Extracting Substation Cyber-physical Architecture Through Intelligent Electronic Devices' Data

Hao Huang, *Student Member, IEEE,* Katherine Davis, *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*—Intelligent electronic devices (IEDs) are widely used in power systems and result in diverse heterogeneous cyber-physical architectures. A scalable and fast way of accessing these IEDs and automatically extracting substation cyber-physical architecture for power systems from the data would benefit engineering design, power system analysis, security analysis, and cyber-physical security analysis. This paper presents a framework of automated cyber-physical architecture extraction and management. The proposed system will greatly reduce the time and human effort on extracting the cyber-physical architecture. This feature provides new capabilities for power system contingency analysis, cyber-physical security analysis, network connectivity examination, and improved intra- and inter-organizational event planning, preparation, and response capabilities.**

I. INTRODUCTION

As increasing numbers of IEDs are becoming deployed in substations, the architectures of power grids are becoming more digitalized and automated. Measurements from sensors in the field reach the control room through multiple layers of computers and communication systems. Control signals from a human machine interface (HMI) can command specific devices in the field via this cyber-physical system to act. Cyber-physical systems integrate computation with physical processes where behavior is defined by both computation and physical parts [1].

IEC 61850 [2] lays a foundation for substation automation systems (SAS), wide area network (WAN) applications, and Phasor Measurement Units (PMUs). IEC 61850 defines communication between IEDs in substations for the purpose of meeting specific requirements [3]. Mohammad et al in [4] simulate the power system substation communication architecture based on IEC 61850 and demonstrate acceptable performance for substation automation. Substation architectures are designed to benefit power system protection and control, while contingency analysis helps prioritize power system operation and control.

There is a need for a more comprehensive set of activities for ensuring that critical infrastructure systems are prepared to operate in an uncertain multi-hazard environment [5]. Traditional N-1 contingency analysis typically focuses on the loss of single elements such as generation, transmission lines, and transformers to provide guidance for operating the power system. The controls of the system are optimized in the pre-contingency state with a security-oriented optimal power flow (SCOPF) [6] or security constrained economic dispatch (SCED) [7] so that when one of these "credible" contingencies happens, the system should be able maintain its stability and reliability [8]. With increasing substation automation and more intelligent and connected IEDs, traditional contingency analysis is not enough. To increase the resiliency of power infrastructure, contingency analysis should also consider the IEDs in the system. Unlike the traditional contingency analysis for the loss of transmission line or outage of transformer, contingency analysis of IEDs should include both cyber-attack and physical loss, which could provide a better situational awareness for the power system.

Directing the industry's attention to cyber security and cyber-physical security in these architectures is timely and prudent. While cyber-attacks in power system can be mitigated in different ways, including conventional state estimation, with increasing knowledge and examples of intelligent cyber-attacks, one must be prepared for attacks that can bypass bad data detection in the state estimator, which has been demonstrated in [9]. A method of creating unobservable attacks in AC power flow equations is also introduced in [10]. With more sophisticated methods, cyber-attack can bring adversary effect to the power system without being detected.

Enabling utilities to better prepare to endure and respond to unknown hazards such as cyber-attacks will result in greater grid resilience. The recent report by the National Academies of Sciences, Engineering, and Medicine investigates grid resilience and promotes identifying, developing, and implementing strategies to deal with events that can cause large-area, long-duration outages [11]. Long-duration blackouts are defined as those extending over multiple service areas and lasting at least several days. Risk management focuses on predicting and lessening the likelihood that certain events occur. Resilience is about limiting the scope and impact of events that do occur as well as maintaining or quickly restoring the delivery of essential goods and services services. To achieve resilience is to maintain performance while enduring and recovering from an event. To best operate through and recover from an attack, trustworthy and accurate cyber-

978-1-5386-1006-0/18/$31.00

physical models are essential.

Research on cyber-physical security is also important. In [12], it presents an offline security-oriented cyber-physical contingency analysis in power infrastructures. It combines power system contingency and cyber compromise analysis to rank the control network vulnerabilities according to the underlying power system impact. In [13], there is an online framework for assessing the operational reliability impacts due to the threats to the cyber infrastructure. Moreover, to meet the fast-growing energy demand and to alleviate environmental concerns, direct current (DC) microgrid technology currently attracts a lot of research. Dinesh Kumar et al present a state-of-the-art DC technology in [14], which covers alternating current (AC) infrastructure, system architecture, power quality issues, and communication networks. Moreover, the cyber-physical architecture covers the whole infrastructure. All applications mentioned above need a reliable and current cyber-physical architecture of the power system.

The design challenge of cyber-physical systems has been deliberated in [1]. Several promising advances of cyber-physical systems are provided in [15], where they are illustrated in context of smart energy systems and next-generation automotive systems. Recent research for cyber-physical systems in power grids is focused on the application side and cyber threats. Cyber-physical system security of the smart grid are discussed in [16] and [17] discuss, which focus on monitoring, protection and control. In [18], the authors present a cyber-physical security testbed for electric grids.

However, the only source for determining a system's cyber-physical architecture tends to be disparate historical databases, and the information in these databases can be outdated or inaccurate. Thus, when engineers need to use the cyber-physical architecture for power system analysis or cyber security analysis, manually recreating the templates of the cyber-physical architecture for specific substation is often the only option. Thus, it would be ideal to directly and automatically extract the cyber-physical architecture of power systems for the applications mentioned in previous paragraph.

This paper presents a framework of an automated system to extract the cyber-physical architecture of the substation through IEDs' data. Section II presents the framework of the proposed system. In Section III, several applications of the proposed system are introduced. A specific case is demonstrated in Section IV. For future work, more discussions are illustrated in Section V.

II. FRAMEWORK OF THE PROPOSED SYSTEM

The framework of proposed system is presented in Fig. 1, which is an automated cyber-physical model extraction and management system. This system consists of an online connection to one or more data concentration equipment, like the real-time automation controller (RTAC) manufactured by Schweitzer Engineering Laboratories (SEL). Each RTAC is connected with one or more IEDs, such as digital relays, smart revenue meters, etc. The framework is general and will work with a variety of IEDs and connection types. The code in the server is the management system and the code in the data concentrator dictates exactly what data is sent back to the server and how it is returned. The system can use different communication protocols and methods of exchanging this data. The server code should contain the data structures necessary to extract, store, and exchange the data relevant to a cyber-physical power system model. The system can use different interfaces to help accomplish the overall goals.

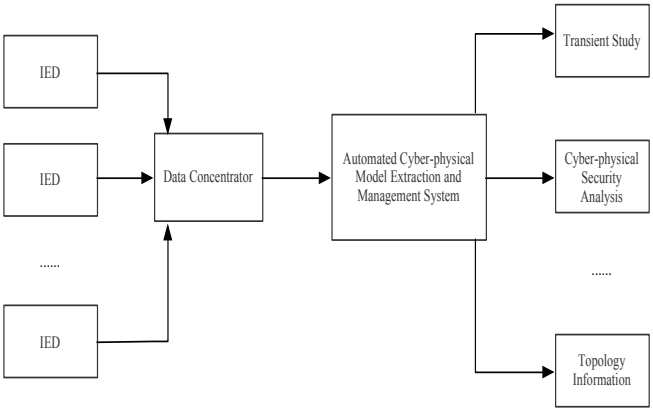

Fig. 1. Framework of Proposed System

III. APPLICATION OF PROPOSED SYSTEM

The automated cyber-physical model extraction and management system is used to pull data out of IEDs and into models for use in specific applications. Major initial applications of the data are transient stability and cyber-link model creation. Besides, the online extraction of cyber-physical architecture could also update exact information of substation topology for utility companies. Feasible applications are demonstrated in Fig. 2.

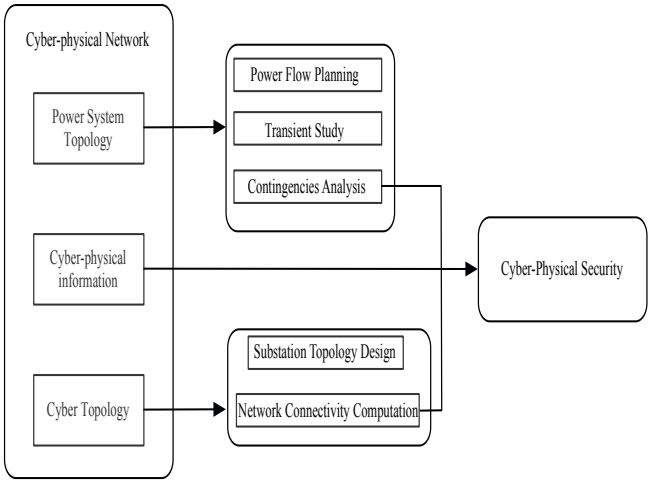

Fig. 2. Overall Application of Proposed System

Fig. 3 demonstrates a typical communication architecture with a data concentrator RTAC (DC RTAC). If the IEDs communicate via Ethernet, each IED will have a unique IP address. If the IEDs connect to DC RTAC through serial, the DC RTAC will have the information about the connection port for each IED. Thus, the DC RTAC will not only have the setting information, measurement, and status of each IED, it will also have the cyber-physical information of the system. With the proposed system, the cyber-physical architecture could be extracted from DC RTAC and applied to different analysis and design.

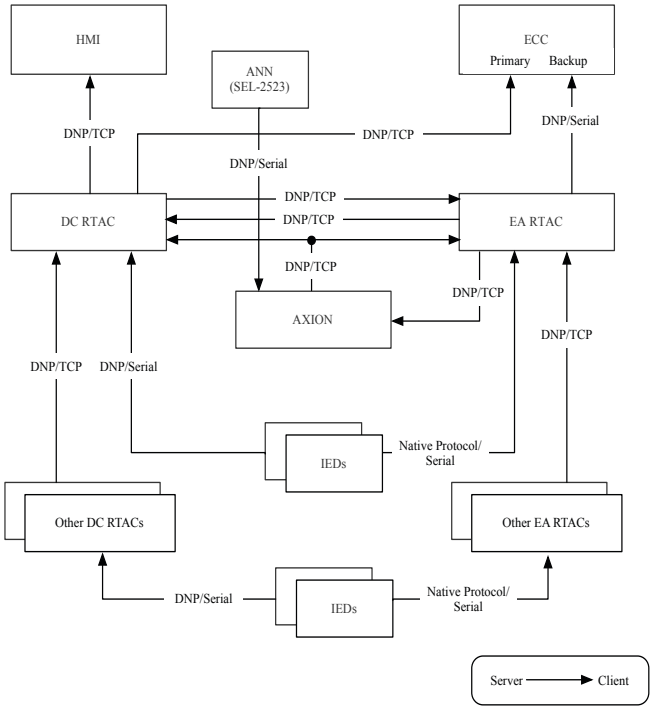

Fig. 3. Typical DC RTAC Communication Structure

The following subsections introduce detailed information of how to apply the proposed framework into corresponding application areas.

A. Power System Contingency Analysis

Power system contingency analysis is a critical part for power system design and planning. It not only provides guideline for operation but also provides significant information for protection, control and etc. Traditional contingency analysis focuses on modeling single-element outage (one-transmission line or one-generator outage), multiple-element outage (two-transmission line outage, one transmission line and one generator outage, etc.), and sequential outage (one outage after another) [19]. Different contingency analysis methods have been proposed for power systems. In [20], an interactive three-dimensional visualization of contingency data is presented along with detailed information of the power system. A more comprehensive approach of power system contingency analysis has been proposed in [21]; this presents a new methodology based on 'extended electromechanical modeling,' which includes security study, modeling of emergency control countermeasures and self-emergency control. With adoption of various IT technologies and programing languages, there are also new methods to solve power system contingency analysis, like cloud model [22], hybrid Petri Nets [23], and parallelizing contingency analysis with D programming language [24].To build these models and solve the contingency analysis, the power system topology is still a critical element. With the proposed system, it could extract the cyber-physical architecture of the power system and manage it to be adaptive to various contingency analysis tools as mentioned.

B. Cyber-physical Security Analysis

The growing need to consider power systems as cyber-physical systems marks a milestone in modern grid development. Improved self-control and protection schemes also bring attention to cyber-physical security. Few of the research efforts on cyber-physical security that have achieved manifest success in practice. With the information of network connectivity, power grid topology and cyber topology, the security oriented cyber-physical contingency analysis could rank the contingencies based on their impact and cyber-attack complexity [12]. In this way, the utilities will know the critical parts of the power system and they could prepare different solutions for those contingencies. An online framework is presented in [13] to evaluate and rank the most critical cyber threats for power system. To achieve that goal, it needs the cyber topology and power topology to generate the analysis model. And cyber-physical architecture is also important for identifying cyber attack path. Since it is an online framework, updating the current cyber-physical architecture and power system contingency analysis will be critical. The authors in [25] present toolsets for cyber-physical security assessment (CyPSA), an evolution of [13]. CyPSA maps the points of interconnection between cyber and physical system to determine what physical actions are possible from any given host in the cyber network and it also prioritize N-x contingency analysis to identify the coupled contingencies situation. With the online analysis and assessment, utilities could get the present security information of the power system. The common part for these applications is that they all need an accurate cyber-physical architecture of the power system. The cyber topology provides important information of cyber attack paths, the power system topology is a critical element for contingency analysis, and the cyber-physical interconnection is necessary for CyPSA.

C. Substation Topology Design

In addition to its application for creating and improving various analyses, the proposed framework could also provide great convenience for substation topology design. When power system engineers design the SAS or upgrade the substation topology, they need to know the information of existing IEDs in the substation and the type of communication protocol employed by IEDs. It always takes several weeks on the

design of the substation topology to install more IEDs in the substation or replace obsolete equipment with new digital equipment. A key reason substation design is so time consuming is because the historical drawings of substation topology may be inaccurate. Then engineers have to go to the field to obtain the correct information. With the proposed framework, the data from IEDs could be transmitted to the proposed system. As long as the IED is connected in the system, its measuring data and its setting information will be available in the proposed framework. In this way, the most accurate cyber-physical architecture of the substation will be available at any time and it will save a great amount of time for checking the substation topology.

IV. Application Demonstration of the Proposed System

Fig. 4 demonstrates a one-line diagram of the IEEE 300 bus system [26], which has been utilized in power system research for decades. The biggest advantage of a planning model is that it consolidates the true node-breaker model and makes the power flow solution process much easier and faster. [27] However, with the loss of detailed physical topology information that is present in conventional planning models, the operation models completely disconnect with the planning models, which makes certain type of contingencies not be able to analyze, like the contingency in split bus. Moreover, the layout of the protection system and control system is also eliminated in the one-line diagram, making the analysis of cyber security and cyber-physical security impossible.

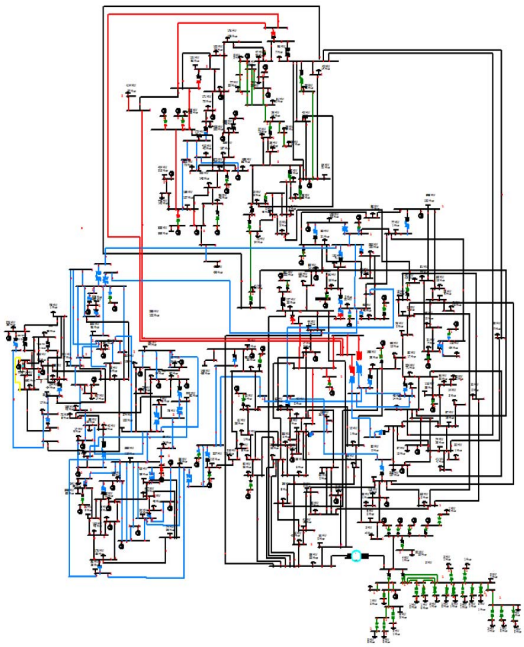

Fig. 4. IEEE 300 Bus One-line Diagram [26]

In [28], there are 6 major bus configurations in common use, including Single Bus, Main and Transfer Bus, Double-bus Double-breaker, Double-bus Single-breaker and Ring Bus. Each configuration has its specific arrangements of equipment. Based on these configurations, this paper proposes an algorithm to distinguish different bus configurations based on the data from IEDs. The algorithm is presented in Fig. 5.

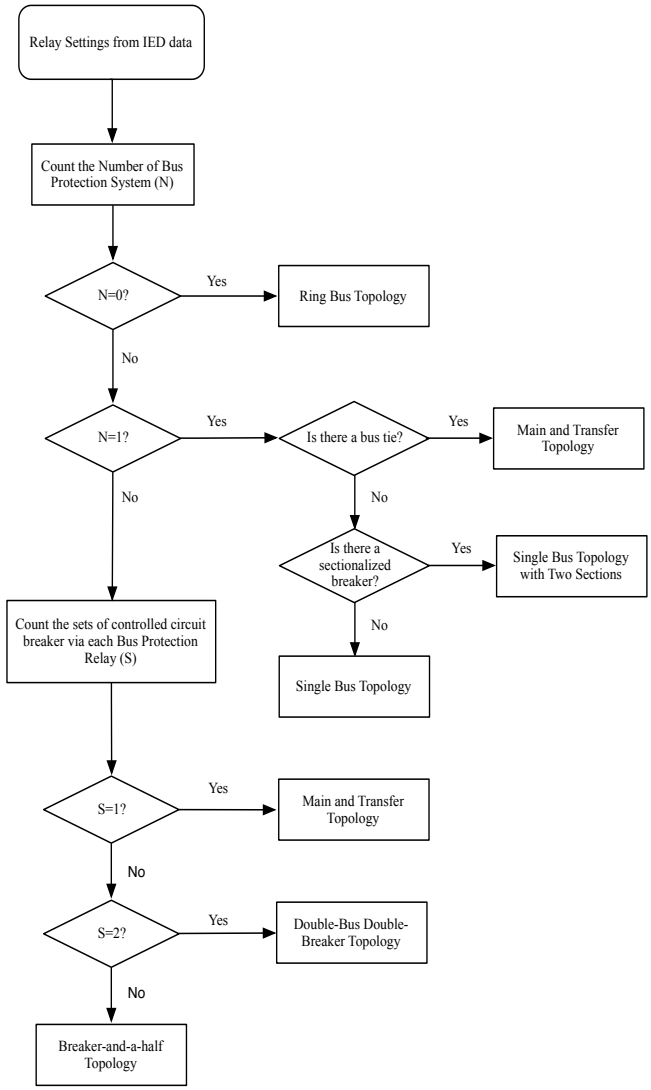

Fig. 5. Bus Configuration Detection Algorithm

With the proposed system and bus configuration detection algorithm, not only could the one-line diagram of power system be extracted but also the cyber-physical topology of specific bus. Taking a double-breaker-double-bus topology as an example, there are two breakers that connect each piece of equipment in Fig. 6, so rather than having a load connected at a bus in the planning model, there are two bus bars and the load is connected between them with two breakers. A planning model cannot provide any information in Fig. 6 whereas the detailed topology information of that substation will include the layout of circuit breaker, recloser, and protection relay and all related cyber information, the IP address of each IED. The proposed system can extract the cyber-physical topology from

the IEDs and convert the planning model and one-line diagram into a detailed physical topology with cyber information. Fig. 7 demonstrates an example cyber-physical topology with the proposed system.

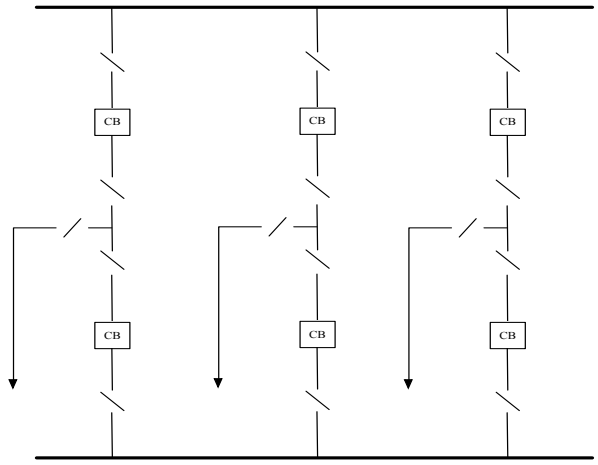

Fig. 6. Double-Bus-Double-Breaker Topology

With a topology like Fig. 7, a detailed contingency analysis could be accomplished and the network connectivity is also accessible. In this way, CyPSA could provide a better assessment of the overall power system. Moreover, the engineers can know the specific IEDs in the system, which provides them great convenience for the design, operation and maintenance.

V. Conclusion

This paper proposes a framework of automatically extracting and managing cyber-physical architecture from IEDs' data and introduces several application areas. First, the proposed system can provide the most accurate cyber-physical architecture of a substation, which can provide great convenience for the upgrading design. Second, the power system topology is fundamental for contingency analysis. With the proposed system, contingency analysis could be faster and more adaptive. Third, for cyber-physical security analysis, the proposed system could directly provide cyber-physical information. This cyber-physical model is a crucial element for contingency information and network connectivity computation.

An application based on the proposed system is presented. The proposed system offers significant advantages for the overall and detailed analyses of power systems, and it is easily implemented. The future work for this system will focus on enriching its database, testing model extraction scenarios with online data and making it adaptive to more applications.

Acknowledgment

The authors would like to thank the National Science Foundation (NSF) under Award Numbers CNS 1446229 and ARPA-E under Award Number DE-AR0000233 for their support and sponsorship of this research.

References

[1] E. A. Lee, "Cyber physical systems: Design challenges," in *Object oriented real-time distributed computing (isorc), 2008 11th ieee international symposium on*. IEEE, 2008, pp. 363–369.

[2] K. E. Martin, "Synchrophasor standards development-ieee c37. 118 & iec 61850," in *System Sciences (HICSS), 2011 44th Hawaii International Conference on*. IEEE, 2011, pp. 1–8.

[3] R. Mackiewicz, "Overview of iec 61850 and benefits," in *Power Systems Conference and Exposition, 2006. PSCE'06. 2006 IEEE PES*. IEEE, 2006, pp. 623–630.

[4] M. Golshani, G. A. Taylor, and I. Pisica, "Simulation of power system substation communications architecture based on iec 61850 standard," in *Power Engineering Conference (UPEC), 2014 49th International Universities*. IEEE, 2014, pp. 1–6.

[5] 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.

[6] 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.

[7] J. Zhu, "Security-constrained economic dispatch," *Optimization of Power System Operation*, pp. 141–210, 2008.

[8] R. N. Allan *et al.*, *Reliability evaluation of power systems*. Springer Science & Business Media, 2013.

[9] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Decision and Control (CDC), 2010 49th IEEE Conference on*. IEEE, 2010, pp. 5991–5998.

[10] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*. IEEE, 2012, pp. 342–347.

[11] E. National Academies of Sciences, Medicine *et al.*, *Enhancing the Resilience of the Nation's Electricity System*. National Academies Press, 2017.

[12] 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.

[13] 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.

[14] D. Kumar, F. Zare, and A. Ghosh, "Dc microgrid technology: System architectures, ac grid interfaces, grounding schemes, power quality, communication networks, applications and standardizations aspects," *IEEE Access*, 2017.

[15] S. A. Seshia, S. Hu, W. Li, and Q. Zhu, "Design automation of cyber-physical systems: Challenges, advances, and opportunities," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 36, no. 9, pp. 1421–1434, 2017.

[16] A. Ashok, A. Hahn, and M. Govindarasu, "Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment," *Journal of advanced research*, vol. 5, no. 4, pp. 481–489, 2014.

[17] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[18] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847–855, 2013.

[19] A. J. Wood and B. Wollenberg, "Power generation operation and control—2nd edition," in *Fuel and Energy Abstracts*, vol. 37, no. 3. Elsevier, 1996, p. 195.

[20] Y. Sun and T. J. Overbye, "Visualizations for power system contingency analysis data," *IEEE Transactions on Power Systems*, vol. 19, no. 4, pp. 1859–1866, 2004.

[21] J. Deuse, K. Karoui, A. Bihain, and J. Dubois, "Comprehensive approach of power system contingency analysis," in *Power Tech Conference Proceedings, 2003 IEEE Bologna*, vol. 3. IEEE, 2003, pp. 6–pp.

[22] G. Venugopal, S. A. Jees, and T. A. Kumar, "Cloud model for power system contingency analysis," in *Renewable Energy and Sustainable*

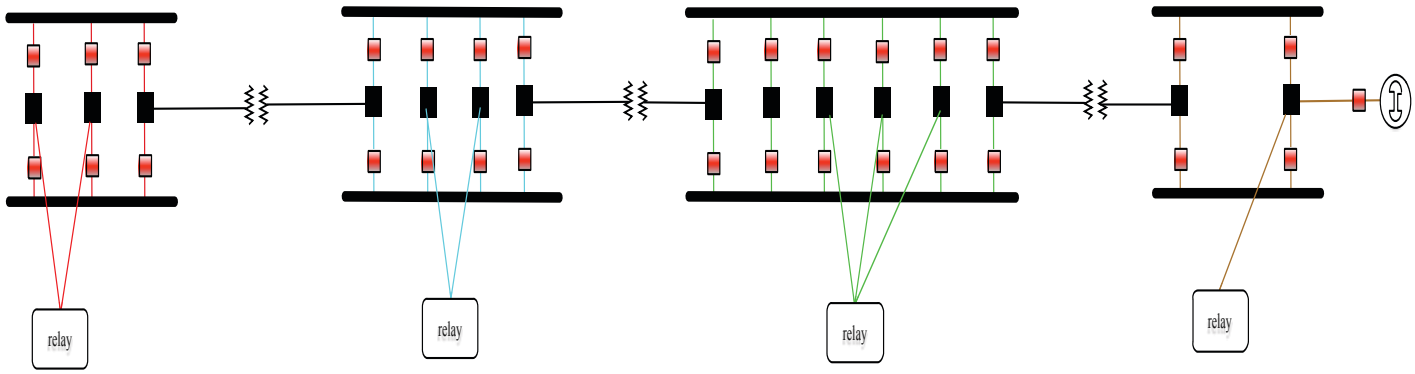

Fig. 7. Extracted Cyber-physical Topology

Energy (ICRESE), 2013 International Conference on. IEEE, 2013, pp. 26–31.

[23] C. A. L. de Alba, V. H. O. Muro, and A. Santoyo-Sanchez, "Modelling hybrid petri nets to analyze contingencies in power systems," in *North American Power Symposium (NAPS), 2015*. IEEE, 2015, pp. 1–6.

[24] S. K. Khaitan and J. D. McCalley, "Parallelizing power system contingency analysis using d programming language," in *Power and Energy Society General Meeting (PES), 2013 IEEE*. IEEE, 2013, pp. 1–5.

[25] 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.

[26] M. Adibi, *IEEE 300-Bus System*, 1993.

[27] S. Grijalva, "Integrating real-time operations and planning using same-format power system models," in *Power Engineering Society General Meeting, 2007. IEEE*. IEEE, 2007, pp. 1–6.

[28] *IEEE Guide for Protective Relay Applications to Power System Buses*, 2009.