OWL Cyber Defense

OWL ADVANTAGE
THE GOLD STANDARD IN DATA DIODE TECHNOLOGY

NERC CIP Compliance
Addressing NERC CIP Compliance with Owl Data Diode Technology

NERC CIP

Virtually all major facilities involved in the North American bulk electric system (BES), including non-nuclear electricity generation, distribution and transmission, are subject to regulation by the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) plan.

The essence of NERC CIP is in identifying and protecting those connected Cyber Assets which, if compromised, would have a negative impact on the BES. Table R1 in Section 005 of CIP lays out a number of requirements to ensure the protection of the Cyber Assets including: creating a strong Electronic Security Perimeter (ESP), disconnecting BES Cyber Systems from external connections, limiting or eliminating the use of routable protocols (which expose IP information within the ESP, are bi-directional, and are susceptible to hacking), and forcing all traffic through a protected Electronic Access Point (EAP).

Owl has a well-established history of success in helping organizations to meet the cybersecurity requirements of NERC CIP compliance, including v5 & v6. We have created this document to assist BES operators in finding approved data diode solutions to each of the section 005 requirements. Examples (starting on page 2) are provided to demonstrate specific use cases of data diodes being used to help satisfy these requirements.

Changes to NERC CIP

In the latest iteration, NERC CIP v6 moves further toward a risk-based approach, with regard to electronic perimeter security and cybersecurity. The new version effectively broadens the scope of Cyber Assets and BES Cyber Systems which fall under required protection while allowing for greater flexibility in how these protected Cyber Assets are classified and segmented. Previously each BES Cyber System, defined as a set or group of Cyber Assets, would be classified at the highest impact rating of the Cyber Assets contained within it. In v6, High and Medium Impact Cyber Assets are classified equally, recognizing the importance of strong security across all sensitive assets. All other assets default to Low Impact.

Owl Data Diode Cybersecurity

Approved by NERC for the use of network segmentation and one-way data transfer, Owl data diodes are currently supporting compliance with CIP v5 and v6, where they are just as important. Data diodes combine absolute information assurance and unhackable cybersecurity with the ability to share and monitor operational data. For those unfamiliar with them, a data diode is a hardware-based electronic device with two circuits – one send-only, and one receive-only – which allows the transfer of data in only one direction. As one-way data transfer systems, data diodes isolate and protect networks from external cyber threats, while allowing systems within these networks to securely transfer data to other networks in a highly controlled, deterministic manner.

With a non-routable, hardware-based platform, data diodes create an absolute ESP by physically only permitting data to transfer in one direction, from one network segment to another, across a network security boundary. When utilized effectively, data diodes can help operators achieve NERC CIP compliance, eliminate all external cyber threats, and provide a path to business continuity through remote monitoring and offsite data analytics.

As the world leader in data diode technology, as well as a strategic technology partner for many industrial automation vendors, Owl is uniquely positioned to provide both the strongest network security available with the broadest range of data transfer services, supported file types, and software integrations on the market. Owl's breadth of supported file types and specialized interfaces, including PI System, Wonderware, OPC, Modbus, and Syslog, among others, enable customers to seamlessly replicate and transfer historians, HMIs, email, and more.
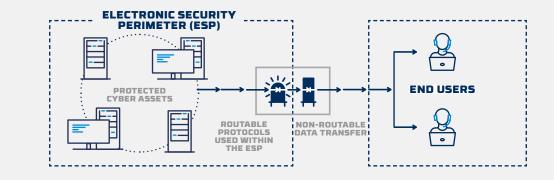
PART 1.1

Applicable System(s)	Requirements	Owl Data Diodes
High/Medium Impact BES Cyber Systems & PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP	Non-routable network security eliminates external access to Cyber Assets and creates a defined ESP

NERC-Approved Data Diode Applications

In addressing NERC CIP compliance, data diodes are approved and perfectly suited to meet the criteria laid forth in CIP-005, regarding cybersecurity and Electronic Security Perimeter(s). The following table explains how Owl data diodes enable responsible entities to meet each applicable requirement in Table R1 of CIP-005.
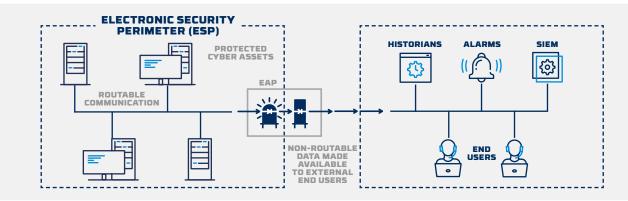
PART 1.2

Applicable System(s)	Requirements	Owl Data Diodes
High/Medium Impact BES Cyber Systems with External Routable Connectivity & PCA	All external routable connectivity must be through an identified Electronic Access Point (EAP)	Non-routable network security eliminates external routable connectivity, securing BES Cyber Systems without the need to allow routable connectivity through an EAP

PART 1.3

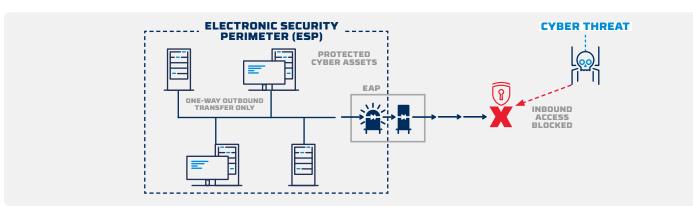| Applicable System(s)	Requirements	Owl Data Diodes
EAP for High/Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default	One-way-only data transfer eliminates all inbound access, denying all access by default and preventing any possibility of manipulating the configuration to create unauthorized access. Outbound access permissions can be configured as needed to transfer data

PART 1.4

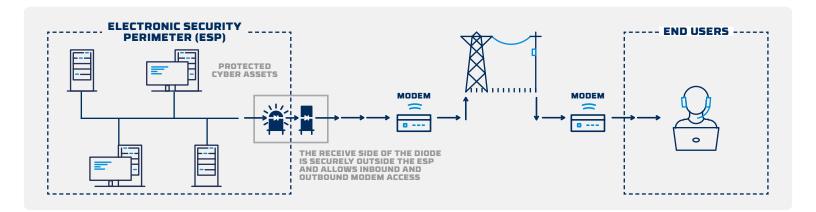| Applicable System(s)	Requirements	Owl Data Diodes
High/Medium Impact BES Cyber Systems with Dial-up Connectivity & PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets	Data diode moves inbound and outbound dial-up communication outside of the ESP. Remote users can dial into the diode to retrieve data or the data diode can place an out bound call to deliver data

ELECTRONIC SECURITY PERIMETER (ESP)

PROTECTED CYBER ASSETS

MODEM

MODEM

END USERS

THE RECEIVE SIDE OF THE DIODE IS SECURELY OUTSIDE THE ESP AND ALLOWS INBOUND AND OUTBOUND MODEM ACCESS

PART 1.5

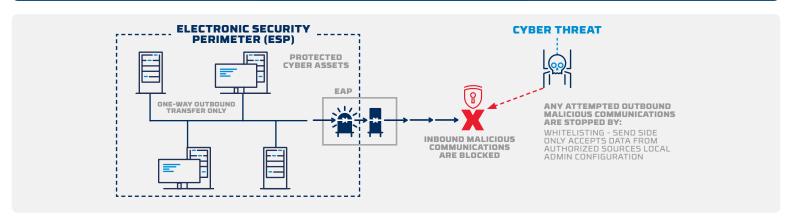| Applicable System(s)	Requirements	Owl Data Diodes
Electronic Access Points for High/Medium Impact BES Cyber Systems	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications	All inbound communication to the EAP is eliminated. In outbound communications, the sending side is blind to the receiving side, preventing malicious manipulation or communication over the data diode

ELECTRONIC SECURITY PERIMETER (ESP)

PROTECTED CYBER ASSETS

CYBER THREAT

ONE-WAY OUTBOUND TRANSFER ONLY

EAP

INBOUND MALICIOUS COMMUNICATIONS ARE BLOCKED

ANY ATTEMPTED OUTBOUND MALICIOUS COMMUNICATIONS ARE STOPPED BY:
WHITELISTING - SEND SIDE ONLY ACCEPTS DATA FROM AUTHORIZED SOURCES LOCAL ADMIN CONFIGURATION

✓ Success Stories

For over seven years, with hundreds of deployments in North America alone, Owl has been helping critical infrastructure operators reduce cyber risk, achieve NERC CIP compliance and simplify administration while enabling the secure transfer of data offsite. Our unrivaled expertise in data diode deployment for critical infrastructure reduces time to deployment and increases reliability across a single device up to an entire fleet of power stations.

Owl data diodes can relieve up to 30-40% of the administrative compliance burden of NERC CIP, saving valuable time and money while allowing operators to focus on the vital aspects of their plants and infrastructure. They allow operational data to be sent to other networks or the cloud for analysis, predictive modeling, remote monitoring and other applications, improving business continuity and ROI in facility technology.
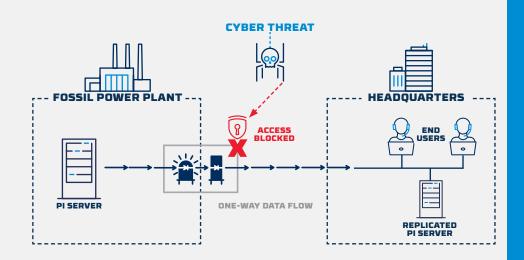
ENVIRONMENTS INCLUDE:

- Coal, hydro, oil, and natural gas power plants

- Transmission and distribution substations

- Fuel and materials storage facilities
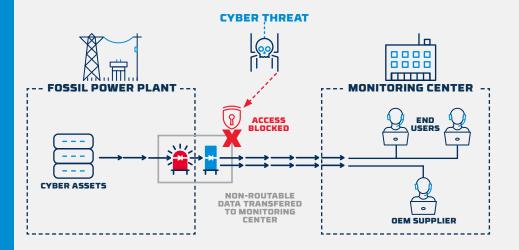
DATA TYPES TRANSFERRED:

- Historians & HMIs – PI System, Wonderware, GE Historian, MC Historian, FactoryTalk

- Modbus, OPC, DCS data

- Nearly any file type or streaming source (TCP, UDP)

USE CASE #1:
HISTORIAN REPLICATION AT FOSSIL PLANT

To achieve NERC CIP compliance, a US-based fossil power facility had to disconnect critical operational technology (OT) networks from outside access. However, it also needed to retain access to OSIsoft PI System historian data by the business IT unit. Owl data diodes were deployed along with specialized PI System replication software to transfer the historian data back to HQ for the business IT unit. This secured the OT network from external threats without disrupting access to OT data by the business end-users.
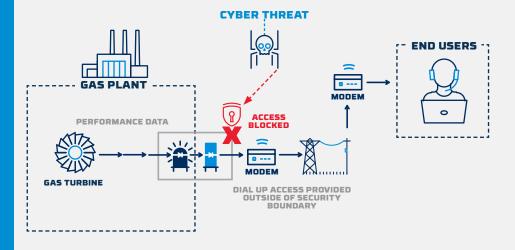

CYBER THREAT

FOSSIL POWER PLANT

PI SERVER

ACCESS BLOCKED

ONE-WAY DATA FLOW

HEADQUARTERS

END USERS

REPLICATED PI SERVER

USE CASE

CYBER THREAT

FOSSIL POWER PLANT

CYBER ASSETS

ACCESS BLOCKED

MONITORING CENTER

END USERS

OEM SUPPLIER

NON-ROUTABLE
DATA TRANSFERED
TO MONITORING
CENTER

USE CASE #2:

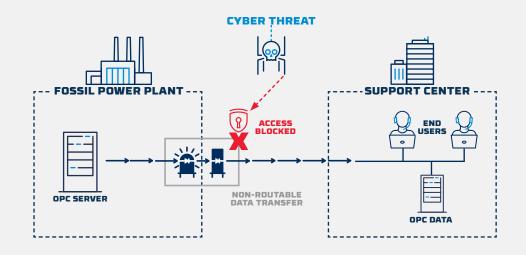### OEM REMOTE EQUIPMENT MONITORING AT POWER SUBSTATION

An OEM supplier required remote monitoring of their assets at a power substation. However, due to NERC CIP compliance requirements, the asset owner must also comply with strict cybersecurity regulations limiting routable access from outside networks. An Owl data diode was installed to enable the free transfer of monitoring data out of the substation for the OEM supplier. Meanwhile it also removed all external routable connectivity and kept the BES Cyber Systems and the Cyber Assets secure from external threats.

CYBER THREAT

END USERS

GAS PLANT

MODEM

PERFORMANCE DATA

ACCESS BLOCKED

GAS TURBINE

MODEM

DIAL UP ACCESS PROVIDED
OUTSIDE OF SECURITY
BOUNDARY

USE CASE #3:

REMOTE MONITORING VIA DIAL-UP CONNECTIVITY AT NATURAL GAS PLANT

Threatened with the loss of daily performance monitoring data, a gas turbine power plant operator required a cybersecurity product stronger than a firewall that would allow for the continued remote dial-up collection of data. An Owl data diode with built-in modem hardware provided a hardware-enforced electronic security perimeter. The data diode also separated the BES Cyber System from dial-up connectivity, while preserving the ability to transfer and collect data remotely via the dial-up connection on the receiving side of the diode.

CYBER THREAT

FOSSIL POWER PLANT

OPC SERVER

ACCESS BLOCKED

NON-ROUTABLE DATA TRANSFER

SUPPORT CENTER

END USERS

OPC DATA

USE CASE #4:
REAL-TIME DATA MONITORING AT OIL FIRE PLANT

A fossil power plant required real-time systems monitoring with OPC data, but also wanted to remove external routable connectivity for NERC CIP compliance. An Owl data diode was installed to enable the real-time transfer of OPC data out of the plant for the support unit to monitor. Meanwhile it also removed all external routable connectivity and kept the BES Cyber Systems and the Cyber Assets secure from external threats.

ONE-WAY BY DESIGN	SECURE COMMUNICATION	COMPLETE SEPARATION OF NETWORKS	UNMATCHED PERFORMANCE	UNPARALLELED SCALABILITY	MULTIPLE FORM FACTORS
LOWEST TOTAL COST OF OWNERSHIP	TESTED & ACCREDITED SOLUTION	SIMULTANEOUS MULTI-FUNCTION SOLUTION	DEFENSE IN DEPTH	INDUSTRY-LEADING MTBF	FAST & EASY DEPLOYMENT

OWL ADVANTAGE
THE GOLD STANDARD IN DATA DIODE TECHNOLOGY

OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com