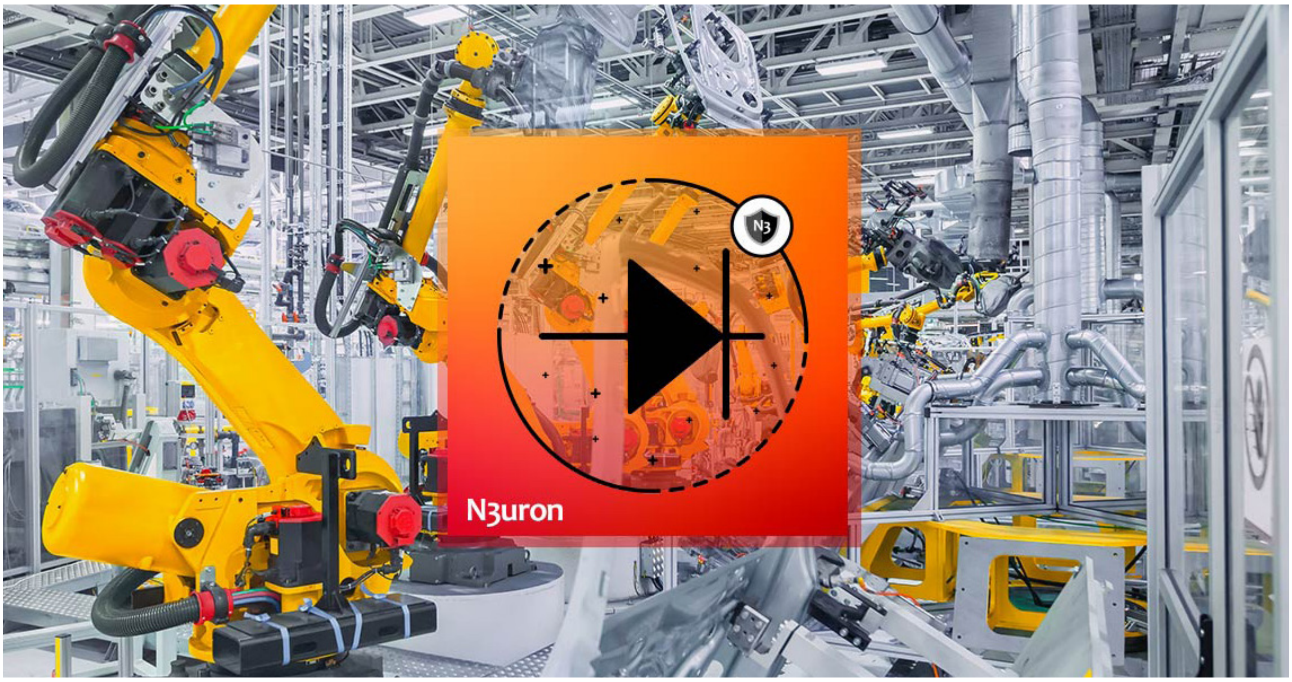
Author: Jose Granero

How to Improve Industrial Asset Security Using Data Diode

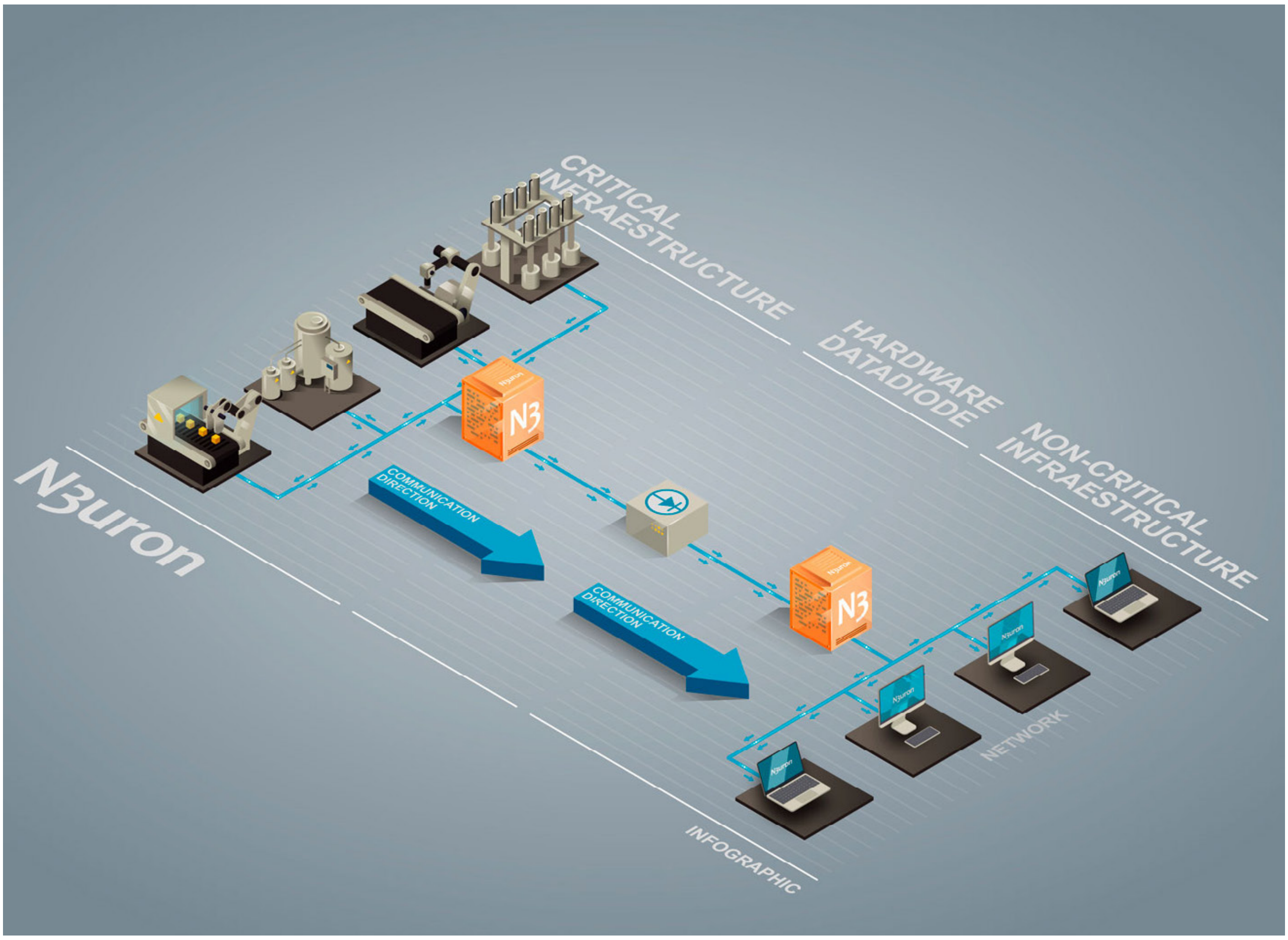


An Overview of Data Diode

The Industrial Internet of Things (IIoT) is revolutionizing industrial operations by enabling unprecedented levels of connectivity. However, every new connection to external infrastructures with which the OT network exchanges data is vulnerable to becoming a new attack vector and as a consequence, can be used to send back an attack via encrypted connections directly to critical industrial facilities.

As the digitalization process continues to evolve across all levels of a company, the risks linked to cyber-attacks also increase exponentially. **Although cybersecurity awareness** has progressed in leaps and bounds in recent years, there is still an overwhelmingly large number of industrial exposed devices and systems that can be found on shodan.io with just a quick search for any of the major industrial hardware and software vendors, not to mention the vast number of computers on OT networks that can be accessed via a certain very well-known remote desktop control software.

In general, many of the attacks that occur today are about money, be it attempting to steal valuable information or simply looking to compromise the system and hold data for ransom. However, when it comes to critical infrastructures, these kinds of threats aren't typically the most worrying. For these facilities, the major concern is usually preventing attackers from sabotaging the plant, poisoning water, disrupting energy supplies, or otherwise causing damage to property or potential harm to persons. Therefore, when dealing with this category of assets, it's wise to consider additional security measures that go beyond those employed for non-critical IT networks. OT security is a complex topic as there are many different techniques that can be employed. However, one of the most popular methods used nowadays is **Unidirectional Gateway technology, which guarantees data transmission in one direction only.** Used extensively for decades in military facilities, this technology is now starting to become popular for many other critical industrial applications due to the extra security levels it can provide in comparison with traditional firewalls.



Data Diode: Unidirectional Gateway Implementation in Industrial Environments using N3uron

What is a Data Diode?

Data Diode, also known as a Unidirectional Gateway, is a cybersecurity solution that acts as a barrier between OT critical networks and untrusted networks, such as a corporate IT network or the Internet. Unlike firewalls, which broadly speaking are purely software based and designed to implement a set of rules, Unidirectional Gateways are made up of a combination of hardware and software, which only allows network traffic to flow in one direction.

Typically, the hardware component of a modern Unidirectional Gateway has an optical transmitter and an optical receiver, each one connected to a different network. The receiver is not capable of communicating to the transmitter, which means there is no way for an attack to reach the OT network. Due to their simple nature, **Unidirectional Gateways are inherently immune to vulnerabilities and misconfiguration**. On the other hand, the software component ensures safe unidirectional real-time data transfer between networks.

One of the **main differences between Unidirectional Gateways and firewalls** is that since firewalls are software based, they may have bugs or back doors that attackers can exploit in order to pass through network layers. Moreover, firewalls need to be maintained by someone qualified in order to allow or restrict data transfers between networks and therefore, can be susceptible to improper configuration.Finally, complex sets of rules will introduce high network latencies. Even when dealing with the most powerful firewalls, these delays – which aren't usually relevant for IT networks – may affect the performance of real-time applications such as SCADA or DCS systems in the OT network.

In terms of software, there are many different solutions available on the market. The purest and easiest to configure involves transmitting broadcast UDP/IP packets from the OT network to the untrusted network, and in this way, guarantee one-way data transmission. However, there are other alternatives to this solution, such as Proxy Gateways that enable server replication, device emulation and TCP connections, although such implementations allow for bidirectional communications.

What About Applications That Still Need to Receive Data from an Untrusted Network?

Although apparently in contradiction with everything mentioned thus far, several use cases do exist where it is still necessary for data to be received from an untrusted network. For example, in the case of power generation plants, where power curtailments or hourly production setpoints are sent from Control Centers or Delegated Dispatches. In these cases, **the obvious answer is to set up a pair of Unidirectional Gateways**, one to allow outbound information from the OT network to the untrusted network, and a second one allowing information to travel in the opposite direction.

The key to understanding why this architecture is still more secure than a Firewall is realizing that these devices do not let TCP/IP packets pass, as in fact, they only send specific messages that they have been configured to send. Another alternative to the above-mentioned setup is to use a method called Flip, which consists of reversing the transmission direction within a pre-scheduled period.

N3uron Data Diode Module for Secure Critical Infrastructures

Data Diode is just one of many modules available in the N3uron IIoT communication modular platform. It's a software-based cybersecurity solution that ensures safe unidirectional real-time data transfer between segmented networks. It allows data to be sent through physical Data Diodes and Unidirectional Gateways that maintain the physical and electrical separation of source and destination networks, by establishing a non-routable, completely closed, one-way real-time data transfer between them. The Data Diode module's main features include:

- A configurable UDP port for increased flexibility.
- Data integrity algorithms for the prevention of data loss.
- Compression for reducing required bandwidths.
- Data encryption for increased security.
- Network interface assignment for network isolation.
- Whitelisting to ensure data is only received from approved sources.
- One-way Keep-alive for managing data quality on the receiver side.
- Compatibility with all main hardware vendors.

Sending Data Using an Affordable Hardware Data-Diode

Data Diodes are most commonly used for high-security government and military networks. Given this sensitive target market, the costs tend to be extremely high, no matter which vendor you choose. N3uron Data Diode module is compatible with all the main hardware Unidirectional Gateways and Data Diode vendors that support unidirectional protocols such as UDP.

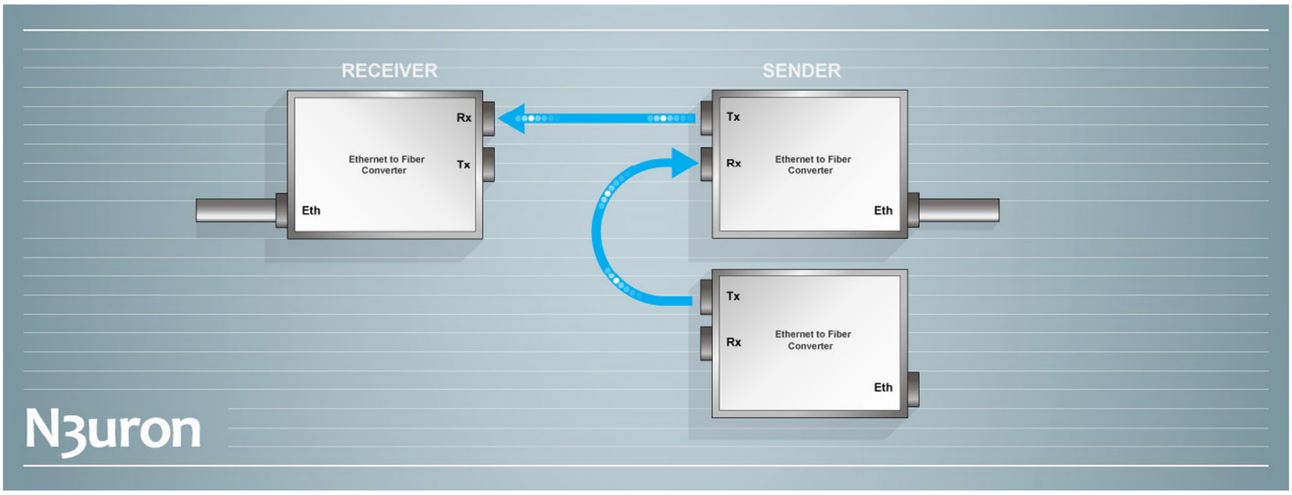
For industrial applications where official certification for the solution is not required, an affordable Unidirectional Gateway implementation can be easily deployed using N3uron, together with three Fiber-to-Ethernet media converters, as described below.

In this example, the N3uron Data Diode module is used to send one-way-only data through a hardware data-diode based on inexpensive and commercial "off the shelf" products. The hardware data-diode component is built using two Ethernet-to-fiber media converters, with separate fiber optic lines for transmitting and receiving. One converter acts as the sender, whilst the other acts as the receiver. In this way, only one fiber is connected from the Tx port of the sender to the Rx port of the receiver to ensure the data only flows in one direction. A third fiber optic transceiver is required for simply supplying a carrier signal to the sender converter.

Configuraton:

– **Step 1:** Since Address Resolution Protocol broadcasting (ARP) is not possible – given the total restriction of data transmission from the receiver to the sender – the IP and MAC address of the receiver must be added to the ARP table of the sender. The way to do this will differ depending on the operating system N3uron is running on.

- **Step 2:** Connect the media converters and machines according to the following diagram.
- **Step 3:** Download N3uron from our website and install it on both machines.
- **Step 4:** Configure N3uron sender and receiver nodes following the Data Diode Manual.


RECEIVER
SENDER
Rx
Tx
Ethernet to Fiber Converter
Eth
Tx
Rx
Ethernet to Fiber Converter
Eth
Tx
Rx
Ethernet to Fiber Converter
Eth
N3uron

Envisioning the Data Diode future

There has been an ever-growing interest in Unidirectional Gateways/Data Diodes for industrial applications in areas where they have not yet been used until now. Once configured properly with the software for unidirectional network traffic, Data Diodes provide a low latency and are an unbreakable way to secure communications.

The N3uron Data Diode module provides an affordable mechanism to implement effective defense elements in sectors where the deployment of these types of solutions have not been explored before due to the elevated associated costs, and thus, democratizes its use.

How to Get Started with Data Diode

If you're ready to try using Data Diode, download the N3uron free trial version and read our Data Diode manual on how to implement and use N3uron's Data Diode software module on our communication platform. Download the Data Diode Manual