Grid Modernization Research at Sandia: Cybersecurity

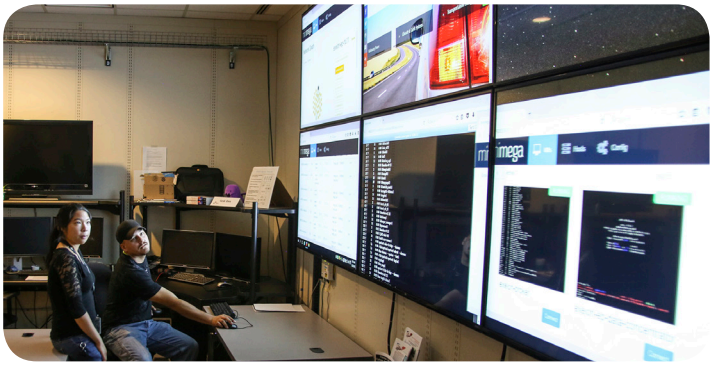
Sandia delivers grid security and grid modernization through research, development, and evaluation of solutions to maintain operations in an adversarial, compromised environment.

Sandia's Grid Modernization Program Vision

The U.S. electricity grid is central to the nation's infrastructure, security, and economy. Modernizing this complex system of interconnected networks and enhancing its resiliency ensures seamless, efficient availability of low-cost, reliable, and secure electricity. Sandia National Laboratories supports this effort as a national research leader in cross-disciplinary fields including grid integration, cybersecurity, power electronics, microgrids, microsystems, materials science, energy storage, and transportation.

The laboratory's grid modernization cybersecurity work includes:

- **grid control monitoring using advanced analytics** for asymmetric cyber defense
- **risk management and consequence analysis** focused on interdependencies between multiple critical infrastructures
- **situational awareness** across multiple domains simultaneously
- **cyber agility** through Emulytics™
- **supply chain integrity**
- **protocol and firmware** reverse engineering
- **vulnerability assessment** and red teaming



Sandia's SCADA Controls Lab allows for simulating and monitoring virtual cyber attacks on the grid.

The Challenge

Cybersecurity across the national electric grid is made difficult by a highly constrained solution space. Constraints on addressing grid cybersecurity include:

- strong and growing levels of technical ability in the nation's adversaries
- 20-year technology refresh cycle
- limited avenues for utilities to fund security
- system owner reluctance to adding hardware or software that could potentially impact warranties
- a focus on availability over integrity or confidentiality of data

Control system cybersecurity, including grid control, has operated as a niche for some time. That status is ending, however, as the nation's grid now operates in a world where grid vulnerabilities can be easily discovered through open Internet research.

Sandia's Solution

Cybersecurity work at Sandia leverages extensive federal investment over many decades and the laboratory's 60-year history ensuring a safe, reliable nuclear stockpile. Since the dawn of electronic information processing, Sandia has been required to ensure secure operations from the level of individual computing devices to national-scale networks. This mission has evolved into several unique capability areas that now range far beyond weapon assets.

Sandia's successful early focus on adversary-based vulnerability analysis has resulted in the laboratory serving federal sponsors through more than 300 technical system security assessments. Supply chain integrity has received dedicated analysis from the days when engineering and manufacturing were large Sandia missions through to the modern state where engineering is still a Sandia specific mission

but manufacturing is nationally distributed. Sandia's influential role in the national nuclear security enterprise has led to the development of rigorous risk management capability to help the national enterprise make risk mitigation investment decisions. For example, the laboratory launched a high performance computing (HPC) capability to evaluate engineering results after the Test Ban Treaty eliminated the option of physical nuclear explosion experiments. HPC has evolved in numerous directions, including emulation, analytics, and interdependency-based consequence analysis. In the context of grid security, emulation is vital because experiments at scale are prohibitively expensive to configure on test hardware and excessively risky to run on operational systems. Analytics are also important because cybersecurity needs cannot be met through manual methods; the number of skilled cybersecurity practitioners available is insufficient, and humans cannot react at machine speeds.

Finally, for as long as electromechanical systems have been used in nuclear assets, Sandia has been required to understand their fundamental operations and apply that understanding up to the level of system operation. Sandia's deep technical understanding at all levels gives the lab unique capabilities in communication protocols and the reverse engineering and analysis of computing device firmware.

Research Areas

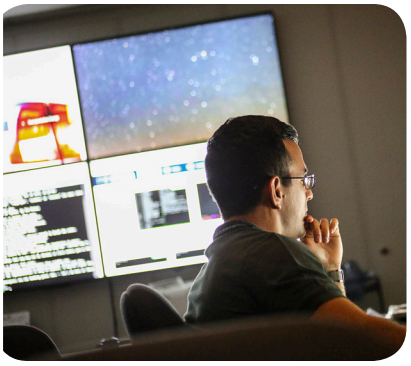
Control System Analytics

Weaselboard is an analytics capability fielded on a federal sponsor's operational systems. Weaselboard provides independent introspection into control system backplane signals such that system compromise is detectable even if the system's computing resources are being deceptive.

Vulnerability Analysis

More than 300 **Information Design Assurance Red Team** projects have been and are being executed across a wide range of targets, from individual embedded systems to global enterprise systems. Sandia has conducted initial assessments of Advanced Concept Technology Demonstrations for military prototypes and assessments for the Defense Advanced Research Projects Agency. This work has been conducted through many years and across diverse sponsors including the energy, finance, manufacturing, and information technology sectors. Federal sponsors have included the Departments of Energy, Defense, Interior, Homeland Security, and State.

Emulytics



For more than a decade, Sandia's **Emulytics™** program has continued to develop a suite of emulation, modeling, and analysis tools for exercises and training that include forensics, predictive simulation, and real-time dynamic defense. Emulytics provides a safe environment in which a broad array of parameters and technologies can be evaluated with an appropriate level of fidelity, without impacts to critical operations. Sandia researchers combine emulated, simulated, and physical test bed environments as appropriate to achieve the required level of fidelity.

Partnerships

In order to ensure the effectiveness and success of cybersecurity research in an environment where utilities rely on commercial integration of security, Sandia partners with commercial entities to both inform and execute research and development. Sandia also partners with diverse federal sponsors on many aspects of cybersecurity, as well as with most other Department of Energy national laboratories.

Impact

Sandia is leveraging decades of federal investment to address the challenge of enabling the modern electric grid to operate in an environment threatened by adversaries. The alternative is a grid that may not operate when the nation most needs it—making the only conscionable approach to leverage every available advantage to ensure that never occurs.

For more information please contact:
Zachary Benz
E-mail: zobenz@sandia.gov
Phone: (505) 284-1510
Website: energy.sandia.gov

Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2016-9339 M.