Enabling Collaborative Research for Security and Resiliency of Energy Cyber Physical Systems

Alefiya Hussain, Ted Faber, Robert Braden, Terry Benzel
USC/ISI

Tim Yardley, Jeremy Jones, David M. Nicol, William H. Sanders
UIUC

Thomas W. Edgar, Thomas E. Carroll, David O. Manz
PNNL

Laura Tinnel
SRI

***Abstract*—The University of Illinois at Urbana Champaign (Illinois), Pacific Northwest National Labs (PNNL), and the University of Southern California Information Sciences Institute (USC-ISI) consortium is working toward providing tools and expertise to enable collaborative research to improve security and resiliency of cyber physical systems. In this extended abstract we discuss the challenges and the solution space. We demonstrate the feasibility of some of the proposed components through a wide-area situational awareness experiment for the power grid across the three sites.**

I. Introduction

Our society is highly dependent upon large-scale, complex, physical systems that, in turn, depend upon computers for monitoring and control. Conceptually, these cyber physical systems are composed of, and can be decomposed into, physical subsystems that interact with cyber subsystems. These interactions typically occur at well-defined points and follow carefully crafted algorithms.

The electric power grid is one important example of very large-scale and complex cyber physical systems. Its cyber subsystem is a communications network that carries physical domain state measurements to control centers and returns control signals to the physical domain. In steady state, each subsystem could be described as if it operates independently. However, the coupled cyber physical system exhibits very complex dynamics.

A current introduction of more complex cyber components is rapidly transforming the electric power grid. This transformation is enabling a smarter electric grid that utilizes enhanced communication, digital information, and control technology to improve overall resiliency, reliability, and security of the system.

It is both difficult and essential to evaluate and predict the effects of the introduction of this new cyber technology into the power system. The emerging smart grid technology, algorithms, and processes must be evaluated, tested and validated to ensure their efficacy before large-scale deployment. Due to the nature of critical infrastructure, as well as the great expense of large-scale deployment, new technology cannot be deployed without a rigorous and systematic program of research that includes scientifically sound experimentation. This experimentation cannot, however, be conducted on the live grid without impacting its operations; the research community therefore requires a contained environment for investigation and experimentation. This environment must include modeling and simulation of integrated smart electric grid models and be composed of a wide range of networked physical, computational, social and organizational models and components.

The University of Illinois at Urbana Champaign (Illinois), Pacific Northwest National Labs (PNNL), and the University of Southern California Information Sciences Institute (USC-ISI) have formed a consortium, that provides capabilities and expertise to the research community. The consortium provides sharable models, data sets, and testbeds to facilitate collaborative science for resilient and secure energy cyber physical systems.

II. The Challenge

The consortium's goal is a distributed, collaborative cyber physical experimentation facility that will be available and useful for a wide range of power system research. Reaching this goal presents significant challenges. It will require suitable experimental resources, including physical hardware as well as simulations. It will require a cadre of researchers with deep knowledge of at least one of the domains and some knowledge of both in order to understand complex inter-domain interactions. The more ambitious experiments on this facility will require tools and interfaces to support large scale power system experiments with sufficient fidelity and realism. They will typically require researchers with experience at large scale, scientifically valid experiments [1], [2], [3], [4], [5].

On the other hand, the facility should provide support for organizations that need to experiment with the new technology but do not have the necessary facilities, knowledge, or experience. An important aspect of the facility must be education and training to disseminate the combined knowledge to prospective users. We also expect to need repositories of models, configurations, tools, and past experiments, which will be accessible by the larger power research community as well as the consortium members. These repositories will be essential for the less experienced researchers but also vital for the more sophisticated. They will encourage efforts to reproduce and validate experimental results, in accordance with good science.

Translating these resources and knowledge to a contained, flexible, and reproducible environment with the necessary fidelity and realism presents even more challenges. The scientific basis for modeling these cyber and physical domains will stretch the capabilities of experimental methodology and technology, and in some cases it will be constrained by fundamental physical laws.

III. The Solution Space

The consortium seeks to collect and provide tangible resources and expert knowledge spanning the following eight areas.

Testbed: Leveraging the resources and capabilities of its members, the consortium has constructed closed testing environments in the form of cyber physical testbeds. The experimental environments provided by these testbeds are scaled down from the real cyber physical systems. However, they must allow experiments of sufficient scale and fidelity to give assurance that there will be no surprises when real world deployment of the new technology ensues. All consortium testbeds are developed with the underlying ability to federate – that is, to link together resources from different testbeds – to support research on large scale, sector-crosscutting distributed systems with a wide range of varied equipment.

Models: Models are typically domain-specific and describe physical processes, networks, and data. Physical process models are used to define and control the physical configuration. In the case of energy systems, a physical process model might define the location of generators or Phasor Measurement Units, i.e., the coupling between cyber and physical domains. Network models define how the sub-systems are interconnected for communication and which sub-systems can communicate. Finally, the data model defines the data exchanges between sub-systems. To accelerate research and to support medium and large-scale experiments, the testbeds must be able to generate range of configurations under control of constraints provided by appropriate models. Our models provide input to use cases to support reproducibility of results and comparative studies. They form a basis for developing new models for a specific experiment. Models generally incorporate domain-specific rules and procedures that can aid a researcher who is not a domain expert.

Methods: Experimentation methods define the procedures for valid and correct execution of the models in appropriate experimental environments. These methods must handle the range of time scales and the possibly non-linear dynamics of the system components. Using these methods to compose models with different time scales and dynamics allows researchers to explore crucial subsystem interactions that would otherwise be invisible, while they provide a coherent framework for experimentation.

Data: Researchers are clamoring for data. Real world data has been difficult to obtain from organizations due to concerns about privacy, reputation, and loss of competitiveness. Models can be instantiated and their data collected to support research that does not need full experimental control. The consortium builds instrumentation to assist in generating and collecting data. The consortium is developing a repository of relevant datasets through our involvement in cyber physical systems research, which we plan to share with the community. Datasets in this repository will be available to any researcher for experiment and/or analysis.

Expertise: The biggest contribution of the consortium is its collective expertise. Executing cyber security research in critical infrastructure requires broad expertise, such as network communications, cyber physical, testbed, critical infrastructure, and cyber security at a minimum, along with deep domain knowledge. This level of skill and amount of expertise is difficult to achieve on a small research team within a single institution. Through the consortium, this expansive resource can be leveraged by the research community to accelerate and deepen their research impact. We want to support researchers so they can focus on their specific research questions within their domain of expertise.

Policy: Large-scale cyber physical systems are generally composed of distinct organizational and enterprise entities. These entities can be represented at multiple levels of fidelity to include the policy constraints imposed by human operators, controllers, and consumers. Each of these entities may have different privacy and security policies, which will influence the distributed command and control structures and the dynamics of the energy market. The experimentation framework should support expression of these different policies to rigorously capture the effects of human actors and administrative organization on these crucial systems.

Education: There is a dire need for trained personnel to evaluate and validate cyber physical systems. The models, data, expertise, methods, and use cases developed in and for our experimental environment will provide an active learning experience and engage students at both undergraduate and graduate levels. Additionally, they will provide an environment for training researchers, providing both foundational and practical knowledge of operations within the energy critical infrastructure.

Use cases: The use cases within the experimentation framework will codify sets of configurations, constraints, and scenario goals from cyber physical research, to planning and design, to live operations. A wide range of approaches and tools can be leveraged for cyber physical system modeling and simulation. Incremental development of use cases will significantly reduce the entry barrier for experimentation, reduce the costs of evaluation and testing for new systems, and shorten the development lifetime of new technologies.

IV. Initial Capabilities

The consortium demonstrated an initial capability applied to wide-area situational awareness (WASA) for the electric power grid. This initial use case leveraged the (1) extensive expertise in testbeds and in grid technology distributed among three sites: UIUC, PNNL, and USC/ISI; (2) the DETERlab testbed technology [1] to provide automated, highly reconfigurable, and repeatable experiment control; (3) federation of three geographically distributed testbeds to achieve scalability; (4) virtualization, simulation, and emulation of a heterogeneous set of physical and cyber components at member sites.

Each site represented a portion of a national power grid while providing the necessary information to the other organizations. The information was shared across all organizations in a distributed situational awareness experiment framework. The use case explored the streaming of PMU (Phasor Measurement Unit) data from multiple sites to a control center for visualization of the power grid. The cyber or network model included a wide-area router mesh with dynamic routing. The inter-site links traversed the Internet with roughly 100 ms round trip times, which modeled the delay, jitter, and packet loss of a real wide area network. The PMUs in the physical model had three different types of data sources; (1) from the output of real PMU devices attached to physical power systems; (2) the output of simulated PMUs; (3) pre-recorded PMU data streams that were replayed. These PMU data streams were sourced from the PNNL and UIUC sites across an emulated wide-area network and combined in an openPDC at USC/ISI. We subjected the power grid model to different types of failures and studied the effect of disruptions to the physical components and the network. For example, we disrupted the physical models by disabling a PMU and the cyber models by creating an Internet routing failure. These scenarios were then visualized at USC/ISI.

This demonstration was primarily designed to exercise the unified experimentation capability and to explore the potential utility of the capabilities such as expanded expertise, collected models and data sets. During the demonstration we did not explore policy constraints at the three consortium sites. The collaboration did highlight the challenge in surmounting real-world security barriers to achieve the experimentation facilities.

V. Conclusion and Future Work

The consortium's goal is to provide tools and expertise to enable collaborative research to improve security and resiliency of cyber physical systems. To date, the consortium has explored the use of federated testbeds to examine the wide area situational awareness research use case. We intend on making available testbeds, models, methods, data, policy, education, use cases, and expertise to the community. The consortium is presently analyzing community needs to support research in the area of dynamic islanding and is seeking a research partner to help flesh out requirements and beta test assets.

Acknowledgement

All authors are equal contributors. The consortium is sponsored by the DHS Science and Technology Directorate, Cyber Security Division and The Office of Electricity Delivery and Energy Reliability, DOE. Coordination is provided by SRI International.

References

[1] T. Benzel, "The science of cyber security experimentation: the deter project," in *Proceedings of the 27th Annual Computer Security Applications Conference*, ser. ACSAC '11. New York, NY, USA: ACM, 2011, pp. 137–148. [Online]. Available: http://doi.acm.org/10.1145/2076732.2076752

[2] A. Hussain and S. Amin, "NCS security experimentation using DETER," in *Proceedings of the First Conference on High Confidence Networked Systems*, 2012.

[3] D. C. Bergman, D. Jin, D. M. Nicol, and T. Yardley, "The virtual power system testbed and inter-testbed integration," in *Proceedings of the 2Nd Conference on Cyber Security Experimentation and Test*, ser. CSET'09. Berkeley, CA, USA: USENIX Association, 2009, pp. 5–5. [Online]. Available: http://dl.acm.org/citation.cfm?id=1855481.1855486

[4] T. Yardley, R. Berthier, D. Nicol, and W. H. Sanders, "Smart grid protocol testing through cyber-physical testbeds," in *Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES*. IEEE, 2013, pp. 1–6.

[5] D. P. Chassin, K. Schneider, and C. Gerkensmeyer, "GridLAB-D: An open-source power systems modeling and simulation environment," in *Proc. of the IEEE Transmission and Distribution Conference and Exposition (PES) 2008*, 2008, pp. 1–6.