# Modeling, Simulation, and Emulation as Tools for Experimental Research in Energy Cyber Physical Systems

Alefiya Hussain

Energy infrastructure is composed of heterogeneous cyber and physical systems spatially distributed across wide areas. The tight coupling of the continuous and the discrete dynamics in the energy infrastructure make the design and analysis of control mechanisms in the presence of security threats particularly challenging. An obvious challenge arises from the scale of the infrastructure; while each individual system may have a small state space, the coupling between these systems leads to a very large number of interacting states. Additionally, the faults in one part of the infrastructure can propagate to adversely affect other systems. A more subtle challenge is balancing the diverse requirements and constraints of the composite system. The optimum control strategy for one system may not align with the global requirements leading to compromises.

The information network plays a crucial role in the stability of energy systems. The recent adoption of measurement and networking technologies, for example synchrophasors, provide timely measurements that can be used to design control strategies for the stability of the energy network during a failure or a fault. However, these technologies also have significantly increased the exposure of the energy systems to novel security threats and risks.

While there are mature tools for the design and analysis of each of the sub-domains within energy cyber physical systems, there is a pressing need to develop a methodological experimentation framework to explore the composite cyber physical design space. Such a framework will enable propagating and evaluating the uncertainty within the energy infrastructure and capture the complex cyber physical interactions. The experimentation framework can thus be viewed as a *system to study* the particular large and complex energy systems that characterize this domain. It needs capabilities along the following axes:

- **Sensing** mechanisms to discern real-time system conditions. The measurements provide situational awareness and allow studying the impact of different control strategies on the reliability and security of the energy system.
- **Communication** infrastructure to transfer the measurement and control signals with predictable latency. It needs to be flexible to accommodate the changes in scale and fidelity of the energy cyber physical models.
- **Computation** capabilities to enable real time and prediction analyses of the reliability and security of the energy infrastructure. The experimentation tools will allow exploring several *what-if* conditions and propose remedial control actions to handle unstable and insecure contingencies.
- **Control** strategies for rigorous security and reliability assessments. The experimentation strategies will be based on a hybrid dynamical formulation that allow systematically exploring scale and fidelity of the components.

Energy utilities connect their networks together to create a shared energy infrastructure. The security and reliability strategy adopted by one utility will affect the other participating utilities. Due to the complexity of these dependencies, it is imperative that the security and reliability strategies be based on guidance from a rigorous quantitative risk assessment and mitigation methodology that takes into account both technology and policy constraints of the various participants.

At DETERLab, we are developing capabilities to evaluate control strategies for the energy infrastructure. We model the physical system dynamics at the continuous level and cyber system dynamics discretely by state space models. Leveraging the technologies developed for cyber security assessments, we study the impact of various attacks and faults on the coupled system [1] [2]. Working closely within the DEFT consortium [3] and actively participating in the NASPI working group [4], we are currently developing techniques to evaluate energy infrastructure risks based on techniques drawn from cyber security, game theory, control theory, and economics. We envision significantly expanding these capabilities to provide a comprehensive security and reliability assessment framework for energy cyber-physical systems in the near future.

[1] Alefiya Hussain, Saurabh Amin, "NCS Security Experimentation using DETER", In the proceedings of HiCoNS'12, April 17–18 2012, Beijing, China.

[2] Saurabh Amin, Galina A. Schwartz, Alefiya Hussain "In quest of benchmarking security risks to cyber-physical systems." IEEE Network 27(1): 19-24 (2013)

[3] DEFT is a collaboration between USC/ISI DETERLab, University of Illinois, and the Pacific Northwest National Laboratory.

[4] DETER for Cyber-Physical System Experimentation `http://www.deter-project.org/blog/deter_cyber-physical_system_experiments_-_news_front_line`