DATADIODE
BY FOX IT

Protecting Critical Assets and Production Environments

Production facilities being part of the national Critical Infrastructure are endangered by digital threats coming from the Internet. Over the past decade we've seen many cases where nation states and/or cybercriminals have successfully attacked and infiltrated production facilities causing huge harm, delay in production and even cost lives. Separating production facilities entirely from any network connection is not an option as important production data needs to be shared with other parts of the organization. The Fox DataDiode is a solution that protects assets from digital threats coming from the internet while at the same time making sure production data can be shared with for example the plants headquarter.

Making secure connections between critical information networks

The current cyberthreat landscape is characterized by ever-increasing professionalism on the part of the attackers and the number of attacks, posing great risks to Industrial Control Systems (ICS). Cyber criminals and also Nation States constantly specialize and improve the quality of their methods, thereby increasing the effectiveness and efficiency of criminal activity.

Networks should be segmented to the greatest extent possible. In particular, one must be vigilant concerning interconnections between an ICS and a public network (telephone, Internet), between an ICS and a corporate network, or between ICSs of different cyber security classes.

Reference:
ANSSI Classification Method
par. 2.2.10

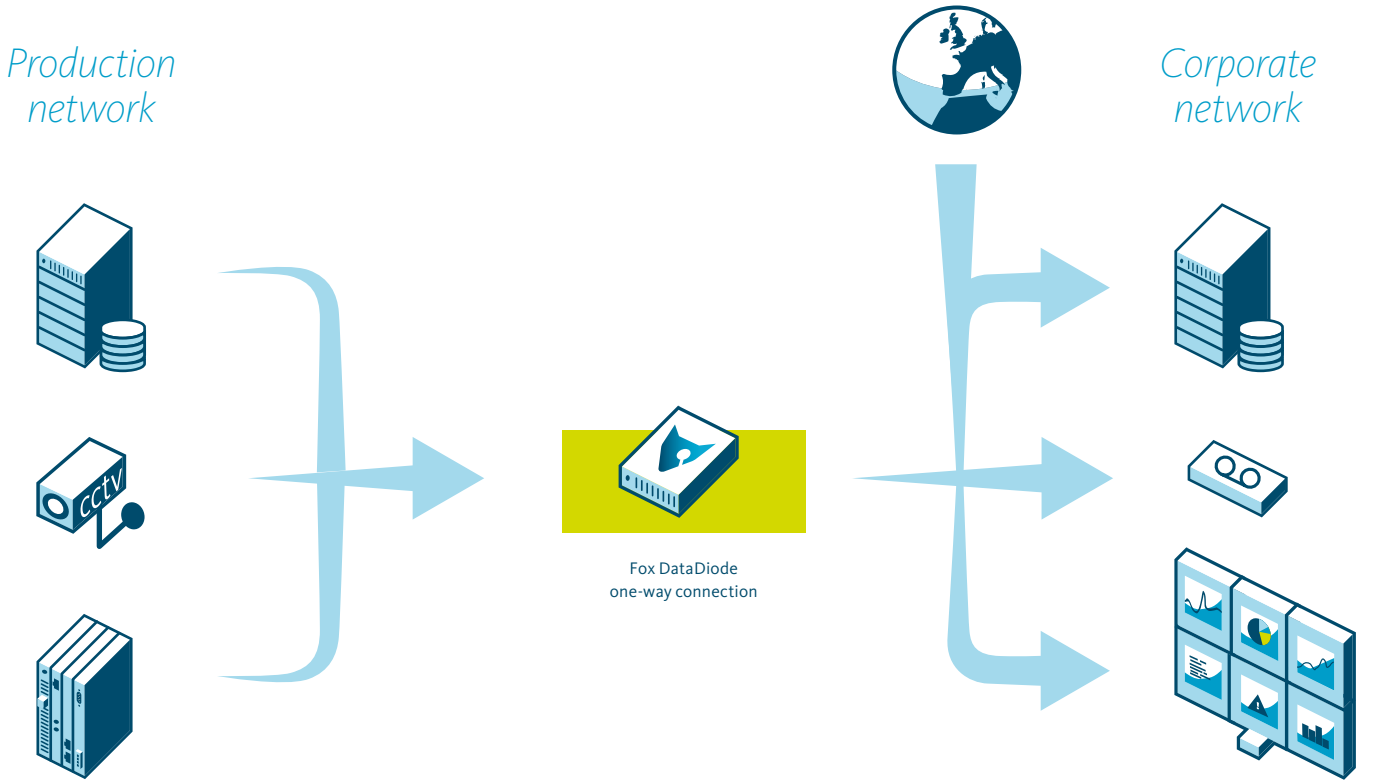
The clandestine sale of criminal technology and services – and even the development of managed services in this area – lowers the threshold for interested parties to become active in cybercrime. Experience teaches us that the latest methods and complex techniques that are used by top players such as intelligence services quickly find their way to economically-driven cyber criminals. ICS systems and critical infrastructures are strategic targets for Nation States, criminals, terrorists and hacktivist, given the impact that disruptions caused by attacks will have on society.

The uninterrupted and correct functioning of ICS is crucial for today's society. We expect power to come out of sockets, water to flow from taps, and trust in the safe travel of trains and planes from A to B. ICS systems are key in this process. The ICS production network (OT) is connected to a separate corporate (IT) network environment. Integration between the two is important for the business side as it needs to work with data from production. Unfortunately, this network connectivity also opens the door to abuse of these ICS infrastructures, making production systems vulnerable to malware and attacks. Ultimately, when vulnerabilities are exploited, safety, availability and integrity of production systems and critical assets are at risk. Fox DataDiode one-way data connection protects the integrity and availability of critical assets in Industrial Control Systems (ICS) networks. It enables you to securely utilize the benefits of business intelligence integration while preventing all cyber attacks, abuse and even mistakes from the Internet or the corporate network directed at your corporate or critical infrastructure. Operational critical ICS assets are protected against cyber attacks, abuse and even unintentional mistakes from Internet connections or the corporate network. Prevalent examples of these dangers are custom-made industrial malware and hacker activity. Fox DataDiode renders these attacks ineffective.

We need to share data to produce

When we work together, the sharing of data is both inevitable and valuable. The value of what we do is reflected in the data we share. Data is one of the critical assets in our businesses and it needs to be protected.

We need to share data generated in production environment (ICS) in real time with corporate (IT) networks
Integration means that connections are set up. These connections could be used for purposes other than data sharing between the production environment and the corporate network. Corporate networks are connected to the Internet. When connections exist between corporate networks and ICS production environments, these systems become vulnerable to malware and attacks. Ultimately, if this vulnerability is exploited, availability and integrity of production systems and critical assets are at risk.



Fox DataDiode protecting input data and CCTV camera footage

Safeguarding the connections between your processes
Placing a Fox DataDiode between the corporate networks and the ICS production networks safeguards the integrity of the production systems, thus ensuring that data is guaranteed to only flow from the production systems to databases or monitoring stations in the corporate network. Fox DataDiode is a 100% hardware-only solution to enforce this.

We replicate historian data for analysis and interpretation to corporate environments

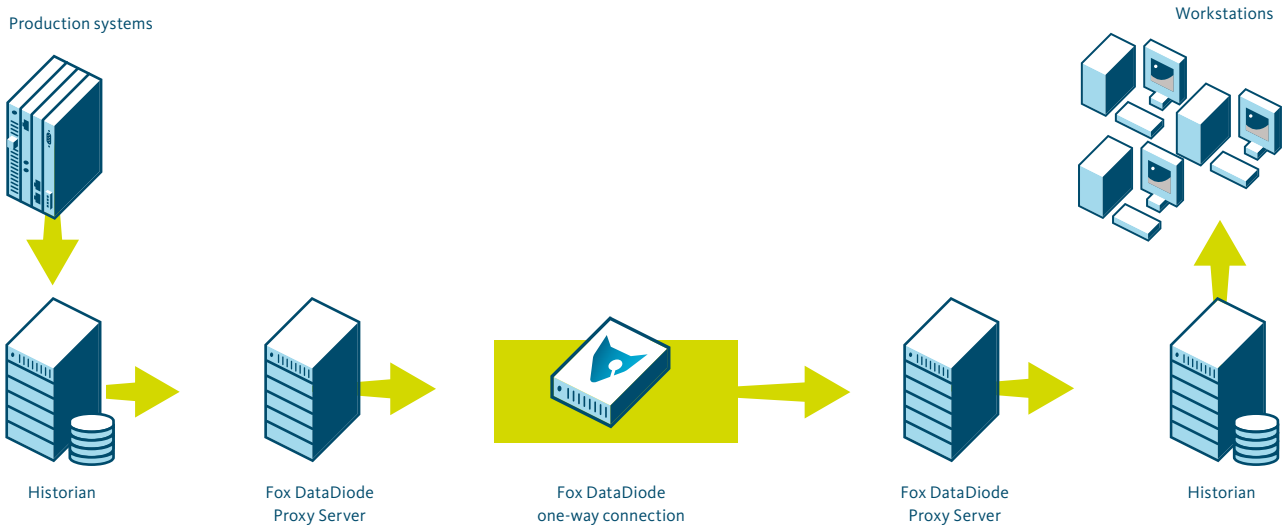
In many situations, information collected in so-called data historians should be accessible not only to the plant floor, but also to the corporate departments. One of the options is to open a (network) connection between the corporate networks and the plant network. However, this exposes the plant network to enormous risks, as a direct connection from the corporate network to the plant is now created – the issue being that the corporate network is often connected to the Internet.

Traditionally, production data is stored in historians like OSIsoft PI, Honeywell, Yokogawa, and Wonderware: large databases in ICS production networks. These historians store vast amounts of data, such as sensor values that are written to them multiple times each second. To explain: for a plant of reasonable size, this results in millions of values stored each day, each of those threatening business continuity; on the corporate side, the values generated from the production environment are essential for business processes such as invoicing, planning, tuning, and optimizing production scheduling and the ability to track the origin of changes in the production quality.

FOX-IT has an extensive suite of protocol data replication solutions available, such as Fox Modbus Replicator, Fox OPC Replicator and Fox PI Replicator.

We need to protect our data assets and safety systems

In industrial environments, the flow of status information from an ICS production network to a corporate environment is crucial. Businesses require up-to-date information on production results which for instance can then be used for planning and billing. But often there is no need for the corporate environment to directly have access to the ICS production environment.



Protecting your valuable historian data

By replicating historian data from a historian server in the ICS production environment to a historian server in the corporate environment using a Fox DataDiode, it is no longer necessary to provision a DMZ or to require a bidirectional network connection between the ICS production and corporate environments.
In fact, a replica historian server is created in real time and updated with live data. This way, information can be shared with the corporate network, without the danger of exposing control systems to digital threats from the outside world. On the corporate network, users can work with live data, without the ability to interfere with production systems – either intentionally or unintentionally.

We need to protect our assets

US ICS-CERT recommends to take defensive measures to minimize the risk of exploitation due to unsecure device configuration. Users should minimize network exposure for all control system devices. Control system devices should not directly face the Internet.

Reference:
AUSA ICS-CERT Alert
ICS-ALERT-14-281-01E

For the protection of our valuable assets, we implement safety systems, which inevitably need to be protected themselves, as the data they share produces a new vulnerability.

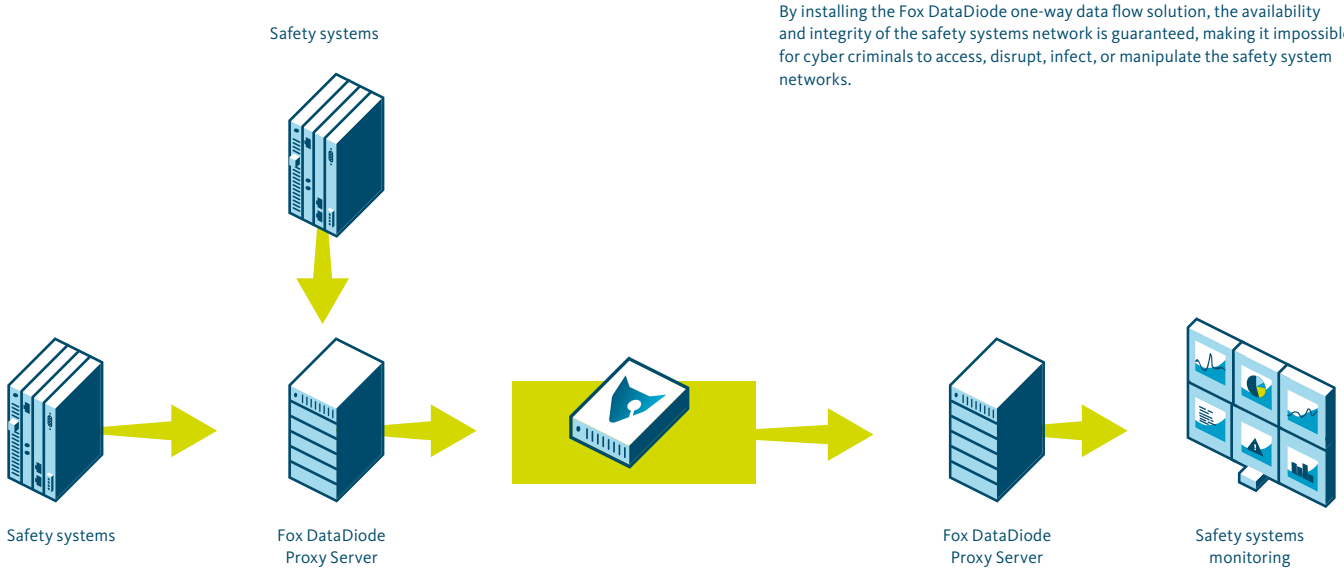
Safety systems should be able to securely send alerts to their production and corporate environment

Within ICS production environments, the purpose of safety systems is to ensure the safety of a plant, its operators and the environment. They are devices that operate separately from the ICS systems and constantly monitor the plant. Metrics such as temperature, volume, pressure, viscosity, humidity and radiation are monitored 24/7 based on preset thresholds. When exceeding a threshold, alarms are raised and preventive measures can be taken.

Safety systems are crucial for the safe operation of a plant. They should operate independently and may not be manipulated under any circumstances. At the same time, there is a need to communicate the safety metrics data to the ICS production network monitoring stations, and further to the corporate network. This clearly dictates that it is critical that safety systems should be protected accordingly.

Securing your security system

By installing the Fox DataDiode one-way data flow solution, the availability and integrity of the safety systems network is guaranteed, making it impossible for cyber criminals to access, disrupt, infect, or manipulate the safety system networks.



We need to monitor production sites

A Security Information and Event Management (SIEM) solution centralizing all security event logs should be implemented. It should allow for correlating logs to detect security incidents. To avoid considering the SIEM solution as class 3, it should be placed behind a data diode as indicated in directive D.159.

Reference:
ANSSI Detailed measures report [R.278]

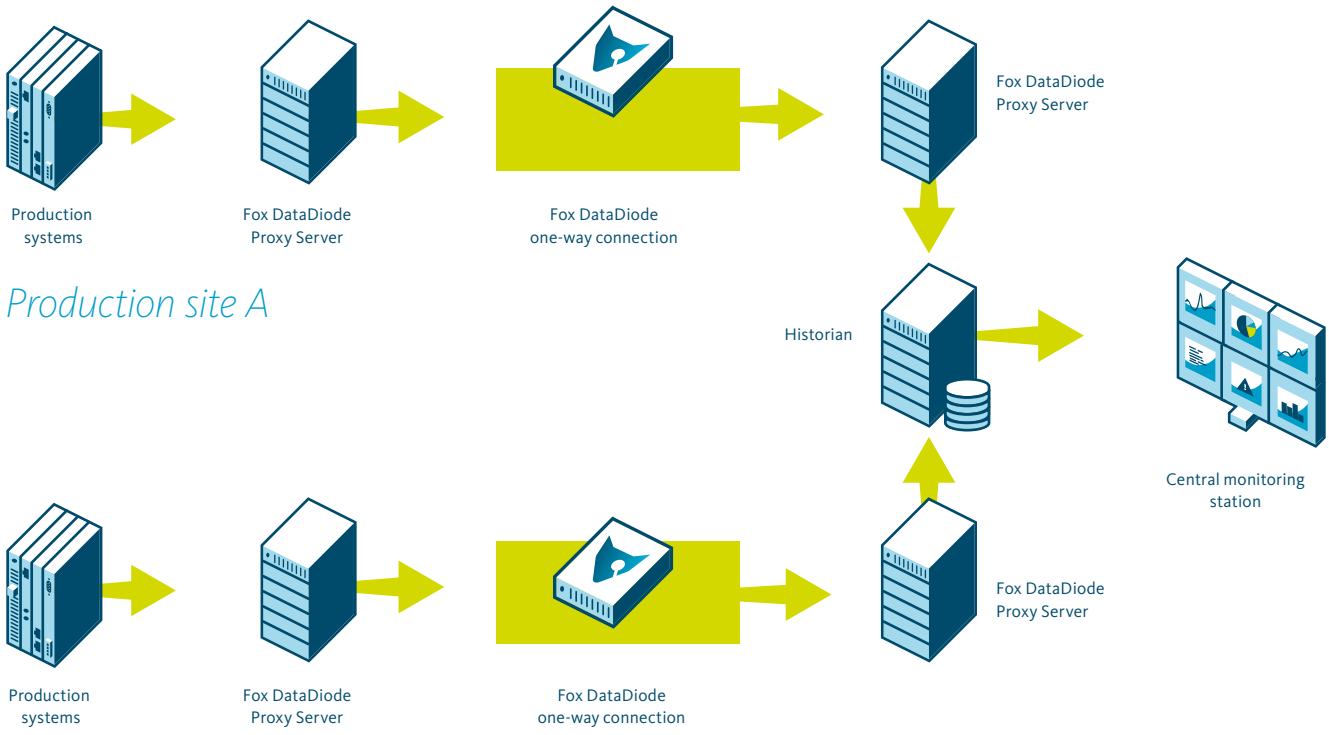
Larger companies and organizations may operate from different sites, adding the need for yet another secured network that allows them to monitor these sites from a central location.

Central monitoring of production sites and factory locations

The one-way technology implemented by Fox DataDiode enables organizations to send information from one physical site to another – and not the other way around – giving large organizations the opportunity to centrally monitor their various production sites. This is achieved without opening the individual plant's network and thus keeps its availability and integrity protected. At the same time, information sharing with HQ is still possible. By enforcing data to be sent in one direction only – in this case out of the plant – attacks on the plant from the outside network are physically impossible because of the Fox DataDiode.

Monitoring the OT with a SIEM

With a real-time one-way connection, it is possible to feed events from the production (OT) environment into a SIEM (Security Information and Event Management) in the corporate (IT) environment. Cost savings and ROI are even greater when not just one but multiple production (OT) environments are connected into one SIEM environment. Moreover, collecting information from multiple production (OT) environments enhances the analysis, as events from multiple plants can be correlated, giving substantiated insights at lower costs.

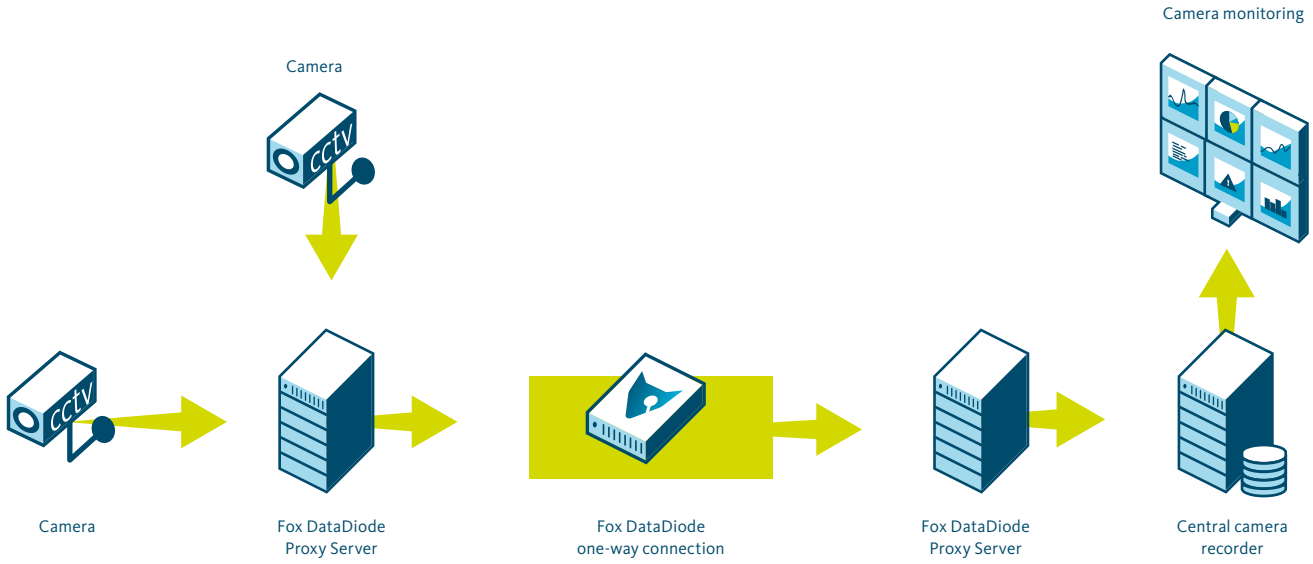


We need to secure CCTV systems

By design, CCTV cameras need to be placed 'outside' and connected to the 'inside', which calls for the protection of these connections.

CCTV systems present vulnerabilities

Digital CCTV cameras installed on a company's premises, such as nuclear facilities, power plants, storage facilities, drilling platforms, or factory plants send footage to a central recording station in the network. Since it is necessary to record what takes place outside, the camera itself is often placed in an insecure, publicly-accessible environment. It is important to realize that the camera, and more significantly its IP network connection, can be used to gain access into the company network. In other words, the recordings of all cameras and other systems within the network are vulnerable to infiltration.



Secure the results of the physical system

Placement of a Fox DataDiode between the cameras and the recording station. The cameras are able to send their footage to the recording station securely. At the same time, information from the network cannot be extracted using the camera's connection. Hijacking the camera's wire will not help the attackers gain access to the company's network.

The assurance of Fox DataDiode

When a Fox DataDiode is used in an Industrial Control Systems (ICS) network, it serves to protect the integrity and availability of assets. This is guaranteed because Fox DataDiode is computer hardware that enforces unidirectional flow of network traffic.

Arm yourself with the best protection: Fox DataDiode fits perfectly in an approach to become and remain NERC-CIP compliant.

Reference:
NERC document CAN-0024
Fox DataDiode has been awarded numerous certifications and is trusted by international organizations and governments worldwide.

Fox DataDiode has the highest levels of certification and recognition

Fox DataDiode is the only product that has been awarded the Common Criteria EAL7+ certification.

Fox DataDiode is the only solution that guarantees one-way connection on a physical level (OSI layer 1). Fox DataDiode hardware does not have software, firmware, or FPGAs. Hence, it cannot be exploited or wrongly configured.

Since 2006, FOX-IT has successfully installed hundreds of Fox DataDiodes in over 40 countries, covering every geographical region except Antarctica.

The recommended set-up includes a Fox DataDiode hardware unit and a proxy server on each side of the unit in order to convert bi-directional protocols into a one-way protocol (on the upstream side) and vice versa (on the downstream side). These proxy servers are equipped with turnkey software solutions to hook into environments and provide secure one-way data transfer from production networks to a corporate environment.

Enhancing security in the Nuclear Facilities by promoting the importance of security by design; e.g. the further adoption of secure optical DataDiodes.

Reference:
Chatham Report

Network boundary options

The network boundary options: **Firewall > Air gap > DataDiode**

A **DataDiode** provides great advantages over an (industrial) firewall.

By design, a **firewall** is vulnerable for three reasons: it is firmware, it has software running on it, and the way in which it is configured. Furthermore, the costs of maintaining and managing a firewall are far higher when compared to the Fox DataDiode.

Air gap implies the complete segregation of networks. However, this approach offers a questionable sense of security and has a negative impact on productivity. It is a fact that companies use storage media such as USB sticks. These can be physically exfiltrated and as such provide a means for data leakage.

'Fox DataDiode brings us compliant protection against cyber attacks by segregation of operations from the monitoring network.'

source:
Nuclear installation in Spain

'Fox DataDiode protects our Control Center at the same time enabling us to comply with National Safety Regulations.'

source:
Oil company in the Middle East

'Fox DataDiode makes it possible to receive real-time production information combined with the high assurance to prevent cyber attacks.'

source:
Power utility company in Asia

The **Purdue Model** gives a clear overview of where the Fox DataDiode can be placed, so as to maximize the protection of the OT network and equipment. Commonly positioned between level 3 and level 4, the Fox DataDiode safely provides a copy of the production data historian to the corporate network. The OT side remains secure, all the while providing the requested historian information. Heavily regulated organizations may enforce powerful security measures at the lower levels. The Fox DataDiode can also be placed in the lower levels of the OT environment, nearer to the high-value equipment. Safely separating PLC based OT assets from the potential dangers of connected computer equipment. Everywhere traditionally an air gap was put in place, the Fox DataDiode is the ideal and safer drop in replacement.