MARKET SHEET

# griDNA

Sandia National Laboratories

## griDNA leverages AI analytics and cyber-physical situational awareness to enhance effective power grid operations by transforming critical infrastructure monitoring

**Patent Pending**

**Technology Readiness Level (TRL) 4**

### Business Problem

Current monitoring solutions for critical infrastructure systems operate in silos, focusing either on network traffic from cyber systems or physics based measurements from physical systems. This fragmented approach creates significant gaps in situational awareness because operators lack a unified view of how cyber and physical events interact.

Without integrated monitoring, it becomes challenging to detect and respond to disturbances that may originate from either domain or arise from their interdependencies. This can lead to delayed responses to disturbances and vulnerabilities, reducing system resilience.

For instance, a cyberattack on an operational technology network may not be immediately recognized as impacting physical operations, leading to cascading failures across the infrastructure.

### Customer Need

Operators of critical infrastructure systems require a comprehensive monitoring solution that provides real-time insights into both cyber and physical states to achieve Cyber-Physical Situational Awareness (CPSA).

They need early indicators of potential disturbances, improved planning capabilities, and enhanced coordination between cyber defenders and physical system operators to mitigate risks effectively.

### Sandia Approach

Sandia researchers have developed griDNA which offers a multilevel CPSA solution that integrates advanced data fusion and AI/ML techniques such as autoencoder neural networks. By deploying sensors at local, enclave, and global levels, griDNA collects and analyzes data concurrently, providing a holistic view of interconnected systems. This architecture enables localized analysis and early detection of anomalies, which can be escalated for broader awareness and action.

## Competitive Advantage

griDNA offers several key advantages in the market. Unlike existing monitoring systems that operate independently, griDNA uniquely fuses cyber-physical data to deliver a unified perspective on system health. Its AI/ML capabilities adapt to changing conditions, allowing for real-time classification of events and automatic connections between operators and defenders. This innovative approach not only enhances cybersecurity but also optimizes operational processes.

## Benefits

griDNA offers:

- Comprehensive CPSA: Achieve situational awareness across interconnected systems.
- Early Warning Indicators: Detect potential disturbances before they propagate.
- Improved Planning and Operations: Gain insights into interdependencies to enhance system resilience.
- Flexible Deployment: Utilize low-cost, plug-and-play solutions suitable for resource-constrained environments.

## Industries & Applications

- Water supply
- Transportation
- Telecommunications
- Electric utilities
- Natural gas systems

## Next Steps

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


**Contact Us**
SD 16375

ip@sandia.gov

ip.sandia.gov

## Technical Figures

### griDNA sensor and architecture design

**Local griDNA (Lg)**

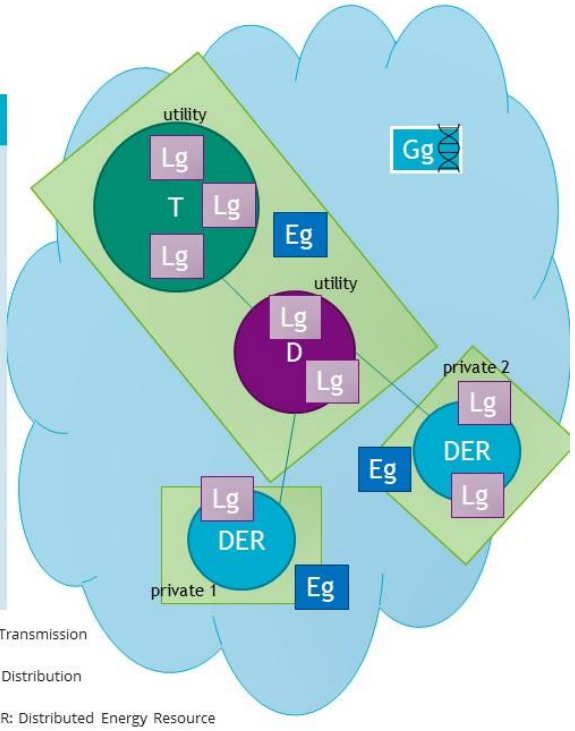
- Raw Cyber Data
- Raw Physical Data
- Single node
- Peer-to-peer communication
- Classification (input as feature to enclave; time)
- Feature extraction (low-level)

**Enclave griDNA (Eg)**

- Raw cyber data
- Raw physical data
- Local griDNA classification output
- Other local sensor input (e.g., PIDMS)
- Feature extraction (higher-level)
- Classification (time)
- Alerting
  - Alert other griDNA of issues that may propagate
  - Alert mitigation tools and operators to isolate certain parts of the system

**Global griDNA (Gg)**

- No raw data input
- Enclave griDNA classification result
- Aggregate CPSA results
  - Affected areas/nodes
  - Causality of events
  - Cyber-physical event correlation
  - Inform cyber-physical mitigation
- Visualization dashboard to inform operators/owners




T: Transmission

D: Distribution

DER: Distributed Energy Resource

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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. SAND 2025-04196M