Energy &
Homeland Security
energy.sandia.gov

SECURING INVERTER COMMUNICATIONS: TAP, ANALYZE AND ACT

As more distributed energy resources (DERs) such as solar photovoltaics (PV) are introduced to the electric grid, securing smart inverters at these sites from cyberattack has become critical for grid protection and resiliency.

INNOVATING SECURITY

To control the flow of power onto the grid from solar PV sites, inverters are used to change direct current to alternating current energy. As smart technology has allowed inverters to become more efficient and flexible, it has also left them vulnerable to cyberattacks.

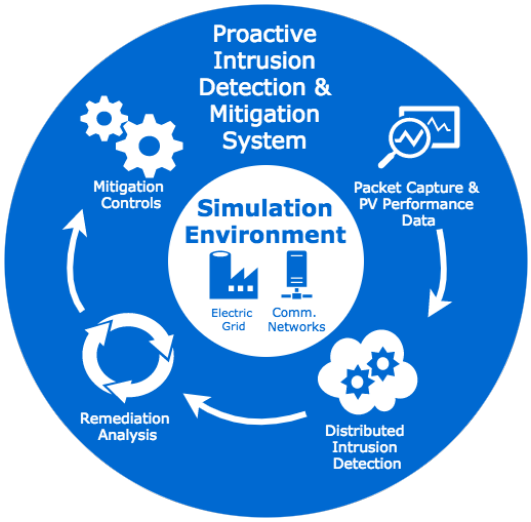
To combat these threats, Sandia is developing a Proactive Intrusion Detection and Mitigation System (PIDMS) sensor that will tap into and analyze cyber-physical data from the DER system. The PIDMS sensor will monitor and store real-time traffic from multiple networks at the same time. Specifically, a hybrid intrusion detection approach will be developed that combines signature- and behavior-based IDS methods and process the cyber-physical data simultaneously.

The PIDMS sensor will also continuously learn system behavior to enable faster detection of attacks and/or abnormal events for DER system operators. Furthermore, the sensor will act by deploying response action to prevent or lessen attacks' impact.

To effectively respond, the PIDMS sensor will evaluate the state of the grid and type of attack detected. The sensor will deploy corrective actions to reduce the magnitude and duration of the attack. Some of these actions can include: resetting inverters to their initial state, disabling future setting changes by preventing communications to the inverter, and triggering network defenses (e.g., moving target defense).

AN ALL-IN-ONE SOLUTION

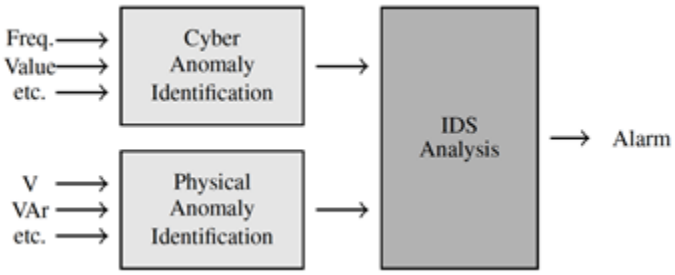
To be truly effective in protecting the grid, a monitoring system that detects cyberattacks should also anticipate attacks and repair or mitigate any damage done. The response actions deployed would be specific to DER system operation and be computed in real-time such that the most effective action is taken for the current system state.



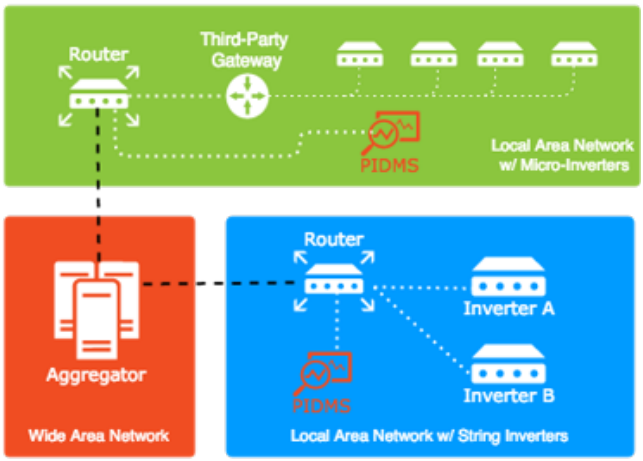
Capabilities of PIDMS sensor.

With an overall goal to create global-scale protection for grid-edge devices, the PIDMS sensor is being built and tested at Sandia, in a high-fidelity emulation environment that combines grid components with advanced communications networks; this environment is being developed with our partners at the Electric Power Research Institute (EPRI) and OPAL-RT Technologies.

PIDMS sensors will be an inexpensive, device-level solution that captures cyber-physical data, detects intrusion, and computes mitigation controls.



Visualization of hybrid IDS approach that will process cyber-physical data.

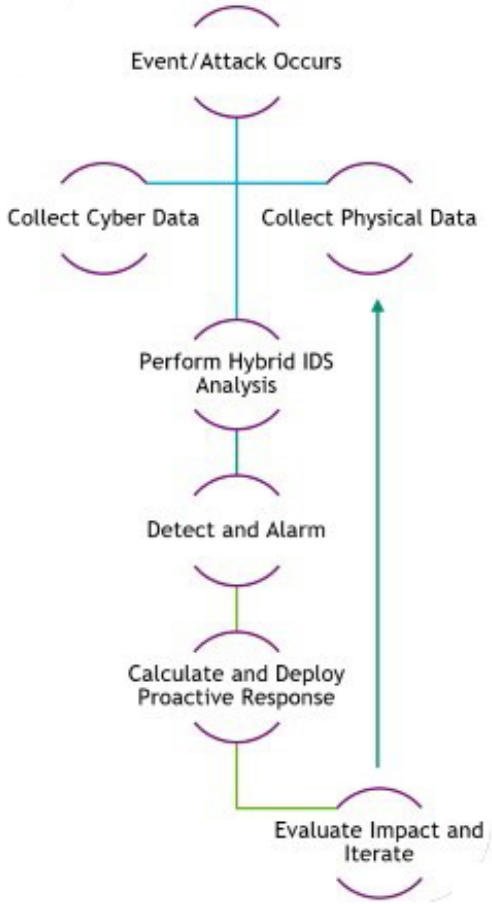


An example of how the distributed PIDMS sensors could be placed in DER systems.

What are the Risks?: With the energy industry relying more on smart technologies for the distribution of power, the risk of cyberattacks is growing exponentially. The electrical grid of the future will be comprised of an increasing amount of solar PV power generation that will use automated and controllable DERs to maintain stability.

Currently there are minimal cyber security defenses for PV systems. Smart inverters are grid-edge devices that have increasing connectivity and automated functions; their communications must be secured. Cyber attackers no longer have to hack into a utility's control center but can gain access to the grid from the site of solar farms through the smart inverters that are used to communicate and access interfaces associated with DERs.

Where to Start: Sandia and its project partners are developing state-of-the-art emulation environment that enables advanced simulation of networked communications, grid operations, and solar PV production; this environment will be used to develop and apply attack scenarios to test the PIDMS sensor against. While this environment is being created, work will commence on creating and testing the PIDMS sensor and its hybrid IDS analysis methodology. The PIDMS sensor will be iteratively tested in the emulation as hardware-in-the-loop (HIL).



The Ultimate Goal: The main goal of this project is to develop a distributed, cost-effective bump-in-the- wire (BITW) PIDMS sensor that will improve the resiliency of DER systems; it will be capable of analyzing network and PV performance data simultaneously, detecting various types of cyberattacks, and deploying remedial actions to prevent or lessen impact to the overall DER system.

CONTACT:

Shamina Hossain-McKenzie
Principal Investigator
shossai@sandia.gov
energy.sandia.gov
Phone: (505) 844-7454

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2012-5572OP.