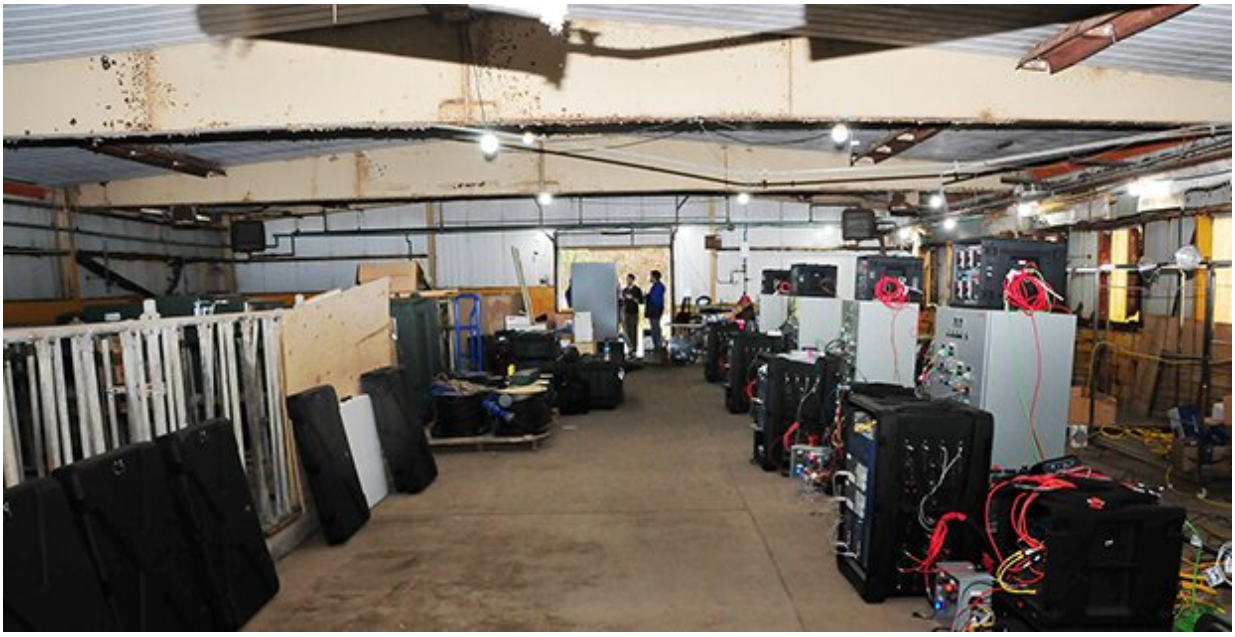
Technologies to rapidly restore the electrical grid after cyberattack come online

March 1 2021



The RADICS Substations-In-A-Box crankpath being restored as part of the exercise at Plum Island, NY in October 2020. Credit: DARPA

Some 330 million Americans rely on the nation's critical infrastructure to keep the country humming. Disruptions to electrical grids, communications systems, and supply chains can be catastrophic, yet all of these are vulnerable to cyberattack. According to the government's 2019 World Wide Threats Hearing, certain adversaries are capable of launching cyberattacks that can disrupt the nation's critical

infrastructure—including electrical distribution networks.

In recognition of the disruptions cyberattacks can cause, DARPA in 2016 established the Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program. The goal of RADICS has been to enable black-start recovery during a cyberattack. Black start is the process of restoring power to an electric substation or part of the grid that has experienced a total or partial shutdown without relying on an external power transmission network to get things back online. Researchers in the program have spent the past four years developing tools and technologies that cybersecurity personnel, utilities, and first responders could use to understand and characterize an attack, isolate networks during remediation, and ultimately accelerate the restoration of power to the part of the grid that has been affected. The idea is that, if the U.S. can handle the worst case scenario, it will be well positioned to handle other attacks.

"Cyberattacks on the grid can essentially do two things—make the grid not tell you the truth, and make the grid operate in an unexpected way," said Walter Weiss, the program manager responsible for RADICS. "For example, the grid could show you that a substation has power when in reality it does not. This could unintentionally prevent power restoration to an entire area since no one thinks there is a need to bring power back online. The technologies developed under RADICS help provide ground truth around grid status, giving responders the ability to quickly detect anomalies and then chart a path towards recovery."

Delivering a Greater Grid

RADICS researchers developed technologies that deliver enhanced situational awareness to grid operators by providing accurate and timely information about grid state before, during, and after an attack. With this improved awareness, operators are better able to thwart an attack or

blunt its effects before it can cause significant damage to any physical infrastructure. To prevent an adversary from continuing attacks on a compromised network during recovery efforts, researchers also developed technologies that isolate emergency networks, allowing for secure responder coordination and communication.

In addition to improving situational awareness, RADICS researchers have developed countermeasures to cyberattacks designed to corrupt configuration files, introduce malicious code in control systems, or perpetrate others types of damage. Among these countermeasures are tools that could automatically map and assess the state and configuration of electrical power networks and detect and characterize power-grid malware.

To test and evaluate new grid-saving tools developed by RADICS researchers, the program featured a custom-built testbed that replicates real-world conditions that utilities and first responders could encounter during a cyberattack. To design the testbed, RADICS leveraged over a decade of testbed-architecture work by researchers (and program performers) based at the University of Illinois Urbana-Champaign (UIUC). The RADICS testbed is comprised of miniaturized substations that were designed to operate as they do in the real world, but with safeguards to protect the system and those operating the substations. The substations are connected via power lines, forming a multi-utility crank path. With a crank path, power is generated to black start one utility that then powers the next utility and the next until the grid is fully restored. The testbed was designed around commonly deployed systems in North America and configured in ways that actual utilities use. Further, the UIUC team implemented a distributed, state-of-the-art computer network that allowed for the necessary data collection, dynamic reconfiguration, and adaptation of the environment, which was needed to meet the requirements that Weiss and his team at DARPA specified for the program.

"Testbeds are more than just hardware and software; they are the people, the knowledge, the data, and the assets that are necessary to build out an environment to serve the designed purpose," said Tim Yardley, the principal investigator responsible for the testbed effort at UIUC. "The RADICS testbed provided a state-of-the-art environment to explore the unknown, test theories and approaches, and accomplish what has never been tried before—live-fire cyberattacks on critical infrastructure systems in a controlled and observable way."

Working collaboratively with the Department of Homeland Security (DHS), the RADICS team developed and deployed the testbed at Orient Point, New York, which is home to the DHS Plum Island Animal Disease Center (PIADC). The island provided an isolated environment for the safe construction and use of the multi-utility crank path. While first constructed in 2017, the test system was deployed iteratively every six months thereafter to continuously challenge and evaluate the RADICS technology as it advanced and evolved.

Starting in 2017, RADICS tools emerging from the research were put to the test against various threat scenarios during a series of evaluation exercises using the testbed. The goal of each exercise was to use the technologies to help power the crank path and restore power to a "critical asset" on the island. Each exercise required consistent communication, collaboration, and problem solving between the research teams and other exercise participants. Volunteers from organizations responsible for the nation's electrical grid were recruited by the U.S. Department of Energy (DOE) for the exercises. These utility volunteers partnered with the research teams to restore power and combat a skilled Red Team as it deployed malicious attacks and exploits. Utilities having the ability to see a cyber-attack in an exercise prior to seeing it in the real-world enhances emergency preparedness and the robustness of U.S. response efforts. As such, bringing in real volunteers from utilities was critical to making the exercises relevant.

"There was significant participation from our energy sector partners over the two year partnership between DOE CESER and DARPA, resulting in a total of 12 private sector entities sending teams of cyber and power professionals to take part in the exercise and assist DARPA in developing and refining tools" says Michael Toecker, Senior Cybersecurity Advisor in DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER). "The partnership was equally valuable to our energy sector partners, who had the opportunity to observe and respond to simulated attacks in a consequence-free environment not unlike their own electric power environments."

The volunteers' expertise and input continuously helped RADICS improve both the technologies in development as well as the exercise.

The RADICS technologies were tested one last time during a live five-day exercise in October 2020 and the program concluded at the end of the year. This was the seventh exercise in the evaluation series and was conducted jointly with other U.S. departments and agencies—including DOE, DHS, and the National Guard. An already complex task was further complicated by the COVID-19 pandemic, but the team managed to provide a safe work environment through rigorous testing, limited personnel on the island, and the development of a virtual-presence platform that allowed exercise participants to join remotely.

"With COVID, the UIUC team was asked to accomplish another monumental task—to make the testbed environment seamlessly accessible remotely to the participants that were scattered around the country, while still maintaining a high level of engagement," said Weiss. The UIUC team delivered an online/remote environment that enabled the successful execution of the final exercise. Today, other government agencies are looking closely at the remote environment for guidance on how to respond to real-world cyberattacks when resources are spread out.

"The RADICS exercise held at PIADC grew and matured significantly over the lifetime of the program," said Weiss. "It started out as an exercise operating in the confines of a lab, and evolved into a three-utility testbed with multiple substations and a supporting virtual environment. By the program's conclusion, we weren't just managing one workforce that was trying to build one crank path across the grid, but three separate 'organizations' that had to work together to figure out how to feed power to each other. The testbed and exercise proved beneficial not only for the program, but also for the broader community involved in grid restoration."

Amplifying Value

Another DARPA program—the Leveraging the Analog Domain for Security (LADS) program—also was able to use the RADICS testbed as a means of program evaluation. LADS is focused on developing low-cost "cyber smoke detectors" to provide real-time situational awareness for the many devices—like power-grid controllers—that support critical infrastructure and military systems, but cannot be monitored using anti-virus or other current endpoint security technologies. Under LADS, a team (dubbed CASPER) from New-Jersey-based Perspecta Labs, developed a sensor for detecting anomalous software execution on a SCADA (supervisory control and data acquisition) device from a distance. The sensor uses machine learning to measure side-channel, radio-frequency (RF) emanations of the device and correlate those emanations with the normal software that runs on those devices.

The CASPER team participated in multiple RADICS exercises, both improving and validating its sensor's performance in a realistic testing environment and, by the final exercise, contributing alerts to warn the RADICS teams of potentially malicious activity in power-grid controllers.

"During the first exercise that the team participated in, the LADS sensors were neither hardened to handle a harsh, real-world environment nor tuned to provide the high-confidence indicators needed to support real-time analysis," said Ian Crone, the DARPA program manager leading LADS. "By the end of the program, however, the team was able to deploy a ruggedized and reliable sensor to meet the mission need. The RADICS exercises provided a unique environment to test both LADS and other technologies that could really improve power grid security and resilience today and in the future."

A key accomplishment of the final RADICS exercise was the transition of control from the researchers to the participants with day jobs in operational settings. Volunteers from utility companies and the National Guard took over the reins and were able to operate the technologies as they would in a real event. "We often find that research is only usable by the developers or researchers, which in my mind means it's not operationally relevant," said Weiss. "What really changed during exercise seven was this shift from our researchers being the people that operated the tools to the operational people taking charge and running the technologies. This program milestone is helping us chart a path for continued tech transition."

Perhaps the most significant output of the final exercise however was proof that the RADICS tools are capable of catching threats on the grid. These tools have proven they work in the controlled, testbed environment but also already have transition into commercialized platforms. One example is Perspecta Labs' SecureSmart solution. SecureSmart is a system for detecting wireless network intrusions, including those involving SCADAs. The system provides real-time network health, anomaly detection, security analysis, and visualization. Utilities are currently using the platform for enhanced situational awareness and network visibility, enabling faster response times to threats.

In addition to hastening the transition of RADICS-born technologies for commercial use, the testbed design and accompanying exercise format are expected to transition to the DOE. These value-added outputs of the program will continue to support training and evaluation efforts for utilities and others in the fight against cyberattacks on the nation's critical infrastructure.

"DOE CESER and our energy sector partners realized several benefits from working with the RADICS program, most especially in utilizing testbed platforms to inform and enhance exercises, training, and workforce development goals in cyber security for energy systems. We will be examining where RADICS-style cyber-physical testbeds can and should be used to improve DOE's preparedness and coordination efforts" said Brian Marko, CESER's Program Manager for Energy Sector Exercises and Cyber Training.

The UIUC team is working to leverage its RADICS work to support future research and looking into how its new know-how applies to workforce development and training. Through curriculum and training development, hands-on demonstration platforms, future exercises, and integration with fundamental and applied research, the university researchers will continue to develop, adapt, and advance the platforms they have built to aid the U.S. and help close remaining security gaps.

Girding for More Grid Protection

"While we've made significant progress against RADICS' mission of rapid grid restoration, there remains an opportunity to further explore technologies capable of thwarting attacks, such as enhanced forensic analysis on grid devices to better understand the threats," noted Weiss.

Today, first responders lack ways of interfacing with infected devices, understanding what these devices are doing under malicious influence,

and ultimately applying a fix. Forensics—in this case the practice of deliberately extracting and preserving data about an intrusion—is not yet a supported feature of grid devices. This is further complicated due to the difficulty of removing a device from the grid to understand what happened to it after an attack. To address this challenge, a team led by SRI International is developing a forensics port that provides a physical opening in these devices for local access to a variety of diagnostic information. With the port, authorized users can perform a variety of incident response actions, such as memory validation and forensic imaging without compromising vendor IP or a utility's proprietary information. SRI is sharing the design for this port with DOE, vendors, and other community leaders to jumpstart a discussion on what additional tools are needed to properly equip grid response teams.

Also still to address is the current need for utilities and grid operators to fall back to manual procedures to restore the grid during blackouts if SCADA or EMS functionality is lost. Today, this involves spending weeks manually creating reliability and resiliency models for tens of thousands of grid nodes. The process typically requires multiple servers and engineers that must rely on incomplete data for grid restoration. To help accelerate this process, researchers from Carnegie Mellon University (CMU) developed a foundational technology for modeling, simulating, and optimizing power flow of the grid. The prototype software tool, called Simulation with Unified Grid Analyses and Renewables (SUGAR) provides unprecedented speed and robustness for developing real-time grid models—reducing the process to seconds or minutes from several days—and can be done on a standard laptop.

"The continued research happening at SRI and CMU stands to greatly benefit electrical grid restoration efforts," said Weiss.

The question of how to prevent an attack from happening in the first place, however still remains. There is additional research happening at

DARPA that could help address this challenge by rethinking computer security from the ground up. The Guaranteed Architectures for Physical Security (GAPS) program is looking at more intelligent ways of connecting in-network computers so that these critical assets are not put on computer networks that are directly connected to the Internet. "With GAPS, we are looking at how to filter what is allowed so that a device on the power grid, for example, could still upload everything it needs to, but if someone came in remotely they wouldn't be able to compromise its activities or disrupt the flow of critical data," noted Weiss who is also leading this program.

The second program is SSITH, which stands for System Security Integration Through Hardware and Firmware. SSITH is focused on developing secure processors capable of thwarting common hardware attacks that derive from software vulnerabilities. The secure hardware architectures and associated design tools in development on the program could ultimately be used across a wide array of systems, including those found within the electrical grid.

Provided by DARPA