

FINAL REPORT

Low-Cost, Plug-and-Play Data Diodes for Protection and Monitoring of DoD Facility Equipment

January 2022

Colin Dunn
Fend Incorporated



ESTCP Project EW19-5156

DISTRIBUTION STATEMENT A
This document has been cleared for public release.

This report was prepared under contract to the Department of Defense Environmental Security Technology Certification Program (ESTCP). The publication of this report does not indicate endorsement by the Department of Defense, nor should the contents be construed as reflecting the official policy or position of the Department of Defense. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the Department of Defense.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188		
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 27-01-2022		2. REPORT TYPE ESTCP Final Report		3. DATES COVERED (From - To) 23 Aug 2019 - 27 Jan 2022	
4. TITLE AND SUBTITLE Low-Cost, Plug-and-Play Data Diodes for Protection and Monitoring of DoD Facility Equipment - Final Report			5a. CONTRACT NUMBER W912HQ19C0048		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Dunn, Colin P. Patel, Tapan C.			5d. PROJECT NUMBER EW19-5156		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Fend Incorporated 4600 Fairfax Dr Ste 410, Arlington, VA 22203 USACE Construction Engineering Research Laboratory 2902 Newmark Dr, Champaign, IL 61822			8. PERFORMING ORGANIZATION REPORT NUMBER EW19-5156		
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Environmental Security 4800 Mark Center Drive, 16F16 Technology Certification Prog Alexandria, VA 22350-3605			10. SPONSOR/MONITOR'S ACRONYM(S) ESTCP		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S) EW19-5156		
12. DISTRIBUTION / AVAILABILITY STATEMENT DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The objective of this project is to demonstrate that Fend's low-cost, easy-to-install data diode provides the security of an air gap between high-security and low-security networks while increasing the accessibility and quantity of data to managers across DoD in order to enhance energy and water management and operational efficiency. The functional tests showed that the diode was able to successfully send files and streams of data in a variety of common protocols, enabling the collection of facility performance data in an efficient manner. Cybersecurity testing showed the data diode's ability to block malicious data transmissions and withstand outside attacks. These results show both the capabilities and limitations of the current state of this technology. Data diode technology may not be appropriate for system designs requiring the transmission of both outbound telemetry and incoming commands (requiring a two-way connection), but for systems where remote monitoring of data is used to inform actions by human operators this technology can provide security and access to information.					
15. SUBJECT TERMS Data diode, one-way communication diode, unidirectional gateway, facility related control systems, FRCS, cybersecurity, data acquisition, network segmentation					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UNCLASS	18. NUMBER OF PAGES 66	19a. NAME OF RESPONSIBLE PERSON COLIN DUNN
a. REPORT UNCLASS	b. ABSTRACT UNCLASS	c. THIS PAGE UNCLASS			19b. TELEPHONE NUMBER (include area code) 571-970-1382 X700

FINAL REPORT

Project: EW-5156

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	ES-1
1.0 INTRODUCTION	1
2.0 TECHNOLOGY DESCRIPTION	2
2.1 ADVANTAGES AND LIMITATIONS OF THE TECHNOLOGY	4
3.0 TECHNICAL PERFORMANCE OBJECTIVES	6
3.1 SUMMARY OF PERFORMANCE OBJECTIVES	6
3.2 PERFORMANCE OBJECTIVES DESCRIPTIONS	7
4.0 MATERIALS AND METHODS	10
4.1 TESTING OVERVIEW AND ASSIGNMENTS	10
4.2 PO-1 – TSMO AND CSTB	10
4.2.1 Test Location	10
4.2.2 Test Design	11
4.3 PO-2, 3, 4, AND 5 - CSTL	13
4.3.1 Test Location	13
4.3.2 Test Design	14
4.3.3 Performance Assessment	21
4.4 PO-6 - FEND INCORPORATED	21
4.4.1 Cost Assessment	21
5.0 RESULTS AND DISCUSSION	23
5.1 PO-1 TEST RESULTS	23
5.1.1 TSMO Penetration Test Results	23
5.1.2 CSTB Penetration Test Results	24
5.2 PO-2, 3, AND 5 TEST RESULTS	26
5.2.1 Objective	26
5.2.2 Architecture	26
5.2.3 List of CSTL tests	28
5.2.4 List of CERL tests	28
5.2.5 Data Analysis	30
5.3 PO-4 RESULTS	45
5.4 PO-6 RESULTS	45
5.4.1 Cost Assessment Results	45
6.0 CONCLUSIONS AND IMPLICATIONS FOR FUTURE RESEARCH/IMPLEMENTATION	48
7.0 LITERATURE CITED	49

TABLE OF CONTENTS (Continued)

	Page
APPENDIX A	SUPPORTING DATA..... A-1
APPENDIX B	LIST OF SCIENTIFIC/TECHNICAL PUBLICATIONS..... B-1
APPENDIX C	OTHER SUPPORTING MATERIALS..... C-1

LIST OF FIGURES

	Page
Figure 1. Conceptual Schematic of Fend’s Data Diode Solution.	2
Figure 2. Fend’s Latest Data Diode.	3
Figure 3. Fend Diode Equipped with Cellular Outbound.	3
Figure 4. Fend Offers the Security of Traditional Data Diodes at a Far More Affordable Price.	4
Figure 5. Fend Data Diode Connection Interfaces	12
Figure 6. Fend Data Diode Testing Architectures	12
Figure 7. US Army Construction Engineering Research Laboratory in Champaign, IL.....	13
Figure 8. Scenarios for Fend Diode Implementation in DOD CS 5 Level Architecture	15
Figure 9. CSTL Diode Architecture	26
Figure 10. i.Lon 600	29
Figure 11. Screenshot of UMCS for Building 3 - West at CERL	29
Figure 12. Solar House Facility	30
Figure 13. Test 3 Baseline Wireshark.....	31
Figure 14. Test 3 – Baseline BACnet Wireshark Output (Detailed)	32
Figure 15. Test 3 Baseline CASBACnet Tool.....	32
Figure 16. Test #4 Baseline Packet Capture	34
Figure 17. Test #4 Post-Retrofit Data	35
Figure 18. Test #5 Baseline Wireshark Summary	35
Figure 19. Test #5 Baseline (Detailed), Relative Humidity	36
Figure 20. Test #5 Baseline (Detailed), Temperature.....	36
Figure 21. Test #5 Post-Retrofit, Relative Humidity	37
Figure 22. Test #5 Post Retrofit, Temperature	37
Figure 23. Test #6 Baseline Wireshark Capture	38
Figure 24. Test #6 Wireshark Modbus Details	38
Figure 25. Test #6 Post Diode Data.....	39
Figure 26. Test #5 Post Diode Setpoint Change.....	39
Figure 27. Test #6 Post Diode Temperature Reading.....	39
Figure 28. Test #11 Baseline Wireshark Capture	41
Figure 29. Niagara Front-End Export	41
Figure 30. Post Retrofit Diode Output.....	42
Figure 31. Test #12 Baseline Wireshark Capture	43
Figure 32. Niagara Front-End Export	44
Figure 33. Post Retrofit Diode Output.....	44

LIST OF TABLES

	Page
Table 1. Summary of Project Results by Objective	2
Table 2. Performance Objectives	6
Table 3. Test Leads by Performance Objective	10
Table 4. LON Controls Network Test Equipment List	16
Table 5. BACNET Controls Network Test Equipment List	16
Table 6. Mixed Controls Network Test Equipment List (Including Modbus).....	16
Table 7. Other Supporting Hardware / Software	17
Table 8. Fend Data Diode Test Locations and Configurations	17
Table 9. Cost Assessment Technologies Considered.....	22
Table 10. Summary of Project Results by Objective with Metric	23
Table 11. Summary of TSMO Tests and Findings	24
Table 12. Summary of CSTB tests and findings.....	25
Table 13. Hardware and Device Schedule by Scenario	27
Table 14. List of CSTL Tests.....	28
Table 15. List of CERL Tests	29
Table 16. Cost and Security Comparison Between Data Diodes and Common Alternatives	46

ACRONYMS AND ABBREVIATIONS

ACAS	Assured Compliance Assessment Solution
AHU	Air Handling Unit
BAS	Building Automation System
CAGE	Commercial and Government Entity
CAN	Controller Area Network
CERL	Construction Engineering Research Laboratory
CSTB	Control System Test Bed
CSTL	Control System Test Lab (at CERL)
CRN	Closed Restricted Network
DISA	Defense Information Systems Agency
DoD	Department of Defense
DOE	Department of Energy
DUNS	Data Universal Numbering System
ERDC	Engineer Research and Development Center
ESTCP	Environmental Security Technology Certification Program
FRCS	Facility Related Control System
GSA	General Services Administration
HVAC	Heating, ventilation, and air-conditioning
ICS	Industrial Control Systems
IoT	Internet of Things
IIoT	Industrial Internet of Things
ISAC	Information Sharing and Analysis Center
IT	Information technology
I/O	Input / output
LAN	Local area network
NAVFAC	Naval Facilities Engineering Command
NIST	National Institute of Standards and Technology
OBD	On-board diagnostics
ODC	Other direct cost
R&D	Research and development
RDE	Research and Development Enterprise Network (at CERL)
RMF	Risk Management Framework

RTU	Rooftop (air-conditioning) unit
SF	Square feet
SME	Subject matter expert
TRL	Technology readiness level
TSMO	Army Threat System Management Office
UFC	Unified Facilities Criteria
UMCS	Utility monitoring control system
USACE	US Army Corps of Engineers
VPN	Virtual Private Network

KEYWORDS

Data diodes, unidirectional gateways, one-way communication diodes, equipment monitoring, cybersecurity hardware, CERL, IIoT, penetration testing, cybersecurity, facility-related control systems, UFC 4-010-06, Fend.

ACKNOWLEDGMENTS

This project was able to successfully demonstrate the performance of the technology because of the support of several teams and organizations. The Principal Investigator (PI) would like to thank the following contributors:

ESTCP: The Energy and Water (EW) Program team led by Tim Tetreault saw the potential of data diode technology to strengthen and simplify cyber defenses across DoD's building and equipment portfolio. The ESTCP team's selection of this project provided the project team with access to stakeholder feedback, testing resources, technology transfer activities, and product enhancement that would not have otherwise been possible during the project's duration.

Engineer Research and Development Center, Construction Engineering Research Lab (ERDC-CERL): The CERL team, led by Tapan Patel, provided analytical rigor, facilities, expertise, and feedback that accelerated the technology's maturity and strengthened the chances for rapid deployment and commercialization.

The Fend engineering team: The team's agility and skill allowed for rapid enhancements when initial testing required hardware or firmware changes. Some of these changes were required to support an evaluation project that occurred largely during a global pandemic, and those changes led to better, easier-to-use products that have won favor with early adopters.

The Army's Threat Systems Management Office (TSMO): The team's rigorous approach to testing provided valuable information that helped enhance the security of the data diodes under evaluation.

NAVFAC's Control System Test Bed (CSTB): The team at Port Hueneme validated Fend's design premise while providing valuable insight into ways to accelerate adoption of this data diode technology across Federal IT/OT applications.

EXECUTIVE SUMMARY

OBJECTIVES

The objective of this project is to demonstrate that Fend's low-cost, easy-to-install data diode provides the security of an air gap between high-security and low-security networks while increasing the accessibility and quantity of data to managers across DoD in order to enhance energy and water management and operational efficiency. To ensure the product can achieve this goal, the project focused on the following specific performance objectives:

- Complete isolation of protected equipment
- Uninterrupted equipment operation
- Interoperability with various equipment
- Ease of installation
- Data transmission to desired network location
- Cost performance

TECHNICAL APPROACH

Managers of facilities and equipment across the Department of Defense, energy infrastructure, water treatment, and other critical sectors need real-time operational intelligence to improve efficiency and resilience. Integration of this equipment, from legacy facility related control systems (FRCS) to new microgrids, into remote monitoring environments or the industrial internet of things (IIot) can help managers prioritize investment and maintenance personnel labor. The connectivity that makes these advancements possible has traditionally opened the door to attackers who would steal data, inject ransomware, and modify or destroy equipment through changes to setpoints and firmware. The economic and mission benefits of real-time monitoring are great enough that operators continue to bring this equipment online with defenses borrowed from the information technology (IT) world that are not well-suited to operational technology (OT) environments. Firewalls require patches and updates that only protect against known threats and prepare the user for yesterday's war. Software and intrusion detection systems alert operators after an attacker may have already caused irreparable harm to an industrial system.

Data diodes (also known as one-way communication diodes or unidirectional gateways) are security appliances that enable a physically-enforced, one-way information stream about the state of this equipment. These devices use light as the medium to transmit data from one side to the other, physically isolating the equipment from lower-security networks. 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 its release of [*Critical Infrastructure Control Systems Cybersecurity Performance Goals And Objectives*](#). Legacy data diodes are used today to protect the most critical of assets, like nuclear power plants, but at an expense often exceeding \$100,000 per connection. Diode customization has historically added to the cost and complexity of this technology.

Fend's next-generation data diode is a low-cost device that provides the physically-enforced one-way data transfers of one-way communication diodes while removing the need for extensive on-site configuration. On-board processors enable the data diode to communicate with protected equipment using common protocols and communicate this information to an on-site network or cloud service. Fend's data diode would serve the unmet needs of critical infrastructure managers across DoD by quickly enabling secure access to equipment data. For example, performance data collected as part of an energy savings performance contract (ESPC) is often done through physical retrieval of hard drives. This process can cost thousands of dollars in travel and labor and result in stale data that may be 6 months old. A continuous stream of data sent through a data diode could be obtained with data diodes for less than the cost of one business trip.

To test the objectives listed above, the project team including Fend Incorporated and the USACE Engineer Research and Development Center, Construction Engineering Research Lab (ERDC-CERL) performed and oversaw tests that 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, Lon, BACnet, FTP). Long-term tests required 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 (CSTB) at Port Hueneme.

RESULTS

The functional tests showed that the diode was able to successfully send files and streams of data in a variety of common protocols, enabling the collection of facility performance data in an efficient manner. Cybersecurity testing showed the data diode's ability to block malicious data transmissions and withstand outside attacks. The following summarizes results by objective:

Table 1. Summary of Project Results by Objective

Objective	Success	Summary
Unidirectional Flow	Yes	Blocked outside attempts to send data upstream
Non-interference	Yes	Equipment functioned normally when connected to diode
Compatibility	Yes	Transmitted data using the industry protocols tested
Ease of Installation	Yes	Installation generally took less than one hour
Data Collection	Yes	Data sent across diode was complete / accurate
Cost Performance	Yes	Cost-effective relative to other secure data collection methods

These results show both the capabilities and limitations of the current state of this technology. Several of the most common communication standards can be accommodated with this technology, but some projects may require additional equipment and effort to convert data into a supported format (such as proprietary OEM-specific protocols). Some data-intensive projects may exceed the transmission bandwidth of these devices. Data diode technology may not be appropriate for system designs requiring the transmission of both outbound telemetry and incoming commands (requiring a two-way connection), but for systems where remote monitoring of data is used to inform actions by human operators this technology can provide security and access to information.

BENEFITS

For applications where a one-way stream of information would satisfy the technical requirements of a facility management approach (e.g.: equipment status monitoring), this class of industrial data diode can prove a secure, cost effective option relative to manual data collection or data transfers using physical media. These devices have the potential to open the door to Federally-approved, cloud-based tools that make use of predictive analytics and machine learning. By providing access to information that was previously locked behind an air gap, these next generation of data diodes can enable greater operational efficiency and resilience.

OBJECTIVE

The objective of this project is to demonstrate that Fend's low-cost, plug-and-play data diode provides the security of an air gap between high-security and low-security networks while increasing the accessibility and quantity of data to managers across DoD in order to enhance energy and water management and operational efficiency.

To ensure the product can achieve this goal, the project focused on the following specific performance objectives:

- Complete isolation of protected equipment
- Uninterrupted equipment operation
- Interoperability with various equipment types
- Ease of installation
- Data transmission to desired network location
- Cost performance

1.0 INTRODUCTION

Managers of critical infrastructure benefit from the situational awareness provided by remote monitoring.¹ This information leads to improved equipment performance and reduced unplanned downtime. However, this connectivity creates vulnerabilities to cyberattack. Recent attacks on US and international power grids, energy infrastructure, and building systems highlight the need for improved security on the industrial internet of things.^{2,3} Relatively few manufacturers provide the majority of control systems, exacerbating the impact of a distributed cyberattack. Legacy systems often run outdated, unsupported operating systems and will never receive security patches. Firewalls and software-based security are vulnerable to compromise by hackers. Without a cost-effective security solution, much of this equipment is left disconnected from the network (“air-gapped”) and unmonitored.

Data diodes are security appliances that enable a physically-enforced, one-way information stream about the state of this equipment. These devices use light as the medium to transmit data from one side to the other, physically isolating the equipment from lower-security networks. Data diodes are used today to protect the most critical of assets, like nuclear power plants, but at an expense often exceeding \$100,000 per connection. On-site diode configuration adds to the cost and complexity of this technology.

Fend’s data diode is a low-cost device that provides the physically-enforced one-way data transfers of one-way communication diodes (also known as unidirectional gateways) while removing the need for extensive on-site configuration. On-board processors enable the data diode to communicate with protected equipment using common protocols and communicate this information to an on-site network or cloud service. Fend’s data diode would serve the unmet needs of critical infrastructure managers across DoD by quickly enabling secure access to equipment data.

Fend’s solution enables the following:

- Delivery of complete and accurate information to decision makers with minimal data processing.
- Compliance with cybersecurity requirements for handling facility-related data.
- Enhancement of energy analytics, demand management, and reporting capabilities.
- Reduction of time and cost associated with installing and connecting data points to existing systems.
- Integration with data from multiple disparate sources to create higher value information.
- Improvement of the operational efficiency of facility managers and maintenance staff.

To operate in today’s OT cyber threat landscape, operational technology solutions must provide a greater level of security required by Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.⁴ This technology could be applied to any facility across DoD components, particularly those with geographically dispersed equipment that is unmonitored today. Some 85% of industrial and mechanical equipment currently goes without remote monitoring, requiring expensive manual inspection and providing no real-time information about performance or impending failure.⁵

2.0 TECHNOLOGY DESCRIPTION

Traditionally, operators have relied on firewalls and software-based security to limit access to industrial control systems (ICS). Some of these solutions provide protection at the edge, whereas others rely on cloud-based machine learning to detect an attack. However, the patches and updates to these systems always lag behind cybersecurity weaknesses, leaving infrastructure managers vulnerable to current and future threats. With attackers using unlimited cloud computing, rentable botnets, and artificial intelligence, some malicious code is going to get through these defenses.

Data diodes are security appliances that enable a physically-enforced, one-way information stream about the state of ICS equipment. These devices use light as the medium to transmit data from one side to the other, physically isolating the protected equipment from lower-security networks (an alternative to the approach of hardware I/O interfaces described in Appendix F of UFC 4-010-06: Cybersecurity of Facility-Related Control Systems⁶). Data diodes are used today to protect the most critical of assets, like nuclear power plants, but at an expense often exceeding \$100,000 per connection. On-site diode configuration adds to the cost and complexity of this technology. A simpler-to-use, lower-cost alternative would serve the unmet needs of critical infrastructure managers across DoD by quickly enabling secure access to equipment data.

Fend has developed a new type of data diode to protect a much broader set of equipment and facilities than are served by current data diodes. Fend's goal is to reduce the cost of data diode protection by 90% or greater. This new data diode is designed to be the easiest way to connect equipment to a less secure network, improving upon methods described in UFC 4-010-06, Appendix F. Fend's data diode has on-board microprocessors that enable the transition from a two-way data connection to the light-based, one-way network connection. This arrangement prohibits any malicious code from reaching the protected equipment.

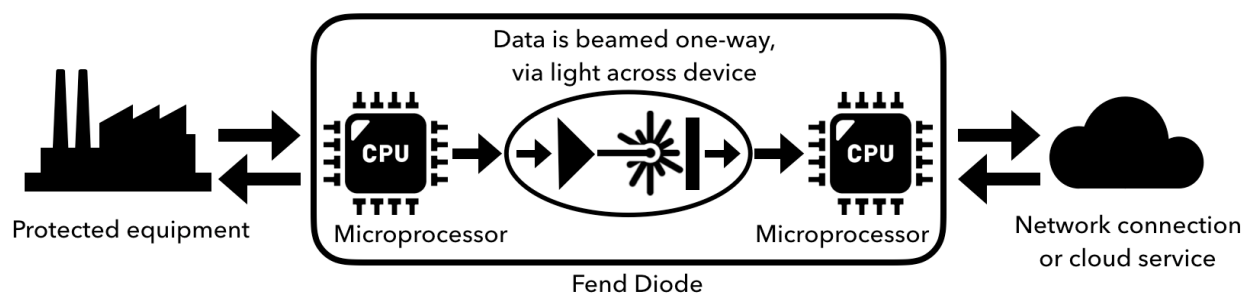


Figure 1. Conceptual Schematic of Fend's Data Diode Solution.

On-board computing capacity enables connection to the protected equipment and sends data to the desired network location.

The hardware's key innovation is its ability to speak multiple machine languages / protocols and connect to a variety of equipment types and manufacturers. Traditional data diodes require trained network engineers to setup. Fend's goal is to have any controls technician or maintenance person be able to install the device in minutes.

Fend's new type of data diode has been made more affordable by right-sizing the equipment to the data streams required for mechanical and industrial equipment monitoring. Incumbent data diode providers advertise data throughput as high as 9 Gbit/s⁷, which is up to 1 million times more data than is needed to monitor HVAC and industrial equipment. Fend's data diode form factor is small enough to fit in most control panels and run on common control voltages. The ruggedized enclosure and components will allow for years of operation in environments that suffer from vibration and dust exposure. Attempted physical access to Fend's data diode for protected equipment will trigger an alert to the equipment manager.



Figure 2. Fend's Latest Data Diode.

Some users will want to connect the diode to an existing Utility Monitoring and Control System (UMCS) or other internal networks, whereas others may want to connect to Fend's secure, cloud-based monitoring service that collects data from a diode and enables a user to view equipment performance trends and set alerts (such as equipment failure or unexpected temperature drift). An ideal application of this optional service is for currently disconnected equipment, like many remote rooftop air conditioners, with a connection via onboard cellular modem. This combination allows for the rapid establishment of a base-wide equipment management system that is both vendor and equipment-type agnostic. Internet of things (IoT) monthly data plans from major US carriers can be as low as \$1 per device. Because data diodes cannot be remotely compromised and can use existing networks, this option is worth a look by operators considering an equipment-only LAN.



Figure 3. Fend Diode Equipped with Cellular Outbound.

2.1 ADVANTAGES AND LIMITATIONS OF THE TECHNOLOGY

The principal objective of Fend's data diode is provide the security of an air gap between high-security and low-security networks while increasing the accessibility and quantity of data to enhance energy and water management and operational efficiency.

Three main categories of alternatives to Fend's data diode are:

- Air gap: Leave equipment completely disconnected from the outside world
 - Low implementation cost, potentially high opportunity cost due to lost energy savings and reduced operation awareness
- Incumbent Diodes: Use an expensive incumbent data diode technology
 - Typically 10x more expensive
 - Requires additional servers and complex installation
 - Designed for IT environments
- Software: Deploy an alternative software-based form of protection (firewalls, VPNs, cloud-based threat detection)
 - Requires ongoing maintenance expense (patches)
 - Security updates are reactive to known threats rather than protecting against future unknown threats

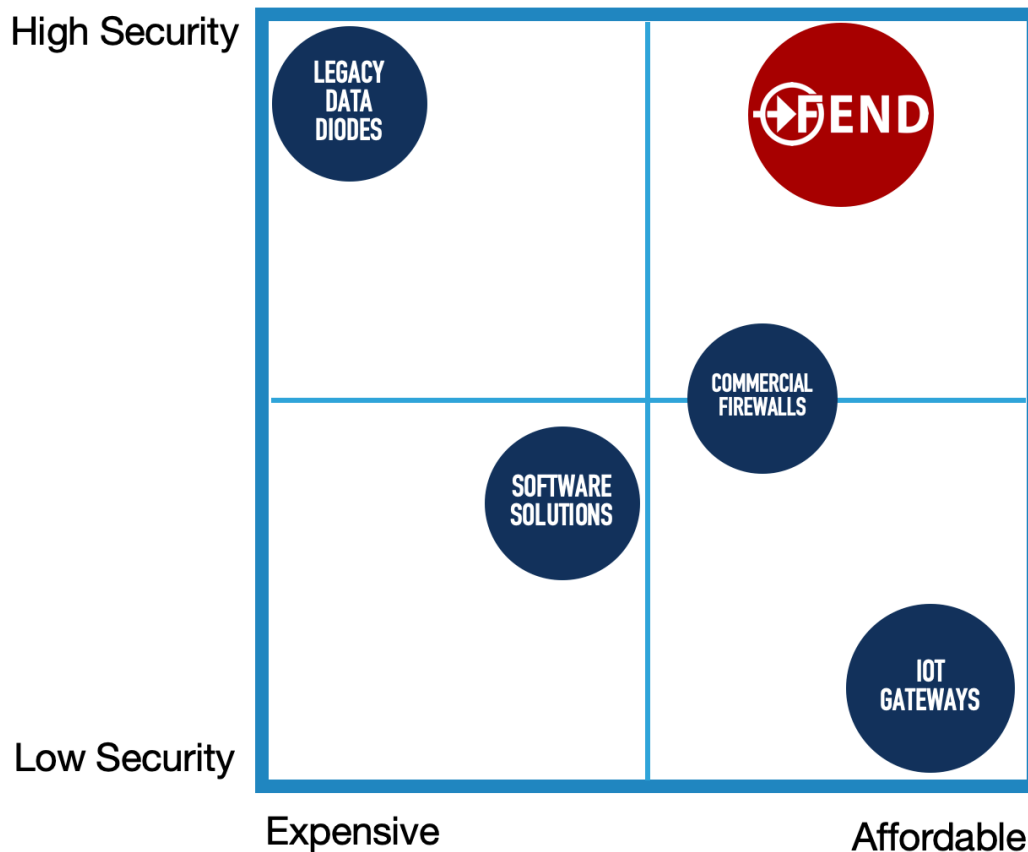


Figure 4. Fend Offers the Security of Traditional Data Diodes at a Far More Affordable Price.

It is also important to note that data diode technology is specifically suited for applications where one-way traffic is advantageous and does not decrease functionality. For example, temperature readings between a high impact system (such as a chiller serving a critical facility) to a low impact system (such as a base-wide UMCS). In this case, the temperature readings are one-way outbound data points to the UMCS. An adversary cannot use that connection to compromise the system by obtaining unauthorized access from the UMCS into the critical system.

In some systems, two-way traffic is required to perform command and control functions. For example, in a low-impact system, the operator may need to use the UMCS to adjust the sequence of operations or perform a manual override of a particular device from the front-end. If a data diode is used to limit data transfer from the device to the front-end, the operator at the front-end will not be able to remotely adjust the sequence of operations or perform a manual override.

3.0 TECHNICAL PERFORMANCE OBJECTIVES

Fend's low-cost, easy-to-use data diode provide the security of an air gap between high-security and low-security networks while increasing the accessibility and quantity of data to managers across all DoD components in order to enhance energy and water management and operational efficiency. To ensure the product can achieve this goal and in order to provide additional value described below, the project will meet the following objectives:

- Complete isolation of protected equipment
- Uninterrupted equipment operation
- Interoperability with various equipment types
- Ease of installation
- Data transmission to desired network location
- Cost performance

3.1 SUMMARY OF PERFORMANCE OBJECTIVES

Table 2. Performance Objectives

#	Performance Objective	Metric	Data Requirements	Success Criteria
PO-1	Unidirectional Data Flow	Pass / Fail - Unidirectional nature of data flow	Penetration testing to determine effectiveness of physical barrier	Pass - No data flows across the diode from the network / "low security side" to the equipment / "high security side"
PO-2	Non-interference	Comparison vs baseline - Observation of equipment operating characteristics	Logged performance data from equipment controller, before and after data diode installation	No difference in behavior of protected equipment after data diode installation
PO-3	Compatibility	Percentage of systems types successfully sending data across data diode	Connection test data sets with and without data diode	>= 70% during this ESTCP project
PO-4	Ease of Installation	Installation time	Average of 10 timed installs for routine installations	<=1 hour for standalone equipment <=4 hours for BAS to private network.
PO-5	Facilitation of Data Collection	Time interval of data provided (minutes), Integrity of data (comparison with data at source)	Data contents and time intervals from transmission logs	Accurate data sent at regular intervals (such as <=1-minute granularity)
PO-6	Cost Performance	Payback period or breakeven relative to other data acquisition methods	Cost build up for equipment, installation, and ongoing costs	< 5 years

3.2 PERFORMANCE OBJECTIVES DESCRIPTIONS

- **PO-1 - Unidirectional Data Flow**

- Name and Definition: Unidirectional data flow means the complete isolation of protected equipment “high security side” from downstream intrusion “low security side.” The unidirectional nature of data diodes’ light-based data broadcast should make the “backflow” of malicious code across a properly designed data diode physically impossible.
- Purpose: The purpose of this performance objective is to confirm that the data diode is functioning as designed and is only allowing data flow in an outbound manner.
- Metric: Pass / Fail - Does the diode prevent all data that is sent from the low security side from reaching the high security side of the device?
- Data: Penetration testing report results
- Analytical Methodology: The team subjected the device to DoD-led penetration testing in a controlled laboratory DoD environment to confirm proper operation. The penetration testing team produced a report outlining the findings of the penetration tests.
- Success Criteria: Pass, the diode prevents all data that is sent from the low-security side from reaching the high-security side of the device.

- **PO-2 - Non-interference**

- Name and Definition: Non-interference with equipment operation means that installed data diodes only monitor and report equipment status and have no impact on equipment behavior.
- Purpose: The purpose of this performance objective is to confirm that the data diode is functioning as designed and that adding a data diode to a piece of equipment does not impact the functionality of that equipment, specifically that data continues to flow across the controls network without corruption or data loss.
- Metric: Comparison vs baseline operation
- Data: Baseline reference data and post-installation performance data
- Analytical Methodology: Reference conditions were established using data loggers and information from an existing UMCS. The team installed data diodes and then left the data diodes in place at a representative set of equipment. The reference data set was then be compared with the post-installation data set (see Section 4.3 for detailed methodology).
- Success Criteria: Installation of the data diode does not affect equipment functionality. Post-installation data set and baseline data set show no indication of diode-related deviation.

- **PO-3 - Compatibility**

- Name and Definition: Compatibility with DoD equipment means that the diode’s configuration process should recognize the applicable equipment communication protocol and transmit the available data successfully.
- Purpose: The purpose of this performance objective is to confirm that the data diode can address the needs of DoD through compatibility with DoD equipment and systems.
- Metric: Percentage of tested systems that recognize and successfully send data across the data diode

- Data: Equipment communication test results
 - Analytical Methodology: The team connected the diode into a variety of equipment types (see Section 4.3 for a list of specific protocols and equipment tested), prioritizing by share of DoD equipment portfolio, and noting the characteristics of successful and unsuccessful data transmission transactions. The team utilized equipment testing labs where available to accelerate progress. Any connection problems found were diagnosed and adjustments made to the setup procedure software. Fend plans to grow its “supported protocol list” over time, with the most common DoD equipment and control systems receiving priority.
 - Success Criteria: The data diode successfully identifies and communicates data for $\geq 70\%$ of systems tested.
- **PO-4 - Ease of Installation**
 - Name and Definition: Ease of installation means that the diode is installable by anyone who would normally touch an equipment control panel, as opposed to requiring a specially trained installer.
 - Purpose: The purpose of this performance objective is to confirm that the data diode can address the needs of DoD through plug and play compatibility with DoD equipment and systems.
 - Metric: Installation time in hours
 - Data: Average of 10 timed installs measured under standard conditions. Installs performed by the typical installer of the final product.
 - Analytical Methodology: The team installed data diodes using team members without extensive training and observed how long the process took, noting required changes to the user experience.
 - Success Criteria: Installation takes ≤ 1 manhour (on average) for a standalone equipment installation. Installation takes ≤ 4 manhours (on average) for BAS to private network installation.
 - **PO-5 - Facilitation of Data Collection**
 - Name and Definition: Facilitation of data collection means that the data diode can connect to an external destination network and send accurate and consistent equipment data.
 - Purpose: The purpose of this performance objective is to confirm that the data diode can successfully deliver accurate and consistent equipment data to an external network.
 - Metrics: Time interval of data provided (minutes), Integrity of data (comparison with data at source)
 - Data: Contents of original data and contents of data transmitted through diode. Time intervals from transmission logs.
 - Analytical Methodology: The project team measured/logged data sent at the source equipment and compare against data sent through the diode. The frequency and integrity of the data was recorded.
 - Success Criteria: Accurate data sent in $\geq 99\%$ of data transmissions at regular intervals (such as ≤ 1 -minute granularity)

- **PO-6 - Cost Performance**

- Name and Definition: Cost performance means managing the various aspects that contribute to the cost of data acquisition using the data diode.
- Purpose: The purpose of this performance objective is to ensure that use of one-way communication diodes can have a lower total cost over time than alternatives including the use of firewalls, physical media, and air gaps.
- Metric: Payback period or breakeven point
- Data: Product costs, market data on substitute products and methods, recurring fees, labor expenses.
- Analytical Methodology: The project team compared the cost of the data diode and typical installation labor expenses to pricing data on industrial firewalls (including ongoing licenses, automated patch management, labor), retrieval of physical media such as DVDs and hard drives (media cost, labor, travel costs), dedicated equipment-only LANs, and traditional control “point” connections.
- Success Criteria: Payback period or breakeven of less than 5 years (typical energy retrofit project threshold)

4.0 MATERIALS AND METHODS

4.1 TESTING OVERVIEW AND ASSIGNMENTS

Due the specialized expertise and equipment required to test the performance objectives, each objective was assigned to a team with skills in the relevant area of interest, as follows:

Table 3. Test Leads by Performance Objective

#	Performance Objective	Lead	Test Location
PO-1	Unidirectional Data Flow	Army Threat Systems Management Office (TSMO) Navy Control Systems Test Bed (CSTB)	Redstone Arsenal, Huntsville, AL Naval Facilities Engineering Command (NAVFAC) Engineering and Expeditionary Warfare Center, Port Hueneme CA
PO-2	Non-interference	U.S. Army Corps of Engineers Control System Test Lab (USACE CSTL)	Construction Engineering Research Laboratory (CERL) Champaign, IL
PO-3	Compatibility	USACE CSTL	CERL, Champaign, IL
PO-4	Ease of Installation	USACE CSTL	CERL, Champaign, IL
PO-5	Facilitation of Data Collection	USACE CSTL	CERL, Champaign, IL
PO-6	Cost Performance	Fend Incorporated	Arlington, VA

Test plans for each performance objective were developed in conjunction with the assigned test teams. Details regarding each test team, location, test methodology, are described below.

4.2 PO-1 – TSMO AND CSTB

Confirmation of unidirectional data flow was tested through a series of penetration tests hosted by the Army’s Threat Systems Management Office (TSMO) and the Navy’s Control Systems Test Bed (CSTB).

4.2.1 Test Location

4.2.1.1 TSMO Penetration Test Location

The Army’s Threat Systems Management Office is located at Redstone Arsenal in Huntsville, Alabama.

TSMO manages the Army Threat Systems Program, including total life cycle and operations of threat systems for testing and training in live, virtual, and constructive environments. TSMO provides the threat capability operations support for testing and training events supporting Army and Tri-Service threat portrayal requirements.

4.2.1.2 CSTB Penetration Test Location

CSTB is managed and operated by the Engineering Expeditionary Warfare Center (EXWC) Control Systems Engineering (CSE) Division, which is an Echelon III command for Naval Facilities Engineering Systems Command (NAVFAC). CSTB's responsibility is to apply and maintain cybersecurity resilience for NAVFAC control systems while ensuring cybersecurity awareness throughout the organization. Through partnership with academia and federal entities, CSTB is capable of supporting other DoD agencies and industry partners. CSTB and its personnel with the proper skillsets, cyber tools, and training facilities are hosted at Port Hueneme, CA.

4.2.2 Test Design

4.2.2.1 TSMO Penetration Test Design

The TSMO penetration test was designed as an adversarial assessment to verify the ability of the Fend Data Diode to deny all inbound traffic. During this test, the penetration testing team represented nearsider and outsider threats in an attempt to:

- Penetrate – Verify data can only be sent one way through the device (that control systems on the protected side of the device cannot be accessed through the device)
- Disrupt – Attempt to disrupt, reroute, manipulate data
- Disable – Attempt to remotely disable or reengineer device

The test system consisted of a Fend Data Diode in FTP mode, an FTP client computer such as a data historian often found in commercial and industrial equipment settings, an FTP server computer, and a network switch. The FTP client computer (considered “high security” or “protected”) was configured to push files at intervals through the diode to the FTP server computer (considered “low security”). The same system was also used to test FTPS on the outbound side of the diode.

A series of attacks were performed in an attempt to send data upstream through the diode.

Due to the controlled nature of the tests performed, details of the test plan and procedure are available to government organizations upon request and approval. Inquiries should be directed to Tapan Patel, Tapan.C.Patel@usace.army.mil.

4.2.2.2 CSTB Penetration Test Design

Like the TSMO test, the CSTB penetration test was designed as an adversarial assessment to verify the ability of the Fend Data Diode to deny all inbound traffic. During this test, the penetration testing team represented insider, nearsider, and outsider threats.

The tests performed included four distinct architectures, as shown below in Figure 6: Fend Data Diode Testing Architectures. All architectures included the Fend Data Diode, two to four testing computers, and either ethernet or serial connections between the diode and computers.

Connections were made to the data diode's "input-side" and "output-side" respectively in accordance with the flow of information design and labelling.

Model FD-5M-SE1-CE2-B3 / Ethernet + Cellular

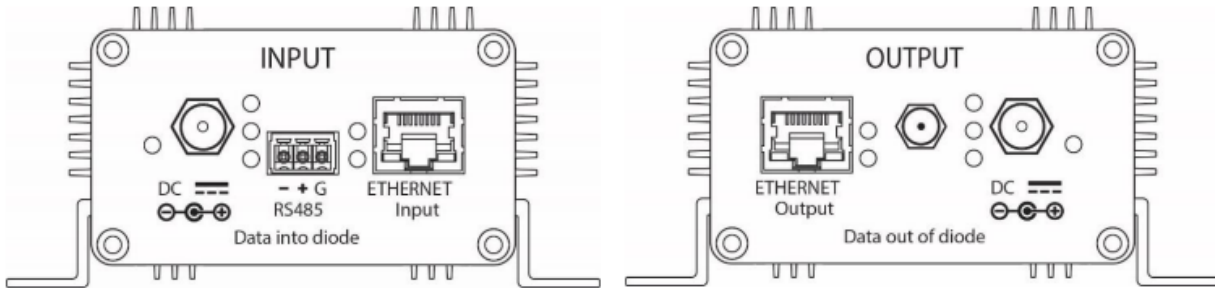


Figure 5. Fend Data Diode Connection Interfaces

- Architecture 1 is intended for performing tests and observing the Fend Data Diode in its intended configuration (that is to say, sending client data through the "input" side of the data diode and having the data received by a server on the "output" side).
- Architecture 2 is intended for performing tests and observing the Fend Data Diode when the data flow is attempted in reverse.
- Architecture 3 is intended for performing tests and observing the Fend Data Diode when both the client and server are connected via the input side (The client will attempt to use the diode's "input" side as a pivot point for indirectly reaching the server).
- Architecture 4 is intended for performing tests and observing the Fend Data Diode in a similar fashion to Architecture 3, but from the "output" side.

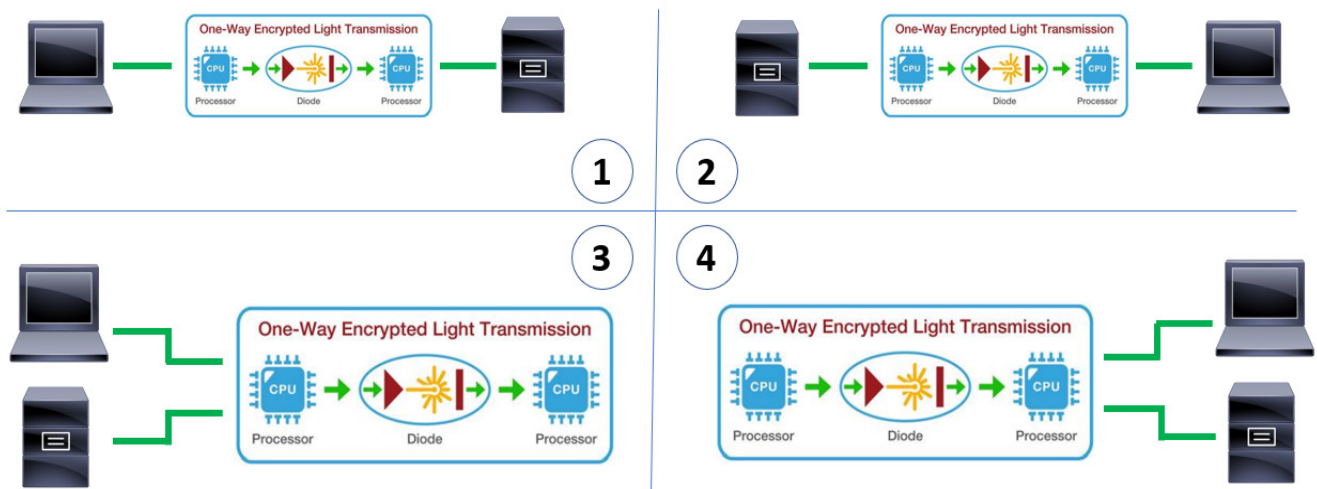


Figure 6. Fend Data Diode Testing Architectures

The testing environment used two computers with the Fend Data Diode connected between them; however, logical/physical architectures varied between tests with respect for was being tested (see Figure 6). For FTP-based data transfers, Computer 1 (FTP client) acted as the input side of the connection and Computer 2 (FTP server) acted as the output side with devices connected via ethernet cabling. For Modbus communications over serial connection, traffic was emulated on Computer 1 and connected via a USB-to-Serial converter.

A series of attacks were performed in an attempt to send data upstream through the diode.

Due to the controlled nature of the tests performed, details of the test plan and procedure are available to government organizations upon request and approval. Inquiries should be directed to Tapan Patel, Tapan.C.Patel@usace.army.mil.

4.3 PO-2, 3, 4, AND 5 - CSTL

4.3.1 Test Location

Tests for PO-2, 3, 4, and 5 (Non-interference, Compatibility, Ease of Installation, and Facilitation of Data Collection) were performed at the US Army Construction Engineering Research Laboratory located at 2902 Newmark Dr., Champaign, IL 61822. Two locations on base were used as test sites. The first is the Control System Test Lab (CSTL). The second is an existing building used for administrative processing.



Figure 7. US Army Construction Engineering Research Laboratory in Champaign, IL

The CSTL was used to perform bench testing of the devices before they were integrated into live facility tests. CERL pursued integration of Fend's data diodes into the existing Research and Development Enterprise (RDE) network which is used to host the Utility Monitoring and Control System (UMCS).

For this demonstration, existing Facility Related Control System (FRCS) at CERL are being used as a test case. Note that these use cases are limited to monitoring applications not requiring two-way remote control.

CERL operates and maintains a Utility Monitoring and Control System (UMCS) which provides command and control for multiple buildings and a central heating/ cooling plant across the campus. The UMCS is hosted on the RDE network. CERL is representative of many military installations because there are a number of security assessments that will need to be conducted before the diodes can be placed into operation. First, RDE IT staff runs an Assured Compliance Assessment Solution (ACAS) scan on the diode(s) and any CAT I findings must be remediated before the team will receive approval to install the diode(s). Second, RDE typically runs security scans on the network to identify any potential vulnerabilities. Once the diodes were operational, they underwent these scans and be subject to normal IT operations. The diodes were implemented in systems where “monitoring only” is required. This includes the CSTL, where heating and cooling is performed locally, but some limited monitoring points are needed at the front-end.

When the diodes are installed with any equipment, a physical enclosure will be required. This will typically require a suitable space (approximately 6 inches by 8 inches by 4 inches) near equipment or within a cabinet to accommodate the diode, data cables, and power connections. An optional approach is to mount the diode to wall or cabinet using four screws, ideally within a lockable enclosure.

Approval for operation on RDE - For initial purposes, the CERL team performed an ACAS scan on the Fend diodes to determine the cybersecurity posture of the devices.

For bench and field tests, Fend's diode was connected to a fully segmented network, a live operational UMCS which is hosted on the RDE. Obtaining RDE approval was critical and required before the diodes can be place on the operational network.

Interconnect agreements with local utilities are not needed for this project as no grid-connected, energy-generating equipment will be tested as part of this project. Further permits will not be necessary as installation of the diodes will not alter the structure or designs of the buildings to be protected.

Once RDE approval was obtained, the Fend devices were installed. After testing, if the diodes need to be removed, the process is fairly simple. The existing connections can simply be removed from the diode and the UMCS devices can then be connected as usual. The costs associated with any decommissioning are minimal and require less than 10 minutes of labor per diode.

4.3.2 Test Design

4.3.2.1 Test Design Overview

- **Fundamental Problem:** The fundamental issue facing DoD control systems is their ability to obtain and maintain cybersecurity authorization. This demonstration will demonstrate the use of Fend's data diodes to secure control system infrastructure to lower the risk to various components. Reducing the risk to these components will improve the DoD's ability to obtain and maintain cybersecurity authorization for their systems.

- **Demonstration Question:** The demonstration addressed the following questions as they relate to the use of data diodes in control systems:
 - 1) Do the data diodes provide adequate security to prevent unintended backwards data flow (intentional or unintentional)?
 - 2) Do the data diodes allow connected devices to maintain their required functionality? Functionality is determined by compatibility with existing equipment, any interference (data or otherwise) with existing equipment and any added network latency or bandwidth issues related to the control system.
 - 3) Are the data diodes cost effective to install? I.e. What is the cost benefit of secured connectivity and ability to maintain an authorization versus price of installation and maintenance?

Figure 8 below, describes the potential scenarios where the data diodes would be installed in DoD installations. Each scenario shows typical data flow along with the typical physical transport mechanism and some examples of common implementations of protocols across the devices.

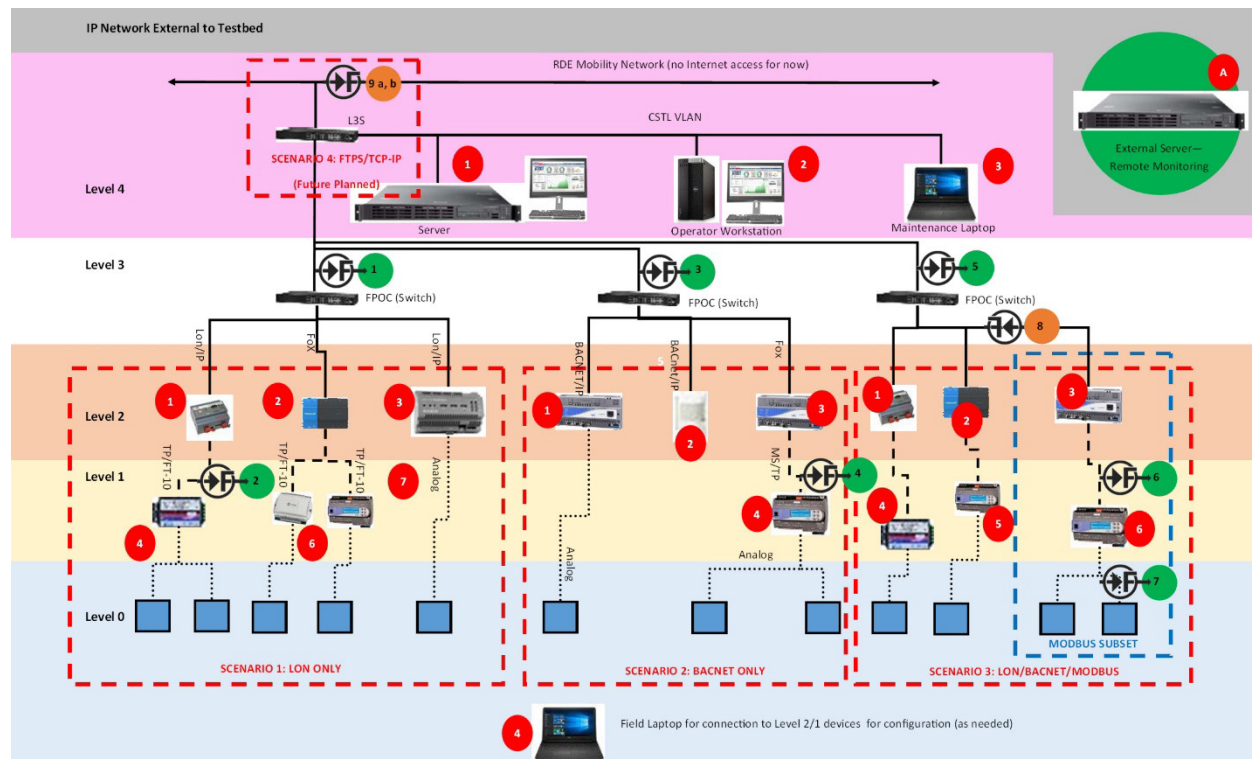


Figure 8. Scenarios for Fend Diode Implementation in DOD CS 5 Level Architecture

Table 4 through 6 show the list of hardware and tools used for the various scenarios.

Table 7 list the test equipment that was used to simulate DOD building controls. The “Device #” listed in the tables corresponds to the red circled numbers in Figure 8 above.

Table 4. LON Controls Network Test Equipment List

Scenario 1: LON ONLY		
Device #	Make/Model	Purpose
1	Echelon Lonpoint Router	Level 2, TP/FT-10 to LON/IP Router
2	JACE 800	Level 2, TP/FT-10 (or others) to IP. Can use as web server
3	Echelon iLon 100	Level 2, TP/FT-10 to LON/IP. Web server. Analog input
4	TAC MNL 10RF3	Level 1, Analog and S-Link to LON/IP. Integrate w/ MN-S3HT-500 Level 0 device
5	N/A	
6	TAC Xenta 100	Level 1, Analog to TP/FT-10
7	Loytec L-switch XP EIA-709	Level 1, TP/FT-10 to LON/IP and Analog to TP/FT-10

Table 5. BACNET Controls Network Test Equipment List

Scenario 2: BACNET ONLY		
Device #	Make/Model	Purpose
1	TAC MNB 1000	Level 2, MS/TP to BACNET/IP or Analog to BACNET/IP
2	Honeywell	CIPer 10
3	Lynxspring Jenesys-PC 3000 (JACE)	Level 2, MS/TP to BACNET/IP. Can use as Webserver
4	MNB 300	Level 1, Analog to MS/TP

Table 6. Mixed Controls Network Test Equipment List (Including Modbus)

Scenario 3: Mixed Protocol		
Device #	Make/Model	Purpose
1	Echelon Lonpoint Router	Level 2, TP/FT-10 to LON/IP Router
2	JACE 800 (Make TBD)	Level 2, TP/FT-10 (or others) to IP. Can use as web server
3	Anybus	Modbus Gateway
4	TAC MNL 10RF3	Level 1, Analog and S-Link to LON/IP. Integrate w/ MN-S3HT-500 Level 0 device
5	Datanab	Temperature reader
6	Pixsys DRR245	Modbus/RTU

Table 7. Other Supporting Hardware / Software

Miscellaneous Hardware Software		
Device #	Make/Model	Purpose
1	Dell R440 Server	Niagara Front-End Host
2	Dell Workstation	Front-Ends (Niagara AX)
3	Dell Laptop	Tools if needed
4	Field Laptop	Engineering Tools for level 2 and level 1 configuration that can't happen through front end
A	Maintenance Laptop	Data receiving server / End point for data sent through diode

Table 8 lists the Fend data diode placement locations in the test controls network, the protocols to be tested, and the operating mode. The “Test #” listed in the table corresponds to the green and orange circles in Figure 8 above.

Table 8. Fend Data Diode Test Locations and Configurations

Test Description						
Test #	Diode Type / Model	Input Protocol	Output Protocol	Target Location	Multiple Device?	Function
1	FD-1M-SE1-SE2-B2	LON-IP	TCP/IP	CSTL	N	Tap
2	FD-1M-SE1-SE2-B2	LONTalk-Serial (with serial converter)	TCP/IP	CSTL	N	Tap
3	FD-1M-SE1-SE2-B2	BACnet-IP	TCP/IP	CSTL	N	Tap
4	FD-1M-SE1-SE2-B2	BACnet-Serial	TCP/IP	CSTL	N	Tap
5	FD-1M-SE1-SE2-B2	Modbus-TCP	TCP/IP	CSTL	N	Tap
6	FD-1M-SE1-SE2-B2	Modbus-Serial	TCP/IP	CSTL	N	Tap
7	FD-1M-SE1-SE2-B2	Modbus-Serial	TCP/IP	CSTL	Y	Tap
8	FD-1M-SE1-SE2-B2	Modbus-TCP	Modbus-TCP	CSTL	N	Passthrough
9a	FD-5M-SE1-CE2-B2, FD-5M-SE1-SE2-B2, and FD-5M-SE1-XE2-B2	FTP (Data in file format)	FTP/FTPS (Data in file format)	TSMO & CSTB	N	Passthrough
9b (Future Planned)	FD-1M-SE1-SE2-B2	TCP/IP	Secure TCP/IP	CERL UMCS RDE Mobility Network	N	Passthrough
10 (Future Planned)	FD-1M-SE1-SE2-B2	Modbus-Serial	Modbus-Serial	CSTL	N	Tap
11	FD-1M-SE1-SE2-B2	LON-IP	TCP/IP	CERL UMCS RDE Mobility Network	Y	Tap
12	FD-1M-SE1-SE2-B2	BACnet-IP	TCP/IP	CERL UMCS RDE Mobility Network	Y	Tap

4.3.2.2 Conceptual Test Design

- Hypothesis: The overall hypothesis for this effort is that the Fend data diodes can provide a cost effective secure 1-way communication channel for control system components in an easy-to-use manner that does will not require reconfiguring control system devices.
- Independent variable: The independent variable in all phases, will be the insertion of the diode into the existing control system architecture.
- Dependent variable(s): The team measured the following variables: 1) Impact of diode on communications in control system (i.e. does the control system keep functioning as it did before diode was installed?) 2) Does the diode add or reduce overall maintenance requirements for the control system (e.g. patching, calibration, re-configuration)? 3) Does the device add or reduce any RMF requirements on system operators? For example, enhanced security of the control system with the diode could reduce the overall risk to the system while reducing the number of CCIs that the system operators have to address for RMF authorization.
- Controlled variable(s): All variables in the control system were held constant. If there were any issues such as non-communication after the diode is installed, the team made changes to the diode firmware before retesting. Due to the nature of this project and testing already conducted, minimal changes to the control system were required.

At a high level, the test design for the demonstration at CERL occurred in the following key phases:

- 1) **Testing at CERL Control System Test Lab (CSTL)**: The Fend data diodes were installed in a representative tested bed at the CERL CSTL. The CERL CSTL environment is a testbed which replicates common Level 0 – Level 4 systems found on DoD installations. In this testbed environment, the team attempted to test each Scenario described in Table 8.
 - After the diodes were installed, the CERL team evaluated POs related to Compatibility, Ease of Installation and Facilitation of Data Collection between various devices.
- 2) **Penetration Testing by Army Red Team**: The project team worked with the Army Threat System Management Office (TSMO) and the Navy Control Systems Test Bed (CSTB) to perform red team testing on the various scenarios in the testbed. Using findings from the TSMO and CSTB operations, the team evaluated whether the diodes meet the unidirectional data flow PO and determined the general cybersecurity posture of the diodes.
- 3) **Integration with CERL facilities**: After integration into the testbed, the team integrated the data diodes into the CERL UMCS through the RDE network. Because the CSTL has local controls and houses IT equipment, a monitoring only scenario between Level 2 and Level 3 was adequate. An additional facility used for testing was the “Solar House” at CERL. This facility is a small administration building which operates on a BACnet network. The team worked with the UMCS operators and Solar House occupants to determine procedures for implementing on site testing.

4.3.2.3 Baseline Characterization

The baseline Phase 1 CSTL environment included a combination of several level 2 devices, and at least 1 or 2 level 1 devices, followed by multiple level 0 sensors and actuators. In total, about 10-12 devices and sensors were tested. In all cases, including Phase 2, baseline characterization consisted of the steps identified below. In addition to steady state operations, the team also baselined:

- 1) For a period of 1 week, performed trend logging of devices, sensors and actuators in the sub-system where the data diode will be installed. For example, within an AHU, this could be temperature logs, or CO₂ logs. The trend logging included activities such as startup and shutdown or other activities that the diode will be subjected to in the operational testing plan. This trend logging will occur through the front end where the logs will be stored. At the end of the 1-week period, review all the trend data to identify whether there are any drops or incorrect data. Quantify the amount and type of data issues. If possible, attempt to rectify the issue and re-establish baseline for 1 week. This quantified data error/data loss rate will serve as the baseline.
- 2) Install data diodes in identified systems, sub-systems. Monitor trends closely for 1-2 days to identify any immediate issues which may need to be resolved. If there are any major issues (such as loss of availability of any particular equipment and not identified during Phase I), remove diode from system/sub-system and rectify issue.
- 3) If there are no major issues in step 2, commence 1 week of trend logging. After 1 week, analyze trend data and quantify data error/data loss rate. Compare data error/loss rate before and after data diode installation.

In addition to step 1, previous data logs (if any) were used to determine longer term data error/loss rates in those particular systems. For example, it is possible that a 1-week trend log may not identify any issues that occur bi-annually or on a monthly basis. The team reviewed any historic data logs to determine if there are any issues.

4.3.2.4 Operational Testing

Operational testing occurred in Phase 2 of the test plan, namely testing in CERL facilities. All existing systems in Phase 2 under which the data diodes were installed were already operational. In Phase I, there was flexibility to perform testing which were not possible for live operational systems in Phase 2. For each Phase 1 and 2, the following operational tests will be conducted for systems or sub-systems under the data diode:

- 1) Install into steady state environment. In this step, which is expected to be representative of most DoD systems, the diode will be installed into an operational steady state environment. Prior to this test, all system communications will have been verified as operational. Any systems or sub-systems that are not operational will be identified and noted. Any issues such as data communications, latency, etc. from installing the diode will be identified and noted.
- 2) System shut down/start up. In this step, sensors or devices both upstream or downstream (such as sensors, level 2 devices or front-ends) will be unplugged or turned off. In phase I, this will include the front end. In phase 2, the front end may not be included because of logistics associated with turning off the front-end for the entire CERL campus. If possible, the team will test this scenario. Note that each sensor/device will be turned on and allowed to reach steady state before the team moves on to the next sensor. This will allow the team to isolate whether any issues are sensor/device specific or diode specific.

The team will then move on to the next sensor/device. At the end of this sequential testing, all devices upstream and downstream of the diodes (not including the diodes) will be turned off together and then turned back on. This will identify any potential issues with multiple devices rebooting under any particular diode.

- 3) Diode shut down. In this step, each diode will be turned off and turned back on. The team expects data loss while the diode is shut off. However, when the diode is back on, the system should become operational without any significant delays (<5 minutes).
- 4) Diode removed. In this step, the diodes will be turned off and removed. The components up-stream and downstream of the diodes will be plugged in to each other. This test is representative of a scenario where the diode is no longer needed or experiences some issues where removal is necessary. The system should go back into an operational state within 5 minutes after the diode is removed.

The list below outlines the tasks and subtasks for operational testing at CERL in Phases 1 and 2.

- Phase 1: CSTL Test Bed
 - Baseline: Steady State
 - Baseline: Startup/Shutdown
 - Operational Test: Steady State
 - Operational Test: System Shutdown/Startup
 - Operational: Diode Shut Down
 - Operational: Diode Removal
 - Resolve Issues and Adjust Procedures
- Phase 2: Integration with CERL Facilities
 - Baseline: Steady State
 - Baseline: Startup/Shutdown
 - Operational Test: Steady State
 - Operational Test: System Shutdown/Startup
 - Operational: Diode Shut Down
 - Operational: Diode Removal
 - Resolve Issues and Adjust Procedures

4.3.2.5 *Sampling Protocol*

- Data Collector(s): The CERL UMCS team setup and collected trend data during the baseline and operational testing phases.
- Data Recording: Trend logs were established at 1-minute intervals for particular sensors and devices for which data was collected under the baseline and operational testing periods.
- Data Description: Data samples included sensor data and device data such as temperature, ping successful/unsuccessful, equipment status (on/off) and others.
- Data Storage and Backup: Backup data was stored on a shared location on the RDE network to enable redundancy in case the front-end data is lost for any reason.

4.3.2.6 Equipment Calibration And Data Quality Issues

- Equipment Calibration: No equipment calibration is required.
- Quality Assurance Sampling: At the start of data collection, data was monitored closely for a few hours to determine and ensure that the data was being collected. After any setup issues were resolved, the team reviewed the data every morning for the week during the baseline data collection. For testing lasting a single day, the data was checked at least hourly to ensure logging and collection was still active. During the first few hours after data collection occurred for both baseline or operational testing, the intervals were adjusted as needed. In CERL's experience with the UMCS 1-5 minute intervals are generally sufficient to identify any issues.
- Post-Processing Analysis: All trends were plotted in excel. Any data error/drop issues were identified visually. In addition, further analysis of the data was conducted non-visually. The team has expertise in importing excel data and writing analysis algorithms in VBA or python.

4.3.3 Performance Assessment

The analytical methodology for each performance objective is described in Section 3.3.2. Several analysis techniques will be employed during the course of this demonstration:

- Statistical Methodologies: The test design involves a series of pass/fail tests which are best represented by a list with results.
- Modeling and Simulation: Simulated mechanical equipment protocols and interfaces can expand the number of connection tests will be used as practical to expand upon the physically connected control equipment communicating via the data diode.
- Anecdotal Perspectives: Personnel interviews with staff describe perceived ease of use and installation.
- Internal Validity: The team's use of data logging equipment to create a baseline before diode installation validated the performance of the equipment under evaluation. Data integrity tests provided further controls.
- External Validity: The quantity and type of equipment to which Fend's diode will be connection represents a large portion of DoD's building stock. The equipment is often housed in indoor environments (mechanical rooms) with a relatively limited range of environmental conditions experienced by the data diode. Fend's diode is designed to withstand a wide variety of temperatures.

4.4 PO-6 - FEND INCORPORATED

4.4.1 Cost Assessment

These next-generation data diodes are intended to provide a high level of cybersecurity while improving cost performance over alternative methods of data collection. The project team compared the use of these data diodes to other methods of data extraction, including retrieval of data using physical media (hard drives, DVDs), hardware input/out interfaces, equipment only LANs, and industrial firewalls. These do not all provide the same level of security as a data diode (addressed in Section 5.4), but can be compared on an economic basis.

Table 9. Cost Assessment Technologies Considered

Technology	Description
Fend data diodes	One-way communication diode hardware that sends data in a physically-enforced unidirectional fashion.
Transport of physical media	Use of removable hard drive, thumb drives, or optical media (CD, DVD) to carry data sets across an air gap or to another location.
Hardwired control “points” and I/O interfaces	These systems designed to send specific data points across a boundary using binary or analog signals. Interfaces between two devices are typically hard-wired using low-voltage connections. ⁶
Separate equipment-only LAN	Installing a separate, isolated local area network (LAN) for the control and monitoring of FRCS. This system is somewhat common within a single building, but maintaining a separate network across an entire installation (or beyond) for remote visibility requires laying new fiber.
Industrial Firewalls	Hardware that uses software and lists of known vulnerabilities to allow some data traffic to pass through the device while prohibiting other transmissions.

These alternatives were compared on the basis of first cost (hardware), ongoing fees / licenses, and labor expenses. Payback periods and breakeven points were calculated using a diode cost of \$5,000 (though some Fend data diode models cost less). Cost data was taken from online resources including government-focused resellers and purchasing contracts. Labor costs were based on a fully burdened rate (including benefits, taxes) of \$150,000 per year or \$72 per hour. Depending on local labor costs or the need to use contracted labor, these rates may be higher or lower for an individual site. An example calculation is one used in the comparison to the transport of physical media. For this cost, the task is a daily DVD burn with information to be carried across an air gap to another network:

Task effort = 5 minutes per day = 1/12 hour (0.083 hours)

Labor rate = \$72/hour

Task frequency = 365 days per year

Total labor cost = (0.083 hour / day) * (\$72/hour) * (365 days / year) = \$2190 / year

5.0 RESULTS AND DISCUSSION

Table 10. Summary of Project Results by Objective with Metric

#	Performance Objective	Metric	Success (Yes/No)	Remarks
PO-1	Unidirectional Data Flow	Pass / Fail - Unidirectional nature of data flow	Yes	Diode blocked outsider attempts to send data “upstream” or disable data diode
PO-2	Non-interference	Comparison vs baseline - Observation of equipment operating characteristics	Yes	Equipment functioned normally when connected to diode
PO-3	Compatibility	Percentage of systems types successfully sending data across data diode	Yes	Diode was compatible with 100% of protocols tested. Although 2 of the 11 originally planned testbed tests were unable to be completed due to test design / equipment availability issues. Two additional testbed tests are still contemplated for future testing. 100% of the two on-site long-term tests were completed and successful.
PO-4	Ease of Installation	Installation time	Yes	Installation took less than one hour in most cases.
PO-5	Facilitation of Data Collection	Time interval of data provided (minutes), Integrity of data (comparison with data at source)	Yes	Input side (source) and output side (destination) data sets were consistent.
PO-6	Cost Performance	Payback period or breakeven relative to other data acquisition methods	Yes	Payback period or breakeven was less than 5 years when compared to industrial firewalls. Data diode was economical relative to other substitutes.

5.1 PO-1 TEST RESULTS

The purpose of this performance objective was to confirm that the data diode functioned as designed allowing data flow only in an outbound manner. This was tested by both TSMO and CSTB using similar test structures.

5.1.1 TSMO Penetration Test Results

USACE ERDC-CERL worked with the Army’s Threat System Management Office (TSMO) to conduct penetration and operational survivability testing in accordance with the predefined test plan. During this cyber assessment, the TSMO team represented nearsider and outsider threats. The tests were conducted at Redstone Arsenal from 8 to 11 June 2020 and 15 to 18 September 2020. Diode models FD-5M-SE1-CE2-B2, FD-5M-SE1-SE2-B2, and FD-5M-SE1-XE2-B2 were tested.

The overall objectives were to:

1. Test if data can be only sent one way.
2. Attempt to disrupt, reroute, or manipulate data.
3. Find out if the device could be disabled or re-engineered.

Table 11 below summarizes the tests performed, findings, and potential impacts after the conclusion of testing on 15-18 September. Where fixes and retests were required, the table also describes the finding after verification of fixes was performed. Due to the controlled nature of the tests performed, detailed results are available to government organizations upon request and approval. Inquiries should be directed to Tapan Patel, Tapan.C.Patel@usace.army.mil.

Table 11. Summary of TSMO Tests and Findings

Test	Finding	Potential impact
Attempt to send data “upstream” through diode	Scans revealed no data flowing from output to input side. Multimeter continuity checks showed no continuity between output and input sides	Performed as expected
Attempt to disrupt device operation via various methods (file manipulation, DDoS, physical attacks)	Diode continued to operate successfully	Performed as expected
Attempts to tamper with or gain access to diode	Diode did not allow access. Tamper event was detected and locked diodes	Performed as expected
Radio Frequency (RF) emissions during normal operation	No significant RF emissions were found to be present	Performed as expected

5.1.2 CSTB Penetration Test Results

The Naval Facilities (NAVFAC) Engineering Expeditionary Warfare Center (EXWC) Control Systems Test Bed (CSTB) penetration testing team was tasked with executing the penetration test of the Fend Incorporated Data Diode in order to identify security vulnerabilities. The testing was conducted at the NAVFAC EXWC Control Systems Test Bed (CSTB), Port Hueneme, California the week of May 24, 2021. Diode model FD-5M-SE1-XE2-B3 was tested.

All activities were conducted in a manner that simulated either a non-adversarial or adversarial threat actor engaged in a targeted attack against the Fend Data Diode with the test objectives of:

- Testing if data could only be sent in one direction (input-to-output).
- Discovering if the device could be disabled or re-engineered.
- Attempting to use the device as an attack “pivot” to its connected network(s).
- Evaluating the device against DISA-approved metrics

Efforts made on the identification and exploitation of security weaknesses emulated those of an attacker seeking to subvert the purpose-built functionality of the Fend data diode. These attacks presumed varying levels of access (in consideration of both general external users from the “output” side of the device and non-authorized insider threats from the “input” side). The assessment conducted followed recommendations outlined in NIST SP 800-115. All tests and actions conducted were under controlled conditions.

Table 12 below summarizes the tests performed, findings, and potential impacts after the conclusion of testing. Where fixes and retests were required, the table also describes the finding after verification of fixes was performed. Due to the controlled nature of the tests performed, detailed results are available to government organizations upon request and approval. Inquiries should be directed to Tapan Patel, Tapan.C.Patel@usace.army.mil.

Table 12. Summary of CSTB tests and findings

Test	Finding	Potential impact
Attempt to send data “upstream” through diode	Attempts to send data upstream or otherwise log into the diode from the output side were unsuccessful	Performed as expected
Attempt to disrupt device operation via various methods (file manipulation, DDoS, physical attacks)	Diode continued to operate successfully	Performed as expected
Attempts to use the device as an attack “pivot” to its connected network(s)	Attempt to perform a same-side pivot transfer (compromising a target to move laterally through a network) were unsuccessful	Performed as expected
Attempts to manipulate the device from an insider threat perspective	Identified some potential areas for improvement regarding the configuration login and settings processes including time allowed to log in and ability to change password.	Fend took subsequent mitigation steps through firmware updates to resolve identified issues. A “verification of fixes” retest was performed.

In addition to the testing described above, ERDC-CERL also scanned the diodes with the DoD Assured Compliance Assessment Solution (ACAS), and more specifically, the Nessus tool. The Nessus tool is a DoD wide tool which scans target machines/systems for vulnerabilities. Nessus is updated daily to include Common Vulnerabilities and Exposures (CVE). A Nessus scan will scan the target to identify any potential vulnerabilities that could be exploited. These could be items such as open ports and protocols, misconfiguration of devices, outdated software, or operating system. Findings are often listed by severity ranging from CAT I (high severity) to CAT III (low severity). ERDC CERL requires scanning devices before adding them to the network.

The Nessus tool did not have any findings on the diode. This means that, where possible, the Nessus tool scanned the diode for vulnerabilities but did not detect any issues/misconfigurations. The Nessus tool is configuration specific; while the tool did not find any issues with the particular configuration tested, the diodes should be tested anytime any configurational changes are made.

5.2 PO-2, 3, AND 5 TEST RESULTS

5.2.1 Objective

The goals of this effort were to determine the compatibility of the data diodes with common Utility Monitoring and Control System (UMCS) front-ends and devices, confirm non-interference, ease of installation, and facilitation of data collection. There were two specific objectives:

- 1) CSTL testing: The diodes were first tested at USACE ERDC CERLs Control System Test Lab (CSTL). The CSTL replicates common devices and software typically found with a UMCS. These tests were to ensure compatibility with Lon, BACnet and MODBUS serial and IP devices. The tests also ensured the integrity of the data being reported by the diode. Note: Certain proprietary protocols such as Fox were not tested as part of this effort. This testing focused on open protocols which can readily be tested/configured for use with the data diodes
- 2) Real-world testing at CERL: After testing in the CSTL, the diodes were then tested in a real-world control system. The objective of these real-world tests was to ensure data integrity and long-term availability of the data.

5.2.2 Architecture

The architecture used to test the diode is shown in Figure 9, below provides a schedule of the hardware and devices.

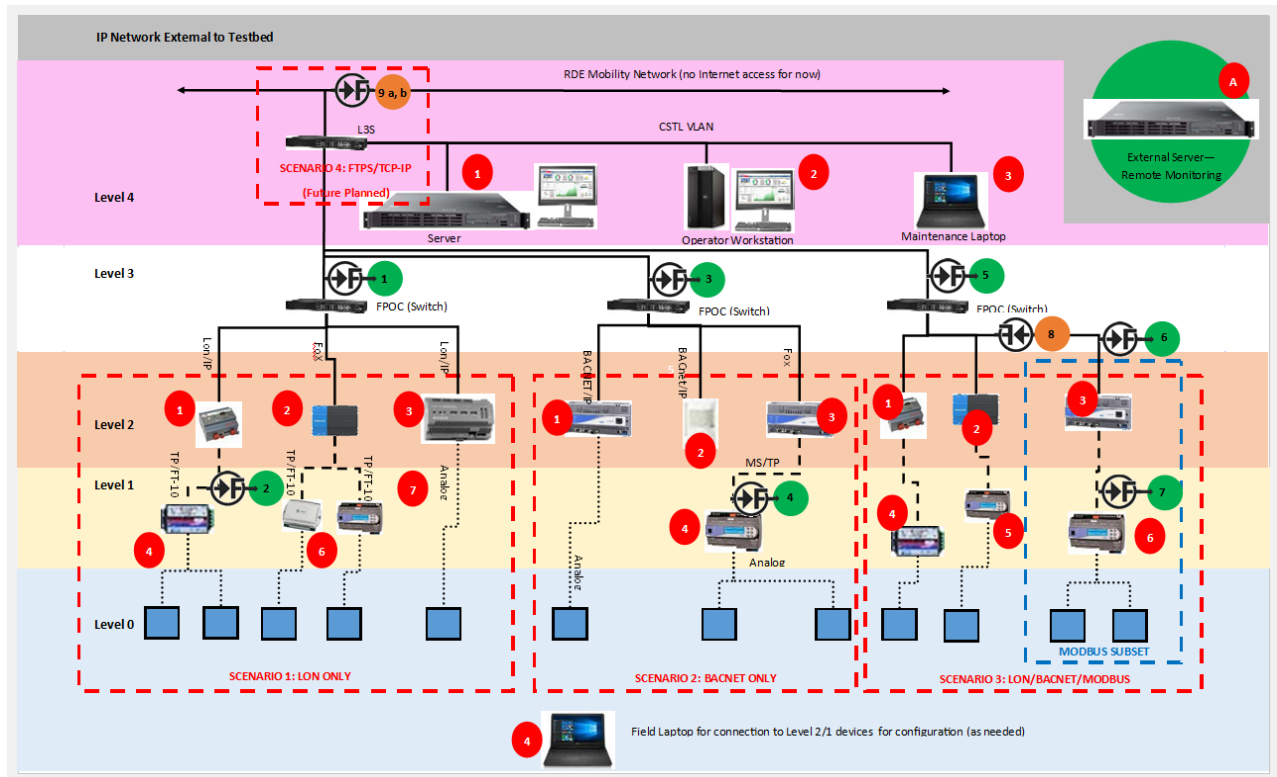


Figure 9. CSTL Diode Architecture

Table 13. Hardware and Device Schedule by Scenario

Scenario 1: LON ONLY		
Device #	Make/Model	Purpose
1	Echelon Lonpoint Router	Level 2, TP/FT-10 to LON/IP Router
2	JACE 800	Level 2, TP/FT-10 (or others) to IP. Can use as web server
3	Echelon iLon 100	Level 2, TP/FT-10 to LON/IP. Web server. Analog input
4	TAC MNL 10RF3	Level 1, Analog and S-Link to LON/IP. Integrate w/ MN-S3HT-500 Level 0 device
5	N/A	
6	TAC Xenta 100	Level 1, Analog to TP/FT-10
7	Loytec L-switch XP EIA-709	Level 1, TP/FT-10 to LON/IP and Analog to TP/FT-10

Scenario 2: BACNET ONLY		
Device #	Make/Model	Purpose
1	TAC MNB 1000	Level 2, MS/TP to BACNET/IP or Analog to BACNET/IP
2	Honeywell	CIPer 10
3	Lynxspring Jenesys-PC 3000 (JACE) - Now JACE 8000	Level 2, MS/TP to BACNET/IP. Can use as Webserver
4	MNB 300	Level 1, Analog to MS/TP

Scenario 3: Mixed Protocol		
Device #	Make/Model	Purpose
1	Echelon Lonpoint Router	Level 2, TP/FT-10 to LON/IP Router
2	JACE 800 (Make TBD)	Level 2, TP/FT-10 (or others) to IP. Can use as web server
3	Anybus	Modbus Gateway
4	TAC MNL 10RF3	Level 1, Analog and S-Link to LON/IP. Integrate w/ MN-S3HT-500 Level 0 device
5	Datanab	Temperature/Humidity Sensor (Modbus TCP)
6	Pixsys DRR245	Modbus/RTU

Other Hardware/Software		
Device #	Make/Model	Purpose
1	Dell R440 Server	To host Niagara Front-End
2	Dell Workstation	Engineering Tools, if required
3	Dell Laptop	Engineering Tools, if required
4	Field Laptop	Engineering Tools, if required
A	Maintenance Laptop	Data receiving server

5.2.3 List of CSTL tests

A list of the planned CSTL testbed tests is provided below in Table 14. The last column indicates whether those tests have been completed (as of the date of this report). Due to some technical/test design issues and the COVID-19 pandemic, only 7 of the 11 originally planned tests have been completed. Two of the remaining tests 9b and 10 are still contemplated for future testing. Results for the completed tests are discussed in this report and are sufficient to confirm project objectives.

Table 14. List of CSTL Tests

Test Description						
Test #	Input Protocol	Output Protocol	Target Location	Function	Test Complete?	Test successful?
1	LON-IP	TCP/IP	Maintenance Laptop	Tap	Yes ^a	Yes
2	LONTalk-Serial (with converter)	TCP/IP	Maintenance Laptop	Tap	No ^b	N/A
3	BACnet-IP	TCP/IP	Maintenance Laptop	Tap	Yes	Yes
4	BACnet-Serial	TCP/IP	Maintenance Laptop	Tap	Yes	Yes
5	Modbus-TCP	TCP/IP	Maintenance Laptop	Tap	Yes	Yes
6	Modbus-Serial	TCP/IP	Maintenance Laptop	Tap	Yes	Yes
7	Modbus-Serial (Multiple Devices)	TCP/IP	Maintenance Laptop	Tap	No ^c	N/A
8	Modbus-TCP	Modbus-TCP	Maintenance Laptop	Passthrough	Yes	Yes
9a	FTP (Data in file format)	FTP/FTPS (Data in file format)	TSMO & CSTB	Passthrough	Yes	Yes
9b (Future Planned)	TCP/IP	Secure TCP/IP	RDE Mobility Network	Passthrough	N/A ^d	N/A
10 (Future Planned)	Modbus-Serial	Modbus-Serial	Maintenance Laptop	Tap	N/A ^e	N/A

a – Due to technical difficulties with Lonworks equipment, this test was not conducted in the CSTL. However, test #11 at CERL showed that the diode performed as expected. Therefore, this test is considered successful

b – Due to technical difficulties with Lonworks equipment, this test was not conducted in the CSTL

c – Unable to procure multiple Modbus serial test devices required for CSTL test

d – This feature is currently unavailable within the diodes, but is a planned feature. This test is plan for the future (date TBD)

e – This feature is currently unavailable within the diodes, but is a planned feature. This test is plan for the future (date TBD)

5.2.4 List of CERL tests

After the CSTL tests were complete, the following tests were conducted at CERL in a real-world operational UMCS. Table 15 described the list of tests conducted at CERL.

Table 15. List of CERL Tests

Test Description						
Test #	Input Protocol	Output Protocol	Target Location	Function	Test Complete?	Test successful?
11	LON-IP	TCP/IP	Maintenance Laptop	Tap	Yes	Yes
12	BACnet-IP	TCP/IP	Maintenance Laptop	Tap	Yes	Yes

Test #11 occurred at Building 3 at CERL. The LON-IP controller, an Echelon i.Lon® 600 LonWorks/IP Server, monitors an HVAC system within a portion of the facility. Figure 10 shows a picture of the controller.



Figure 10. i.Lon 600

Figure 11 shows an example of the various parameters that are reported to the i.Lon 600. Note that because of the large quantity of parameters (and how often they are typically polled/reported), only a few parameters were analyzed/investigated for integrity. As seen, the temperatures reported below are for various VAVs.

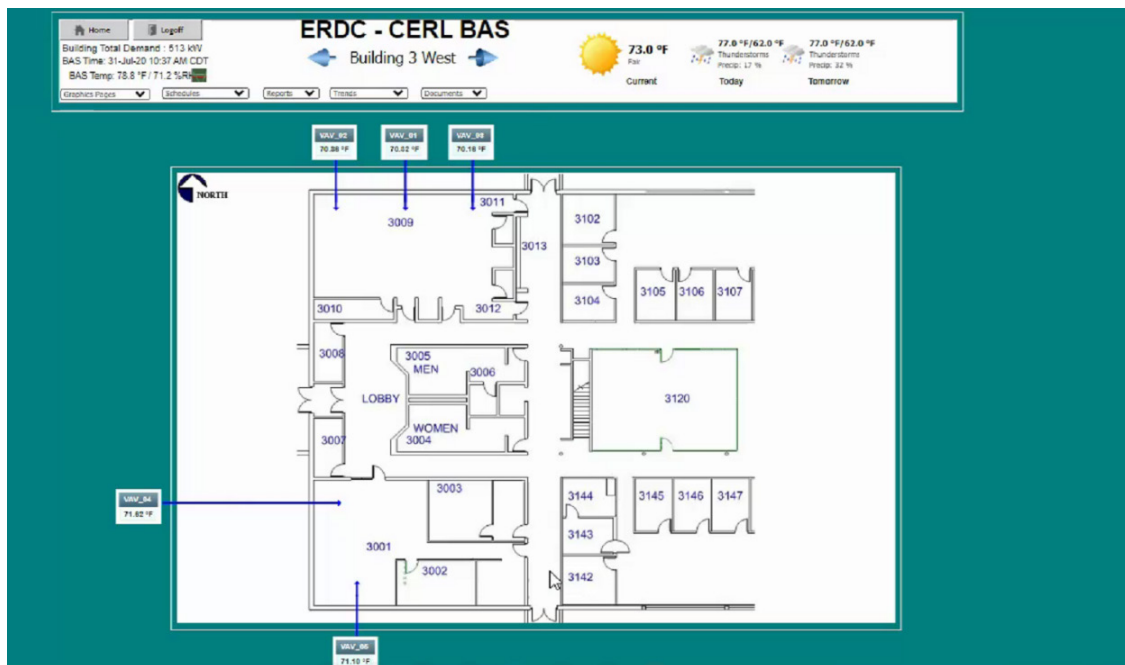


Figure 11. Screenshot of UMCS for Building 3 - West at CERL

Test #12 occurred the “Solar House” facility. This facility is a small administration building which operates on a BACnet network. Figure 12 below shows a screenshot of the single HVAC unit that serves the Solar House facility.

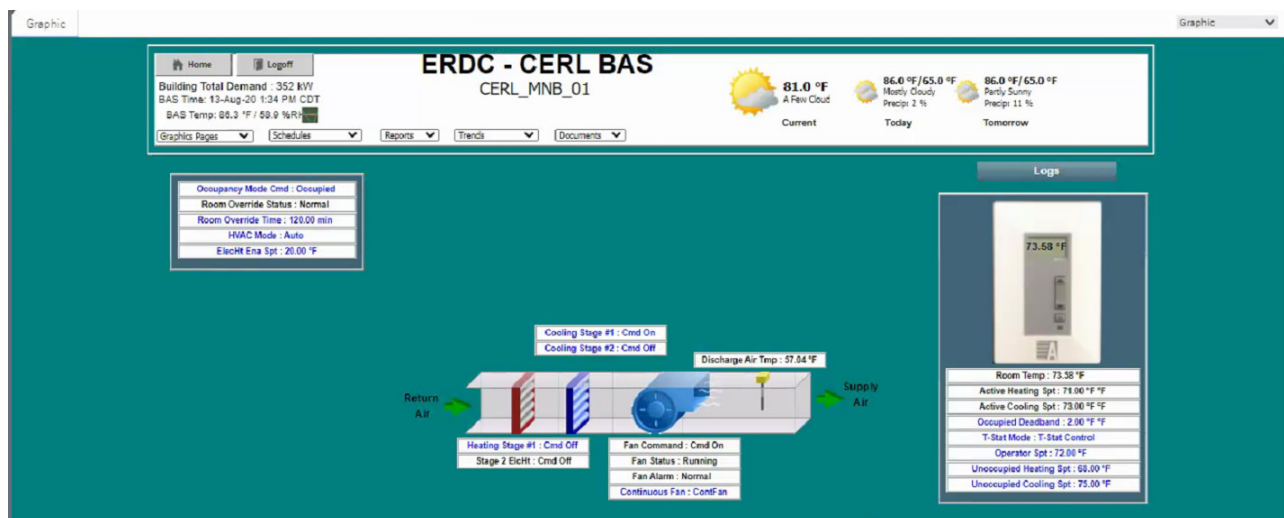


Figure 12. Solar House Facility

The screenshot shows the various parameters that are collected from the UMCS.

5.2.5 Data Analysis

For each of the tests described in Table 14, two packet capture activities were conducted:

- 1) Baseline data capture: This baseline data capture was conducted to establish the information contained in any particular packet
- 2) Post-retrofit data capture: After the data diodes were installed, this data capture looked at the information sent by the diode

For any tests labeled as “Tap”, a span port (mirrored port) was set up on the switches. Any traffic between the front-end and the controller was mirrored and forwarded into either 1) Wireshark capture or 2) Into the diode. Any data coming out from the diode was collected using a TCP client or serial client, depending on the specific test requirements.

A comparison between the baseline data capture and post-retrofit data capture was conducted to determine if the integrity of the data was maintained. The tools used for each of the capture varied and are discussed within each of the tests, below.

5.2.5.1 Test # 1 Lon/IP to Lon/IP

Due to technical difficulties with Lonworks equipment, this test was not conducted in the CSTL. However, test #11 at CERL showed that the diode performed as expected. Therefore, this test is considered successful. For detailed results, see Section 5.2.5.11.

5.2.5.2 Test # 2 Lon/Serial to Lon/Serial

Due to technical difficulties with Lonworks equipment, this test was not conducted in the CSTL

5.2.5.3 Test # 3 - BACNET IP to BACNET IP

For this test, a Schneider Electric MNB-1000 was used to collect basic temperature data. The data was reported to a Tridium Niagara Front-End.

5.2.5.3.1 Baseline

Two tools were used to analyze the baseline, Wireshark and CASBACnet tool. Wireshark is a widely used network protocol analyzer. CASBACnet is a purpose-built tool to analyze BACnet packets. It can accept Wireshark pcap files and perform an analysis on those files.

Looking at Wireshark, we can see that the BACnet traffic present on this capture is valid BACnet IP traffic. The packet list pane, shown below, shows the Confirmed Request/Complex Acknowledgement exchange routine to BACnet traffic.

No.	Time	Source	Destination	Protocol	Length	Info
170	129.172680	170.168.0.15	170.168.255.255	BACnet-APDU	66	Unconfirmed-REQ i-Am device,1110000
171	129.178099	170.168.0.5	170.168.255.255	BACnet-APDU	72	Unconfirmed-REQ i-Am device,1110000
204	155.224907	170.168.0.15	170.168.0.16	BACnet-APDU	60	Confirmed-REQ readProperty[1] device,1111001 system-status
205	155.237071	170.168.0.16	170.168.0.15	BACnet-APDU	62	Complex-ACK readProperty[1] device,1111001 system-status
206	156.187003	170.168.0.15	170.168.0.16	BACnet-APDU	205	Confirmed-REQ readPropertyMultiple[2]
207	156.247278	170.168.0.16	170.168.0.15	BACnet-APDU	302	Complex-ACK readPropertyMultiple[2]
218	161.187304	170.168.0.15	170.168.0.16	BACnet-APDU	205	Confirmed-REQ readPropertyMultiple[3]
219	161.207055	170.168.0.16	170.168.0.15	BACnet-APDU	302	Complex-ACK readPropertyMultiple[3]
228	166.204451	170.168.0.15	170.168.0.16	BACnet-APDU	65	Confirmed-REQ writeProperty[4] binary-value,14 present-value
229	166.247091	170.168.0.16	170.168.0.15	BACnet-APDU	60	Simple-ACK writeProperty[4]
230	166.247095	170.168.0.15	170.168.0.16	BACnet-APDU	62	Confirmed-REQ writeProperty[5] analog-value,16 present-value
231	166.257261	170.168.0.15	170.168.0.16	BACnet-APDU	61	Confirmed-REQ readPropertyMultiple[6]

Figure 13. Test 3 Baseline Wireshark

Additional details of packet 206 is provided below. As can be seen, this particular packet contains several analog and binary values that are reported with the readPropertyMultiple property in the BACnet packet. Expanding further on analog-value #14 shows additional information including the reported value. This can be correlated back to a specific output in the controller if desired.

The image shows a Wireshark capture of BACnet traffic. The top pane displays a list of 27 packets. The bottom pane shows the detailed view of the selected packet (No. 285), which is a BACnet readPropertyMultiple request. The decoded structure is as follows:

```

> User Datagram Protocol, Src Port: 47808, Dst Port: 47808
> BACnet Virtual Link Control
> Building Automation and Control Network NPDU
  > Building Automation and Control Network APDU
    0000 .... = APDU Type: Confirmed-REQ (0)
    > .... 0010 = PDU Flags: 0x2
    .000 .... = Max Response Segments accepted: Unspecified (0)
    .... 0011 = Size of Maximum APDU accepted: Up to 480 octets (fits in an ARCNET frame) (3)
    Invoke ID: 2
    Service Choice: readPropertyMultiple (14)
    > ObjectIdentifier: binary-value, 14
    > listOfPropertyReferences
    > ObjectIdentifier: analog-value, 14
    > listOfPropertyReferences
      > {[1]
        .... 1... = Tag Class: Context Specific Tag
        0001 .... = Context Tag Number: 1
        .... .110 = Named Tag: Opening Tag (6)
        > Property Identifier: present-value (85)
        > Context Tag: 0, Length/Value/Type: 1
          .... 1... = Tag Class: Context Specific Tag
          0000 .... = Context Tag Number: 0
          Length Value Type: 1
          Property Identifier: present-value (85)
          > {[1]
            .... 1... = Tag Class: Context Specific Tag
            0001 .... = Context Tag Number: 1
            .... .111 = Named Tag: Closing Tag (7)
          }
        > ObjectIdentifier: analog-value, 16
        > listOfPropertyReferences
        > ObjectIdentifier: binary-value, 7
        > listOfPropertyReferences
        > ObjectIdentifier: analog-value, 15
        > listOfPropertyReferences
      }
    > listOfPropertyReferences
  }

```

Figure 14. Test 3 – Baseline BACnet Wireshark Output (Detailed)

The report generated using the CASBACnet tool also indicates that the traffic is normal. As the below statistics show, the tool was able to successfully process and interpret the entire capture, indicating that the traffic is valid.

The image shows the output of the CASBACnet Tool report. The statistics are as follows:

```

WIRESHARK BACNET REPORT TOOL v1.0.0
-----
FYI: Packets received: 75
FYI: Packets successfully processed: 75
FYI: Packets unsuccessfully processed: 0

Global PDU Count
-----
- Complex-Ack: 25
- Confirmed-REQ: 37
- Simple-Ack: 12
- Unconfirmed-REQ: 1

```

Figure 15. Test 3 Baseline CASBACnet Tool

The report, corresponding XML files, and the original capture are provided in the appendix.

5.2.5.3.2 *Post-Retrofit*

The diode was installed as a tap to the BACnet MNB-1000 controller. This means that any traffic that was being sent/delivered between the MNB-1000 and the Niagara Front-End was forwarded to the diode. The diode would then inspect those packets and repackage them into a human readable format (i.e. JSON, ASCII). This was done to make it easier for the operator to ensure the integrity of the data being reported.

5.2.5.3.3 *Test #3 Outcome*

This test was successful. The output identifiers and their corresponding values are the same as that represented by the front-end.

5.2.5.4 *Test # 4 – BACnet Serial to TCP/IP*

For this test, an MNB-100 (which communicates over BACnet MS/TP) was connected to a JACE 8000, which converts the MS/TP packets into IP packets.

5.2.5.4.1 *Baseline*

For the baseline test, individual MS/TP packets were not captured, but rather were reported through a Wireshark packet capture of the IP traffic being generated by the JACE 8000 from the serial traffic off the MNB-100. This IP traffic showed the values contained within the MS/TP packets and served as an easier comparison for the TCP/IP traffic exiting the diode.

An example of the packet collected for this baseline is shown below and is similar to that in Figure 14. Although the structure of the packets is different between the BACnet serial and BACnet IP, the important information is contained within the BACnet packet. For example, in the example below, the field “analog-value (x)” appears multiple times. This analog-value property is a function of the BACnet protocol. This analog-value represents a particular analog sensor that’s connect to the MNB-1000 (e.g. temperature sensor, 4-20 mA current signal, 2-10 VDC signal, etc).

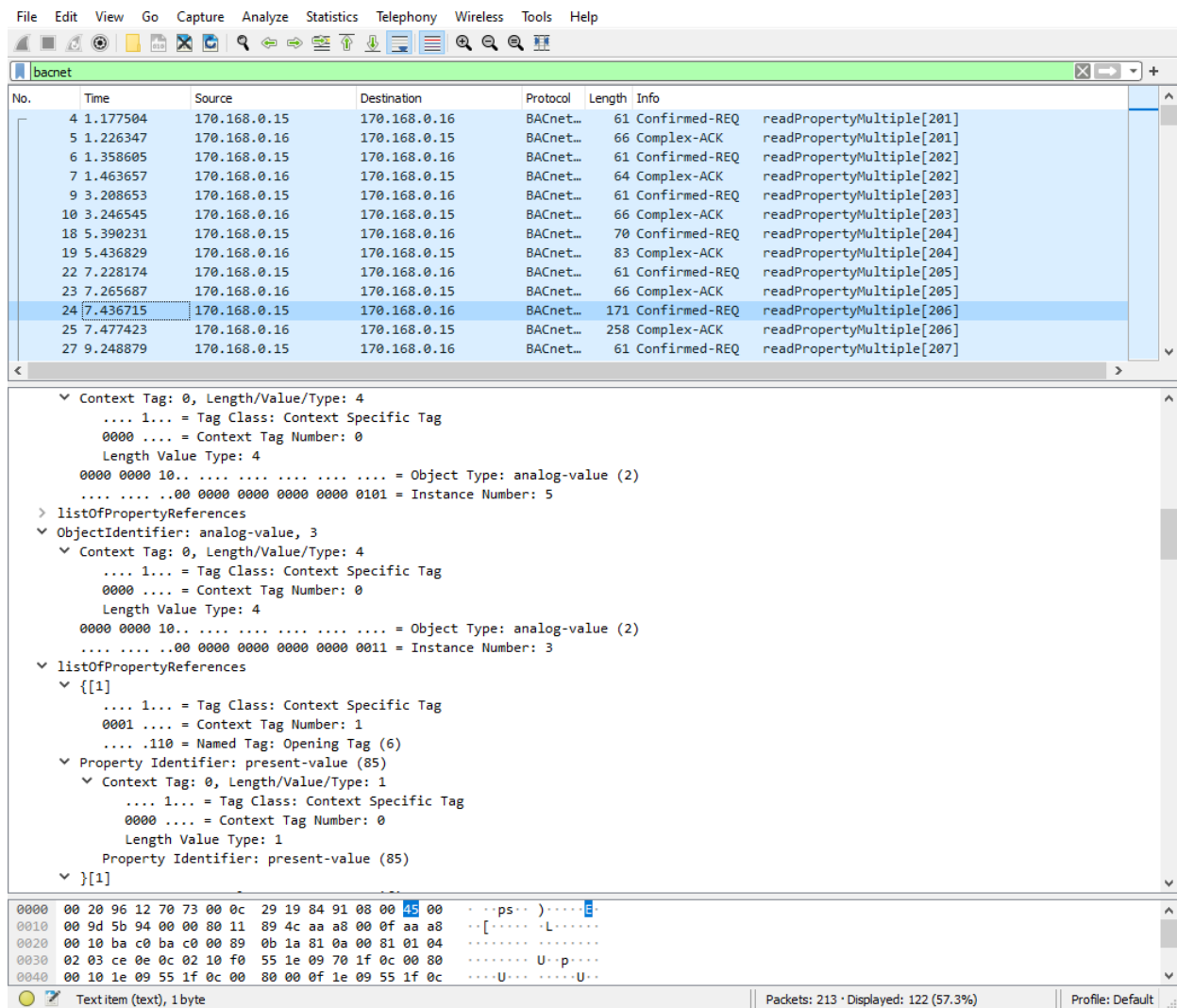


Figure 16. Test #4 Baseline Packet Capture

5.2.5.4.2 Post-Retrofit

In this scenario, the diode was installed as a tap to the MNB-1000. The twisted pair conductors were connected to the diode input. A set of twisted pair conductors were connected to the diode output. The data export from the diode was formatted as ASCII to make it human readable. While the data was presented on screen, the live readings from the Niagara front-end were confirmed. The figure below shows the data produced by the diode.

```

#4BACNET_SERIAL-IP.txt - Notepad
File Edit Format View Help
Src: 1
Dst: 0
analog-value #389
{
  present-value: 70.999992
  instance-of: BACnet Error: device: other
}

16:03:39 :
Src: 1
Dst: 0
analog-value #17
{
}

16:03:43 :
Src: 1
Dst: 0
analog-value #390
{
  present-value: 72.999992
  present-value: 72.999992
  present-value: 72.999992
}

```

Figure 17. Test #4 Post-Retrofit Data

As seen, the diode reports similar data to what's shown in the Wireshark packet. For example, the analog identifier for each point along with the present value of that particular identifier. In this case, analog value #389 shows a value of 72.99F which is consistent with what was shown on the Front-End.

5.2.5.4.3 Test #4 Outcome

This test was successful. The output identifiers and their corresponding values are the same as that represented by the front-end.

5.2.5.5 Test # 5 – Modbus Serial to TCP/IP

In this test, a Modbus TCP/IP temperature and humidity probe were connected to the Niagara Front-End.

5.2.5.5.1 Baseline

The traffic for this baseline test was captured using Wireshark. A screen grab of the filtered Modbus traffic is shown below.

No.	Time	Source	Destination	Protocol	Length	Info
133	13.322415	170.168.0.37	170.168.0.15	Modbus/TCP	67	Response: Trans: 583; Unit: 2, Func: 3: Read Holding Registers
150	15.319787	170.168.0.15	170.168.0.37	Modbus/TCP	66	Query: Trans: 587; Unit: 2, Func: 3: Read Holding Registers
151	15.325650	170.168.0.37	170.168.0.15	Modbus/TCP	65	Response: Trans: 587; Unit: 2, Func: 3: Read Holding Registers
160	18.320326	170.168.0.15	170.168.0.37	Modbus/TCP	66	Query: Trans: 593; Unit: 2, Func: 3: Read Holding Registers
161	18.323591	170.168.0.37	170.168.0.15	Modbus/TCP	67	Response: Trans: 593; Unit: 2, Func: 3: Read Holding Registers
165	20.320447	170.168.0.15	170.168.0.37	Modbus/TCP	66	Query: Trans: 597; Unit: 2, Func: 3: Read Holding Registers
166	20.323410	170.168.0.37	170.168.0.15	Modbus/TCP	65	Response: Trans: 597; Unit: 2, Func: 3: Read Holding Registers
171	23.319088	170.168.0.15	170.168.0.37	Modbus/TCP	66	Query: Trans: 603; Unit: 2, Func: 3: Read Holding Registers
172	23.321627	170.168.0.37	170.168.0.15	Modbus/TCP	67	Response: Trans: 603; Unit: 2, Func: 3: Read Holding Registers
177	25.320417	170.168.0.15	170.168.0.37	Modbus/TCP	66	Query: Trans: 607; Unit: 2, Func: 3: Read Holding Registers
178	25.325432	170.168.0.37	170.168.0.15	Modbus/TCP	65	Response: Trans: 607; Unit: 2, Func: 3: Read Holding Registers
181	28.320602	170.168.0.15	170.168.0.37	Modbus/TCP	66	Query: Trans: 613; Unit: 2, Func: 3: Read Holding Registers

Figure 18. Test #5 Baseline Wireshark Summary

A detailed look at packet 161, below, shows that register 304 reads 395. This value corresponds to the humidity at that time (39.5% Relative Humidity). For this controller, register 100 reads the temperature in Fahrenheit (762 or 76.2F) as shown in Figure 20.

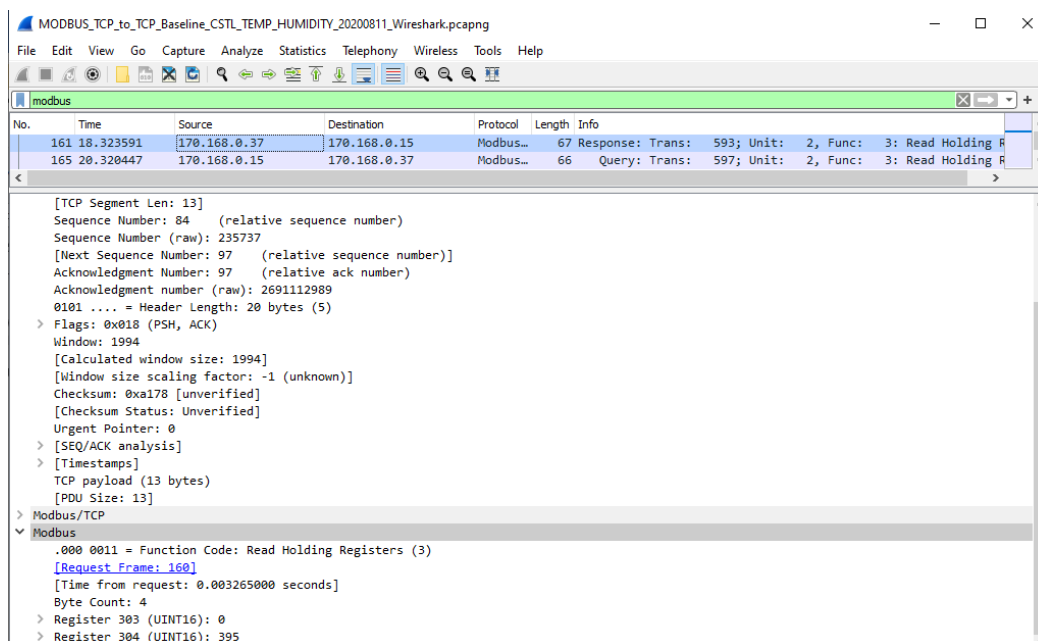


Figure 19. Test #5 Baseline (Detailed), Relative Humidity

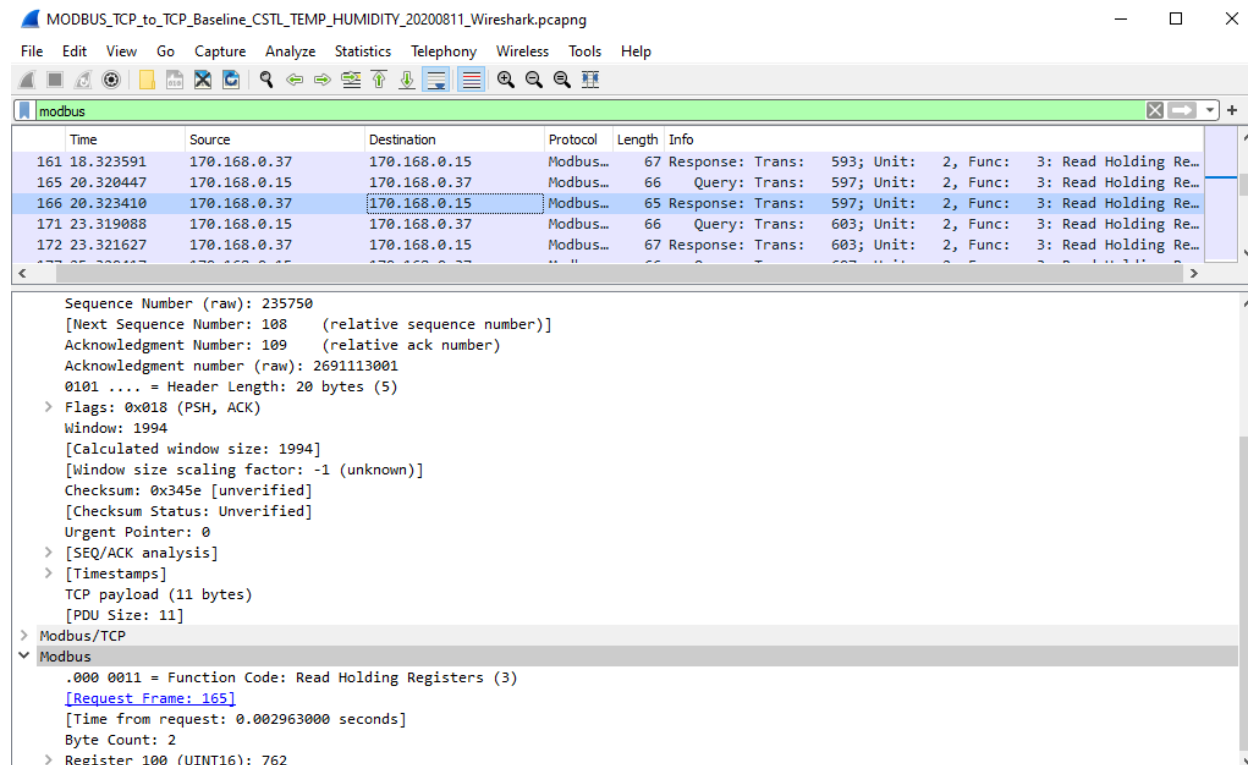


Figure 20. Test #5 Baseline (Detailed), Temperature

5.2.5.5.2 *Post-Retrofit*

The diode was installed as a tap between the Temperature/Humidity sensor and the Front-End. Any queries/responses were replicated by a port mirror and transmitted to the diode. The output format was human readable (ASCII). The same registers, as shown above, were clearly evident in the diode output:

```
16:09:46 :  
Modbus TCP  
Source IP: 170.168.0.37  
Destination IP: 170.168.0.15  
Transaction ID: 118  
Device Addr: 2  
Function code: 3  
Register Start Addr: 303  
Data Byte Cnt: 4  
Register vals:  
    303      : 0  
    304      : 397
```

Figure 21. Test #5 Post-Retrofit, Relative Humidity

As seen in the figure above, the diode transmitted the relative humidity information (39.7% RH) which was verified by the Front-End as well. Similarly, the temperature data was also available (76.1 F, register 100) as shown below:

```
16:09:48 :  
Modbus TCP  
Source IP: 170.168.0.37  
Destination IP: 170.168.0.15  
Transaction ID: 122  
Device Addr: 2  
Function code: 3  
Register Start Addr: 100  
Data Byte Cnt: 4  
Register vals:  
    100      : 761  
    101      : 0
```

Figure 22. Test #5 Post Retrofit, Temperature

5.2.5.5.3 *Test #5 Outcome*

This test was successful. The output identifiers and their corresponding values are the same as that represented by the front-end.

5.2.5.6 *Test # 6 – Modbus Serial to TCP/IP*

For this test, a Modbus RTU temperature controller (Pixsys DRR245) was connected to an Anybus Gateway, which translates the Modbus RTU traffic into Modbus/IP. The Modbus IP traffic was analyzed through Wireshark for the baseline. The IP traffic was then sent to the diode for the post-retrofit analysis.

5.2.5.6.1 *Baseline*

The traffic in the baseline captures is Modbus RTU traffic which has been converted into TCP traffic through the Anybus Gateway. For example, the packet highlighted in the screen grab below, frame 2, is a **Query** packet with the function code for **Read Holding Registers**. The register in question has the reference number 1009. All of this can be seen by looking at the **Info** section in the packet list pane and under the **Modbus** tab in the packet details pane.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_a6:95:81	Spanning-tree-(for-...	STP	60	RST. Root = 32768/1/00:76:86:07:8b:80 Cost = 4 Port = 0x8001
2	0.406484	170.168.0.15	170.168.0.38	Modbus/TCP	66	Query: Trans: 162; Unit: 5, Func: 3: Read Holding Registers
3	0.406906	170.168.0.38	170.168.0.15	TCP	60	502 → 49704 [ACK] Seq=1 Ack=13 Win=5840 Len=0
4	0.445043	170.168.0.38	170.168.0.15	Modbus/TCP	65	Response: Trans: 162; Unit: 5, Func: 3: Read Holding Registers
5	0.454905	170.168.0.15	170.168.0.38	TCP	60	49704 → 502 [ACK] Seq=13 Ack=12 Win=2049 Len=0
6	1.400861	170.168.0.15	170.168.0.38	Modbus/TCP	66	Query: Trans: 164; Unit: 5, Func: 3: Read Holding Registers
7	1.401480	170.168.0.38	170.168.0.15	TCP	60	502 → 49704 [ACK] Seq=12 Ack=25 Win=5840 Len=0
8	1.434628	170.168.0.38	170.168.0.15	Modbus/TCP	65	Response: Trans: 164; Unit: 5, Func: 3: Read Holding Registers
9	1.446377	170.168.0.15	170.168.0.38	TCP	60	49704 → 502 [ACK] Seq=25 Ack=23 Win=2049 Len=0
10	1.452136	170.168.0.15	170.168.0.38	Modbus/TCP	66	Query: Trans: 165; Unit: 5, Func: 3: Read Holding Registers
11	1.452139	170.168.0.38	170.168.0.15	TCP	60	502 → 49704 [ACK] Seq=23 Ack=37 Win=5840 Len=0
12	1.485438	170.168.0.38	170.168.0.15	Modbus/TCP	65	Response: Trans: 165; Unit: 5, Func: 3: Read Holding Registers

> Ethernet II, Src: VMware_19:84:91 (00:0c:29:19:84:91), Dst: HWSIndus_fa:a9:21 (00:30:11:fa:a9:21)
 > Internet Protocol Version 4, Src: 170.168.0.15, Dst: 170.168.0.38
 > Transmission Control Protocol, Src Port: 49704, Dst Port: 502, Seq: 1, Ack: 1, Len: 12
 > Modbus/TCP
 Transaction Identifier: 162
 Protocol Identifier: 0
 Length: 6
 Unit Identifier: 5
 > Modbus
 .000 0011 = Function Code: Read Holding Registers (3)
 Reference Number: 1009
 Word Count: 1

Figure 23. Test #6 Baseline Wireshark Capture

Frame 3 is a TCP acknowledgement packet, showing that the receiving device acknowledges the query.

Frame 4 is a Modbus TCP response packet to the query in frame 2. The screen grab below shows the packet details pane for this frame. Underneath the **Modbus** tab it shows that the register with the reference number 1009 contains the value 1. This particular register 1009 is the position of a relay. The relay is inactive (0) if the measure temperature is above the setpoint. The relay becomes active (1) if the measured temperature is above the setpoint. In the figure below, the relay is active (1).

Transaction Identifier: 162
Protocol Identifier: 0
Length: 5
Unit Identifier: 5
▼ Modbus
.000 0011 = Function Code: Read Holding Registers (3)
[Request Frame: 2]
[Time from request: 0.038559000 seconds]
Byte Count: 2
▼ Register 1009 (UINT16): 1
Register Number: 1009
Register Value (UINT16): 1

Figure 24. Test #6 Wireshark Modbus Details

This sequence of Modbus queries followed by TCP acknowledgements and Modbus responses repeats throughout the capture without issue.

5.2.5.6.2 Post-Retrofit

The diode was installed as a tap into the 3 wire RTU connection. Any polls from the Gateway and any responses by the RTU controller were both captured and reported by the diode. Similar to the BACnet captures, the diode was configured to produce the data in a human readable format. Due to the increased number of modifications possible in the RTU controller, several temperature changes/setpoints were tested and discussed here. In the first case, the Modbus Gateway polled the RTU controller for Register 1009. The response, as reported by the diode is shown below in Figure 25.

```

15:52:47 :
Modbus RTU
Device Addr: 5
Function code: 3
Register Start Addr: 1009
Data Byte Cnt: 2
Register values:
      1009      : 1

```

Figure 25. Test #6 Post Diode Data

During this test, the temperature reading was ~24.7 C and the setpoint was 20 C. Therefore, the controller relay was off. A short while later, the setpoint was changed to 90C. This change is setpoint was recorded by the diode as shown in Figure 26.

```

15:52:52 :
Modbus RTU
Device Addr: 5
Function code: 3
Register Start Addr: 1001
Data Byte Cnt: 2
Register values:
      1001      : 900

```

Figure 26. Test #5 Post Diode Setpoint Change

The temperature reading was also verified. The temperature in the Front-End was reading 24.1 C. As seen below, the register 1000 (which is the temperature reading register) shows 241 or 24.1 C

```

15:54:54 :
Modbus RTU
Device Addr: 5
Function code: 3
Register Start Addr: 1000
Data Byte Cnt: 2
Register values:
      1000      : 241

```

Figure 27. Test #6 Post Diode Temperature Reading

5.2.5.6.3 Test #6 Outcome

This test was successful. The output identifiers and their corresponding values are the same as that represented by the front-end.

5.2.5.7 Test # 7 Modbus Serial to TCP/IP with Remote monitoring

Unable to procure multiple Modbus serial test devices required for CSTL test. Though the test was not performed at the CSTL, these tests have been conducted by Fend and shown to be successful.

5.2.5.8 Test # 8 Modbus TCP to Modbus TCP

The diode was installed in a passthrough configuration for the Pixsys temperature controller in conjunction with the Anybus Gateway. The diode was configured to poll the sensor for the temperature value. The output from the diode was then recorded.

5.2.5.8.1 Baseline

Similar to test #6, above, Wireshark packets along with readings from the Niagara front-end were used as a baseline test.

5.2.5.8.2 Post-Retrofit

The output from the diode correctly showed the temperature and yielded results identical to Figure 27.

5.2.5.8.3 Test #8 Outcome

This test was successful. The output identifiers and their corresponding values are the same as that represented by the front-end.

5.2.5.9 Tests #9a/#9b – FTP and TCP/IP to TCP/IP

Test 9a was conducted as part of testing by the Threat System Management Office (TSMO) and those results are provided in a separate report.

Test 9b is planned in the future once Secure TCP/IP is supported by the diode.

5.2.5.10 Test #10 – Modbus Serial to Modbus Serial

Test 10 is on hold and planned for the future once the diode can support Modbus-serial passthrough. However, this feature is not anticipated to be used widely due to the sheer number of serial devices in any plant. The cost of installing a diode in every Modbus/serial device would be prohibitive. It is generally better to add the diode at the Modbus/TCP level.

5.2.5.11 Test # 11 – Lon IP to TCP/IP

Due to the success of several tests above, the ERDC-CERL team made a decision to put the diodes in operation at CERL. The first of those tests included a short-term data capture to test the integrity of the data. In this test, an i.Lon 600 was used. The i.Lon communicates with a Niagara Front-End.

5.2.5.11.1 Baseline

In the baseline test, data between the i.Lon 600 and the Front-End was mirrored to a laptop containing the Wireshark tool.

Figure 28 below shows the output from the Wireshark capture

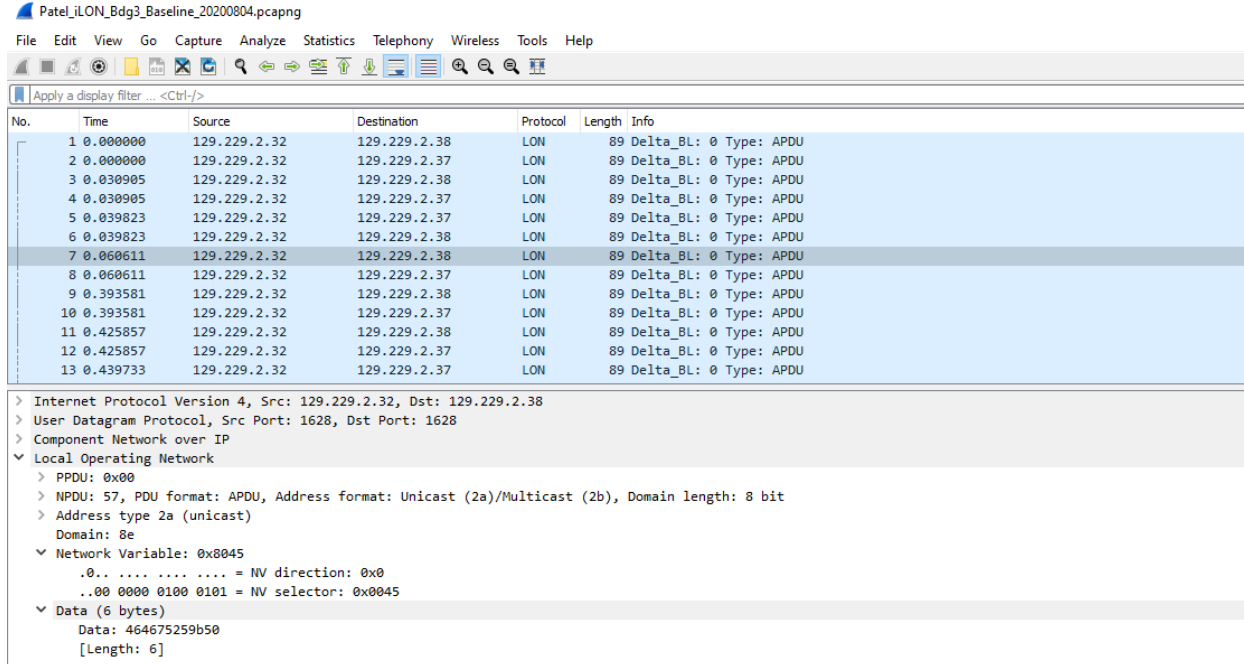


Figure 28. Test #11 Baseline Wireshark Capture

As seen, Wireshark recognizes the protocol as LON. Some key elements such as the Domain, Network Variable including NV Direction and NV Selector are visible in the frames of the packet. The data is also visible.

In the front-end it is possible to view some of these variables and to confirm/correlate that they are visible in the Wireshark data packet. The screenshot below shows an output from the Niagara Front-End which shows each point and its respective data. As seen, some of the variables such as Domain, Network Variable, etc., are clearly identifiable. This spreadsheet is used to correlate packets within Wireshark and the Diode Output to variables within Niagara.

1	Name	Summary	Nv Index	Snvt Type	Object Index	Member Index	Poll Enable	Polled	Auth Conf	Service Conf	Priority Conf	Modify Offline	Sync	Changeable
2	nviSatTemp1	-16.660 °C	9	105	0	4	TRUE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE
3	nvoSpaceTemp	22.310 °C	2	105	0	3	TRUE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE
4	nvoSatState1	false, false, false, false, ...	44	83	0	39	TRUE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE
5	nvoSatTemp1	24.380 °C	29	105	0	24	TRUE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE
6	nviOccSchedule	ocUnoccupied, ocNul, 65535 min	7	128	0	2	TRUE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE

Figure 29. Niagara Front-End Export

In this case, the value of Space Temperature (Row 2) is 22.31 C. The NV Direction is Output and the NV Selector is 188.

5.2.5.11.2 *Post Retrofit*

In this example, the diode was installed in a tap configuration. It was configured to provide a human readable format. As seen in Figure 30 below, the same variables and their values are present. The values are the same as those represented by the front-end and as shown in the baseline capture.

```
13:56:39 :  
{"events":[{"type":"LON/IP","diode":"AB00001","payload":{"srcIP":"129.229.2.32","destIP":"129.229.2.38","SrcSubnet":9,  
"SrcNode":2,"DstSubnet":1,"DstNode":126,"Domain":"8e","NVDirection":0,"NVSelector":65,"Data":"4104c6e81c4c"}}]}
```

Figure 30. Post Retrofit Diode Output

5.2.5.11.3 *Test #11 Outcome*

This test was successful. The output identifiers and their corresponding values are the same as that represented by the front-end.

5.2.5.12 *Test # 12 – BACnet IP to TCP/IP*

The second test included a short-term data capture to test the integrity of the data. In this test, the Solar House MNB-1000 was communicating with the Niagara Front-End

5.2.5.12.1 *Baseline*

In the baseline test, data between the MNB-1000 and the Front-End was mirrored to a laptop containing the Wireshark tool.

Figure 31 below shows the output from the Wireshark capture. As can be seen, these are mostly BACnet packets. Additional details of the packet show a large number of variables that are being reported including: Analog Values #14, 391, 386, etc. and binary values #50, 9, 18, 13.

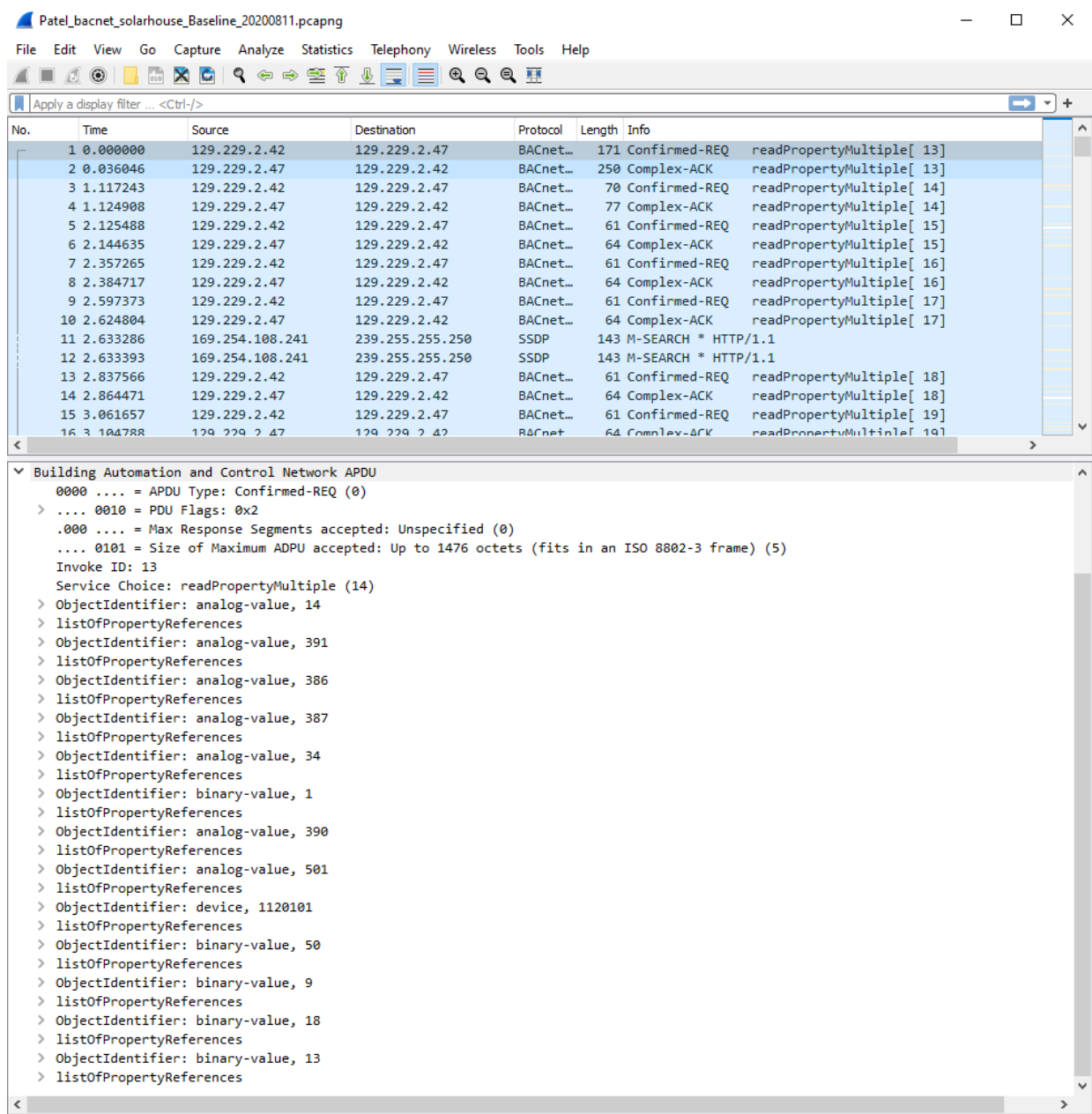


Figure 31. Test #12 Baseline Wireshark Capture

In the front-end it is possible to view some of these variables and to confirm/correlate that they are visible in the Wireshark data packet. The screenshot below shows an output from a tool used to configure the MNB-1000.

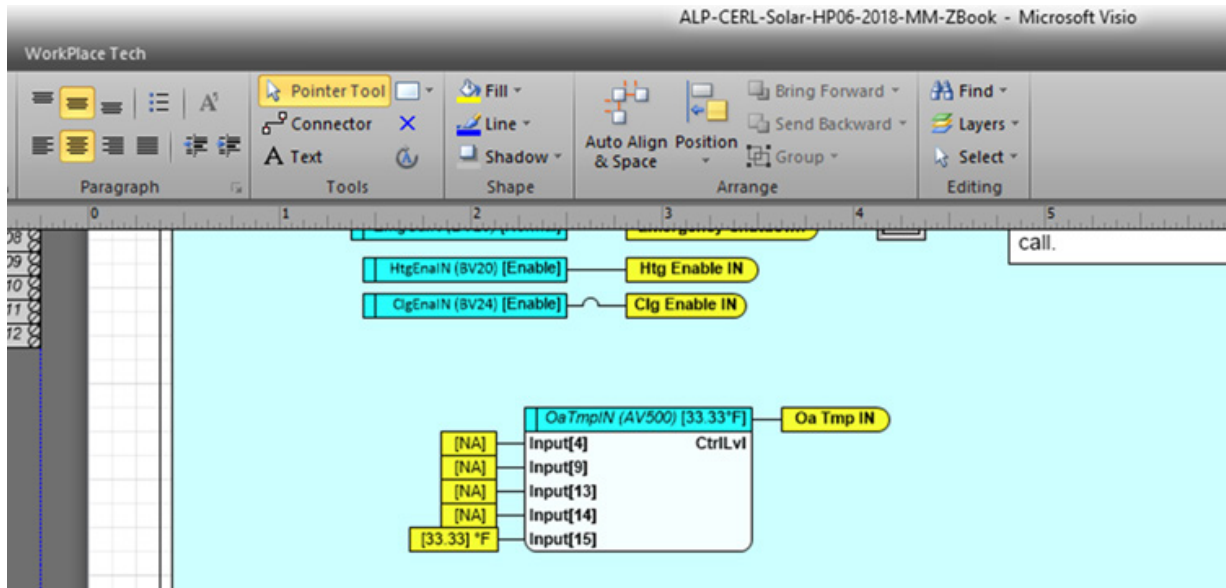


Figure 32. Niagara Front-End Export

In this case, analog value #500 (AV500) corresponds to the Outdoor Air Temperature.

5.2.5.12.2 Post Retrofit

In this example, the diode was installed in a tap configuration. It was configured to provide a human readable format. As seen in Figure 33 below, the same variables and their values are present (Analog Value #500 and Binary Value #4). The values are the same as those represented by the front-end and as shown in the baseline capture.

```
15:10:34 :
Src IP: 129.229.2.47
Dest IP: 129.229.2.42
PDU type: 3
analog-value #500
{
  present-value: 66.049995
}

15:10:39 :
Src IP: 129.229.2.47
Dest IP: 129.229.2.42
PDU type: 3
binary-value #4
{
  present-value: inactive
}
```

Figure 33. Post Retrofit Diode Output

5.2.5.12.3 Test #12 Outcome

This test was successful. The output identifiers and their corresponding values are the same as that represented by the front-end.

5.3 PO-4 RESULTS

Over the course of the project, ERDC CERL personnel repeatedly setup, configured and installed diodes under multiple scenarios. Once the underlying control system network has been configured, and changes have been approved (e.g., port mirroring, adjust firewall, etc), the installation process generally involves:

- 1) Identify data streams/configurations required at the input and output of the diode
- 2) Connect to and configure the diode for required input/outputs
- 3) Install diode physically in cabinet/room
- 4) Attach network cables and power up diode
- 5) Run data collection software to ensure data is flowing

Using the user's manual provided, various ERDC CERL team members were able to install the diodes in less than 1 hour (usually 30 minutes or less), which included steps 1-5, above. Most users were not extensively trained in the data diode software. In many cases, adjusting the non-diode-related upstream controls system network switches took more time due to multiple levels of coordination/approval required to make adjustments.

5.4 PO-6 RESULTS

5.4.1 Cost Assessment Results

Without appropriate cybersecurity measures in place, a breach of an OT systems goes beyond loss of data; the mission is at stake. Loss of a chiller to cyberattack may set off a chain reaction of loss: servers, network access, communications. Loss of a facility may also mean loss of staff productivity. Though the COVID-19 pandemic has shown many job functions can be moved to remote work / work from home settings, DoD has many specialized facilities and roles that cannot be rapidly reassigned. Productivity losses for a team of 100 workers could exceed \$50,000 per day. The private sector has turned to costly insurance to cover some of these losses, though premiums are rising sharply and claims stand a good chance of denial as defense of OT networks becomes more commonplace. As a "self-insured" entity, the government needs to invest in risk mitigation to avoid these losses from draining budgets and weakening our nation's defenses.

The potential operational savings from efficient, timely collection of data from FRCS and other industrial networks across the DoD portfolio makes the cybersecurity challenge one worth overcoming. Visibility into the overall energy performance, with granular data, can provide facility managers with the incentive to reduce costs (an average of 2.4% according to the Environmental Protection Agency)⁸. Such data, even at the meter level, might otherwise require manual data collection or the mitigation of cybersecurity vulnerabilities associated with advanced metering infrastructure (AMI). Incorporation of this data with more granular machine telemetry into increasingly capable analytics platforms (using artificial intelligence and machine learning) can yield further savings through automatic work ticketing and avoidance of premature equipment failure. Data diodes can enable this flow of data without allowing a physical channel for an outsider to exploit.

When compared to other methods of data acquisition, these next generation data diodes can provide economically attractive on a cost basis alone.

The analysis below examines both upfront costs (or first costs) and ongoing annual costs.

For technologies with substantial annual costs, attractive paybacks can be achieved by switching to a diode at any point in the incumbent technology lifecycle. For these scenarios we provide payback metrics below that answer the question: *How long would it take to pay back the cost of installing a diode using the money saved by switching from the previous technology?*

In other cases, where no data acquisition technology is currently installed, we use breakeven to answer the questions: *At what point in the product lifecycle would the total cost of ownership of a diode be less than that of the alternative technology?* In these cases, first cost is often a bigger driver of value.

In order to answer these questions, the project team created a baseline scenario representing typical use case. The typical use case is assumed to be a 50,000 square foot facility with 100 data points to extract.

Table 16 below shows the payback period or break-even point when comparing next-generation data diodes to incumbent technologies.

For the purpose of these payback calculations, an upfront data diode price of \$5000 per unit was used and annual costs were assumed to be negligible.

Table 16. Cost and Security Comparison Between Data Diodes and Common Alternatives

Technology	Security Considerations	Cost Comparison	Payback / Breakeven vs Data Diode
Transport of physical media	Manual transportation (“sneaker net”) can introduce human error. Disks and drives can be lost in shipment. Data can be stale, leading to lost opportunities to detect intrusions or identify energy savings.	Costs include media, labor, and transportation. Daily DVD burns are dominated by labor, and a 5 minute task daily could cost over \$2,100 in labor each year. Hard drives obtained every six months by an ESCO as part of an ESPC M&V process are often gotten via an in-person pickup. A single international trip could exceed \$5000, with a domestic retrieval costing as much as \$2500 including travel and labor. Total Upfront Cost: Negligible Total Annual Cost: \$2,100 (local no travel) to \$10,000 (international travel required) annually	Payback: 0.5 to 2.4 years.

Table 16. Cost and Security Comparison Between Data Diodes and Common Alternatives (Continued)

Technology	Security Considerations	Cost Comparison	Payback / Breakeven vs Data Diode
Hardwired control “points” and I/O interfaces	Systems provide a path for side-channel attacks (via electrical wiring). A network-connected controller may become compromised while maintaining the ability to send signals into a critical system.	Per point installation basis can range from \$300 to \$500 (for reference the Fend Diode can support thousands of points). Additional controller hardware may be required. No ongoing annual cost is assumed. Total Upfront Cost: Given a building monitoring 100 points, the initial cost can could range from \$30,000 (100pts x \$300/point) to \$50,000 (100pts x \$500/point) Total Annual Cost: Negligible	Breakeven: Immediate, between the two options diodes are lower cost in terms of first cost and comparable in terms of annual cost.
Separate equipment-only LAN	The physical segmentation of this network must be maintained over time. Expansive networks provide opportunities for tapping into / bridging networks intentionally or accidentally.	Wiring of this type for facilities can cost \$2.00 to \$5.00 per square foot⁹ inside the building, but costs become much higher when information needs to leave the building and reach another part of an installation. Laying new fiber costs an average of \$27,000 per mile.¹⁰ Total Upfront Cost: Networking the industrial controls and other equipment in a 50,000 sqft building would likely cover 2,500 sqft. The initial cost can could range from \$5,000 (2,500 sqft x \$2.00/sqft) to \$12,500 (2,500 sqft x \$5.00/sqft). In addition, connecting that private LAN to other parts of the installation would require \$27,000 per mile in fiber. Total Annual Cost: Negligible	Breakeven: Immediate, between the two options diodes are lower cost in terms of first cost when wiring and connecting facilities and comparable in terms of annual cost.
Industrial Firewalls	Firewalls can be misconfigured. Only known threats are addressed. A lag can occur between threat identification and patch deployment.	First costs of industrial firewalls can be as high as \$40,000, but ones closer to \$3,000 are a more appropriate comparison to the data throughput of the Fend data diode. The frequency of updates has made manual patching impractical from a labor standpoint, so automated patching services / licenses are typically required to keep firewalls up to date. Such expenses range from \$600 to \$2000 year. Total Upfront Cost: \$3,000 Total Annual Cost: \$600 to \$2,000	Breakeven (for new install): 1 to 4 years Payback (replace existing): 2.5 to 8.3 years

6.0 CONCLUSIONS AND IMPLICATIONS FOR FUTURE RESEARCH/IMPLEMENTATION

Cyberattacks are launched against infrastructure targets with an ever-increasing creativity and complexity, but a physical barrier to these attacks can help equipment managers across DoD maintain operational awareness. As demonstrated through this ESTCP project, 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.

These results of this evaluation show both the capabilities and limitations of the current state of this technology. Several of the most common communication standards can be accommodated with this technology, but some projects may require additional equipment and effort to convert data into a supported format (such as proprietary OEM-specific protocols). Some data-intensive projects may exceed the transmission bandwidth of these devices. Data diode technology may not be appropriate for system designs requiring the transmission of both outbound telemetry and incoming commands (requiring a two-way connection), but for systems where the data monitoring is used to inform actions by human operators this technology can provide security and access to information.

For applications where a one-way stream of information would satisfy the technical requirements of a facility management approach (e.g.: equipment status monitoring), this class of industrial data diode can prove a secure, cost effective option relative to manual data collection or data transfers using physical media. These devices have the potential to open the door to Federally-approved, cloud-based tools that make use of predictive analytics and machine learning. By providing access to information that was previously locked behind an air gap, these next generation data diodes can enable greater operational efficiency and resilience.

Widespread adoption of this technology will require technology transfer activities including outreach (conferences, journal articles, webinars, trade shows), inclusion in guidance documents (such as UFC 4-010-06 Cybersecurity of Facility-Related Control Systems), and specification of this technology part of cybersecurity compliance paths and control systems design best practices. Beyond FRCS applications, these next-generation data diodes should be evaluated for other potential use cases including vehicle telemetry extraction and industrial processes monitoring. With data diodes available as part of their toolset, operators can further improve resilience and security.

7.0 LITERATURE CITED

1. Manyika, James et al. "The Internet of Things: Mapping the Value Beyond the Hype". McKinsey.Com, 2015.
2. Lee, Robert et. al., "Analysis of the Cyber Attack on the Ukrainian Power Grid," SANS Institute, 18 Mar 2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.
3. Woolf, Nicky. The Guardian. "DDoS Attack that Disrupted Internet was Largest of its Kind in History, Experts Say," 26 Oct 2016, www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.
4. Trump, Donald. "Presidential Executive Order On Strengthening The Cybersecurity Of Federal Networks And Critical Infrastructure". The White House, 2017, <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.
5. "Connecting Legacy Devices to the Internet of Things (IoT)," Intel, 2014. www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/connecting-legacy-devices-brief.pdf.
6. Department of Defense. "Unified Facilities Criteria (UFC): Cybersecurity of Facility-Related Control Systems". Wbdg.Org, 2018, https://www.wbdg.org/FFC/DOD/UFC/ufc_4_010_06_2016_c1.pdf.
7. Raytheon. "High Speed Guard™ Industrial Control Systems". Raytheon.Com, 2015, https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/cyber/documents/content/rtn_245008.pdf.
8. ENERGY STAR. "The Business Case For Energy Efficiency". Energystar.Gov, 2018, <https://www.energystar.gov/buildings/about-us/how-can-we-help-you/build-energy-program/business-case>.
9. "Costing Out a Cabling System." Cabling Installation and Maintenance. <https://www.cablinginstall.com/design-install/cabling-installation/article/16469357/costing-out-a-cabling-system>
10. Intelligent Transportation Systems, US Department of Transportation. <https://www.itskrs.its.dot.gov/its/benecost.nsf/ID/4a7585077dbf0e21852576ac004ec144>

APPENDIX A SUPPORTING DATA

Supporting data from individual tests is provided separately from this report in the form of original source files. Baseline and post-retrofit data for each test has been provided, as follows:

#1 Baseline - See test #11

#1 Post Retrofit - See test #11

#2 - N/A

#3 Baseline - **#3 Baseline.pcapng** is a Wireshark packet analysis file. It shows the baseline BACnet IP traffic between 170.168.0.15 and 170.168.0.16.

#3 Post Retrofit - TO BE PROVIDED

#4 Baseline - **#4 Baseline.pcapng** is a Wireshark packet analysis file. It shows the baseline BACnet MS/TP, encapsulated as IP traffic, between 170.168.0.15 and 170.168.0.16

#4 Post Retrofit - **#4 BACNET_Serial-IP.txt** is a .txt file in a human readable format that shows the output values of the BACNET MS/TP traffic after the diode.

#5 Baseline - Two difference MODBUS devices were used as a baseline: **#5 - 1 Baseline.pcapng** and **#5 - 2 Baseline.pcapng**. They show traffic between the front end (170.168.0.15) and 170.168.0.38 (Anybus Device) and 170.168.0.37 (Temperature/Humidity Probe), respectively.

#5 Post Retrofit - **#5 - 1 Post Retrofit.txt** and **#5 - 2 Post Retrofit.txt** shows the output from two separate MODBUS devices as a baseline. Various register values are sent from 170.168.0.38 to 170.168.0.15

#6 Baseline - See Anybus file from #5 Baseline. The Anybus device encapsulates MS/TP traffic into IP.

#6 Post Retrofit - **#6 Post Retrofit.txt** is a .txt file in a human readable format that shows the output values from the diode. The input into the diode was MODBUS/RTU traffic.

#7 - N/A

#8 Baseline - The same baseline as #5 was used

#8 Post Retrofit - TO BE PROVIDED

#9a - N/A

#9b - N/A

#10 - N/A

#11 Baseline - **#11 Baseline.pcapng** is a Wireshark packet analysis file with data from the iLON installed in a CERL facility.

#11 Post-Retrofit - A human readable format of the Lon data after the diode is included in the file **#11 Post Retrofit.txt**. The data from the diode was compared to the "LON Front End output.xlsx" values.

#12 Baseline - **#12 Baseline.pcapng** is a Wireshark packet analysis file with data from the BACnet controller installed in a CERL facility.

#12 Post-Retrofit - **#12 Post Retrofit.txt** provides a human readable format of the data output from the diode

APPENDIX B LIST OF SCIENTIFIC/TECHNICAL PUBLICATIONS

Conference and Poster Presentations

The following list represents a selection of events at which this technology was presented. Several abstracts are similar, so a sample abstract is included as a separate file in the appendix attachments (**Abstract - Physical Cybersecurity AEE.pdf**).

- 2019 Association of Energy Engineers (AEE) World Conference
- 2019 Defense TechConnect Conference
- 2019 Green Electronics Council Webinar: Catalyst Awards
- 2019 MITRE Tech Showcase
- 2019 SERDP-ESTCP Symposium
- 2019 WaterISAC Briefing
- 2019 Downstream Natural Gas ISAC Briefing
- 2020 Advanced Surface Engineering Technologies for a Sustainable Defense (ASETSDefense)
- 2020 Cybersecurity Symposium for Smart Cities
- 2020 Joint Military Pitch Day
- 2020 More Situational Awareness for Industrial Control Systems (MOSAICS) Industry Day
- 2020 SERDP-ESTCP Symposium
- 2020 AEE World Congress
- 2021 Control Systems Cyber Security Association International
- 2021 Society of American Military Engineers (SAME) JETC
- 2021 National Cyber Summit

Journal Articles

2021 The Military Engineer – Submission in progress (by 10/12/21)

APPENDIX C OTHER SUPPORTING MATERIALS

The following documents are included as references:

- Fend B Series Diode User Manual (v4.0) – User’s manual for the Fend B-Series Diode. Explains how the install and operate the diode. - **Fend B Series Diode Users Manual v4.0.0_2021_Final.docx**
- Protocol Support Sheet – Provides an overview of the various protocols supported by Fend B-Series Diodes. - **Protocol Chart Sheet_Sep_2021.pdf**
- Fend Use Cases - Provides examples of various ways in which a Fend B-Series Diode can be used - **Fend Use Cases.pdf**
- Summary of Cyber Operational Survivability Testing Results – Provides a summary of the results of the penetration testing carried out by TSMO as part of this project. - **Fend_TSMO_Report_Summary.pdf**
- Defense TechConnect Innovations List (2019, 2021) - <https://defensetechconnect.com/awards/> - **Defense TechConnect Awardee List.pdf**