MARKET SHEET

Proactive Intrusion Detection and Mitigation Systems (PIDMS)

Sandia National Laboratories

PIDMS detects and mitigates cyberattacks to energy utilities and other distributed energy resources in real-time

US Patent Pending

Technology Readiness Level 5

Overview

The Proactive Intrusion Detection and Mitigation System (PIDMS) is an award-winning sensing and monitoring system that detects cyberattacks and secures grid-edge photovoltaic (PV) smart inverters capable of making autonomous decisions to stabilize the grid. Smart inverters and other equipment are used in distributed energy resources (DER) systems, such as rooftop solar photovoltaic units or wind turbines.

Market Need

As new DERs come online, this also brings new opportunities for disruptions and breaches. Customers such as energy utilities, utility photovoltaic (PV) sites, grid cybersecurity defenders, solar power companies, private PV owners and aggregators, PV inverter manufacturers, and grid smart-device manufacturers have struggled to find reliable, affordable protection.

PIDMS provides grid-edge situational awareness for cybersecurity defense by capturing real-time DER network traffic and performance data with a novel approach that improves the detection and prevention of cyber-physical attacks.

Sandia's Approach

PIDMS secures smart inverters and grid-edge devices that have increasing connectivity and automated functions. For example, rather than hacking into a utility's control center, cyber attackers can gain access to the grid from a solar farm's smart inverters. PIDMS has numerous capabilities, including:

- Accessing and analyzing cyber-physical data from the DER system
- Anticipating attacks
- Repairing or mitigating damage

Competitive Advantage

Compared with other solutions, PIDMS is reliable, affordable, and versatile. The PIDMS sensor leverages cyber-physical data and operates at the grid-edge to achieve distributed, device-level defense. It detects and alerts adversarial activity, as well as automatically takes preventative and/or mitigative actions.

Although other grid cybersecurity tools are being developed, they focus only on cyber data and transmission systems. PIDMS technology fills security gaps by incorporating grid-edge systems, devices, and associated physical data to achieve defense-in-depth cybersecurity assessment and solutions.

MARKET SHEET

Proactive Intrusion Detection and Mitigation Systems (PIDMS)

Sandia National Laboratories

Features & Technical Benefits

PIDMS is a hybrid Intrusion Detection System (IDS) approach that combines signature and behavior-based techniques and processes, as well as cyber-physical data:

- Distributed, real-time cyber-physical detection and mitigation analysis.
- Provides cybersecurity defense for grid-edge systems.
- Analysis framework that can be extended to provide situational awareness across the transmission, distribution, and DER systems.
- Uses network IDS tools Zeek and Snort for cyber data collection and signature-based analysis.
- Leverages ML algorithms for behavior-based IDS analysis, specifically adaptive resonance theory artificial neural network.
- Simultaneous online learning and detection via incremental learning.

The PIDMS has been tested with Modbus, DNP3, and IEEE 2030.5 communications, is capable of performing deep-packet inspection with Modbus and DNP3, and is able to only identify IEEE 2030.5 traffic.

Applications & Industries

- Grid cybersecurity
- Distributed energy resource cybersecurity
- Distributed intrusion detection system
- Cyber-physical analysis
- Grid resilience
- Industrial control systems

Awards & Recognition

In 2022, PIDMS received an R&D 100 Award for the Software/Services category as well as the R&D 100 Silver Market Disruptor Award.

Next Steps

Sandia is seeking partners to develop and commercialize this technology. To learn more, contact Sandia National Laboratories' Licensing and Technology Transfer office.

Contact Us SD# 15424

ip@sandia.gov ip.sandia.gov

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

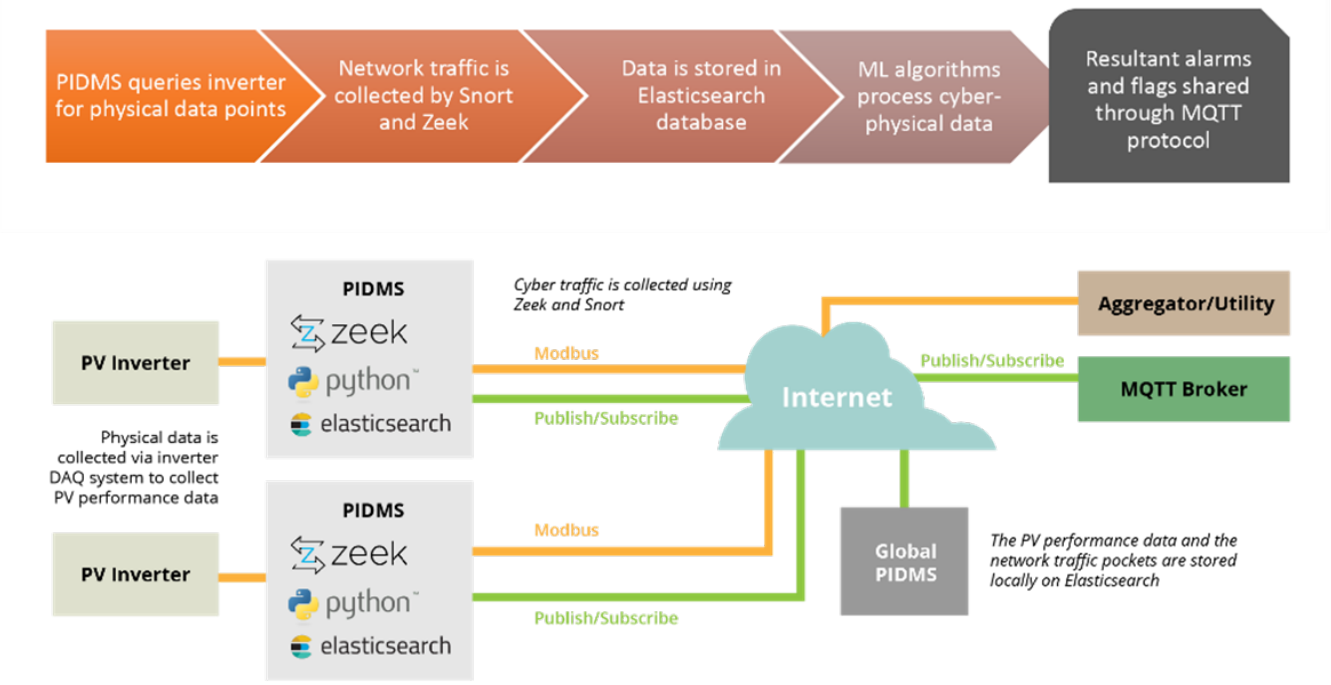
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. SAND2023-01393M

MARKET SHEET

Proactive Intrusion Detection and Mitigation Systems (PIDMS)

Sandia National Laboratories

Technical Figure



Above: Overview of PIDMS cyber-physical analysis process and an example of bump-in-the-wire implementation in a two inverter system.

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-NA-0003525. SAND2023-01393M