Real-time Cyber Analysis to Improve Operational Response to a Cyber Attack

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

Researchers (MIT): Stuart Madnick, Michael Siegel, Keri Pearlson, Keman Huang, Mohammad Jalali, Research Assistants.

Industry Collaboration:

- Austin Energy
- MIT Cogeneration Facility
- Pacific Northwest National Laboratory (PNNL)
- We are also actively seeking additional collaborators from companies involved with EDS. Please contact Keri Pearlson for more information.

Description of research activity:

Solution Approach: The research team has already investigated several cybersecurity simulations available for improving operational performance. These tools offer environments that simulate a variety of cyber incidents and give operators practice in responding. We believe a more complete solution is needed to provide for real-time incident management, as well as training for cyber-incidents.

Our research team has worked together with industry partners to better understand cybersecurity needs for operators. Part of this research is to examine the current operations to better understand the EDS operator environment and to more closely represent that environment in the simulation.

The database of response strategies and the simulator of response plans will benefit from theories of cybersecurity, decision-making, and risk management, as well as experience and knowledge acquired from EDS experts.

Overview of the simulation tool and the database of response strategies: The simulator tool will first assist the operators in diagnosing a cyber incident (a breach, or a threat, or other cyber incidents). The simulator will create consequences of the incident, based upon different levels of uncertainties and the initial actions the operators made in the first step of the simulation. The database of response strategies will offer specific plans for operators to respond to the incident. This allows the operators to consider alternative choices and different levels of uncertainties of their inputs to the simulation, and monitor the potential consequences of their responses. Below we discuss the details of the simulation and the database of response strategies.

As shown in Figure 1, we will develop a database of response strategies based on three main parts: 1) empirical cases (e.g., the Ukrainian power grid incident); 2) simulation cases (e.g., hypothetical cases based on NESCOR failure scenarios or NIST 800-61 R2); and 3) real-time simulation. For the first two parts, the scenarios and response actions will be generated based on the existing standards, guidance, best practices and empirical cyber incidents. Then the response actions will be allocated with the scenarios, using the simulator, to understand the consequences of these actions as well as the operators' behavior patterns. In this way, we can populate the scenario-action database in our database of response strategies. At the time of an incident, an operator can benefit from the database and learn about the consequences of actions. Operators can benefit from the real time simulator where the simulation engine generate outputs (i.e., consequences of actions) based on operators' inputs. These cases will also be saved into the database for future use, helping enhance the database over time.

Within any of the three large boxes on the left in Figure 1, threat intelligence is used to generate cyber-attack scenarios including cyber kill chains. Threat intelligence contains historical information about the case, best practices, and information about the attack. With the generated scenarios, along with information about cyber-physical-systems, we will develop a cyber-related energy delivery system simulation to simulate the consequences of the scenarios and the impacts of attacks on the cyber-side of the power grids. This simulation engine, which will be developed with the assistance of PNNL, is not limited to power grids and can be used in other energy delivery systems (e.g., oil and gas).

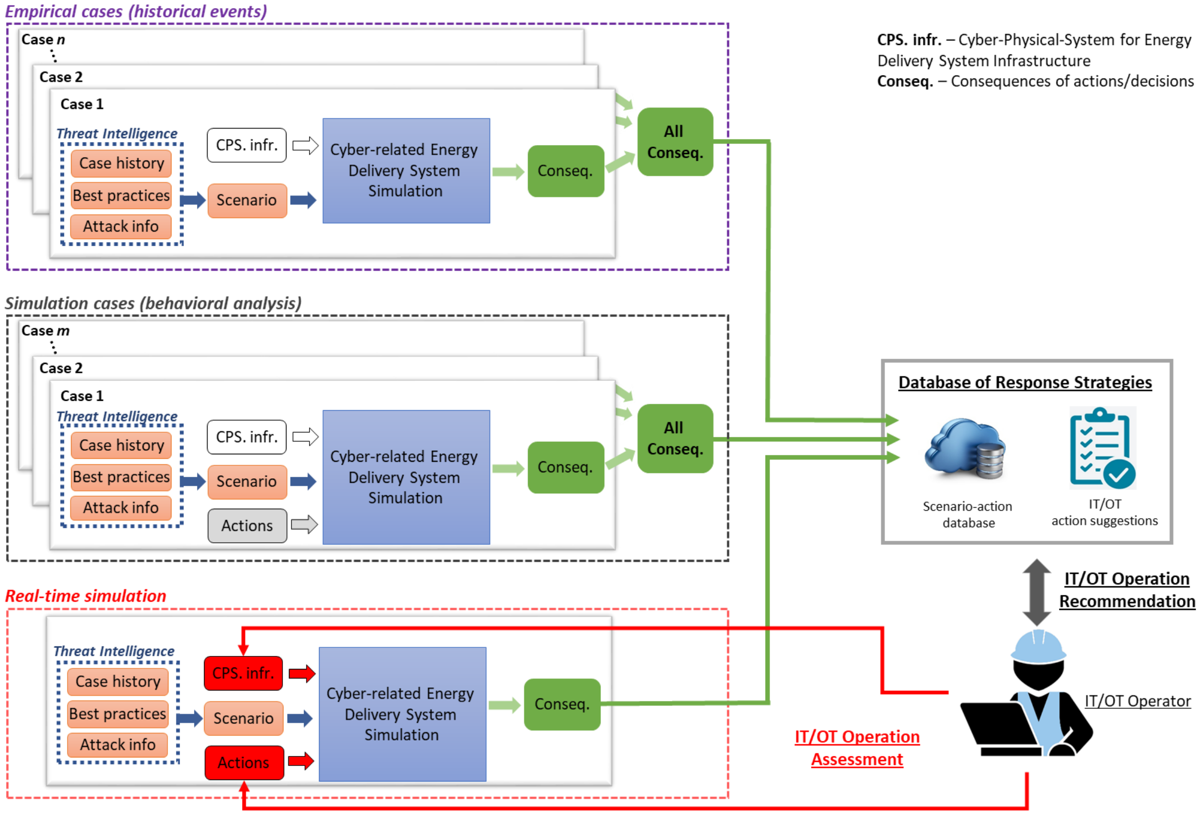
Empirical cases (historical events)
Case n
Case 2
Case 1
Threat Intelligence
Case history
Best practices
Attack info
CPS. infr.
Scenario
Cyber-related Energy Delivery System Simulation
Conseq.
All Conseq.
Simulation cases (behavioral analysis)
Case m
Case 2
Case 1
Threat Intelligence
Case history
Best practices
Attack info
CPS. infr.
Scenario
Actions
Cyber-related Energy Delivery System Simulation
Conseq.
All Conseq.
Real-time simulation
Threat Intelligence
Case history
Best practices
Attack info
CPS. infr.
Scenario
Actions
Cyber-related Energy Delivery System Simulation
Conseq.
CPS. infr. – Cyber-Physical-System for Energy Delivery System Infrastructure
Conseq. – Consequences of actions/decisions
Database of Response Strategies
Scenario-action database
IT/OT action suggestions
IT/OT Operation Recommendation
IT/OT Operator
IT/OT Operation Assessment

Fig 1. The simulation framework and the database of response strategies

The left box in Figure 1 shows the simulation analysis process. The process begins with a review of key principles of cyber resilience from the utility guidebooks (e.g., NIST 800-61 R2). The briefing includes key issues operators might face, and the kinds of responses they have available to them. Based on the NESCOR failure scenarios and other guidelines, the discussion includes a set of possible operator actions. This information along with details about physical infrastructure will be entered into the cyber-related energy delivery system simulation. Consequences of the scenarios are generated and will be used in the database of response strategies to generate new effective response-based recommendations for operators.

Furthermore, our database of response strategies will be used to collect information on the actions and decisions made by operators in a virtual environment to analyze operators' behavior and provide insights about effective strategies to improve operator performance. This information will be used to understand operator behaviors and provide insight into what types of additional information is needed to improve their performance in a cyber crisis—and also to improve the database and the simulator. This information will be useful for the managers of the operators to identify systemic needs and higher level performance improvement strategies. It will also highlight policies and practices that can be used to improve the tool and operator performance in future events. The initial implementation will focus on power systems but the design of the database and simulator will easily facilitate other energy delivery systems.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?

- Manage cyber incidents through:
  - providing all possible response plans in an actionable format
  - choosing effective response plans using the simulator

- Providing suggestions (based on simulation results) for sustaining the impact of response plans and further security improvements

The database of response strategies and the simulator of response plans will assist the EDS operators to make the real-time, effective actions in response to a cyber-incident. Additionally, the simulation tool will use cyber threat intelligence to enhance cybersecurity.

Summary of EDS gap analysis: Energy delivery systems (EDS) operators have multiple guidelines for protecting their environments from a cyber incident. However, all these guidelines are only helpful if the operator can access them effectively in real-time to respond to a crisis. Furthermore, operators typically have much better insight into operating the grid than they do in understanding how the cyber control of the grid actually works. We cannot assume that if guideline suggests, for example, to reboot a router that the operator will understand what affects this action has on situational awareness and control. This research is intended to aid operators in these situations by providing potential actionable plans and the ability to monitor the consequences of each plan. Operators may understand the importance of cybersecurity and make effective response plans to enhance the cyber resiliency of the EDS, but supplementing their abilities with a tool that allows them to incorporate the guidelines and understand outcomes will provide better incident response capabilities, as well as providing a vehicle for training for incident response.

Furthermore, our experience working with the energy sector and our interviews with several EDS experts and operators reveal that these recommendations and guidelines are not being fully implemented in part because the quantity and detail can be overwhelming. The complexity and uncertainties of cybersecurity make rapid decision making a challenge for the operators, especially when they are under pressure. Some approaches to reducing complexities such as security argument graphs [4] and simulation engines such as power world simulators [5] have been developed. However, improving operator cybersecurity awareness and providing tools for real-time incident response remains a challenge.

This project addresses this challenge with a database and a simulation tool for operators that provide them with response strategies and help them monitor the cyber-related consequences of their response plans. Recommendations, best practices, and guidelines will be built into the simulation to insure operators follow the most up-to-date information on managing cyber-attacks.

Full EDS gap analysis:

Motivation: Energy delivery systems (EDS) operators have multiple guidelines (e.g., NISTIR 7628 Guidelines for Cyber Security, Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and the Energy Sector Cybersecurity Framework Implementation Guidance). However, discussions with EDS experts and operators reveal that these recommendations and guidelines may not be fully implemented in part because the details can be overwhelming. In addition, these types of documents may not be reviewed until they are needed (e.g., during a crisis). All these guidelines are only helpful if the operator can access them effectively in real-time to respond to a crisis, and assess the impact that following a given recommendation will have on the state of the cyber system. In addition, choosing the right response plan could be challenging if the guidelines have various and sometimes conflicting recommendations.

We can expect and trust operators to know the grid response to controls they apply, but we cannot expect them to anticipate how actions they must take in the cyber-realm during an incident may affect their situational awareness, and their ability to apply those controls. The tools created from this research are intended to aid operators in these situations. First, operators need a comprehensive database of all guidelines and response actions with an effective search engine that provides them with the right set of actionable suggestions. Second, and more importantly, they need a tool that not only provides them with the most effective response strategy but also give them the ability to simulate and monitor the consequences of various response plans and compare their effects. The importance of this “readiness” is called out in the recent presidential executive order on strengthening the cybersecurity of federal networks and critical infrastructure. An essential part is an assessment of electricity disruption incident response capabilities, including the readiness and the gaps in assets or capabilities to mitigate the consequences of cyber incidents [1].

The complexity and uncertainties of cybersecurity make rapid decision making a challenge for the operators, especially when they are under pressure. Some approaches to reducing complexities such as security argument graphs [4] and simulation engines (e.g., power world simulators [5]) have been developed. However, improving operator incident response capabilities remains a challenge.

Simulations are widely used to help professionals and operators to improve their performance in a variety of industrial settings. Research shows that these interactive simulations are much more effective than conventional decision-making assistants [6]. Similar applications have been developed at MIT Sloan School of Management such as the (IC)3 Cybersecurity Capability Development Tool, Climate Interactive simulator to effect climate change policy-making [7], People Express Simulation to support decisions in strategic management [8], and ReThink Health and posttraumatic stress disorder (PTSD) population to inform health policy decisions [9-10]. These platforms allow for operational responses to complex, unique, and high-risk situations. Furthermore, these tools can be used for training in a crisis. These simulators can be helpful for observing the short- and long-term consequences of a response or series of responses and aid in creating additional diagnostic and instructional tools.

Goal: The goals of this project are three-fold. First is to create a database of response strategies and a real-time simulation tool to assist EDS operators in responding to a cyber crisis—by helping them better understand how actions they take will impact their situational awareness and control of the grid. Second is to better understand how EDS operators decide on a response plan in a cyber crisis situation in order to help them perform better. Third, to improve both the database and simulation tool based on operator experience. To achieve these goals, we will research these questions:

1. What are the response strategies that the operators need to be aware of during a cyber crisis?
2. How can we transform guidelines into effective, actionable activities for operators?
3. What are the cyber-related consequences of response plans and how simulation be used in real-time to provide insights?
4. Given the cyber-related consequences of the response, how can we best assist operators in mitigation?

Approach: Our deliverable product in this project has two components: a database of response strategies and a simulator of response plans. The database includes actions and scenarios extracted from various resources (e.g., guidelines, standards, technical reports, etc.). The simulator provides a real-time platform, in an interactive simulation environment, that helps the operators predict the evolution of cyber incidents and understand the cyber-related consequences of their response plans.

Bibliography

[1] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[2] Electric Sector Failure Scenarios and Impact Analyses – Version 3.0, National Electric Sector Cybersecurity Organization Resource (NESCOR), 2015 December. http://smartgrid.epri.com/NESCOR.aspx

[3] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, http://dx.doi.org/10.6028/NIST.SP.1108r3

[4] Jauhar, S., Chen, B., Temple, W. G., Dong, X., Kalbarczyk, Z., Sanders, W. H., & Nicol, D. M. “Model-Based Cybersecurity Assessment with NESCOR Smart Grid Failure Scenarios”. In Proceedings - 2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing, PRDC 2015, pp. 319–324.

[5] Overbye, T. J. “The Role of Power System Visualization in Enhancing Power System Security”. In Real-Time Stability in Power Systems, 2014, pp. 387–407

[6] Herz, Bernhard, Experiential Learning and the Effectiveness of Economic Simulation Games (February 1998). Available at SSRN: https://ssrn.com/abstract=1002828

[7] Sterman, J., Fiddaman, T., Franck, T., Jones, A., McCauley, S., Rice, P., Sawin, E., and Siegel, L. 2012. "Climate Interactive: The C ‐ Roads Climate Policy Model," System Dynamics Review (28:3), pp. 295-305.

[8] Sterman, J. D. 1992. "Teaching Takes Off," OR/MS Today (35:3), pp. 40-44.

[9] Ghaffarzadegan, N., Ebrahimvandi, A., and Jalali, M. S. 2016. "A Dynamic Model of Post-Traumatic Stress Disorder for Military Personnel and Veterans," PLoS One (11:10), p. E0161405.

[10] McFarland, L., Milstein, B., Hirsch, G., Homer, J., Andersen, D., Irving, R., Reineke, E., Niles, R. D., Cawvey, E., and Desai, A. 2016. "The Naspaa Student Simulation Competition: Reforming the Us Health Care System within a Simulated Environment," Journal of Public Affairs Education (22 (3)), pp. 363-380.