Protecting Critical Facilities with Next-Generation Data Diodes

Case Study: Fend's 2021 ESTCP "Project of the Year" Award-Winning Project with the US Army Corps of Engineers

Key Findings

Data diode technology can be used to transmit machine telemetry data or log files. → The technology provides a physical barrier to cyberattacks on facility-related control systems. → Next-generation data diodes are cost-effective for secure performance data collection.

ESTCP Data Diode Evaluation Project

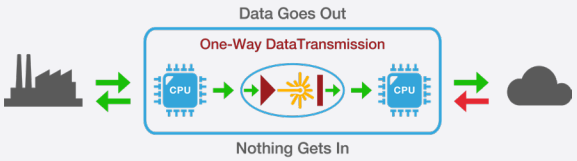
Cyberattacks are one of the fastest growing threats to information technology (IT) and operational technology (OT) infrastructure at Department of Defense (DoD) installations. The DoD Environmental Security Technology Certification Program (ESTCP) sought innovative and cost-effective cyber defense solutions to improve the use, access and quality of utility- and facility-related data for:

- Greater efficiency and resilience
- Improved demand management and decision making
- Optimal operation and maintenance of military facilities and installations

Working with Fend, the ESTCP evaluation validated, tested and demonstrated the cost performance and market potential of next-generation data diode technology in reducing environmental risks and improving efficiency for DoD end users.

Data Diode Technology Overview

Data diodes, also known as "one-way communication diodes," have served as physical barriers to cyberattacks for intelligence operations and highly critical infrastructure like nuclear reactors for years.



Securing Critical Facilities while Physically Blocking Cyberattacks

Diode technology sends information in a one-way fashion using light that can't be reversed. Designed for deployment across FRCS, microgrids and SCADA, diodes optically isolate OT equipment from lower-security networks with the physical security of an air gap while blocking cyberthreats.

ESTCP Evaluation Results

- Can this new class of US-made hardware provide a cost-effective alternative to other methods of performance data extraction?
- Is the technology broadly applicable across DoD's legacy and new operational technology (OT) portfolio?
- Do these devices provide a physical barrier to cyberattack?

The data diode technology was evaluated to determine performance across cybersecurity, compatibility with DoD's equipment portfolio, and cost effectiveness.

Evaluation Project Results

The evaluation conducted 2019-2022 showed that one-way data diodes enable greater situational awareness, efficiency and resilience by providing access to real-time information that was previously locked behind an air gap while blocking cyberattacks. Testing confirmed:

- Outside attempts to send data upstream were blocked
- Equipment functioned normally when connected to the diode
- Diodes transmitted data using common industry protocols
- Installation time/costs were lower than legacy solutions by 90% or more
- The diode is cost effective relative to other secure data collection methods

Financial Performance

Industrial data diodes outperform other methods of secure data extraction from facility-related control systems (FRCS) on an economic basis. These data diodes have both lower first and ongoing costs than separate local area networks (LAN) for controls or hardwired input/output interfaces. Industrial data diodes pay for themselves relative to firewalls in 1 to 4 years, and relative to use of physical media (CDs, hard drives, etc.) in 0.4 to 2.4 years.

Learn more about this project at www.serdp-estcp.org or read the article in The Military Engineer magazine at https://samenews.org/tme-september-october-2022/

Evaluation Methodology

The project team included Fend Incorporated and the USACE Engineer Research and Development Center, Construction Engineering Research Lab (ERDC-CERL). Tests fell into two main categories: functional tests and cybersecurity tests. Functional testing was conducted at CERL's facilities in Champaign, Illinois. This evaluation involved sending data from a variety of controller types using several common industry protocols (Modbus, LonTalk, BACnet, FTP).

Long-term tests involved data collection from running building systems to test reliability and accuracy. Cybersecurity testing included penetration tests designed to mimic attacks by those who would try to send information across the data diode in the reverse direction or otherwise disable the hardware. Testing was completed by the Army's Threat Systems Management Office (TSMO) at Redstone Arsenal and the Navy's Control System Test Bed at Port Hueneme.

Conclusions / Implications

Data diode technology has evolved to a price point and usability to make it a practical, higher-security alternative to both traditional IT defenses (software, firewalls, and intrusion detection systems) and legacy data diodes. When applied to the extraction of data from facility-related control systems, data diodes can securely provide streams of data to be used by work order management systems and predictive analysis software to help maintenance teams work more efficiently.

Fend Project Team Acknowledgements

Department of Defense Environmental Security Technology Certification Program (ESTCP), Engineer Research & Development Lab (ERDC-CERL) Construction Engineering Research Lab, U.S. Army Corps of Engineers (USACE) Army Threat Systems Management Office (TSMO), and Navy Control System Test Bed-Port Hueneme

2021 ESTCP PROJECT OF THE YEAR

Block Cyberattacks on Operational Technology

One-Way Data Diodes Ensure Safe Monitoring of Your Equipment from Anywhere

Monitor Facility-Related Control Systems and Microgrids while Fending Off Attackers to Keep Critical Infrastructure Online!

Securely send equipment data and monitor new and legacy equipment so you always know what's happening with your microgrids. Data diodes safely bring microgrids online using a physically enforced one-way data flow that protects them from cyberattack so you can stay ahead of emergencies.

Get the operational intelligence you need and the security you deserve.

Connect remote equipment to your network, even when it's off the beaten path. Data diodes send sensor data to your organization's servers or the cloud for optimized operational awareness and efficiency.

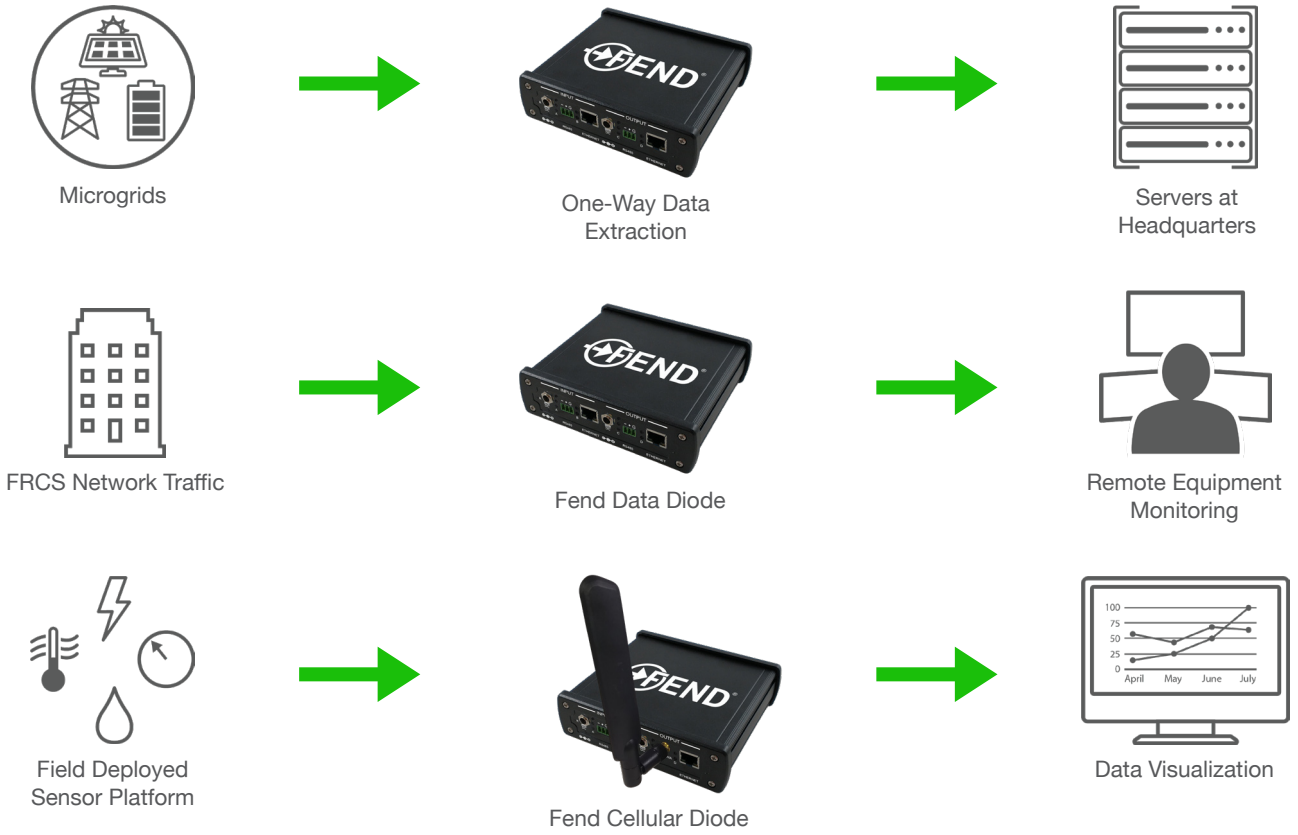
Listen to facility-related control system network traffic and send relevant data to on- or off-premise servers for storage or analysis. Prioritize maintenance tasks and equipment upgrades. Fend supports Modbus, BACnet, and other communication protocols.

Integrate real-time operational data into your centralized control center without putting your critical equipment at risk. Predictive analytics help you detect equipment failures before they happen.

Fend's data diodes are made in the USA.

Learn more at http://www.fend.tech/products

Fend Off Attackers with Physical Cybersecurity



In September 2021, the Department of Homeland Security (DHS) Critical Infrastructure Security Agency (CISA) recommended the use of "one-way communication diodes to protect the boundary of the control system" in Critical Infrastructure Control Systems Cybersecurity Performance Goals And Objectives. Learn more at https://www.cisa.gov/ control-systems-goals-and-objectives