Improving Operational Resiliency of Cyber-Physical Systems to Attacks and Failures

Dr. Clifford Neuman
University of Southern California

Today's critical infrastructure is deployed as large federated systems. Understanding the response of such systems to attacks and failures requires modeling the reaction of the system-of-systems to stimuli including failures and attacks. In the future, attacks on such systems may exploit cyber-characteristics to automate and replicate the imposition of stimuli at the edges, with the goal of inducing more significant effects upon the system-of-systems across the cyber-physical boundary. In order to improve the resilience of such systems we need to better understand how the system as a whole responds to such attacks and failures. We must also design the system so that it may be partitioned into independent zones, each of which is capable of responding autonomously to such events, taking into account situational awareness of both the local and adjacent zones, and the system as a whole.

When designing traditional distributed systems that operate primarily in the cyber-realm, autonomy has been a goal that allows parts of the system to operate in isolation, when central infrastructure is unavailable. This same design element should be (and is) applied in energy systems, but the level of autonomy is limited because of the need to balance generation and load, the distribution of which has often not been balanced along geographic boundaries. Generation is often located at great distances from loads, with vast transmission systems interconnecting them. As we move toward smart-grids, and distributed generation, some of these limitations may become addressable, especially with load-curtailment techniques as supported through demand response, which enable a confirmed load-curtailment capability to be utilized within a region to offset some shortages in generating capacity.

Improving the resilience of such systems will require autonomic response within regions of the system, and may require the ability to isolate self-sustaining regions (islanding). To properly plan such responses requires a situational awareness capability both within such candidate autonomous regions, and system wide. A means to self-organize into such autonomous regions is needed, and the boundaries of such regions will depend in part on such situational awareness, and prediction of the situation over a specified interval (e.g. the next day). Devices in the physical-domain will be needed that will enable the continued operation within regions for short periods during which planning and reconfiguration can occur.

To enable such a vision for reconfiguration will require research in quite a number of areas. Among the new capabilities that are needed is the capability of cross-domain situational awareness, which can blend domain specific knowledge from the design of the physical elements of the system, with monitoring technologies including signature, anomaly, and specification based intrusion detection, to enable better diagnosis of faults (including attacks), and an understanding of the impact of such faults on the system as a whole (including a capability to understand potential goals of an attack).

Planning for such responses will require better modeling of systemic response across both the cyber and physical domains. This might be accomplished by modeling of different functions within the systems under an assumption of failure (not failure probabilities, since we are consider intelligent adversaries), and the ability to demonstrate how the impact of failures of communications and containment at the leaves, ultimately impacts the system as whole. During operation, such analysis might be repeated for candidate partitions of the system, to understand the extent of outages caused with different plans. Since systems are federated, this modeling might occur within different candidate partitions, and it would need to address the lack of a global criteria for success. For example, a particular utility likely considers their success criteria as maintaining operational resilience to their customers, even though fewer customers across the entire grid might be impacted if a utility were to "sacrifice" some of their resiliency for the greater good.

We are only beginning to get a grasp on the implications of smart-grids and distributed generation, especially with respect to the effects of targeted attacks on such systems. This is a research area in which much greater understanding is needed.

Clifford Neuman and Kymie Tan, *Mediating Cyber and Physical Threat Propagation in Security Smart Grid Architecture*, in Proceedings of the 2nd International Conference on Smart Grid Communications (IEEE SmartGridComm), Brussels, October 2011.

Anas AlMajali, Eric Rice, Arun Viswanathan, Kymie Tan, Clifford Neuman, A Systems Approach to Analyzing Cyber-Physical Threats in the Smart-Grid. in Proceedings of the 4th International Conference on Smart Grid Communications (IEEE SmartGridComm), Vancouver, October 2013

Clifford Neuman, *Challenges in Security for Cyber-Physical Systems*, DHS Workshop on Future Directions in Cyber-Physical Systems Security, Newark, NJ, July 22-24, 2009.

Clifford Neuman. *Understanding Trust in SCADA Systems.* Proceedings of Beyond SCADA: Network Embedded Control for Cyber-Physical Systems.

Pittsburgh, November 9, 2006. (Refereed Workshop Position Statement)