2016 IEEE International Conference on Smart Grid Communications (SmartGridComm): Cyber Security and Privacy for the Smart Grid

Cyber-Physical Models for Power Grid Security Analysis: 8-Substation Case

Gabriel A. Weaver*, Kate Davis*, Charles M. Davis†, Edmond J. Rogers*, Rakesh B. Bobba‡, Saman Zonouz§, Robin Berthier*, Peter W. Sauer*, David M. Nicol*
*University of Illinois at Urbana-Champaign, †PowerWorld Corp., ‡Oregon State University, §Rutgers University
{*gweaver,krogers6, ejrogers,rgb,psauer,dmnicol*}*@illinois.edu*, {*matt*}*@powerworld.com*,
rakesh.bobba@oregonstate.edu, *saman.zonouz@rutgers.edu*

***Abstract*—Utilities need to understand and consider the interconnectedness of their electrical system and its supporting cyber infrastructure to maintain system reliability in the face of cyber adversaries. This paper makes two contributions to modeling cyber-physical dependencies within the electrical power sector. First, the paper defines a Common Format using the Cyber-Physical Topology Language (CPTL) to inventory, analyze, and exchange cyber-physical model information. Second, the paper provides an 8-substation cyber-physical reference model. The impact of this work is to enable efficient information exchange of cyber-physical topologies within and among the industry as well as the research community. The reference model and framework will benefit the research community by providing a way to compare analyses on electrical power systems that account for problems within cyber control networks.**

***Index Terms*—cyber-physical systems, network, power grid, CPTL, ontologies.**

I. Introduction

Cyber-infrastructure plays an indispensable role in monitoring, controlling, managing and operating an increasingly complex electrical grid. It is important to understand the connections and dependencies between the cyber and electrical infrastructure underlying the grid in order to maintain reliable grid operations in the face of cyber threats. Realizing this, researchers have proposed different approaches to understand the *cyber-physical* dependence through *cyber-physical modeling and analysis* (*e.g.,* [1], [2], [3], [4], [5], [6], [7], [8], [9]), and through *cyber-physical co-simulation* (*e.g.,* [10], [11], [12], [13], [14]) of power systems.

It is hard to cross-validate or compare the proposed modeling and analysis approaches and results because the cyber-physical models used are not the same and they are not easily reproducible. Real-world models for research are hard to come by, especially grid cyber models, as they are considered highly sensitive information by asset owners and are not shared. An alternative is to use realistic reference models.

Many reference models exist for electrical power systems. IEEE Power Flow Test Cases [15] encode electrical network models of various sizes (14-bus to 300-bus). The 300-bus model was developed by the IEEE Test Systems Task Forces in the early 1990s while other power flow test cases represent a portion of American Electric Power's (AEP) 1960's network. Similarly IEEE reliability test systems of 1979 and 1996, and the 9-bus consolidated model of the Western Electricity Coordinating Council (WECC) system are other examples of electrical network models available to researchers to test their algorithms or control schemes. The ARPA-E GRIDDATA program [16] is undertaking an effort to create and curate a repository of electrical system models for use by researchers and practitioners. There has been work on generating synthetic electrical network models (*e.g.,* [17], [18], [19], [20]) to enable research on test systems larger than the IEEE 300-bus system. However, the focus has been limited to the electrical network and such electrical system test models are not sufficient to describe how current power systems are monitored and controlled.

On the cyber side, efforts to capture and model or visualize the communication infrastructure associated with the power grid have been made. The focus of such efforts, however, has generally been on the analysis or simulation framework and not on developing cyber-physical test models for general use by the community. Hartman *et al.*[20] proposed an approach to generate synthetic communication models for power grids based on analysis of power-line communications used by one utility. The focus of the work was only on the communication network. Just as the "bus/branch" model of the electrical system was extended to a "node/breaker" model to capture circuit breaker configurations and a more accurate topology, extensions are needed to capture the cyber-infrastructure underlying the electrical grid and their interconnections. Recently Skare *et al.* [21] provided an example architecture to share cyber information in a standard way along with electrical information, using Common Information Model (CIM) for cyber security. The information considered included emergency information, information for law enforcement, and security information. This is a step in the right direction but does not yet fully capture the inter-dependencies among cyber and electrical infrastructure.

Furthermore, researchers and practitioners need a common format to catalog, analyze, and share cyber-physical models of the power grid. A common format provides a basis for information fusion and sharing within a utility (*e.g.,* among power engineers, IT staff, and administration), among utilities, between utilities and auditors (for NERC Critical Infrastructure Protection (CIP) compliance), or between utilities and government organizations (as called for by Executive Order (EO) 13636 [22] and Presidential Policy Directive

978-1-5090-4075-9/16/$31.00 ©2016 IEEE

(PPD) 21 [23]). Further, synthetic models expressed in a common format would enable researchers and practitioners to compare algorithms and analysis approaches, without requiring industry to release sensitive data to academia. The current situation is historically analogous to the 1960s in which growth in complexity of interconnected power systems required the ability to efficiently exchange large amounts of load flow data, leading the IEEE to create a Common Format for load flow data [24].

This paper makes two fundamental contributions to address this problem. First, the paper specifies a Common Format to document interactions between the electrical power networks and cyber networks using the Cyber-Physical Topology Language (CPTL) [25]. Second, the paper uses the proposed format to describe and release a synthetic 8-substation cyber-physical model that captures the electrical network, cyber-network and their interconnections.

Section II, introduces several use cases that motivate the creation of the 8 substation model. Section III describes the 8 substation cyber-physical model as well as its creation and implementation using CPTL. Finally, Section IV describes extensions to the current version of the model to support specific types of analyses, and Section V concludes.

II. Use Cases for a Cyber-Physical Reference Model for Electrical Power

Cyber-physical models are essential both to understand the complex inter-dependencies between cyber and power infrastructure, and to assess the risks to the power grid originating from cyber attacks (*e.g.,* [2], [5], [7], [8], [26], [27], [28]). In this section we highlight use cases that are enabled by access to cyber-physical models and their analysis.

Use Case 1: Prioritize Scenarios for N-x Contingency Analysis [28]. Traditional power system contingency analysis takes into account outage of one critical component at a time (e.g., transmission line, generator, large transformer), except when there are dependencies among such components. This is referred to as the N-1 reliability criterion. However, given the threat of cyber attacks, the possibility of losing multiple unrelated critical components can no longer be ignored as an improbable event. At the same time, identifying critical multiple contingencies is in itself a computationally challenging problem given the combinatorial explosion, not to mention the costs of operating the grid to be able to tolerate multiple contingencies. Prioritizing multiple-contingency cases to consider can provide significant cost savings and provide a way to balance reliability and economic operation of the grid. Cyber-physical models and their analysis can be used to prioritize contingencies taking into account both the impact of the contingency and the cyber-exposure of the transmission line. For example, double contingencies involving the most cyber-exposed line with every other line could be considered first.

Use Case 2: Plan for Cyber-Outages and Restoration. Analogous to traditional contingency analysis employed in grid operations, cyber-physical models can be used to undertake contingency analysis and outage planning on the cyber-side. Specifically, using tools like [27] one could assess the impact of a cyber-compromise and proposed cyber remedial actions on power system operations.

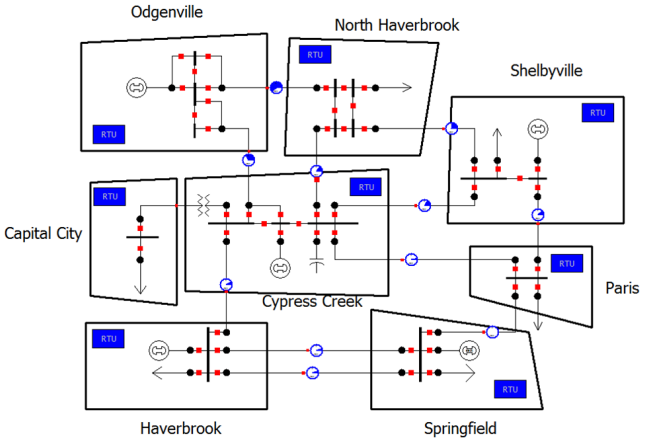

Fig. 1. Electrical Network of the 8 Substation Test Model.

Use Case 3: Prioritize Security Controls for Assets [28]. Cyber security personnel at a utility must prioritize their efforts due to limited resources and time constraints. Expert knowledge combined with security tools make it possible to prioritize defenses based on an asset's likely exposure to attack. Cyber-physical models extend this prioritization by enabling asset rankings to be informed by the significance of the asset to the power system in a formal way. Additionally, assets can be grouped and ranked according to specific cyber-physical properties. For example, the impact of an asset that is exposed because of a new vulnerability might be low when considered individually, but if many similar assets (e.g., relays of the same type) are present, the combined exposure and impact can be significant.

Use Case 4: Assess System Proximity to Destabilizing Attacks. There is much work on identifying cascading outage scenarios for a given power system [29]. Cyber-physical models can be used to assess the proximity of the system to a cascading outage induced via a cyber attack, by taking into account the cyber-exposure of assets involved in cascading outage cases and the current power system state. Similarly, we can assess cyber attack impact on voltage stability and proximity to voltage collapse (*e.g.,* [30], [31], [32]). Proximity to any known destabilizing attacks such as the switching attacks proposed in [2] can also be studied.

III. The CyPSA 8 Substation Model

In this section, we describe the 8-substation cyber-physical model that we release with this work. The model uses the Common Format for cyber-physical networks within the electrical power grid defined using the Cyber-Physical Topology Language (CPTL). The electrical grid of the 8-substation model is derived from the WECC 9-bus, 3-generator bus branch model. Figures 1 and 2 provide more details about

the substation topology and protection layouts of the 8 substation model. Developing this model required visits to and interactions with actual utilities because information on exact network topology at the substation level is rarely available for modeling purposes. Since substation topologies often follow one of a few high-level architectures, templates based on these architectures can be developed and used for analyses. A secondary goal of this section is to provide a high-level overview of how to modify and extend the 8-substation model. Figures 2 and 3 summarize the theoretical approach and its implementation. The model discussed in this section as well as the code employed are available under an open-source license at the CPTL Consortium GitHub[1].

Although a wide variety of formats are available to model the electrical power grid including the Common Information Model (CIM) [33], [34], IEC 61850 Substation Configuration Language (SCL) [35], and the Unified Modeling Language (UML) [36], there is a need within industry and academia to specify *what* information is important to share. CPTL provides an extensible framework to incorporate information attributes and to integrate information at multiple architectural levels including physical, cyber, and even social dimensions (as called for by the National Infrastructure Protection Plan (NIPP) [37]). CPTL graphs serve as a formalism aligned with the etymology of the word *system* ($\sigma\upsilon\sigma\tau\eta\mu\alpha$) which means "an organized whole; body" or a "composition" [38]. The intent of CPTL is to organize resources to support analyses of cyber-physical interactions. CPTL supports requirements for cyber-physical analyses that include the ability to model assets and their dependencies, to integrate diverse data sources under a common language, and to compose previously-defined models to form new systems [25], [39].

A CPTL model consists of (1) a graph that represents connectivity information among assets, (2) a set of ontologies that specify the types of these assets and associated graph attributes, and (3) a mapping from concepts and roles in these ontologies to the graph. CPTL implements these abstractions as (1) a JavaScript Object Notation (JSON) [40] node-link graph whose vertices correspond to assets and edges to links among those assets, and (2) a set of W3C Web Ontology Language (OWL) [41] ontologies that document a controlled vocabulary for vertex and edge attributes, including vertex and edge types. The mapping from ontology concepts and roles to the graph (component 3 of a CPTL model) is implicit in the properties associated with vertices and edges in the JSON graph. A more in-depth theoretical discussion of the theory behind CPTL, including description logics, ontologies, and graph theory, may be found in [25].

The hierarchical structure of the 8 substation model data shown in Figure 3 reflects these formalisms. The 8-Substation Model is available to browse at http://cptl-c.iti.illinois.edu/. The CPTL Consortium GitHub contains source code that demonstrates how to define and validate model components as well as instances of model components. Ontologies and schemas (contained in the `ontologies` and `schemas` directories) define and describe the types of assets (e.g. node, breaker, switch) and relations among them as well as a means to validate the syntax of these networks via JSON schema. In addition, the distribution provides inventories of the component networks referenced within the model and icons for each type of asset (contained in the `graphs` and `icons` directories respectively). Figure 4 shows excerpts of a few files in the source tree pictured in Figure 3. The remainder of this section describes the model components, their representation, and instances within the 8 substation model.

a) Electrical Power Network: Researchers and practitioners must understand how computer networks integrate with the electrical power network. Therefore, the model of an electrical power network must represent physical components that are directly affected by networked Intelligent Electronic Devices (IEDs). The circuit breaker is the most common type of controllable physical actuator within a power system. As such, a node-breaker model, which represents physical components including circuit breakers, is an appropriate starting point to capture cyber-physical dependencies and support their analysis.

The middle panel of Figure 4 illustrates a small example electrical power network based on data provided by PowerWorld [44]. Current types of assets defined within the OWL ontologies for the network include a breaker, bus, node, generator, and transformer. Additional types (and attributes) may be defined based on object models defined within other languages such as IEC 61850 and even device configuration files. The 8-substation model is so named because it defines eight substation power networks.

b) Substation Control Network: Control networks within substations are considered crucial for the resilience of the electrical power infrastructure because they contain most of the IEDs that are directly connected to physical components. Substations include both sensors and actuators for monitoring and control of the system. Substation devices may be connected through a Local Area Network (LAN) but often use serial links.

Figure 4 illustrates a portion of a small substation network. The model distinguishes between overcurrent relays—which trip breakers when the load current exceeds a configurable threshold—and distance relays—which are used to locate the distance to a fault on a line [42]. The current version of the model defines types for serial and ethernet-based connectivity. Other relays, such as the reverse-power relay, are also included in the model. In addition, a simple switch serves as an entry point into the substation control network. There are four serially-connected and four ethernet-connected substation control networks within the version of the model for this paper. These substation control network topologies are based upon visits to real-world substations and discussions with industry experts.

c) Secondary Substation Network: The electrical power network, combined with the substation IT network through cyber-physical dependencies (formalized as a graph join as

[1]https://github.com/cptlc/cptl-models/tree/master/cypsa-8sub

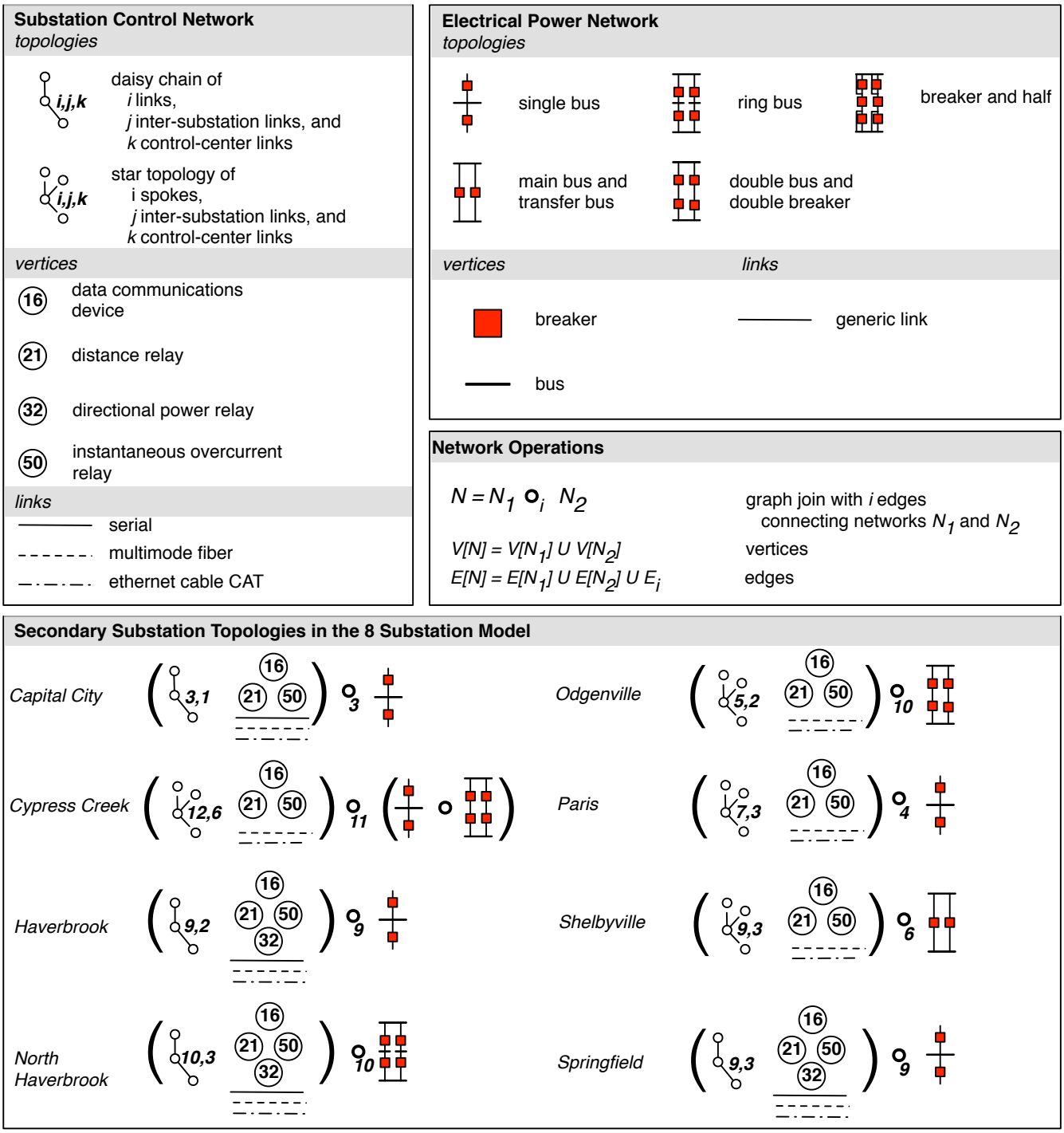

Fig. 2. A detailed view of secondary substation topologies within the 8 substation model. A secondary substation topology consists of a substation control network composed (via graph join) with an electrical power network. In the image above, each substation has exactly one connection to the control center and so this is omitted in the diagrammatic representation of the substation control network. The numbers of vertices within each control network correspond to the standard device and function numbers defined by IEEE Standard C37.2 [42]. The notation was also informed by the schematic representations developed by the IEEE Power System Relaying Committee (PSRC) Working Group 15 [43].

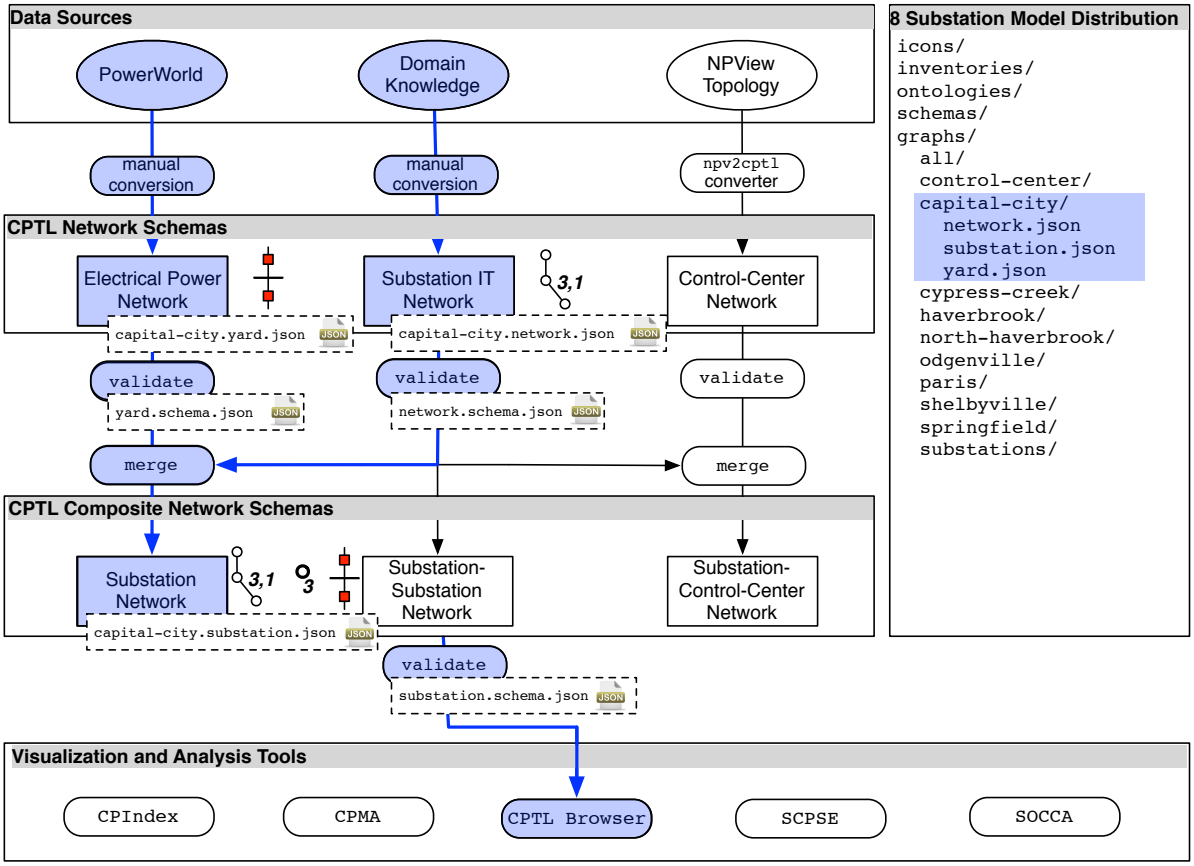

Fig. 3. The pipeline used to generate the 8 Substation Model starts with data sources to instantiate components of eight substation networks and one control center. These components are then combined, via a graph merge tool, to form composite networks. For example, this figure highlights the process to create the Capital City Substation network. Throughout the process, resultant CPTL JSON graphs are validated against schemas for each model component. These models may then be used as input to visualization and analysis tools. The 8 substation model and pipeline code are available via an open-source license.

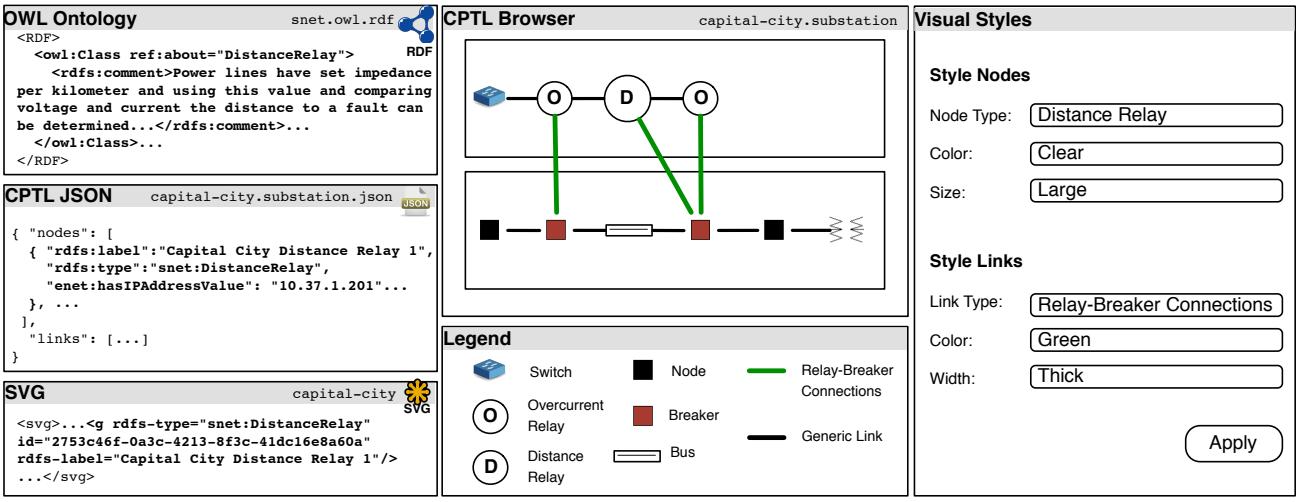

Fig. 4. The CPTL Browser converts CPTL JSON graphs into SVG whose graphical elements are annotated with attribute fields and values defined within OWL ontologies. For example, the distance relay in this figure has both a type definition within the ontology as well as a JSON representation that the CPTL Browser translates to SVG. Users may apply visual styles to the models based on model attribute values.

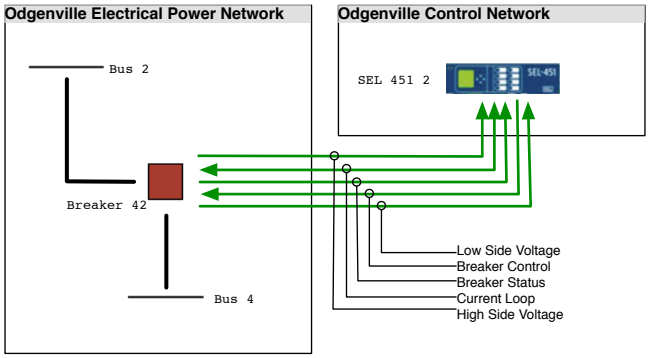

Fig. 5. Dependencies between an overcurrent relay (`SEL 421 2`) and a breaker in the Odgenville substation yard. These dependencies are represented within the model currently via the `hasBreakerConnections` relation.

described in [25]) creates a cyber-physical model of a substation network. The cyber-physical dependence upon which this initial release of the model focuses are relay/breaker interactions. For example, the thick green lines between relays and breakers in Figure 4 represent 5 *physical* connections: (1) a line to measure high-side voltage, (2) a line to measure low-side voltage, (3) a line for current, (4) a line to indicate breaker status (open or closed), and (5) a line to control the breaker. Figure 5 illustrates these five connections in more detail.

The Capital City substation illustrated in Figure 4 merges an electrical power network with a substation control network. As shown in Figure 3, given valid CPTL JSON graphs for these two model components, a `merge` tool implements a graph join operation to output a composite graph. Figure 4 shows a snippet of this output graph (`capital-city.substation.json`). The version of the model for this paper defines eight substation networks and provides a graph with all substation networks merged. A similar process is used to instantiate other composite networks for which the distribution includes schemas. These include networks that compose a substation with one or more substations, and a network of several substations with a control-center network.

d) Control Center Network: The control center provides a central solution for operators to monitor their infrastructure and allows operators to issue control commands. Two major components of a control center are the Energy Management System (EMS) and the Supervisory Control And Data Acquisition (SCADA) system. The SCADA system carries telemetry information from the substation Remote Terminal Units (RTU) to the EMS. The EMS uses this information to estimate the state of the grid and to update monitoring displays used by operators to make decisions. The EMS also handles economic dispatch information.

The 8 substation model's control center network is based on that of an actual utility. Synthetic firewall rules were converted into a network topology via the NPView tool [45] and subsequently converted via the publicly-available `npv2cptl` tool. Although detailed interconnections between a SCADA system and EMS are proprietary and internal to management software, there are a variety of high-level architectures for communications between an RTU and control center Front End Processor (FEP). The current model does not include substation RTUs, and a simple link for control-center/substation communications captures this dependency. In future model versions, the model could be extended to include RTUs as well as more specific communications links that include Synchronous Optical Networking (SONET), microwave, or dialup as described in NIST 800-82 [46]. The current model includes a control center network as well as the control center merged with all eight substations.

IV. Future Work

The intent of the 8 Substation Model is to give researchers a realistic, synthetic, and extensible cyber-physical model of an electrical grid system. Future work will focus on developing larger utility-based models and extending the ontologies and schemas to include a wide variety of assets and attributes. Future work will also focus on integrating and extending analyses already in the literature to account for faults introduced by cyber dependencies. Finally, we intend to evaluate the ability to compare the resilience of independently-generated models and their composition.

V. Conclusion

The electrical power grid's increasing dependence on computer networks and electronic devices for monitoring and control necessitates the ability to inventory and analyze the nature and scope of such interactions. Practitioners need a Common Format to understand the extent of such dependencies and to analyze the consequences of such dependencies for planning and risk assessment. Researchers need realistic models to design and compare security metrics grounded in realistic assumptions. The 8-substation model uses CPTL to model disparate network architectures found in electrical power systems. We hope this model will accelerate the research, development, and deployment of cyber-physical analysis tools to improve the security and reliability of power system operation.

Acknowledgements

The authors would like to thank Shaun Anders, Mouna Bamba, Don Borries, Luis Garcia, Tom Hayes, Rod Hilburn, Mayank Mahajan, Panini Patapanchala, Aaron Phelps, Tamer Roussan, and Olivier Soubigou for their help with the integrated model. The material presented in this paper is based upon work supported in part by the Department of Energy under Award Number DE-AR0000342. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

References

[1] M. Ilic, L. Xie, U. Khan, and J. Moura, "Modeling future cyber-physical energy systems," in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, July 2008, pp. 1–9.

[2] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A Framework for Modeling Cyber-Physical Switching Attacks in Smart Grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 2, pp. 273–285, Dec 2013.

[3] A. Dominguez-Garcia, "Reliability Modeling of Cyber-Physical Electric Power Systems: A System-Theoretic Framework," in *Power and Energy Society General Meeting, 2012 IEEE*, July 2012, pp. 1–5.

[4] 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, Jan 2012.

[5] S. Zonouz, C. Davis, K. Davis, R. Berthier, R. Bobba, and W. Sanders, "SOCCA: A Security-Oriented Cyber-Physical Contingency Analysis in Power Infrastructures," *Smart Grid, IEEE Transactions on*, vol. 5, no. 1, pp. 3–13, Jan 2014.

[6] Y. Zhang, L. Wang, Y. Xiang, and C. W. Ten, "Power System Reliability Evaluation With SCADA Cybersecurity Considerations," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1707–1721, July 2015.

[7] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 566–575, March 2015.

[8] C. W. Ten, A. Ginter, and R. Bulbul, "Cyber-Based Contingency Analysis," *IEEE Transactions on Power Systems*, vol. PP, no. 99, pp. 1–11, 2015.

[9] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-Physical Modeling and Cyber-Contingency Assessment of Hierarchical Control Systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2375–2385, Sept 2015.

[10] C. M. Davis, J. Tate, H. Okhravi, C. Grier, T. Overbye, and D. Nicol, "SCADA Cyber Security Testbed Development," in *Power Symposium, 2006. NAPS 2006. 38th North American*, Sept 2006, pp. 483–488.

[11] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury, "EPOCHS: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components," *Power Systems, IEEE Transactions on*, vol. 21, no. 2, pp. 548–558, May 2006.

[12] J. Nutaro, P. Kuruganti, L. Miller, S. Mullen, and M. Shankar, "Integrated Hybrid-Simulation of Electric Power and Communications Systems," in *Power Engineering Society General Meeting, 2007. IEEE*, June 2007, pp. 1–8.

[13] H. Lin, S. Sambamoorthy, S. Shukla, J. Thorp, and L. Mili, "Power system and communication network co-simulation for smart grid applications," in *Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES*, Jan 2011, pp. 1–6.

[14] P. Palensky, E. Widl, and A. Elsheikh, "Simulating Cyber-Physical Energy Systems: Challenges, Tools and Methods," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 3, pp. 318–326, March 2014.

[15] "Power Systems Test Case Archive," University of Washington Electrical Engineering. [Online]. Available: https://www.ee.washington.edu/research/pstca/

[16] "GRID DATA: Generating Realistic Information for the Development of Distribution and Transmission Algorithms," http://arpa-e.energy.gov/?q=programs/grid-data.

[17] Z. Wang, A. Scaglione, and R. J. Thomas, "Generating Statistically Correct Random Topologies for Testing Smart Grid Communication and Control Networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 28–39, June 2010.

[18] J. Hu, L. Sankar, and D. J. Mir, "Cluster-and-connect: A more realistic model for the electric power network topology," in *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Nov 2015, pp. 85–90.

[19] M. Halappanavar, E. Cotilla-Sanchez, E. Hogan, D. Duncan, Zhenyu, Huang, and P. D. H. Hines, "A Network-of-Networks Model for Electrical Infrastructure Networks," *ArXiv e-prints*, Nov. 2015.

[20] T. Hartmann, F. Fouquet, J. Klein, Y. L. Traon, A. Pelov, L. Toutain, and T. Ropitault, "Generating realistic Smart Grid communication topologies based on real-data," in *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, Nov 2014, pp. 428–433.

[21] P. Skare, H. Falk, M. Rice, and J. Winkel, "In the Face of Cybersecurity: How the Common Information Model Can Be Used," *IEEE Power and Energy Magazine*, vol. 14, no. 1, pp. 94–104, Jan 2016.

[22] "Exec. Order No. 13636," *3 C.F.R*, vol. 78, no. 33, pp. 11 739–11 744, 2013.

[23] "Presidential Policy Directive: Critical Infrastructure Security and Resilience," February 2013.

[24] W. Group, "Common Format For Exchange of Solved Load Flow Data," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-92, no. 6, pp. 1916–1925, Nov 1973.

[25] C. Cheh, G. A. Weaver, and W. H. Sanders, "Cyber-Physical Topology Language: Definition, Operations, and Application," in *Proceedings of the 21st IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2015)*. IEEE, 2015.

[26] S. Zonouz, K. Rogers, R. Berthier, R. Bobba, W. Sanders, and T. 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.

[27] K. Davis, C. Davis, S. Zonouz, R. Bobba, R. Berthier, L. Garcia, and P. Sauer, "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures," *Smart Grid, IEEE Transactions on*, vol. 6, no. 5, pp. 2464–2475, Sept 2015.

[28] K. R. Davis, R. Berthier, S. A. Zonouz, G. Weaver, R. B. Bobba, E. Rogers, P. W. Sauer, and D. M. Nicol, "Cyber-Physical Security Assessment (CyPSA) for Electric Power Systems," *The Bridge, IEEE*, 2016.

[29] Vaiman, Bell, Chen, Chowdhury, Dobson, Hines, Papic, Miller, and Zhang, "Risk Assessment of Cascading Outages: Methodologies and Challenges," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 631–641, May 2012.

[30] K. Vu, M. M. Begovic, D. Novosel, and M. M. Saha, "Use of Local Measurements to Estimate Voltage-Stability Margin," *IEEE Transactions on Power Systems*, vol. 14, no. 3, pp. 1029–1035, Aug 1999.

[31] R. Sodhi, S. C. Srivastava, and S. N. Singh, "A Simple Scheme for Wide Area Detection of Impending Voltage Instability," *IEEE Transactions on Smart Grid*, vol. 3, no. 2, pp. 818–827, June 2012.

[32] J. H. Liu and C. C. Chu, "Wide-Area Measurement-Based Voltage Stability Indicators by Modified Coupled Single-Port Models," *IEEE Transactions on Power Systems*, vol. 29, no. 2, pp. 756–764, March 2014.

[33] "Common information model (cim): Cim 10 version," EPRI, 2001.

[34] Y. Pradeep, P. Seshuraju, S. A. Khaparde, and R. K. Joshi, "CIM-based connectivity model for bus-branch topology extraction and exchange," *Smart Grid, IEEE Transactions on*, vol. 2, no. 2, pp. 244–253, 2011.

[35] "IEC 61850, Communication Networks and Systems in Substations," Technical Committee 57, International Electrotechnical Commission, 2003.

[36] J. Rumbaugh, I. Jacobson, and G. Booch, *Unified Modeling Language Reference Manual*. Pearson Higher Education, 2004.

[37] "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience," Tech. Rep., 2013.

[38] H. Liddell and R. Scott, Eds., *An Intermediate Greek-English Lexicon*. Clarendon Press, 2010.

[39] G. A. Weaver, C. Cheh, E. J. Rogers, W. H. Sanders, and D. Gammel, "Toward a Cyber-physical Topology Language: Applications to NERC CIP Audit," in *Proceedings of the First ACM Workshop on Smart Energy Grid Security (SEGS '13)*. New York, NY, USA: ACM, 2013, pp. 93–104.

[40] T. Bray, "The JavaScript Object Notation (JSON) Data Interchange Format," 2014.

[41] OWL Working Group. (2012) Web ontology language (owl). [Online]. Available: http://www.w3.org/OWL

[42] "IEEE Standard Electrical Power System Device Function Numbers, Acronyms, and Contact Designations," *IEEE Std C37.2-2008 (Revision of IEEE Std C37.2-1996)*, pp. 1–48, Oct 2008.

[43] Power System Relaying Committee, "Schematic Representation of Power System Relaying," IEEE, Tech. Rep., May 2014.

[44] PowerWorld Corp. (2014) PowerWorld Trainer. [Online]. Available: http://www.powerworld.com/products/trainer/overview

[45] D. M. Nicol, W. H. Sanders, M. Seri, and S. Singh, "Experiences Validating the Access Policy Tool in Industrial Settings," in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*. IEEE, 2010, pp. 1–8.

[46] K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," *NIST Special Publication*, vol. 800, no. 82.