STORMSHIELD

DPI systems and network security

IPS Stateful DPI technology in OT environments

Executive summary

Today, a basic level of protection in the fight against cyberattacks is provided by segmenting operational networks. However, in the face of new and increasingly sophisticated threats, the deployment of solutions for in-depth analysis (DPI - Deep Packet Inspection) of the messages exchanged is also required to anticipate the protection of these sensitive networks.

To succeed in this challenge for OT, the security solutions that are deployed must meet exacting requirements in terms of **availability, integrity and confidentiality**, arising from the various business challenges supported by operational networks.

Any IPS system that works in close proximity to automated systems must therefore be implemented in compliance with these aspects to ensure it is possible to apply a proactive, sustainable security policy while guaranteeing the in-service safety of the operational systems.

To do this, four major factors must be taken into consideration:

- an **integrated solution** that provides in-depth knowledge of industrial protocols;
- an **ability to manage the compliance of operational messages** to make it possible to detect anomalies and protect OT network assets;
- **proactive protection against the various threat variants** to counter targeted attacks and avoid production stoppages;
- a **context-based approach to message exchanges** to ensure they are compliant with operational processes.

This white paper describes the various mechanisms that an IPS system needs to exploit to satisfactorily fulfil its detection and protection role. It will also give you the basic features an IPS is required to include to ensure it can be tailored to your security requirements.

This white paper is intended for operations managers, maintenance and operational managers in charge of critical infrastructures as well as for chief information security officers.

Stormshield
All around the world, companies, governmental institutions and defence organisations need to guarantee cybersecurity for their critical infrastructure, their sensitive data and their operational environments. Certified and qualified at the highest European levels, Stormshield's technological solutions meet the challenges faced by IT and OT to protect their activities. Our mission: to provide cyber-serenity for our clients so they can concentrate on their core activities, something which is vital to the satisfactory operation of our institutions, our economy and the services provided to our populations. When you choose Stormshield, you are choosing a trusted European cybersecurity provider.

Contents

Context

Cyberattacks against operational infrastructure are becoming increasingly sophisticated. When configured to execute in sequenced stages, they become virulent and complex for the various protection systems to detect. Advanced Persistent Threats (APTs) are cyberattacks that use a collection of strategically combined techniques and methods to target a well-defined goal. Staying under the radar for as long as possible to avoid arousing suspicion, their aim is generally the extraction of high value-added data (patents, industrial secrets, etc.).

> The challenge is to design architecture that is capable of transmitting and processing data and **maintaining its integrity** between systems.
>
> Cigref

Consequently, although most companies and organisations claim to be aware of cyber risks and their potential implications (data loss or theft, production stoppages, etc.), they are very often more at risk than they imagine. With the appearance in recent years of the Industrial Internet of Things (IIoT), cyberattacks are targeting companies in different sectors such as aeronautics, nuclear power, electricity and health… operators of infrastructure of vital importance to society who become preferred targets for such attacks.

In some cases, however, these players know where the vulnerabilities in their system can be found, but do not have the means to replace the applications and/or equipment in question. This is a common scenario in critical operational networks such as the healthcare sector, which use applications that are supported only by older operating systems. In the industrial sector, some components are retained even when obsolete, which increase the risk of being impacted by an attack that has been lying discreetly dormant for some time. As a November 2019[1] study revealed , some flaws and vulnerabilities have been used by cyberattackers for more than ten years, and are still being exploited today.

However, industrial cybersecurity remains a relatively recent discipline. Experience in the IT world[2], including examples such as risk analysis, also proves useful in providing an appropriate, efficient response when appropriately tailored.

This white paper aims to deal with and analyse IPS-type network protection methods and associated issues in securing OT networks.

[1] Stormshield, www.stormshield.com/news/what-will-2020-cybersecurity-trends-be/

[2] Stormshield, www.stormshield.com/news/it-ot-networks-why-convergence-is-delicate/

Cyber risks associated with operational networks

In recent years, the digital transformation marked by IT/OT convergence – as well as the use of Edge / Cloud Computing[3] – has led to increasing levels of hyper connectivity among industrial companies' networks of all sizes. **Operational excellence** projects, in conjunction with Industry 4.0 (such as advanced optimisation between the production chain and corporate ERP), has made operational networks more susceptible to cyber risks.

Recently, with the EKANS (or Snake) attack, **we have been made aware (again) of the severity of the risks** that an intrusion into the industrial network can cause. Some factors can increase the likelihood of this type of risk: a lack of consistency between the equipment in place and the control stations, or industrial components which have different standards and/or requirements. When these elements co-exist in the same environment, the result can be failures leading to the collapse of the whole system.[4]

In the world of IT, it is clear that as soon as connections are established to systems and machines which had hitherto been isolated from the network, the possibility of hacking increases, with serious consequences: physical damage, disrupted production and even theft of industrial processes.

With the IT/OT convergence we are witnessing, many industrial companies are starting to set up comprehensive management systems for their sites to provide a clearer view of their operational networks. Therefore, if they are to obtain a good understanding of industrial cybersecurity issues, **the worlds of IT and OT need to engage in mutual dialogue, analysing and assessing risks in order to facilitate effective implementation of network security administration and management processes.**

[3] Forbes, www.forbes.com/sites/ronshevlin/2020/08/17/cloud-computing-raises-new-cybersecurity-concerns-for-banking/#5f46307f24ae

[4] Stormshield, www.stormshield.com/news/the-manufacturing-industries-faced-with-cyber-threats/

As Vincent Riondet, Cybersecurity Projects and Services Team Leader at Schneider Electric France, points out, at most industrial sites, "*infrastructures that are for the most part fairly old are required to cohabit with network architectures and operating systems that are for the most part fairly recent; the result may well not support advanced security standards, because upgrades are costly.*"

The application of multiple protection barriers, such as segmentation, flow control, detection and intrusion prevention, may be extremely useful in combating threats that come from network data flows. In addition, access control on its own, with its approach of allowing or denying a given communication protocol (via its port), is no longer sufficient; there is also a need to analyse the commands that are sent via the authorised business protocols.

Consequently, the task of securing network architecture must be based on protecting these protection measures and keeping them up to date in order to avoid data leaks or disturbances to the operational process. And the goal? Greater effectiveness in fighting the cyberattacks that may materialise at any time. For that reason, **it is essential to implement proactive defence systems in the closest possible proximity to critical infrastructure.**

Defence systems: industrial sensor or IPS?

Although it is vitally important to monitor industrial infrastructure, there is no single technical assessment matrix that can be applied to all operational architectures. One of the questions to ask is: **who handles the alerts that are generated, and how?** After all, in addition to the technical aspects, setting up an intrusion detection system requires **a trained operations team** able to manage and analyse **a large volume of information** to identify critical events and escalate potential security issues, where relevant.

Although these solutions can complement one another, the potential choice between an industrial sensor and an IPS solution must be based on a set of parameters, depending on your usage requirements. To do so, you need to conduct a detailed examination of your operational network architecture. With reference to your needs, **determine the appropriate protection by assessing how critical safety is for each element**.

It is also vitally important to consider how your new solution will fit into your overall cybersecurity policy, as well as your current and future processes and organisational structure.

DID YOU KNOW?

IPS systems often offer the same IDS (*Intrusion Detection System*) functions as industrial sensors. However, because they do not provide the same level of detail as these sensors in their identification ability, IDS systems are still used to recognise data flows passing through the equipment.

The recommendation is **to implement IPS gradually, via an IDS network traffic analysis phase**. This preparatory step makes it possible to map flows and identify potential false positives before activating the active intrusion prevention system to block suspect flows.

An industrial sensor is a **passive** tool that **detects** potential malicious data flows within the network		**An intrusion protection system (IPS)** is an **active** protection tool that **identifies** and **blocks** potential malicious flows within the network
• OT sensor does not block network packets	VS	• IPS acts by blocking suspicious packets
• OT sensor needs human intervention to manage incidents	VS	• IPS manages alarms autonomously
• OT sensor sees a complete copy of the network	VS	• IPS is located in line with the network
• OT sensor provides a large amount of information	VS	• IPS only raises an alert in the event of a problem
• OT sensor is sensitive to flooding actions	VS	• IPS can stop this kind of attack
• OT sensor is "transparent" on the network in the event of attack	VS	• IPS can be spotted more easily

DID YOU KNOW?

There are IPS solutions that integrate **a safety mode (bypass function) to ensure, if necessary, operational network availability in the event of a failure.**

Principles of the Intrusion Prevention System

In short

The main role of an IPS is to **monitor network packets and their contents in real time in order to apply predefined rules based on the attack detected and the intended target**.

DO NOT CONFUSE

There are 2 different types of IPS:

- **HIPS (Host-Based Intrusion Prevention System)**: IPS for monitoring workstations.
- **NIPS (Network Intrusion Prevention System)**: IPS for monitoring the network.

How does it work?

Intrusion prevention systems are placed in line on the network they are protecting. They analyse network packets, initially to check protocol compliance and monitor commands.

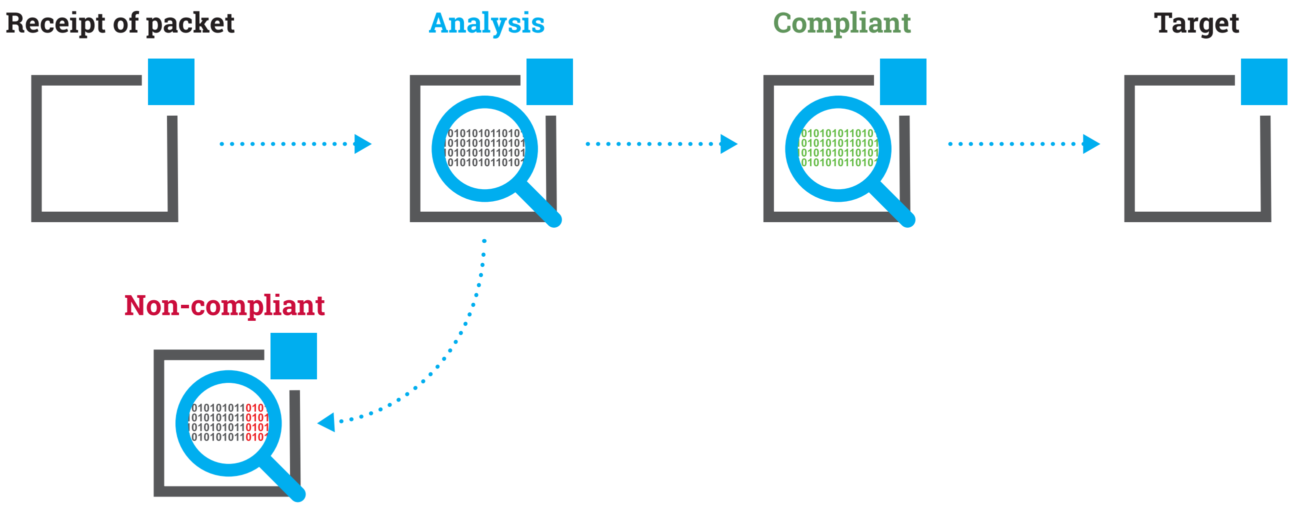
Some IPS systems are able to identify abnormal behaviour.

In order to block attempted attacks, IPS systems then check whether the network packets contain a set of data matching known malware signatures.

What benefits does IPS bring

This technology ensures network protection for IT and/or operational infrastructure.

As such, support for the business protocols used by the organisation is an important criterion for selecting the IPS system in terms of ensuring good coverage in protecting control commands.



Signature or targeted protocol detection:
two approaches for protocol compliance checking

The best IPS engines decode the protocols used and ensure the compliance (data packet length, protocol type, etc.) of each of the messages with respect to the expected format specified in the approved standards for these protocols. They are capable of making a very in-depth analysis of the information, hence the frequently-used term Deep Packet Inspection ***Deep Packet Inspection*** **(DPI)**.

The DPI (Deep Packet Inspection) assesses the header of a transmitted packet and the associated data, eliminating any non-compliance with protocols

Let us take the example of a network packet carrying a command:

Header		Command	Parameters		
1100	0011	1101	1110	1110	1000

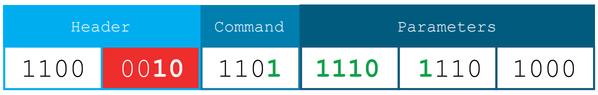
With respect to protocol compliance, an IPS system will search for specific byte strings for two main reasons:

1. **Protocol recognition**: first, look for characteristic markers to identify the transiting protocol,
2. **Protocol compliance**: next, ensure that byte sequences matching the identified protocol are found in the network packet.

DID YOU KNOW?

In the industrial world, the specific implementation of protocols mainly uses custom commands. **Signature-based protocol analysis does not recognize these values, and therefore generates detection errors.**

In this case, a so-called **“signature” analysis** searches for the string ***111101*** at any point in the packet.

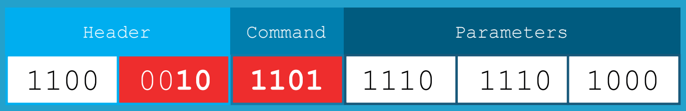


Header		Command	Parameters		
1100	00**10**	110**1**	**1110**	**1**110	1000

Here, the bytes identified by this approach are present, but are not in the correct place in the packet. The signature-based technique lets the badly-formed packet through anyway (leading to a false negative).

The targeted approach looks for the desired information in the correct location, precisely where it is supposed to be, to prevent malformed (and potentially malicious) packets from being allowed to pass.

With the targeted approach, the malformed packet is therefore blocked.



Header		Command	Parameters		
1100	00**10**	**1101**	1110	1110	1000

In this way, **targeted protocol analysis** offers two key advantages:

1. **Exact protocol compliance**
2. **Minimises detection errors**

Contextual analysis at the heart of the security of exchanges

This approach blocks cyberattacks by contextualising the messages exchanged between two network elements. To this end, **context-based analysis** verifies that the sequence of exchanged messages is as specified in the protocol standard, and does not show evidence of abnormal behaviour.

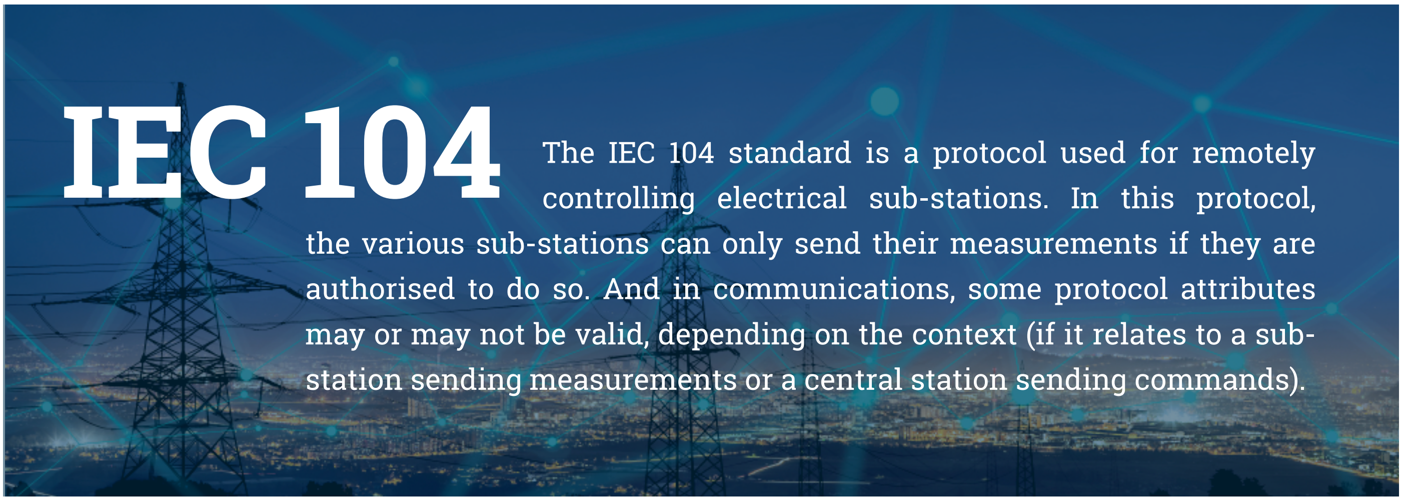
Context-based analysis examines and verifies the message in an exchange between two devices, taking previous messages into account. **This advanced technology protects and ensures the integrity of your operational environments and assets.**

Consider, for example, a robot "A" which can be controlled by a number of controllers. Controller "A" requests to take control by sending an appropriate request. Robot "A" acknowledges this request, sending an acceptance of the command, provided it is not already being controlled by another controller. In this example, imagine that an attacker takes control of robot "A". The IPS system sees a packet sent spontaneously by robot "A", accepting a control request that has not been identified by the system. Because it can see the context, the IPS can identify this behaviour as abnormal, and is able to block it.

By performing **context-based analysis** for sequences of packets passing through the operational network, this type of IPS is able to consider information relating to the exchanges between two devices. **It considers several parameters of the current message compared to messages that have already been exchanged**. These parameters may be: the direction of communication between the two devices, the type of command to be executed, or the command values to be applied.

BENEFITS

This type of IPS solution, known as a ***Stateful DPI***, permet de **renforcer le niveau de sécurité de l'infrastructure opérationnelle pour ainsi réduire la compromission des actifs du réseau.**



IEC 104

The IEC 104 standard is a protocol used for remotely controlling electrical sub-stations. In this protocol, the various sub-stations can only send their measurements if they are authorised to do so. And in communications, some protocol attributes may or may not be valid, depending on the context (if it relates to a sub-station sending measurements or a central station sending commands).

Searching for network threats

The Triton malware reveals the weakness of OT networks and demonstrates the need for an IPS system to be able to identify threats via the network, even in cases where the attack complies with protocols and follows the specifications of the protocol standard. To do this, the IPS searches the network packet data to establish whether a string of bytes corresponds to a known attack signature.

It should also be noted that some malware is able to evolve. Variants of this malware then call for specific new signatures: if they are not incorporated into the IPS, it will not be able to detect them. **For this reason, the recommendation is to use an IPS capable of using proactive signatures, which will include the range of variants of an attack, so that they can be detected.**

BENEFITS

Proactive protection also offers another significant benefit: the number of signatures required in the database is smaller, enabling **faster searches for known attack patterns in the network, and reduced network latency caused by the analysis.**

Better still, if the IPS engine is able to take advantage of the detailed analysis produced during the protocol compliance check and thus search only for relevant attack signatures in each part of the messages, **performance is improved still further and the proportion of false positives is drastically reduced.**

Triton : a cyber-attack against ICSs

The Triton malware was designed to target ICS systems at a Saudi petrochemical plant with the aim of causing an explosion. Fortunately, the attackers made a mistake, triggering an emergency shutdown of critical systems and bringing the network intrusion to light.

Stuxnet worm: illustration of variants

Stuxnet was designed to attack Iranian uranium enrichment centrifuges. The complexity of this malware derives from a detailed knowledge of industrial processes and Windows OS flaws. The cyberattackers used sophisticated, little-known Zero-day exploits.

Stuxnet variants have also since been used against other industrial infrastructure.

A number of industry organisations and experts in the field have published best-practice guides for managing the control systems. Among other things, they illustrate the need to segment the network, control access, acquire rugged systems, and implement antivirus protection and IPS-type intrusion prevention engines.

Faced with this type of threat, a proactive IPS system capable of handling the potential variants of the same malware proves to be essential (or even vital) to the industrial system's survival.

The required customised signatures

An IPS signature must be able to recognise and manage the messages exchanged via industrial protocols if it is to effectively protect the operational system. Each value sent in the command messages must be correctly analysed and verified, because each network communication operates directly on a specific operational process.

An IPS system must be able to offer customised signatures so that controls of command messages can be implemented in compliance with operational industry processes and restrictions

IPS solutions can provide this verification through custom signatures. The goal: to control command messages so that they comply with operational business processes and constraints. This is the most critical point in an operational environment to ensure that values do not exceed certain limits that could jeopardise the entire process.

Let's take, for example, the simplified case of a dam which is controlled by commands which must consider the flow that can be handled by a valve (in this case: a total capacity of 50-5,000m3/s). Even though new ICS/SCADA systems are less sensitive in this respect, it is important for old infrastructure to ensure that the values sent to the controller comply with these limits in order to avoid higher flows which could have serious consequences, such as flooding.

It is essential to be able to check these values in real time.

700+
proprietary protocols

UMAS, S7, TSAA, SAAT, HNZ, ...

20+
standardised protocols

Modbus, UMAS, OPC Classic, S7, EtherNet/IP, CIP, BACnet/IP, IEC 60780-5-104, DNP3, PROFINET, IEC 61850 (MMS/GOOSE/SV), OPC UA...

BENEFITS

With customised signatures, it is possible to:

- **adapt** to the business context;
- **implement** protocol analysis for proprietary protocols;
- **control** "sensitive" values to ensure the safety of the operational system;
- **ensure** that the operational process functions correctly.

Criteria for choosing the right IPS

Choosing an IPS system may appear a delicate, complicated task, considering what is at stake.

The diagram below will give you a quick overview of the necessary features.

IPS intrusion prevention system, for active monitoring of the network and ensuring data integrity and availability

Protection and control of proprietary OT protocols with signature customisation

Reduction of false positives thanks to an **IPS engine that conducts targeted protocol analyses**

Improved analysis consistency, making use of **Stateful DPI** , which performs **context-based** analysis for improved identification of the given context

Protection against unknown attacks with an IPS system **that is able to detect new abnormal behaviour and/or attack variants**

On-board safety function (bypass mode) in the IPS equipment **to guarantee operational business continuity** in the event of a failure.

DID YOU KNOW?

It is more complex to integrate protection systems that consist of multiple components. In addition to the number of management systems, licences and training sessions required, these solutions generally increase network latency.

Improve your teams' productivity by choosing an all-in-one IPS solution that is easy to deploy and simple to use. In the same way, a clear graphical interface will make it easier to integrate and manage the IPS, providing a clearer view of the systems to be protected.

Stormshield's *Stateful DPI* engine

Equip yourself with a high-quality system offering intrusion prevention and segmentation of your operational network, ensuring the availability and integrity of your systems

Powerful flow analysis

PROTOCOL COMPLIANCE CONTROL
combining packet control and application protocol compliance

DPI for 10+ supported protocols
Modbus, OPC Classic, S7, EtherNet/IP, CIP, BACnet/IP, IEC 60780-5-104, DNP3, PROFINET, IEC 61850 (MMS/GOOSE/SV), OPC UA, etc.

An industrial IPS

based on multiple analyses to provide a proactive response which even prevents Zero-day attacks

Context-based analysis

Behavioural study according to a business context

Optimised integration of the IPS into the on-board OS

Context-based signature search in a more granular, targeted database

Targeted, context-based protocol analysis reduces latency time and minimises false positives

Superior performance thanks to...

PERSONALISED SIGNATURE

WHY WILL YOU NEED IT?

1
Monitor compliance with operational processes

2
Adapt to a specific protocol analysis

3
Prevent damage to industrial equipment and the environment

Intuitive setup

All-in-one solution

Clear, easy-to-use UI

EXPERTISE IN PROTECTING OT NETWORKS: CO-DESIGN WITH EQUIPMENT MANUFACTURERS, INDUSTRIAL INTEGRATORS AND CUSTOMERS

www.stormshield.com

STORMSHIELD

The European choice of cybersecurity

All around the world, companies, governmental institutions and defence organisations need to guarantee cybersecurity for their critical infrastructure, their sensitive data and their operational environments. Certified and qualified at the highest European levels, Stormshield's technological solutions meet the challenges faced by IT and OT to protect their activities. Our mission: to provide cyber-serenity for our clients so they can concentrate on their core activities, something which is vital to the satisfactory operation of our institutions, our economy and the services provided to our populations. **When you choose Stormshield, you are choosing a trusted European cybersecurity provider.**
www.stormshield.com