on transient analysis is presented. What if a cyber attack falsifies the settings of digital relays? These latent incorrect settings may cause unsatisfactory dynamics in the system, leading to unstable transients and cascading failures. This kind of cyber attack can invoke hazards to power systems. Thus, both steady-state analysis and transient analysis are necessary for cyber-physical security assessment. Additionally, the Cyber-Physical Security Assessment (CyPSA) [6] is presented as a comparison to the new method. These two methods are tested on an 8-substation system [7].

The contributions of this paper are threefold. First, it proposes a method of evaluating the compromised cyber-physical assets' transient impact to power systems and tests the method on an 8-substation system. Then, by comparing the new method with CyPSA, it can be found that the outcome of steady state impact analysis due to cyber attack can be quite different from the transient analysis. Finally, it presents an online framework that can run these two cyber-physical security assessments simultaneously.

The rest of this paper is organized as follows. Background on modern power grid security is presented in Section II. Section III presents an 8-substation model with its cyber-physical architecture, which is the testbed for subsequent analyses. Section IV illustrates how to use CyPSA to prioritize the digital relays in the 8-substation system. In Section V, we consider the situation of falsifying relay settings to affect critical clearing time (CCT), which is defined as the longest fault duration allowable for system stability [8]. We evaluate the digital relays and specific circuit breakers in the 8-substation model based on transient analysis during the post-fault. In Section VI, the comparison and discussion of two kinds of rankings for digital relay is presented. An online framework that runs CyPSA and CCT based transient analysis to evaluate the cyber-physical assets in power systems is presented in Section VII. More discussion and future work is in Section VIII.

II. Background on Modern Power Grid Security Analysis

Modern power grids are cyber-physical systems (CPS) that integrate cyber networks with physical infrastructure. As stated in [9], there is a need for a more comprehensive set of activities

978-1-5386-7954-8/18/$31.00 ©2018 IEEE

for ensuring that critical infrastructure systems are prepared to operate in an uncertain multi-hazard environment. In modern power grids, hazards may involve contingencies in physical infrastructure and cyber attacks in the cyber network. A lot of work has been done in both areas.

Traditional power system analyses and studies, like contingency analysis [10], stability analysis [11], etc., consider the outcome of the loss of a transmission line or generator and explore the limits of the system to provide a guideline for improved construction and operation of power systems to ensure reliability and stability. The study of security-constrained optimal power flow (SCOPF) [12] and security-constrained economic dispatch (SCED) [13] highlight important contingency situations, for which the system should be able to maintain its stability and reliability. However, such analyses only focus on the physical infrastructure.

For cyber security, the traditional information technology (IT) security system is an important starting point. IT security includes the intrusion detection systems and encryption and authentication mechanisms that can protect the system from potential adversaries. However, it is undeniable that the cyber security systems for CPS require some differences from traditional IT security. One important distinction is that software patching and frequent updates are often not suitable for control systems in CPS due to real-time availability requirements [14]. Such system upgrades need to be scheduled carefully. Moreover, bad data injection is a potentially serious problem in power systems. In [15], it is shown that with enough information on system topology, to bypass state estimation and inject false data is possible.

To deal with cyber-oriented grid threats, vulnerability assessment of the cyber network is necessary. In [16], Ten et al. evaluate the vulnerability of SCADA systems from the perspective of system, scenario, and access point. To quantify the outcome, they study the potential loss of load if there is an intrusion. In [17], Hug et al. present a method to determine which measurements may be utilized by an attacker to keep the attack hidden from bad data detection in AC state estimation, which can provide guidance for operational personnel about which measurements deserve more attention and verification.

Situational awareness studies in power systems are also necessary and helpful for operational personnel in preparing for unexpected incidents. A real-time assessment tool for situational awareness enhancement in modern power systems has been introduced in [18], which utilize phasor unit measurements (PMUs) and decision trees to assess post-contingency issues. Panteli et al. review work on situational awareness in power systems, including its definition, outcomes of insufficient situational awareness, and methods to improve situational awareness in power systems [19]. Recommendations include increasing the accuracy of state estimation, improving graphical user interface (GUI) effectiveness, etc., but it also emphasizes the need for more efforts to optimize the performance of system operators.

For CPS, a vital element to protect is the cyber-physical equipment; in power systems, that connects the physical infrastructure and cyber network. Instead of analyzing power systems separately in physical and cyber domains, a security-oriented cyber-physical situational state estimation (SCPSE) for power systems was proposed in [20], which combines the information from cyber networks and physical infrastructure to detect false data and provide an improved estimation of cyber-physical state. S.Zonouz et al. present a unified formalism to model the cyber-physical system to assess the potential impact of cyber-physical contingency in [21]. Then, [22] presents an online framework for cyber-physical modeling and assessment to model the dependencies between the cyber and physical systems and to identify weak points in systems. The toolset, CyPSA, is presented in [6], which utilizes information about cyber-physical architecture to identify the most critical cyber assets and the attack path that induce the most severe physical impacts to systems.

III. Cyber-Physical Architecture of an 8-Substation System

An 8-substation system [7] is the testbed for cyber-physical equipment assessments in this paper. All the detailed information of the 8-substation system is presented in Fig. 1. Fig. 1a presents the power system model with expanded bus topology. Based on predefined substation topologies, PowerWorld Simulator [23] can convert the case into an expanded substation topology representation. Each red box in the figure represents a circuit breaker (CB). Unlike a traditional planning model, an expanded substation topology, also called a full-topology model [7], shows a detailed cyber-physical architecture of the power system, which is important for analyzing the effect of losing specific cyber-physical equipment. Fig. 1b presents the control network of the 8-substation system in Network Perception's NP-view software [24], which simplifies the task of visualizing and understanding the network connections by showing the firewall and network path. A detailed cyber network with IP addresses of each cyber-physical equipment is demonstrated in Fig. 1c. Each IP address corresponds to a digital relay that controls CBs in Fig. 1a. The cyber-physical architecture is important for the following CyPSA and the CCT perturbation based transient analysis.

IV. CyPSA for the 8-Substation System

Since real-time availability is a requirement for modern power grids, reasonably allocating resources for patching vulnerabilities in power systems is significant. To meet such requirements, CyPSA [6] utilizes the information of cyber-physical architecture to identify the most critical cyber asset and the attack path that induces severe physical impact to the system. In this way, operational and protection teams can be better prepared for such contingencies.

A. Metrics of CyPSA

CyPSA provides a rank for cyber-physical equipment based on performance index (PI), cyber cost (CC) and security index (SI). PI is used to quantify the impact of the outages on the physical system. It measures the severity of the transmission line outages, due to an adversary following path *p(i)*, based on the subsequent line overloads.

$$PI(p(i)) = \sum_{l \in L} [\max\{\frac{f_s(l)}{f^{MAX}(l)} - 1, 0\}]^2 \tag{1}$$

Here, L is the set of all lines, $f_s(l)$ denotes flow on line l in state *s* induced by adversarial actions, and $f^{MAX}(l)$ denotes the maximum flow allowed on line *l*. CC utilizes the lowest cost vulnerability to reach a particular asset. Vulnerability scores $V(a)$ are obtained from the National Vulnerability Database (NVD) [25].

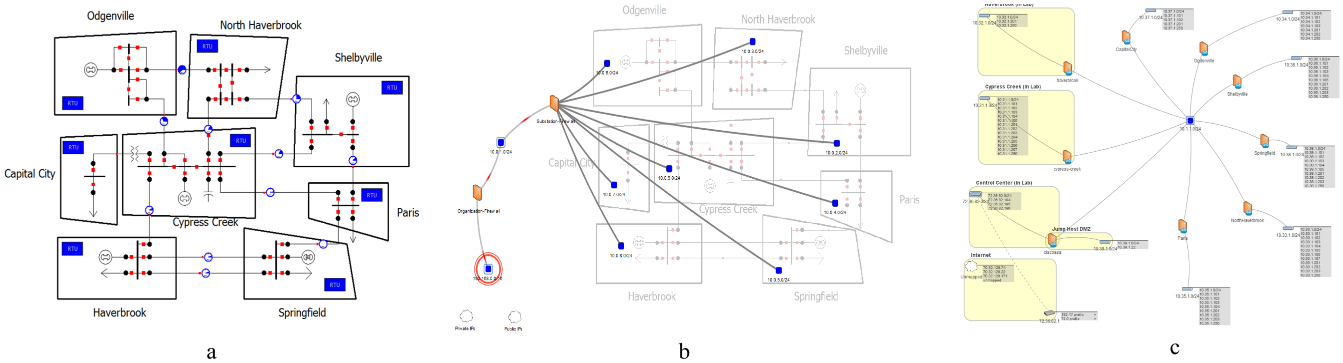


Fig. 1. 8-Substation System: a. Power System Model in Powerworld; b. Cyber-physical model in NP-View; c. Cyber topology with IP address [7]

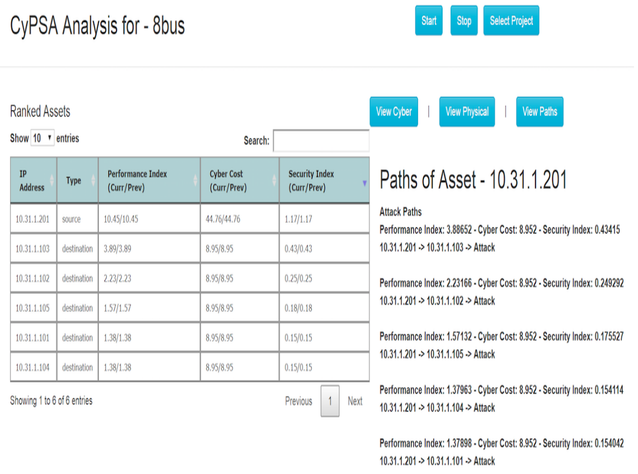
$$CC(p(i)) = \sum_{a \in p(i)} \min\{V(a)\} \tag{2}$$

With *PI* and *CC*, *SI* can be calculated by the inverse cost *CC* multiplying the attack impact *PI* as equation (3).

$$SI(p(i)) = \frac{PI(p(i))}{CC(p(i))} \tag{3}$$

In this way, CyPSA identifies the most critical cyber asset and attack path for operation panel by prioritizing low cost, high-impact attacks.

B. Rank of Relays Based on CyPSA



CyPSA Analysis for - 8bus

Ranked Assets

Show 10 entries Search:

IP Address	Type	Performance Index (Curr/Prev)	Cyber Cost (Curr/Prev)	Security Index (Curr/Prev)
10.31.1.201	source	10.45/10.45	44.76/44.76	1.17/1.17
10.31.1.103	destination	3.89/3.89	8.95/8.95	0.43/0.43
10.31.1.102	destination	2.23/2.23	8.95/8.95	0.25/0.25
10.31.1.105	destination	1.57/1.57	8.95/8.95	0.18/0.18
10.31.1.101	destination	1.38/1.38	8.95/8.95	0.15/0.15
10.31.1.104	destination	1.38/1.38	8.95/8.95	0.15/0.15

Showing 1 to 6 of 6 entries Previous 1 Next

Paths of Asset - 10.31.1.201

Attack Paths

Performance Index: 3.88652 - Cyber Cost: 8.952 - Security Index: 0.43415
10.31.1.201 -> 10.31.1.103 -> Attack

Performance Index: 2.23166 - Cyber Cost: 8.952 - Security Index: 0.249292
10.31.1.201 -> 10.31.1.102 -> Attack

Performance Index: 1.57132 - Cyber Cost: 8.952 - Security Index: 0.175527
10.31.1.201 -> 10.31.1.105 -> Attack

Performance Index: 1.37963 - Cyber Cost: 8.952 - Security Index: 0.154114
10.31.1.201 -> 10.31.1.104 -> Attack

Performance Index: 1.37898 - Cyber Cost: 8.952 - Security Index: 0.154042
10.31.1.201 -> 10.31.1.101 -> Attack

Fig. 2. CyPSA Analysis for Node 10.31.1.201

Fig. 2 shows the result of CyPSA for the 8-substation system. With the compromised node, whose IP address is 10.31.1.201, CyPSA provides a detailed cyber-physical analysis with the calculation of *PI*, *CC*, and *SI*. The results also rank all possible attack paths from the source node to the destination node. The first row of CyPSA shows the *PI* and *CC* that the compromised node 10.31.1.201 induces to the system. And the most critical cyber asset in this scenario is the node 10.31.1.103 with the highest SI. Though the *CC* of all attack paths are the same, the *PI* of the node 10.31.1.103 is the highest, which means the loss of this node brings the most severe hazard to the system among all nodes. Moreover, CyPSA stores the current status of analysis. If any change of physical system or cyber network property happens, CyPSA can update the current analysis, and the previous results can be stored for reference. In this way, a real-time analysis based on CyPSA can provide more insights to operation and protection to prepare for unforeseen contingencies.

V. Critical Clearing Time Based Transient Analysis of the 8-Substation System

When there is a fault in a power system, the protective relays have to clear it before the critical clearing time (CCT) to avoid a cascading event in the system to ensure stability. Therefore, intuitive questions arise. What if the relay is compromised by certain cyber attacks and clears the fault after the CCT requirement? What if the communication from relay to CB is delayed by certain attack? What if the CCT is wrong? With these considerations, this paper presents a rank of digital relay based on the transient analysis considering the situation that the CCT settings of the relay is falsified making the fault cleared after CCT.

A. Methods of Determining CCT

CCT is a complex function of pre-fault system conditions and post-fault system conditions. As a significant parameter of power systems transient stability, there are several ways to determine the CCT, including numerical integration [26], Lyapunov theory (direct method) [27], and artificial neural networks (ANN) [28].

PowerWorld Simulator [23] has implemented a critical clearing time calculator based on the method of bisection [29]. At the beginning, limits are defined for the fault. After that, system stability is checked at the mid-point of these limits. If the system is stable, then the lower stability limit of the interval is replaced by the mid-point value. Otherwise, the upper value is replaced by the mid-point value. This procedure is repeated until reaching the required precision. The simulated system stability depends on power system topology and generator models in the system. In this paper, the generator model is set as $GENOUR$. The required precision is set by the WECC reliability criterion [30].

B. Transient Analysis Based on Falsified CCT

To analyze the transient impact of a digital relay if it is compromised, this paper considers a scenario that a certain cyber attack compromises the digital relay by injecting a small perturbation to relay's pickup time settings, making the system clear the fault after the CCT requirement. Since the falsification of pickup time setting is hard to recognize and the consequence could be catastrophic, the assessment of digital relay from this perspective provides helpful situational awareness for operational panel to prepare against the potential hazards within the system. To quantify the transient impact, this paper introduces the transient impact index (TII) in equation (4)

$$TII(r(i)) = \min\{(f_{max-c} - f_{max-o}), 5\} \qquad (4)$$

Here $r(i)$ represents the digital relay in the system, which could be represented by the relay ID or the CB number controlled by the relay. f_{max-c} is the maximum frequency in the system if the digital relay is compromised. The f_{max-o} is the maximum frequency in the system when the digital relay clear fault on CCT. The difference between these two frequencies provides a good indicator of system stability in the transient realm. From test results, once the difference is bigger than 5Hz, there will be a cascading event making the system completely unstable from the transient perspective and the TII is assigned a value of 5.

C. Rank of Relay Based on Transient Analysis

For the 8-substation system, with the expanded topology, there is communication network with relays, and CBs on transmission line and substations. One relay can control more than one CB in the system. Thus, to present the result in a clear format, the rank of digital relay is classified into two categories, transmission level and substation level. For transmission level, the rank uses the transmission line number, which means the attack happens in the transmission line relay and related CBs. For substation level, a more specific attack on CB is considered, so the rank uses the CB number and relay IP address. Moreover, to have a comprehensive assessment of the cyber-physical equipment in the system, there are two perturbations added into CCT, 0.05 seconds and 0.1 seconds respectively, which are labeled as CCT_1 and CCT_2 in the final result. The footnote pattern is the same for f_{max-c} and TII.

TABLE I and TABLE II present the rank for all digital relay for transmission lines based on the perturbation of 0.05 seconds and 0.1 seconds respectively. TABLE III and TABLE IV show the rank of digital relay and corresponding CB for substation Cypress Creek with the perturbation of 0.05 seconds and 0.1 seconds respectively. From test results, it can be found that, some relay with longer CCT is more sensitive to the perturbation than the relay with shorter CCT, which means the perturbation on CCT affects the transient stability regardless of CCT values.

In TABLE I and TABLE II, the rank for transmission line is the same under two perturbations to CCT. With the increase of the perturbation on CCT, the TII is also increasing. In this way, some transmission line that is more important for the system's stability can be easily found and more attention needs to be paid to those lines. The same pattern also works for the CB rank in TABLE III and TABLE IV. In this scenario, the relay and the CB that need more attention is easily spotted, since the rank is based on the relay IP and CB number.

Transmission line	CCT	CCT_1	f_{max-c1}	f_{max-o}	TII_1
37-39	0.094271	0.144271	61.7494	67.2551	5
38-40	0.094271	0.144271	61.7761	67.2277	5
42-51	0.138542	0.188542	61.8702	67.1567	5
18-36	0.085417	0.135417	61.5257	62.728	1.2023
11-21	0.085417	0.135417	61.5078	62.6836	1.1758
24-48	0.085417	0.135417	61.5281	62.6939	1.1658
22-28	0.076563	0.126563	61.3391	62.4308	1.0917
32-49	0.085417	0.135417	61.0911	61.7688	0.6777
14-26	0.138542	0.188542	61.7029	62.3434	0.6405
3-7	0.15625	0.20625	61.8452	62.4766	0.6314
6-7	0.15625	0.20625	61.8069	62.4019	0.595

TABLE I. TRANSMISSION RELAY ASSESSMENT WITH THE CCT PERTURBATION OF 0.05S

Transmission line	CCT	CCT_2	f_{max-c2}	f_{max-o}	TII_2
37-39	0.094271	0.194271	61.7494	71.6191	5
38-40	0.094271	0.194271	61.7761	70.8092	5
42-51	0.138542	0.238542	61.8702	111.5619	5
18-36	0.085417	0.185417	61.5078	73.8985	5
11-21	0.085417	0.185417	61.5281	83.701	5
24-48	0.085417	0.185417	61.5257	109.4446	5
22-28	0.076563	0.176563	61.3391	64.9319	3.5928
32-49	0.085417	0.185417	61.0911	62.5359	1.4448
14-26	0.138542	0.238542	61.7029	63.1098	1.4069
3-7	0.15625	0.25625	61.8452	63.2212	1.376
6-7	0.15625	0.25625	61.8069	63.1409	1.334

TABLE II. TRANSMISSION RELAY ASSESSMENT WITH THE CCT PERTURBATION OF 0.1S

CB Number	Relay IP	CCT	CCT_1	f_{max-c1}	f_{max-o}	TII_1
23-25	10.31.1.104	0.08542	0.13542	61.5393	62.7301	1.1908
15-18	10.31.1.102	0.08542	0.13542	61.4919	62.6806	1.1887
21-25	10.31.1.105	0.08542	0.13542	61.4969	62.6621	1.1652
24-25	10.31.1.101	0.08542	0.13542	61.5135	62.6641	1.1506
15-19	10.31.1.102	0.08542	0.13542	61.4915	62.6377	1.1462
15-17	10.31.1.102	0.08542	0.13542	61.4912	62.6369	1.1457
17-19	10.31.1.103	0.08542	0.13542	61.4912	62.6369	1.1457
19-25	10.31.1.103	0.07656	0.12656	61.3492	62.4646	1.1154
22-25	10.31.1.105	0.07656	0.12656	61.321	62.3956	1.0746

TABLE III. CIRCUIT BREAKER AND RELAY ASSESSMENT IN CYPRESS CREEK WITH THE CCT PERTURBATION OF 0.05S

CB Number	Relay IP	CCT	CCT_2	f_{max-c2}	f_{max-o}	TII_2
23-25	10.31.1.104	0.08542	0.18542	61.5393	62.7301	5
15-18	10.31.1.102	0.08542	0.18542	61.4919	62.6806	5
21-25	10.31.1.105	0.08542	0.18542	61.4969	62.6621	5
24-25	10.31.1.101	0.08542	0.18542	61.5135	62.6641	5
15-19	10.31.1.102	0.08542	0.18542	61.4915	62.6377	5
15-17	10.31.1.102	0.08542	0.18542	61.4912	62.6369	5
17-19	10.31.1.103	0.08542	0.18542	61.4912	62.6369	5
19-25	10.31.1.103	0.07656	0.17656	61.3492	62.4646	4.2183
22-25	10.31.1.105	0.07656	0.17656	61.321	62.3956	3.5149

TABLE IV. CIRCUIT BREAKER AND RELAY ASSESSMENT IN CYPRESS CREEK WITH THE CCT PERTURBATION OF 0.1S

Generally speaking, the CCT perturbation based transient analysis provides a more detailed evaluation of specific cyber-physical assets in power systems. The relay and CB are both ranked in this transient analysis, which can guide maintenance and protection personnel to check the functionality of those devices according to their priority to the whole system?s security. Additionally, the highest TII is not the relay and CB that have the shortest CCT, which shows the necessity to use perturbation to analyze transient stability of the system.

VI. DISCUSSIONS OF TWO CYBER-PHYSICAL ASSESSMENT METHODS

CyPSA is an online tool that considers the complexity of cyber attacks and the outcome of cyber attacks on different cyber assets to provide situational awareness for operations. Besides, with the change of power system networks, cyber networks or the compromised nodes, the rank is also updated. These features make CyPSA a reliable prototype for cyber-physical assessment in power systems.

The transient analysis based on perturbation on CCT is focused on the outcome from a cyber attack on a specific relay and its circuit breaker. The unexpected action of protection systems can induce more hazards to power systems. From test results, there are two important findings. First, the digital relay and CB have the shortest CCT is not the most sensitive to the perturbation. Thus, it is necessary to utilize this kind of perturbation method to determine the most important cyber-physical equipment in the system to ensure its transient security. Secondly, the kind of transient analysis in this paper can provide a reference for protection systems construction. Not only does the relay need to be carefully set up and secured from both cyber network and physical infrastructure, some CBs and the communication from relay to CB also needs better care. Therefore, the TII is an importance index for cyber-physical equipment in power systems, which indicates system stability if it is compromised.

By comparing the rank in Fig. 2 with TABLE III, it can be discovered that the rank from CyPSA and the rank of TII are quite different. There are several reasons. First, CyPSA considers both the outcome in the power systems and the attack complexity, but TII only considers the outcome from the power system transient stability. Second, TII considers the cyber asset with specific relay and its CB, but CyPSA considers the most sever situation that happens in the system if one cyber asset is compromised. Third, TII assigns the same value to all unstable situations, which may ignore each unstable situation's severity, but CyPSA calculates the specific PI and CC for each relay to indicate the severity. However, the CC for all nodes in CyPSA is the same in the test scenario. The difference of two ranks thus only reflects the outcome of the cyber attack on the power system. TII discovers specific physical nodes in power systems that greatly affect stability to systems, which is not considered in CyPSA.

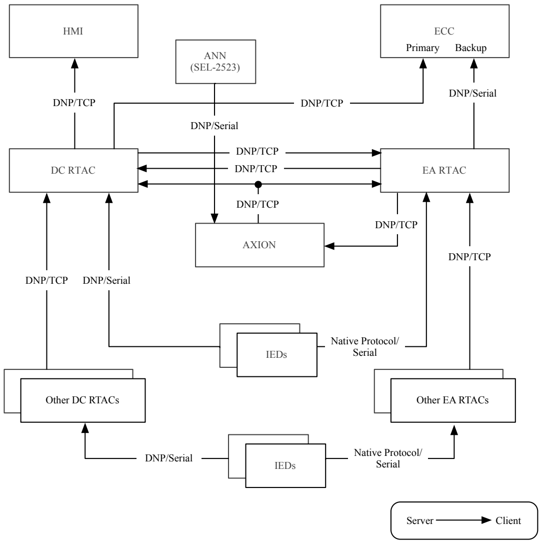


Fig. 3. Typical Substation Automation System Topology [31]

VII. The Online Framework of Running CyPSA and Calculating TII

An automated cyber-physical architecture extraction and management system (AEMS) is presented in [31]. The goal of AEMS is to feed the cyber-physical model from field IEDs to various power system analyses. In order to calculate the TII, AEMS should also collect the relay model and settings. In this way, the transient stability models of relays and the cyber-physical architecture of power systems can both be extracted. Sending such information to PowerWorld Simulator, the TII for each relay and CB can be calculated.

Fig. 3 presents a typical substation automation system (SAS) topology, where the real-time automation controller (RTAC) from Schweitzer Engineering Laboratories (SEL) plays an important role. The data concentrator RTAC (DC RTAC) collects various data from IEDs in the field, which can be utilized in AEMS to extract the cyber-physical architecture, power topology, cyber topology, etc. Besides, RTAC supports Flex Parse protocol, which can be used for polling the relay setting from field digital relays [32]. This feature can help feed PowerWorld Simulator the relay model information, such that the transient stability model and cyber-linked model of relay can be constructed.

The online framework of performing CyPSA and calculating TII is presented in Fig. 4. Using this framework, CyPSA and TII analysis can be automatically applied to any power system networks. With the DC RTAC in the SAS, the cyber-physical architecture, relay settings, and topology information of the power system can be extracted by an AEMS. The AEMS can manage such information to applications including PowerWorld Simulator and construct the cyber-physical architecture with the transient stability model. To calculate TII, two transient contingency analyses for interested relay and CB are required. One is the normal contingency. The other one is injected perturbation on clearing time. With equation (4), the TII can be calculated. Moreover, the cyber-physical architecture information and topology information can also be utilized by CyPSA, as presented in [6] and [32].

VIII. Conclusion and Future Work

This paper presents two methods of assessing cyber-physical equipment in modern power grids to provide situational awareness for operation and protection personnel to enhance grid security. CyPSA utilizes the information of cyber-physical architecture to identify the most critical cyber asset and the attack path. The transient analysis calculates TII for each relay with specific CB under perturbation to CCT, which can be used for finding the most critical cyber host and its physical client. Test on the 8-substation system demonstrates the rank of each digital relay based on CyPSA and TII respectively. Finally, this paper presents a general framework to accomplish online calculation for both methos.

The rank from CyPSA and TII are not exactly the same, because they analyze cyber assets from different perspectives. To utilize these two analyses thoroughly, it is recommended to use the CyPSA in the energy management center since it uses information related to transmission line outages, which is important for operation of transmission networks. The TII analysis emphasizes dynamic impact of cyber assets and their physical hosts. Thus, the rank of TII can provide better situational awareness of power system equipment in substations.

Future work will test both methods via the proposed online framework in more complex systems via a range of threat scenarios. Finally, choosing a good perturbation on CCT and classifying the similar TII into the same rank can make this kind of analysis more practical and easier to implement.

Acknowledgment

The authors would like to thank the National Science Foundation (NSF) under Award Numbers CNS 1446229 for

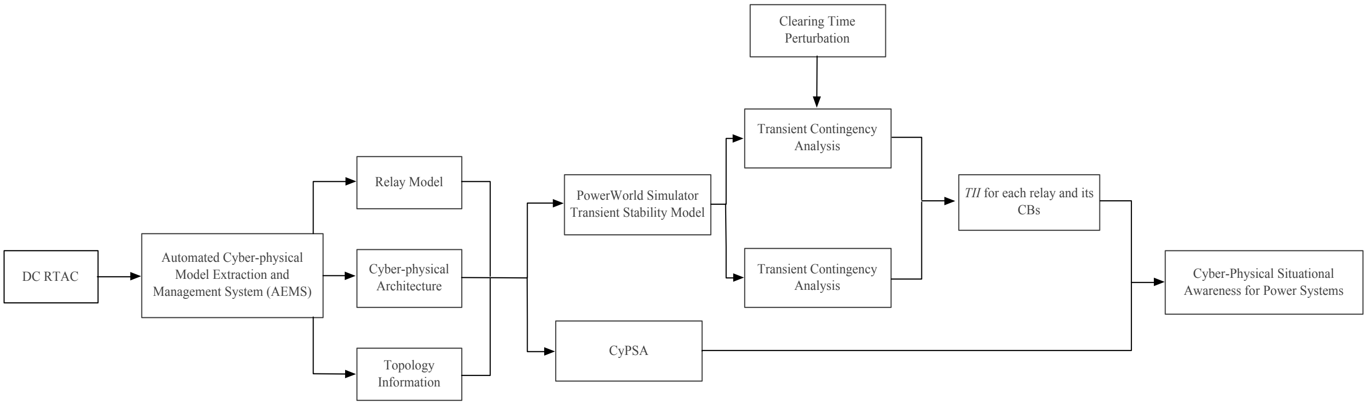

Clearing Time Perturbation
DC RTAC
Automated Cyber-physical Model Extraction and Management System (AEMS)
Relay Model
Cyber-physical Architecture
Topology Information
PowerWorld Simulator Transient Stability Model
CyPSA
Transient Contingency Analysis
Transient Contingency Analysis
TII for each relay and its CBs
Cyber-Physical Situational Awareness for Power Systems

Fig. 4. Automated Cyber-Physical Architecture Extraction and Management System (AEMS) for CyPSA and Transient Impact Analysis

the support and sponsorship of this research.

References

[1] J. D. McDonald, “Substation automation. ied integration and availability of information,” *IEEE Power and Energy magazine*, vol. 99, no. 2, pp. 22–31, 2003.

[2] S. A. Boyer, *SCADA supervisory control and data acquisition*. The Instrumentation, Systems and Automation Society, 2018.

[3] W. Wang and Z. Lu, “Cyber security in the smart grid: Survey and challenges,” *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[4] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca *et al.*, “Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance,” *IEEE transactions on Power Systems*, vol. 20, no. 4, pp. 1922–1928, 2005.

[5] D. U. Case, “Analysis of the cyber attack on the ukrainian power grid,” 2016.

[6] 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.

[7] 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 *Smart Grid Communications (SmartGridComm), 2016 IEEE International Conference on*. IEEE, 2016, pp. 140–146.

[8] J. D. Glover, M. S. Sarma, and T. Overbye, *Power system analysis and design*. China Machine Press, 2004.

[9] E. D. Vugrin, “Critical infrastructure resilience,” *An edited collection of authored pieces comparing, contrasting, and integrating risk and resilience with an emphasis on ways to measure resilience*, p. 236, 2016.

[10] F. Galiana, “Bound estimates of the severity of line outages in power system contingency analysis and ranking,” *IEEE Transactions on Power Apparatus and Systems*, no. 9, pp. 2612–2624, 1984.

[11] M. Pai, *Energy function analysis for power system stability*. Springer Science & Business Media, 2012.

[12] O. Alsac and B. Stott, “Optimal load flow with steady-state security,” *IEEE transactions on power apparatus and systems*, no. 3, pp. 745–751, 1974.

[13] J. Zhu, “Security-constrained economic dispatch,” *Optimization of Power System Operation*, pp. 141–210, 2009.

[14] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry *et al.*, “Challenges for securing cyber physical systems,” in *Workshop on future directions in cyber-physical systems security*, vol. 5, 2009.

[15] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[16] C.-W. Ten, C.-C. Liu, and G. Manimaran, “Vulnerability assessment of cybersecurity for scada systems,” *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836–1846, 2008.

[17] G. Hug and J. A. Giampapa, “Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks,” *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[18] R. Diao, V. Vittal, and N. Logic, “Design of a real-time security assessment tool for situational awareness enhancement in modern power systems,” *IEEE Transactions on Power systems*, vol. 25, no. 2, pp. 957–965, 2010.

[19] M. Panteli and D. S. Kirschen, “Situation awareness in power systems: Theory, challenges and applications,” *Electric Power Systems Research*, vol. 122, pp. 140–151, 2015.

[20] S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, and T. J. Overbye, “Scpse: Security-oriented cyber-physical state estimation for power grid critical infrastructures,” *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1790–1799, 2012.

[21] 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.

[22] 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.

[23] P. Simulator, “Powerworld corporation,” 2005.

[24] Network perception.inc. [Online]. Available: http://www.network-perception.com/

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

[26] G. W. Stagg and A. H. El-Abiad, *Computer methods in power system analysis*. McGraw-Hill, 1968.

[27] P. Varaiya, F. F. Wu, and R.-L. Chen, “Direct methods for transient stability analysis of power systems: Recent results,” *Proceedings of the IEEE*, vol. 73, no. 12, pp. 1703–1715, 1985.

[28] D. J. Sobajic and Y.-H. Pao, “Artificial neural-net based dynamic security assessment for electric power systems,” *IEEE Transactions on Power Systems*, vol. 4, no. 1, pp. 220–228, 1989.

[29] S. Aboreshaid, R. Billinton, and M. Fotuhi-Firuzabad, “Probabilistic transient stability studies using the method of bisection [power systems],” *IEEE Transactions on Power Systems*, vol. 11, no. 4, pp. 1990–1995, 1996.

[30] W. E. C. Council, “Wecc reliability criteria,” 2004.

[31] H. Huang and K. Davis, “Extracting substation cyber-physical architecture through intelligent electronic devices’ data,” in *Texas Power and Energy Conference (TPEC), 2018 IEEE*. IEEE, 2018, pp. 1–6.

[32] *SEL-3530 Real-Time Automation Controller (RTAC) Instruction Manual*, Schweitzer Engineering Laboratories, Inc., 05 2017.