Cybersecurity: How to Strengthen Security in Industrial IoT Systems with N3uron

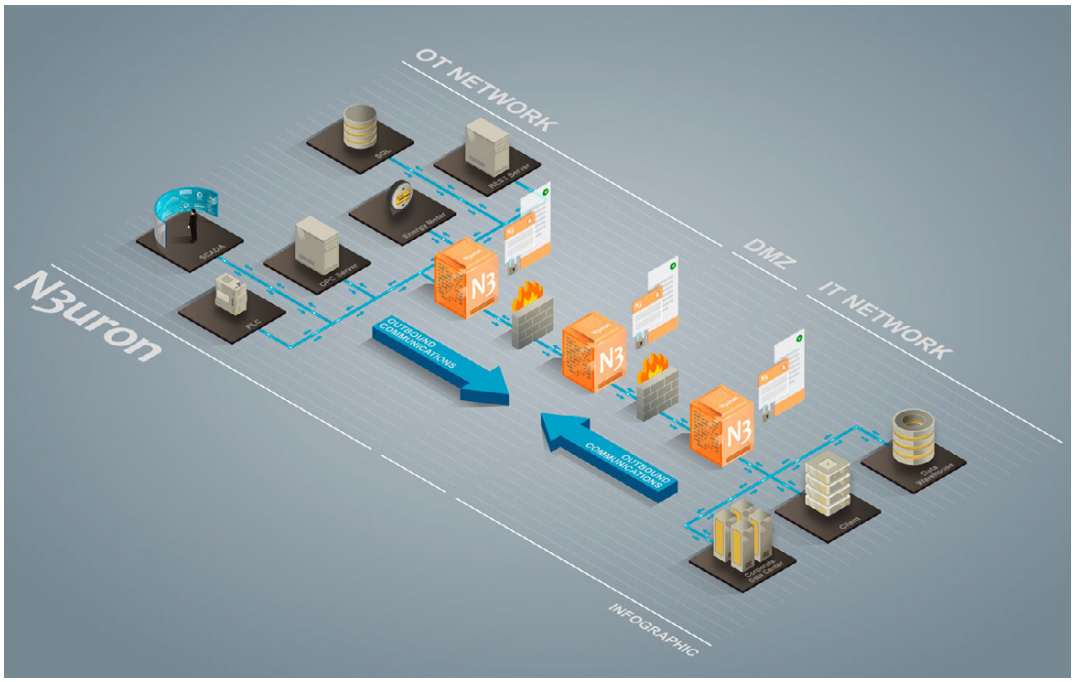
Why Cybersecurity Matters in Industrial IoT Systems

As digital transformation continues to deepen and spread across organizations, the need for data sharing across multiple systems and applications, both corporate and third-party, becomes more and more necessary. Whilst the advantages and opportunities offered by this transformation process, which involves the integration of new technologies throughout all areas of the company, are undeniable, it's also certain that it brings about a number of new threats, highlighting among them those pertaining to the security of data and infrastructures, and therefore of individuals, against malicious intrusions. In this particular scenario, the need for connectivity between corporate IT infrastructures and industrial systems developed on OT (Operational Technologies), which in many cases have been designed as fully isolated systems in which security did not play a key factor in their design and implementation, becomes increasingly important. It is precisely this need for IT/OT integration, which is being accelerated and implemented on a mass scale as part of Industry 4.0 and IIoT, that has led to a serious rethinking of all security related aspects due to significantly increasing exposure to potential cyber-attacks. For example, the European Commission has decided to carry out a review of the NIS2 Directive on security of network information systems, as well as creating a new directive for improving the resilience of critical entities, with the aim to increase the level of cyber resilience in critical sectors, both public and private. Among other initiatives, the NIS2 is ostensibly broadening the range of sectors and services required to adopt the measures outlined in this directive, including establishing a list of administrative penalties, which includes fines for any organization failing to comply with the mandatory provisions to be implemented at community level. In light of the above, a series of measures need to be adopted in order to mitigate, at least in part, any risks deriving from data exchanges between industrial networks and corporate systems or IT networks.

Best Practices for IT/OT Environments in the Industrial Sector

Although security is a complex issue and this article by no means intends to cover all aspects in their entirety, the recommendations considered to be most relevant to this effect are listed below.

Use of DMZs in an Industrial Environment 4.0



Example of DMZ in an industrial environment 4.0 using N3uron

As previously discussed, many OT systems have been designed to exist in isolation. This means that in principle, processes and their data would remain safe, provided that the system is kept isolated from the outside world, something which nowadays is mostly no longer feasible given the need to share data with other systems outside the plant or IIoT ecosystem.

In recent times, one of the most widespread solutions for connecting two separate networks is the use of a VPN (Virtual Private Network). However, this solution does not solve the problem of security, since it expands the attack surface of both networks as a result of them sharing at least a part of their respective networks. This means that a security breach of the VPN, for example when a computer connected to its network is compromised, could expose systems on both networks.

Currently, and in accordance with the recommendations established by the National Institute of Standards and Technology (NIST), as outlined in their SP-800-82 guide, one of the best ways to add extra layers of security is to use DMZs (demilitarized zones). The most secure, manageable, and scalable cross-network segmentation architectures are typically based on a system that uses a minimum of three zones, incorporating one or various DMZs. The DMZ contains at least one intermediate subnet, which segregates the OT control network from the corporate IT network and provides a single indirect point of contact between the two, as well as with unsecured networks such as the internet. These three zones must be separated by firewalls that guarantee traffic of strictly necessary data in both directions.

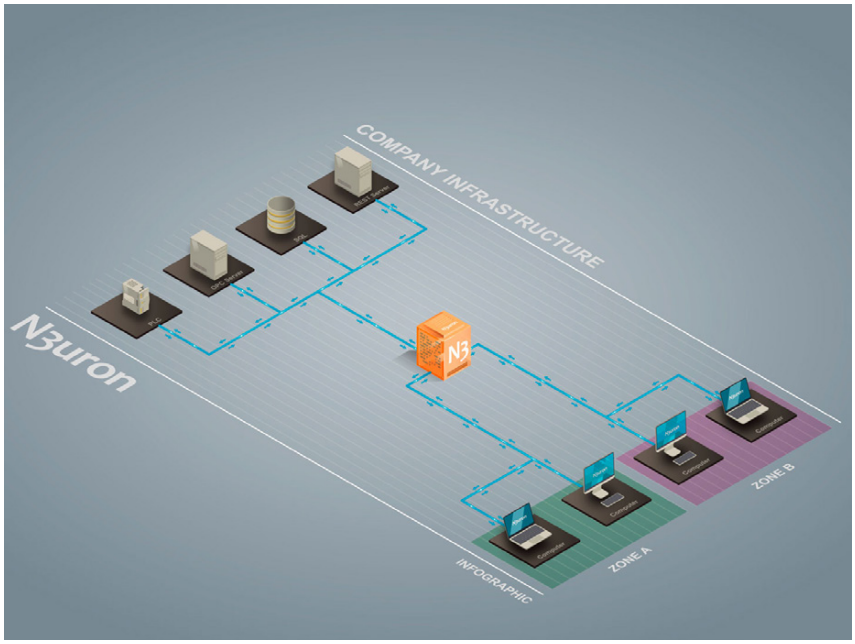
This architecture greatly reduces the risk of any attacks being launched on the OT network from a compromised DMZ computer, provided that the rules established within the firewall only allow for outbound connections from the OT network to the DMZ.

In this regard, N3uron provides the possibility of secure data exchanges through the DMZ by means of creating links between the different nodes and thus, only requires opening of an output port in the firewalls, not being necessary the opening of input ports. This allows for two-way communication, so that each node can both send and receive data in real time through the DMZ. Additionally, the links between nodes include a Store & Forward mechanism to ensure the storage and subsequent submission of this data in the event of any communication failures.

As an additional security measure in N3uron, information exchanges between nodes are always secured using TLS protocol (Transport Layer Security). This means that in order to enable communication, nodes must exchange digital certificates with each other and these certificates must be previously validated in the nodes with which they are intending to communicate.

Encryption and Certificates for Secure Plant Communications

server to encrypt and decrypt data. These certificates are obtained through a CA (Certification Authority). It is also possible for a company to generate its own self-signed certificates. This is a particularly good option if the machines from which clients are launched do not have access to the Internet. To do so, a root certificate is created, from which the signed certificates are then generated. However, it's essential to ensure that the root certificate is distributed across all machines from which clients are launched. For example, on a Windows network, this can be done using the domain controller.



Example security zone in an industrial environment using N3uron

Implementation of Safety Zones in Industrial Systems

Another good practice is to create security zones, so that clients in each zone can only and exclusively access the strictly necessary data. In order to create this zone separation, depending on the information that will be accessed, N3uron allows you to configure groups of variables called Views, in addition to the classic read/write permissions for each variable. This enables any potentially dangerous actions to be blocked, regardless of whether malicious or accidental.

The National Cybersecurity Center of Excellence (NCCoE), among many other organizations, establishes in their Sp 1800-16 guide that it is of vital importance to use TLS protocol for ensuring secure and confidential communications over unsecured networks, such as the internet. This involves the encryption of all data sent using the HTTP protocol, which in the case of N3uron, affects both client access to nodes through the WebUI module (used for configuring and visualizing data), as well as the corresponding WebVision module to SCADA/HMI functionalities. Apart from preventing malicious third-party access to data, this measure also protects against the known vulnerability – session hijacking, which involves exploiting a valid session to gain unauthorised access to information or services. SSL certificates are used as part of the TLS protocol in order for a web server, for example N3uron, to identify itself to a client, such as a web browser or another N3uron node, and allow that

Additional Measures for Critical Infrastructures

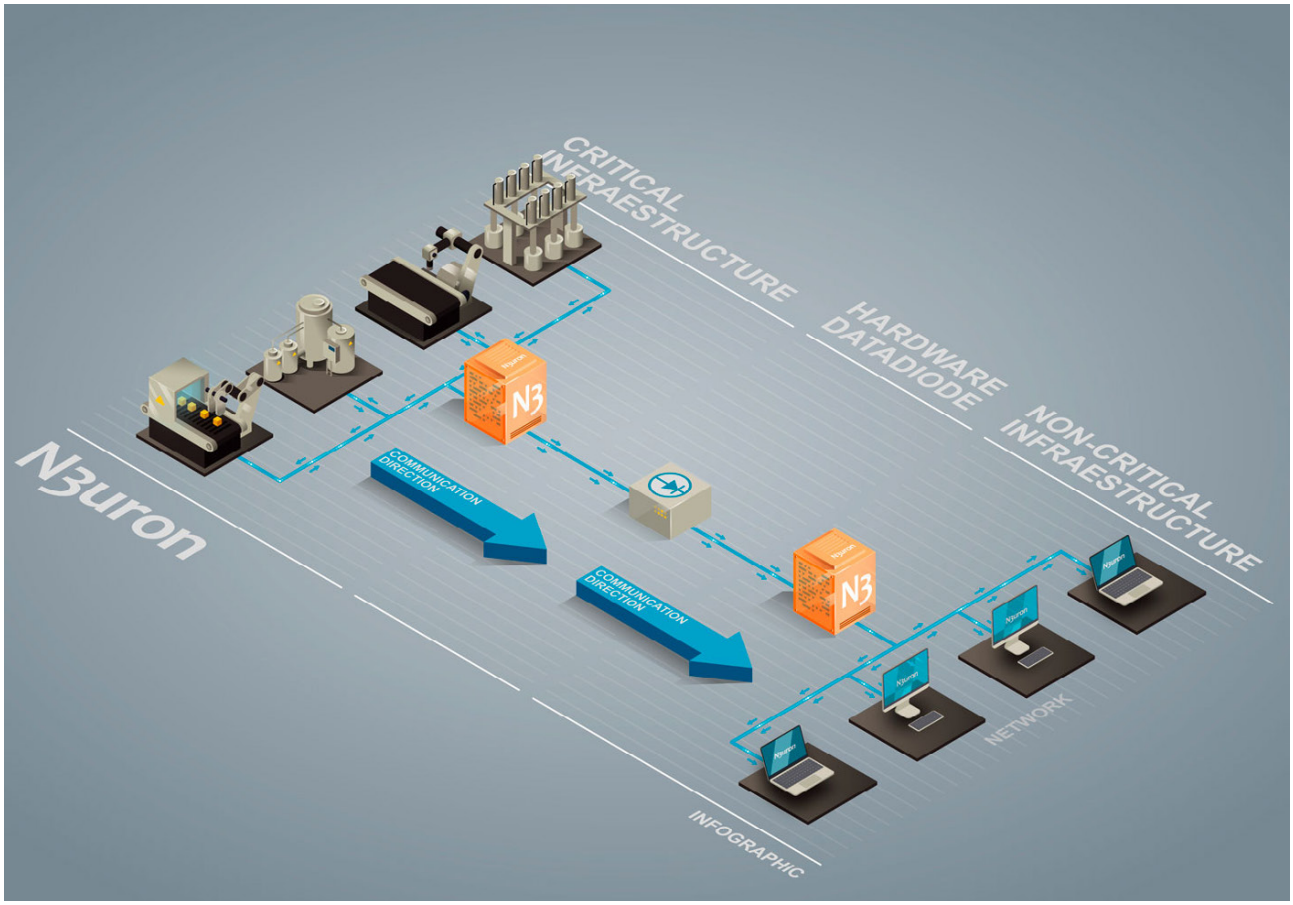
When it comes to critical infrastructures, the focus should be placed especially on prevention. The recommendation for this type of facility is to implement a fully isolated OT network. However, in the event that this network needs to exchange data with the outside world, the most effective way to prevent cyber-attacks (as established by the NIST in their SP-800-82 guide) is to use a "Data Diode". This is a combination of hardware and software that only allows data traffic to move in one direction.

By design, hardware prevents data from being sent to the source network, while software ensures data sending only from the critical network to the outside.

N3uron implements this functionality through the DataDiode module for one-way data sending and

receiving via UDP protocol. This module guarantees data is sent securely through a “Data Diode” network device.

Therefore, a number of different measures can be adopted in order to make the success of a cyberattack on our facilities extremely difficult and costly. As seen throughout this article, N3uron’s focus is permanently set on preventing these types of threats, and hence enables a number of countermeasures to be implemented (in line with the recommendations and regulations established by the most relevant international organisations) in order to significantly reduce the risks that systems are inevitably exposed to as a result of IT/OT convergence.



Representation of additional measures in an industrial environment using N3uron.

Conclusions: How to Secure Industrial IoT systems?

As far as cyber-security is concerned, there are a multitude of techniques and technologies available, each with different costs, implementation difficulties and scopes. Depending on the cyber-attack defence policy established and the measures taken thereon, many of the risks can be mitigated and even eliminated.