Security Gaps due to Coupling of Energy Delivery Sub-systems

Website: http://cred-c.org/researchactivity/coupledsubsystems

Researchers (ASU): Anna Scaglione, Hoi-To Wai, Eran Schweitzer, Raksha Ramakrishna, Ignacio Losada Carreno. External collaborators: Prof. Mahnoosh Alizadeh (UCSB) and Prof. Andrea Goldsmith (Stanford University).

Industry Collaboration:

- Privately managed solar farm in southwest region of the United States
- Currently seeking additional collaborators with power utilities that own multiple types of generation/distribution infrastructures. Contact Anna Scaglione for more details.

Description of research activity: In particular, this activity focuses on the following issues:

1. Natural gas is now the largest source of fuel for electricity generation (according to PJM). The gas network operation is also becoming more reliant on automation and therefore communication. Hence, cyber-attacks become a possibility, the repercussions of which could propagate to the electric grid, which relies heavily on natural gas. For example, SDG&E is rushing to complete a large battery storage project in record time, to avoid potential blackouts as a result of accidental or malicious disruption of service in the Alison Canyon gas storage facility. We will first mathematically model the dependency between these two sub-systems and then identify the security threats arising due to this coupling that may originate from cyber-attacks, and propose preventive/restorative actions. The tool/technology we envision is a protocol for communicating information to EMS and DMS that can trigger remedial actions. This tool would be equipped with an advanced intrusion detection system that comprises of three sub-components: 1) intra-domain intrusion detection for power grid, 2) intra-domain intrusion detection for natural gas grid, and 3) inter-domain intrusion detection that binds the intrusion detection in the gas and electric domain together. The structure of the proposed comprehensive intrusion detection system is illustrated in Fig. 1.

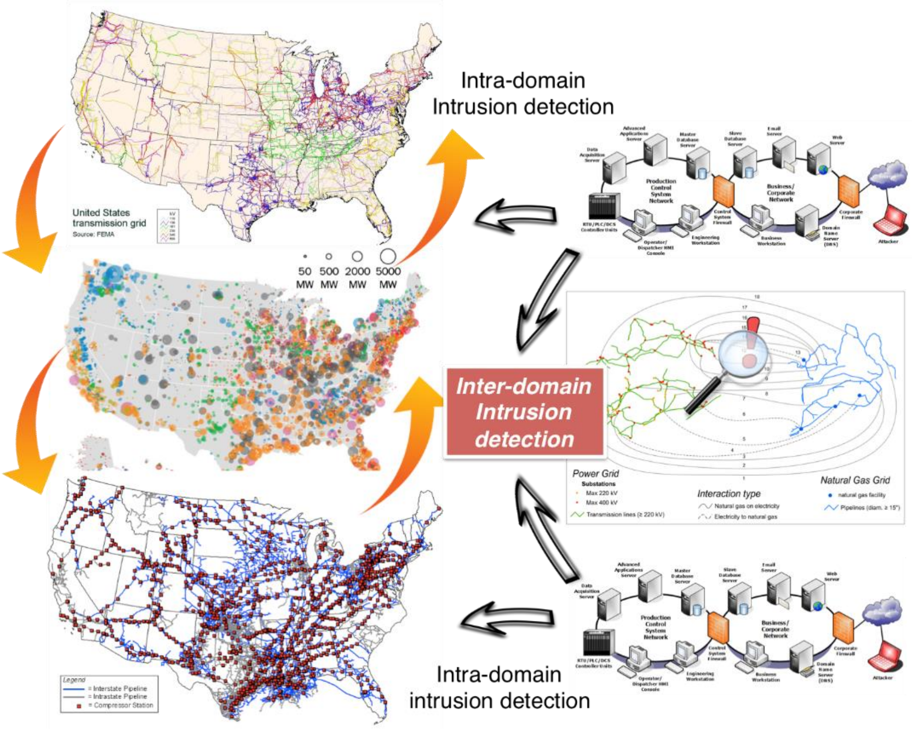

Fig. 1 Comprehensive Intrusion Detection System for Gas-Electric Coupled Infrastructure.

2. Distributed Energy Resources (DERs) integration, especially at the distribution level, including Electric Vehicles (EVs), storage, and renewable energy resources, requires the power grid to interact with a set of new equipment remotely. Often the deployments are managed, monitored and controlled by third parties, while the Utilities are merely metering the power injection from the different sites though dedicated communication networks that allow them to monitor and switch components to manage their response. Electric vehicle charging stations, for instance can be sensitive to the electricity pricing or other signals provided by the EDS. Unstable behavior may arise for the coupled EDS and infrastructure networks. The NESCOR Scenario DER.8 [7] describes an EV charging station that fails to stop fast a charging request from the grid operator, because it fails to receive the control commands. Our results show how such an action can lead to instability in the electrical system. Another example of a threat in this sector can be caused by manipulating the charging/discharging converter as non-linear load in the grid to create harmonics that can potentially put the grid in resonance or cause disruptive power quality issues at the distribution level. These actions would be made possible by tampering and reprogramming with malware the micro-controllers that are used to switch and monitor the charging process. Our aim is to develop models and protocols to share information and prevent such unstable behavior, while searching for a social optimum strategy. Having identified this instability, we will expand to consider the threat it poses to the electrical system if charging stations are not adequately monitored and controlled.

   Like the gas network, distributed solar deployments as well as solar plants typically occupy a wide geographical footprint. Hence, they have to rely on communications for their automation. Increasingly, researchers are considering algorithms to regulate the voltage, track the maximum power point, and perform other monitoring and control functions via inverters in these solar farms. The backbone communication infrastructure is often not owned or managed by the utilities. Therefore, attackers can exploit vulnerabilities that exist in these networks to disrupt the normal operation of the power grid.

   Another inverter-related example of such interruptions is to manipulate On-Load Tap Changers (OLTCs) to put the inverters at the coupling point of DERs with the grid out of the allowed voltage-time zone recommended in the voltage-ride through best practices[1] . OLTCs are controlled by SCADA relays or microcontrollers, which can be vulnerable to cyber attacks. Additionally, the DER paradigm relies heavily on predictive methods. Weather forecasting plays a large role in predicting renewable energy generation. The network of sensors deployed by weather forecasters, therefore has a growing impact on the power grid's operations. This opens up myriad new targets for an attacker, by spoofing the system that provides the weather forecast to the grid operator.

3. Some data collection (for the Independent Systems Operators (ISO) or Utilities) is done over networks from third party companies (AT&T and Verizon). Therefore, disruption to this communication infrastructure could impede data collection for an ISO, resulting in a degraded knowledge of system state. The longer such blindness to the system state persists, the more likely it is that a poor operations choice will be made, resulting in failures. Note that the distinction here from the attacks targeting the SCADA network is that this communication infrastructure is managed by an entity outside the power system operation boundary. This entity, the communication provider, was initially developed with another objective, and is now employed under a specific agreement between two entities (the work we propose focuses on the impact to EDS resulting in loss of access to communication services; models of attacks on the communication network are out of scope.)

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
This activity is tied to the roadmap objective of "Assessing and Monitoring Risk" and "Developing and Implement New Protective Measures to Reduce Risk" accounting for the complex interactions between power generation and transmission, oil and gas suppliers, renewable power generation deployments and end uses that are also coupled through wide-area interconnections (e.g. electric vehicle charging stations coupled with travel patterns on transportation systems).

[1] http://www.pge.com/tariffs/tm2/pdf/ELEC_RULES_21.pdf

Summary of EDS gap analysis: Energy delivery systems have multiple large-scale sub-systems, including natural gas feeds to generators, communication networks, and electrical vehicle charging stations. Considering the interdependency of these sub-systems, one can exploit the security holes in one to cause physical damage to the other. The management of these sub-systems is rarely done in coordination, which means that detecting such attacks is more challenging. Focusing on the electrical grid, we aim to address vulnerabilities that can arise as a result of attacks on the EDS sub-systems and propose remedial actions.

Full EDS gap analysis: Today, we are living in a world with increasing deployment of critical large-scale infrastructure networks that depend on the energy delivery infrastructure. Natural gas pipelines feed a significant amount of the fuel needed for power generators. Datacenters/clouds in computer networks and electric vehicles (EVs) in transportation systems are growing and destined to become large enough to be important players in the energy delivery market in some areas. Our tenet in this activity is that EDS can be severely affected by any fluctuation in the parallel infrastructure networks they are connected to, since these interdependencies effectively create a feedback loop that is not appropriately accounted for in the Operational Technology of EDS. The scenarios we are interested in examining are: 1) situations where the attacks are not producing detectable anomalies in the infrastructure in which they originate; 2) situations in which the closed loop mechanism that includes EDS networks is not sufficiently “damped” to ensure stability of the coupled systems. These interdependencies between sub-systems present new security gap that the current architecture is unable to cope with.

More specifically, the coupled infrastructure systems may easily run into an oscillation behavior without a proper coordination protocol, causing unstable operations of the systems. For instance, in the case of natural gas pipeline network, the oscillation behavior may result in an infeasible pipeline pressure scenario [6], potentially causing the gas pipeline to break; in the case of an electric vehicle network, the sudden surge in power withdrawal from poorly coordinated charging schedules may overwhelm the power grid and lead to blackout [2]. It is conceivable that a monoclonal community of EV charge controllers is compromised, and a large fraction request to charge at once and that such a destabilizing charging schedule may arise from malicious cyber action. The societal impact of such instabilities can be enormous.

In the literature, the issue of interdependent networks has been studied from both theoretical and application perspectives. On the theoretical front, physicists have considered the impact of network topology on cascading failures with coupled networks in general, e.g., [3,4,5]. On the application front, only a few empirical studies of interdependent structures exist. Among these are the simulation-based studies that aim at identifying situations for which unstable behavior can occur. For example, [1] studied vulnerabilities in the gas-power coupled infrastructure; our previous study [2] considered the prescribed oscillation behavior with EV-power coupled infrastructure. Fortunately, as shown in these studies, the unstable behavior can usually be avoided when a full coordination scheme is employed.

That said, a full coordination scheme demands radical change in the current infrastructure as well as in the operation on the grid. The lack of a reasonable coordination protocol is a significant gap from the points of view of security and stability. Furthermore, complications such as having multiple infrastructure operators competing on the same network will present more challenges to the coordination protocol design.

In the special case of EV networks, the security gap analyzed above is also tied to the failure scenarios studied in the NESCOR failure scenario [7, Page 5-58]. For instance, the simultaneous fast charges caused by improper coordination between EDS and transportation network operator will cause overload in the transformers of the power grid, leading to a local outage and the prevention of the EVs from being charged.

Bibliography:

[1] A. Zlotnik, L. Roald, S. Backhaus, M. Chertkov, G. Andersson, “Coordinated Scheduling for Interdependent Electric Power and Natural Gas Infrastructures,” IEEE Trans. On Power Sys., Jan., 2017.

[2] M. Alizadeh, H.-T. Wai, M. Chowdhury, A. Goldsmith, A. Scaglione, T. Javidi, “Optimal Pricing to Manage Electric Vehicles in Coupled Power and Transportation Networks,” IEEE Trans. On Control of Networked Sys., 2016, to appear.

[3] J. Gao, S. V. Buldyrev, S. Havlin, H. E. Stanley, “Robustness of a Network of Networks,” Physical Review Letters, November, 2011.

[4] C. M. Schneider, N. Yazdani, N. A. M. Araujo, S. Havlin, H. J. Hermann, “Towards designing robust coupled networks,” Scientific Reports, June, 2013.

[5] C. D. Brummitt, R. M. D’Souza, E. A. Leicht, “Suppressing cascades of load in interdependent networks,” PNAS, Feb., 2012.

[6] M. Chertkov, M. Fisher, S. Backhaus, R. Bent, S. Misra, “Pressure fluctuations in natural gas networks caused by gas-electric coupling,” in Proc. HICSS, 2010.

[7] NESCOR, “Electric Sector Failure Scenarios and Impact Analyses,” Technical Report, Sept., 2013.