

# DATA DIODE IN OPERATIONAL TECHNOLOGIES (OT)

DATA DIODE USAGE IN PRODUCTION FACILITIES





## TABLE OF CONTENTS

INTRODUCTION	3
DEFINITION AND OPERATION OF DATA DIODE	3
BASIC COMPONENTS AND WORKING PRINCIPLE	4
DATA FLOW CONTROL	4
IMPORTANCE OF DATA DIODE IN OT NETWORKS	6
VULNERABILITY OF OT NETWORKS AND NEED FOR CYBER SECURITY	6
THE ROLE OF DATA DIODE IN OT NETWORKS	6
MECHANISMS TO PROTECT AGAINST CYBER ATTACKS	7
DATA DIODE IN FACTORIES AND ENERGY PRODUCTION	9
REAL EXAMPLES AND ADVANTAGES OF DATA DIODE	9
DATA DIODE TECHNOLOGY IN THE FUTURE	11
EXPECTED INNOVATIONS AND DEVELOPMENTS	11
LEGAL OBLIGATIONS	11





## INTRODUCTION

Industrial production facilities are complex and integrated systems to manufacture and create products that supports our daily routines. These facilities process raw materials and transform them into various end products to meet different day to day requirements, from automotive to food. While speaking about production, we should keep in mind that any kind of energy transformation plants are no exceptions.

Modern industrial production requires sophisticated methods not only in terms of production speed and volume, but also in terms of efficiency, quality control and cost management. Continuously developing technology has become a part of the industry 4.0 revolution and beyond, enabling industrial facilities to operate more efficiently and self-driven.

Operational Technologies (OT) and Information Technologies (IT) are two fundamental pillars of modern industrial environments, although they serve very different purposes. OT is concerned with the direct control and monitoring of physical devices and processes. This side includes technologies directly related to production, such as production machineries, automation systems, and control devices. Slightly different environments exist in IT part. IT focuses on enterprise information management and business processes that are mainly related to data processing, storage, and communication. The interaction between these two areas plays a significant role in efficiency and innovation, but each has its distinct technical and security challenges.

Considering the differences and integration requirements, data diodes in control systems are of vital importance. Data diodes provide one-way data transfer between OT and IT systems, providing protection against external threats and increasing network security. This technology, plays a major role in protecting critical infrastructures in particular, stands out as an important element in defense against todays ever increasing cyber-attacks. Its use in industrial facilities defines the standards for the future of OT and IT integration. This document discusses in details, the functionality, advantages and impact of data diodes in industrial applications.

## **DEFINITION AND OPERATION OF DATA DIODE**

A data diode is a pair devices used in the field of information security and its main function is to provide one-way data flow between two different security classified networks. These devices are generally used in environments with high security requirements, especially in industrial control systems (ICS) and critical infrastructures. Main purpose of a data diode is to protect against external threats and to ensure the security of the internal network while allowing transfer of data from one network to another. Data diodes are also designed to prevent data leaks and network breached. Data diodes are hardened software suites combined with special hardware solutions.





#### **BASIC COMPONENTS AND WORKING PRINCIPLE**

Basic principle of data diodes is that they are designed to transmit data in only one direction. Some manufacturers refer to these devices as "uni-directional gateways." Data diodes are critical for improving network security by creating segmentation. These devices create a physical barrier between the source and destination network, allowing only certain types of data to pass through. Basic components of data diodes include optical data transmission systems, which enable data to be transmitted between the source and destination networks. These systems convert data signals into optical signals, allowing them to be transmitted securely. Also, data diodes often include data filtering, encryption, and other security protocols. These features ensure that only secure, not-changed and authorized data is allowed through.



## **DATA FLOW CONTROL**

The flow controlled by the data diode forms the basis of network security. These devices ensure that data coming from the source network passes certain security checks before reaching the destination network. Data diodes prevent, possibly unsafe or harmful data flow, having necessary awareness of data types and protocols. For example, a data diode only allows the transfer of data packets of a certain file type such as pdf or jpg, or control protocol like modbus, mqtt,, profinet etc, thus protecting the integrity of the network. Data diodes also constantly monitor and analyze network traffic to prevent data leaks and to protect against external attacks. The physical barrier created makes it impossible the return data to pass from the external network to protected zones.

Use of data diodes is especially important in sensitive environments such as factories, power plants, water treatment systems and similar critical infrastructures. These devices provide protection against cyber-attacks while also ensuring an efficient and uninterrupted workflow. The secure transmission of critical information and control commands is fundamental to the proper functioning of these environments.

Data diodes are an essential part of modern cybersecurity strategies and play a key role in increasing the security of industrial control systems (ICS). Using this technology not only protects against current threats, but also increases resilience to future cyberattacks. Effective use of data diodes creates the foundation for a secure and reliable industrial network infrastructure, which also increases industrial efficiency and security in general. By transferring





DATA DIODE IN OPERATIONAL TECHNOLOGIES (OT)

the data required from the OT network to the IT, to generate reports that help increase business productivity, minimize reporting costs in the OT network, while the necessary visibility to business analysis is provided.





## **IMPORTANCE OF DATA DIODE IN OT NETWORKS**

Operational Technology (OT) networks are the veins of modern industry. These networks include manufacturing facilities, power plants, machineries and other critical infrastructures and must be in absolute continuous operation. The vulnerable nature of OT networks requires top level of cybersecurity. So, the role of data diodes is of vital importance. This section describes the vulnerability of OT networks and the need for cybersecurity, the role of data diodes in these networks, and mechanisms to protect against cyber-attacks.

#### VULNERABILITY OF OT NETWORKS AND NEED FOR CYBER SECURITY

OT networks must operate continuously, with absolutely no tolerance of interruption, because the downtime or failure of these systems can lead to economic and reputational losses and may have extreme cumulative consequences in service delivery. These networks are often used to maintain vital processes and services, and therefore any cyber-attack can lead to major crisis. Unlike traditional IT systems, OT systems control physical processes and are therefore more sensitive in terms of cybersecurity. Security breaches in these systems can cause physical damage or serious disruptions to business processes. The protection of OT networks is critical not only in terms of information security, but also physical security.

Most OT devices are made to provide a pre-defined function and are not aware of selfprotection techniques. They usually don't have enough resources to install external protective applications suc as anti-virus and security agents. These devices are usually shipped with preinstalled embedded software, that makes them vulnerable when exposed to external access. This hard-working, less protective nature of industrial devices, makes them require a complimentary solution in todays connected world.

### THE ROLE OF DATA DIODE IN OT NETWORKS

Most easy yet effective approach to protect any asset is to keep it in a well isolated area. No access means no possible threats. Data diodes play a critical role in protecting OT networks from cyber threats by preventing external access. These devices act as a secure bridge between OT and IT systems and control the flow of sensitive data. OT networks must be isolated from the outside world, but in today's data driven production environment, data exchange may be necessary. By controlling this data exchange to be uni-directional, data diodes prevent malware or cyber-attacks from infiltrating OT networks. In addition, these devices protect against internal threats to OT networks, thus maintaining the integrity of the network.







### **MECHANISMS TO PROTECT AGAINST CYBER ATTACKS**

Starting point should always be the physical segmentation. Physical security must be set. This includes ensuring that any physical components of the network are secure and that unauthorized access is prevented, where data diodes play an important role. Physical access to the OT environment is as important as logical access to data. Following by network security. This includes measures such as firewalls, intrusion prevention systems, and continuous monitoring of network traffic. Data diodes and firewalls must work together in harmony. These two technologies are not equivalent and must be properly integrated. Third, is the essential software security. This includes regular updates, patch management, and proactive detection of vulnerabilities. Finally, employee training and awareness play a critical role in securing OT networks. Informing employees about cybersecurity best practices increases their ability to recognize and prevent potential threats.

The sensitive nature of OT networks requires the use of different cybersecurity solutions to comply with above requirements. The security of facilities not only prevents information leaks, but also protects valuable company data, national security and public health. Data diodes play a vital role in protecting facilities against cyberattacks. By providing one-way data flow, they prevent external threats from penetrating OT systems, thus ensuring the security of critical operations. Data Diodes are inherently blocking any data access requests. Good analogy could be the surrounding pits of medieval castles. Request trying to reach into the castle would fall into the pit.







#### DATA DIODE IN OPERATIONAL TECHNOLOGIES (OT)

These devices also allow OT networks to be securely integrated with IT systems, which increases operational efficiency while ensuring security is not compromised. Although multiple measures are taken to secure the IT network, most of the leaks into the OT network are realized using the IT network. Therefore, the access of the IT network to the OT environment should be restricted as much as possible, if not completely.

Particularly in environments where industrial control systems (ICS) and SCADA (Supervisory Control and Data Acquisition) systems are widely used, data diodes are critical to ensuring data integrity and security. These systems often use legacy, non-secure, and externally vulnerable technologies. The use of these old fashioned makes the OT networks unprotected not only to current threats, but also to future cyberattacks. Many of such devices are not using any access control mechanism, that left them unprotected once any external attacker able to reach the device.

Data diodes provide a line of defense against cyberattacks targeting weak points, as a physical barrier against outside world. This way, data diodes support the security of OT networks as well as their overall business continuity and operational integrity. Data generated from ICS systems are received by data diodes, and intelligently processed with different decision engines running into the operating system, tailored for OT protocols.

Different protocols should be supported by a data diode, to comply with a wide range of OT endpoints. Old devices are mostly compatible with Modbus protocols, while new ones adopt widely use of MQTT protocol. Other protocols such as Profinet, OPC and even some proprietary protocols for different vendors must be supported to transfer any data generated within OT network, for data and business analysis.



In summary, the use of data diodes in OT networks is of vital importance not only in terms of security but also in terms of operational integrity and data integrity. This technology ensures the security of critical infrastructures and industrial control systems, while also allowing efficient and uninterrupted operational operations. Therefore, data diodes in OT networks should be considered an integral part of the cybersecurity strategy.





## DATA DIODE IN FACTORIES AND ENERGY PRODUCTION

Factories and energy production facilities are increasingly dependent on advanced technologies for sustainable and safe production. The operational technologies (OT) of these facilities require continuous data transmission and cybersecurity. Data diodes are critical components that meet these requirements. This section provides real-world examples (case studies) of data diode applications in energy production facilities and factories, the advantages of this technology, and the impact on production efficiency and safety.

#### REAL EXAMPLES AND ADVANTAGES OF DATA DIODE

Many factories and power generation facilities use data diodes to increase operational efficiency and security. Attacks on factory OT networks have resulted in many harmful results such as machine calibrations being disrupted, complete shut down or temporarily interruption of service. Even short-term disruption of the daily operation of machines and related components may cause serious financial losses. Non-optimal production that most of times hard to realize due to bad calibration may decrease the quality of the end product. In food industry, it can create severe health issues. For example, a tiny error resulted because of an external attack, targeting the calibration in closing a food package may allow surrounding air to enter into the package, that eventually affects the product lifetime.

A machine that needs to be heated to start, and to keep in optimal conditions, should remain on, unless a maintenance window is defined, must be protected against any external and uncontrolled access. Even short service interruption, may require longer time to recover, thus create severe problems in production lines.

Many factories use data diodes to increase the efficiency of their production lines and secure the data flow in production processes. This way, production-related data is transmitted to business analysis applications almost instantaneously, allowing live tracking and historical reports. It also enables the use of single reporting systems in OT and IT environments. Thus, business process investments become more effective.

Similarly, many power plants in Europe have invested in data diodes to protect against cyberattacks and ensure the secure transmission of operational data. This investment has ensured that critical data is securely shared with the outside world while maintaining the operational integrity of the plant. A popular real-life incident was Stuxnet attack that targets programmable logic controllers (PLC) of nuclear material enrichment facilities. Similar to factories any external action to modify a power plant parameter may cause long and critical service interruptions. If someone able to access and tune the operational status of the plant, recovery may take hours and sometimes even days.

Data diodes provide effective protection against external threats, thus increasing the security of critical operational systems. Especially in a period when the risk of cyber-attacks on industrial control systems is increasing, such protection is of vital importance for these facilities.





#### DATA DIODE IN OPERATIONAL TECHNOLOGIES (OT)

Data diodes also protect the intellectual property and sensitive data of enterprises by preventing data leaks. Another important advantage is the effective management of data flow between systems, ensuring that operational data is processed in a timely and secure manner. So, decision-making processes are accelerated and operational efficiency is increased.

The effects of data diodes on production efficiency and safety are very important for factories and energy plants. Thanks to data diodes, operational data is processed and analyzed securely, which enables more effective management of production processes. For example, the performance of production lines can be continuously monitored and necessary adjustments can be made instantly. This increases both production efficiency and product quality.

In terms of security, data diodes protect production facilities from cyberattacks, which ensures operational continuity. Energy facilities and factories are protected from potential disruptions caused by cybersecurity breaches, which means both cost savings and operational security.

I\*n factories and power generation facilities, the use of data diodes is of great importance in terms of cybersecurity, operational efficiency and production continuity. Real-world examples demonstrate the effectiveness and value of this technology. Data diodes make such facilities resilient to modern cyber threats, while also increasing operational efficiency and overall production safety. Therefore, data diodes should be considered an important part of cybersecurity strategies for power generation facilities and factories.



# DATA DIODE TECHNOLOGY IN THE FUTURE

### EXPECTED INNOVATIONS AND DEVELOPMENTS

Data diode technology quickly finds its place in the field of cybersecurity and will continue to develop and lead to significant innovations in the future. The evolution of this technology would include advancements in both hardware and software. Among the expected developments, increased data transfer speeds and wider bandwidths will be prominent. This will allow data diodes to process larger data volumes more quickly and will be especially critical for big data analytics and real-time data processing requirements.

The integration of AI and machine learning is another major development expected in data diode technology. This will help data diodes detect and prevent cyber threats more effectively, and will also be used to optimize data flow and improve network performance.

In addition, future data diode technologies can be designed to be more modular and flexible, meaning modern devices that can easily adapt to different network structures and changing operational requirements, and offer customizable solutions. Also, advances in wireless communication technologies can expand the use of data diodes and offer new types of connectivity options.

### **LEGAL OBLIGATIONS**

The legal requirements for the use of data diode technology are evolving along with increasing regulations on cybersecurity and data protection. Many countries and regions are introducing stricter standards and regulations to protect critical infrastructures and sensitive data. For example, laws such as the European Union's General Data Protection Regulation (GDPR) set strict rules for the processing and protection of personal data, and such regulations make the use of data diode technologies mandatory. These laws encourage companies to ensure data security and compliance by using data diode.

Legal requirements related to national security may also affect the use of data diode technology. In particular, factories, power plants, water treatment plants and other critical infrastructures are subject to legal regulations related to national security. It would become a legal obligation for such facilities to increase their cybersecurity measures and use data diode technologies. Thus, the use of data diode technology is no longer just a technological choice, but a legal one.

Many security frameworks such as ISO 27001 and COBIT, which are two of the security guides widely used globally, defines the use of data diodes as critical. In addition, Energy regulations in different regions mandate the security accreditation of many institutions and also set out the obligations regarding the use of data diodes.





Bottom line is, data diode technology will undergo a significant evolution in the future, both in terms of technological innovations and legal requirements. These developments will enable the technology to become more efficient, reliable and compatible, and will continue to play an important role in the field of cybersecurity.