



# STORMSHIELD

Network Endpoint Data

## Space's Industrial Control Systems Security

3<sup>rd</sup> Edition – 02<sup>th</sup> of December 2019



*Industrial Security Business Line*

# Stakeholders

Manoël BIZIEN

Industrial Presales

Industrial Security Business Line

[manoel.bizien@stormshield.eu](mailto:manoel.bizien@stormshield.eu)

**+33 (0) 6 99 83 49 59**

Michael CASTRO

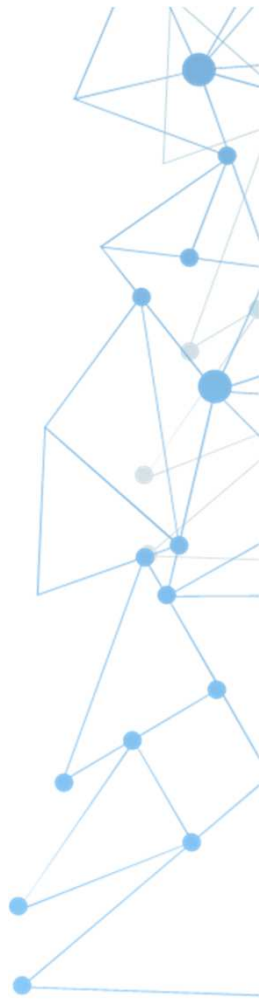
Head of the Western France branch

[michael.castro@stormshield.eu](mailto:michael.castro@stormshield.eu)

**+33 (0)6 71 32 58 98**

**STORMSHIELD**

*ISBL - Industrial Security Business Line*

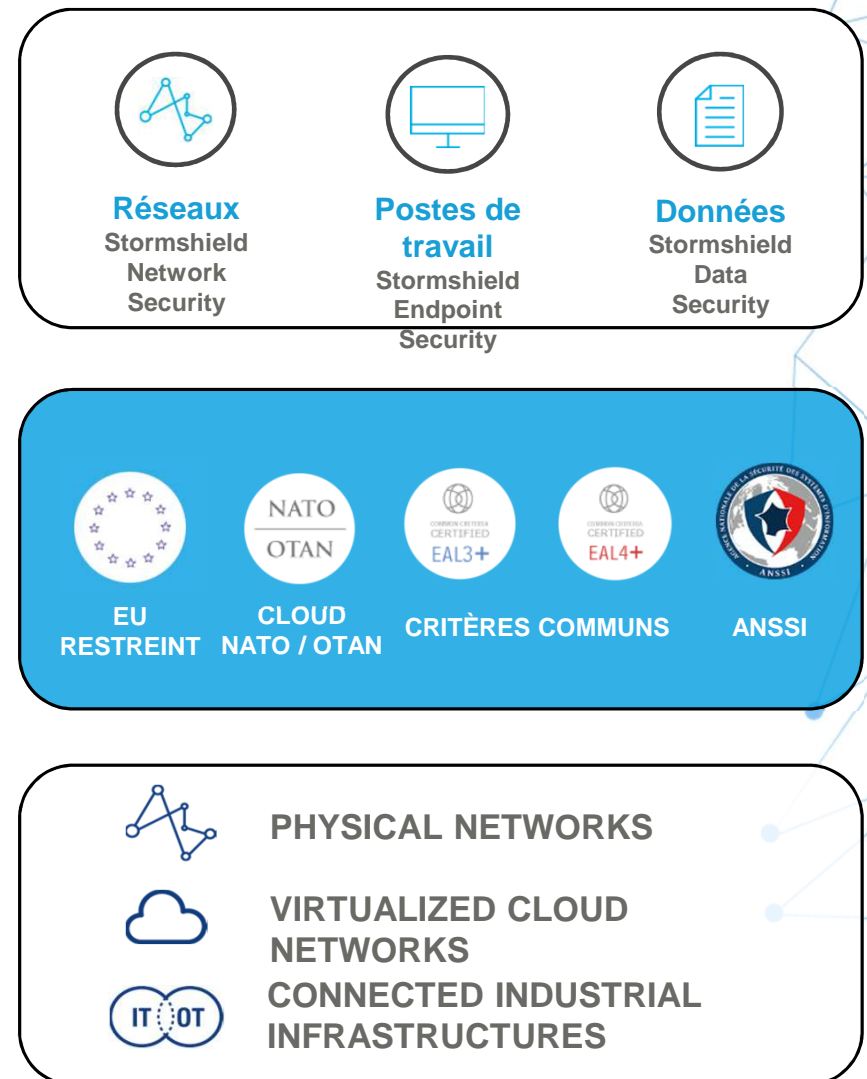


## The themes we are going to address

1. Industrial collaborations
2. What is an industrial IS ?
3. Our detection capabilities
4. What is signature analysis ?
5. What is protocol analysis (DPI) ?
6. Securing data transmission in an industrial environment
7. Stormshield Network Security  
Protection of industrial networks IT & OT
8. Stormshield Endpoint Security  
Engineering workstation



## Stormshield - In a few figures



**STORMSHIELD**

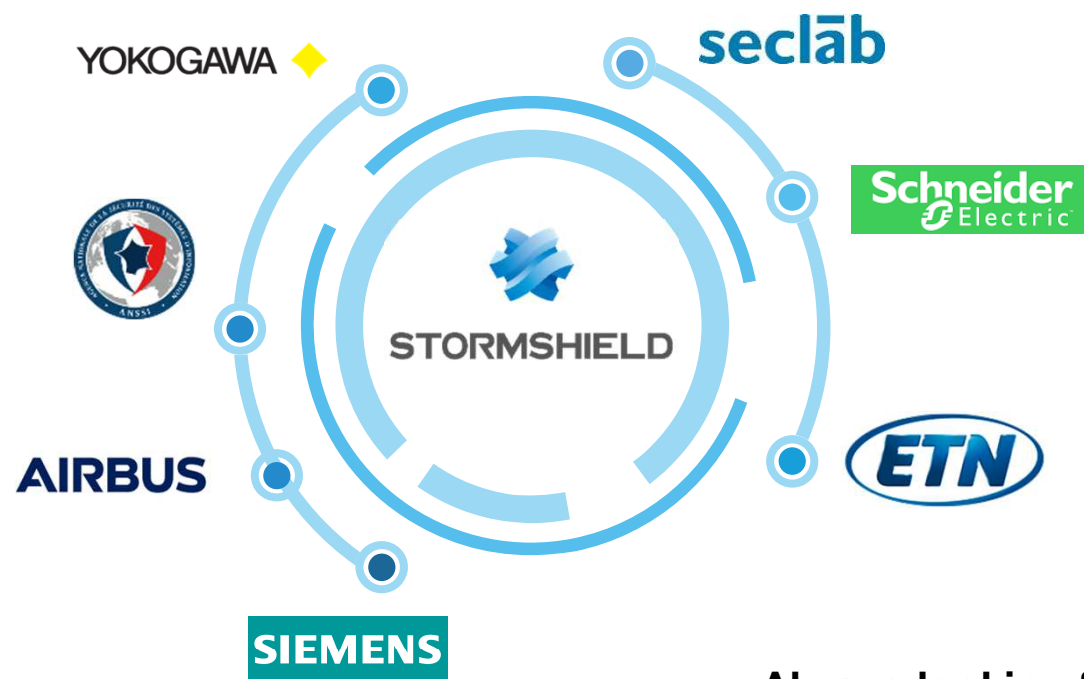
ISBL - Industrial Security Business Line

A high-angle, blue-tinted photograph of two men in business attire sitting at a table. The man on the left is looking up and smiling at the camera, while the man on the right is looking down at a document. On the table are several papers, including one with a colorful bar chart, a pen, and a computer keyboard. The overall scene suggests a professional meeting or collaboration.

# Industrial collaborations

STORMSHIELD

## Stories of our industrial collaborations



**Always looking for new partners**

**STORMSHIELD**

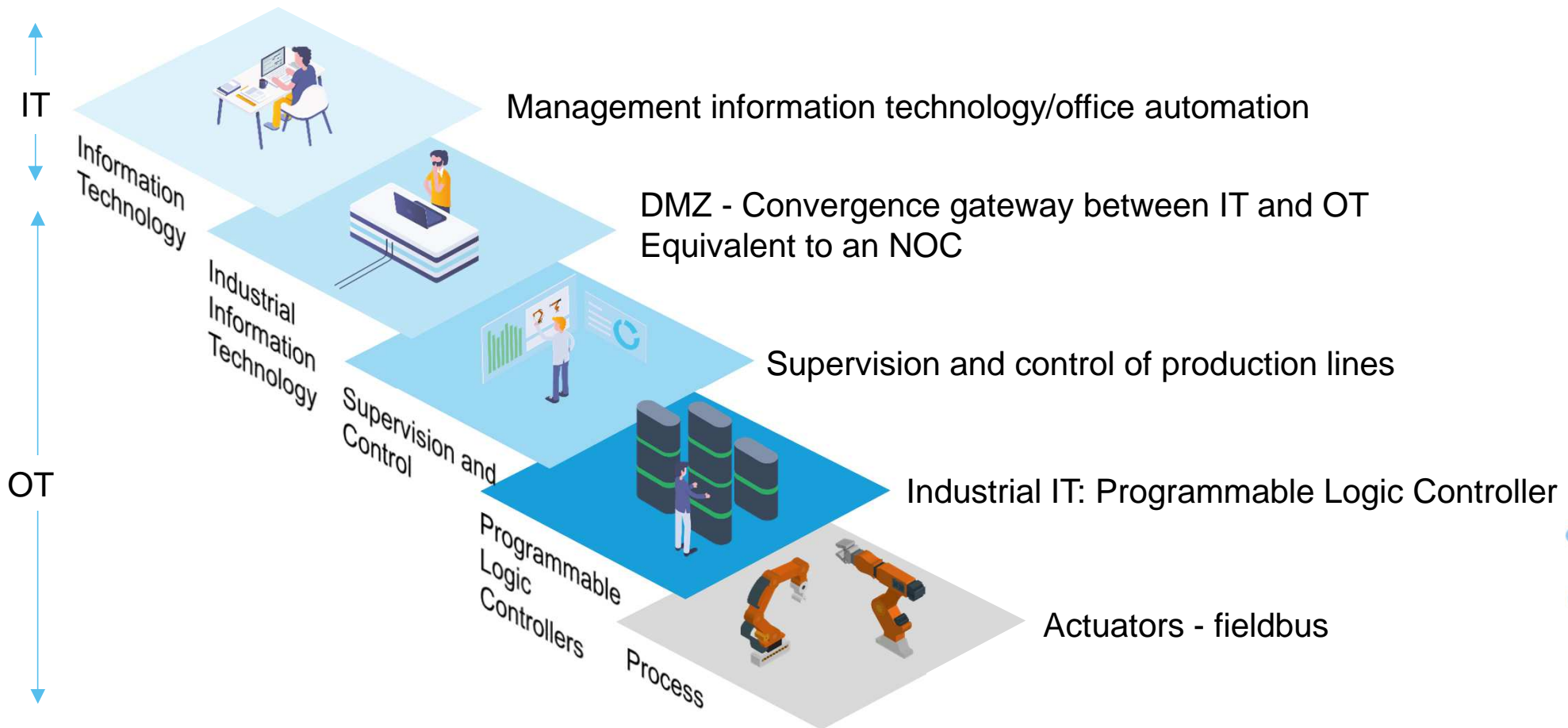
*ISBL - Industrial Security Business Line*

A high-angle photograph of two men in business attire sitting at a desk, looking at a document. The man on the left is smiling at the camera, while the man on the right is looking down at the document. The entire image is covered with a semi-transparent blue filter. The text 'What is an industrial IS' is centered in white. In the bottom left corner, the word 'STORMSHIELD' is written in white capital letters.

# What is an industrial IS

STORMSHIELD

# What is an industrial IS

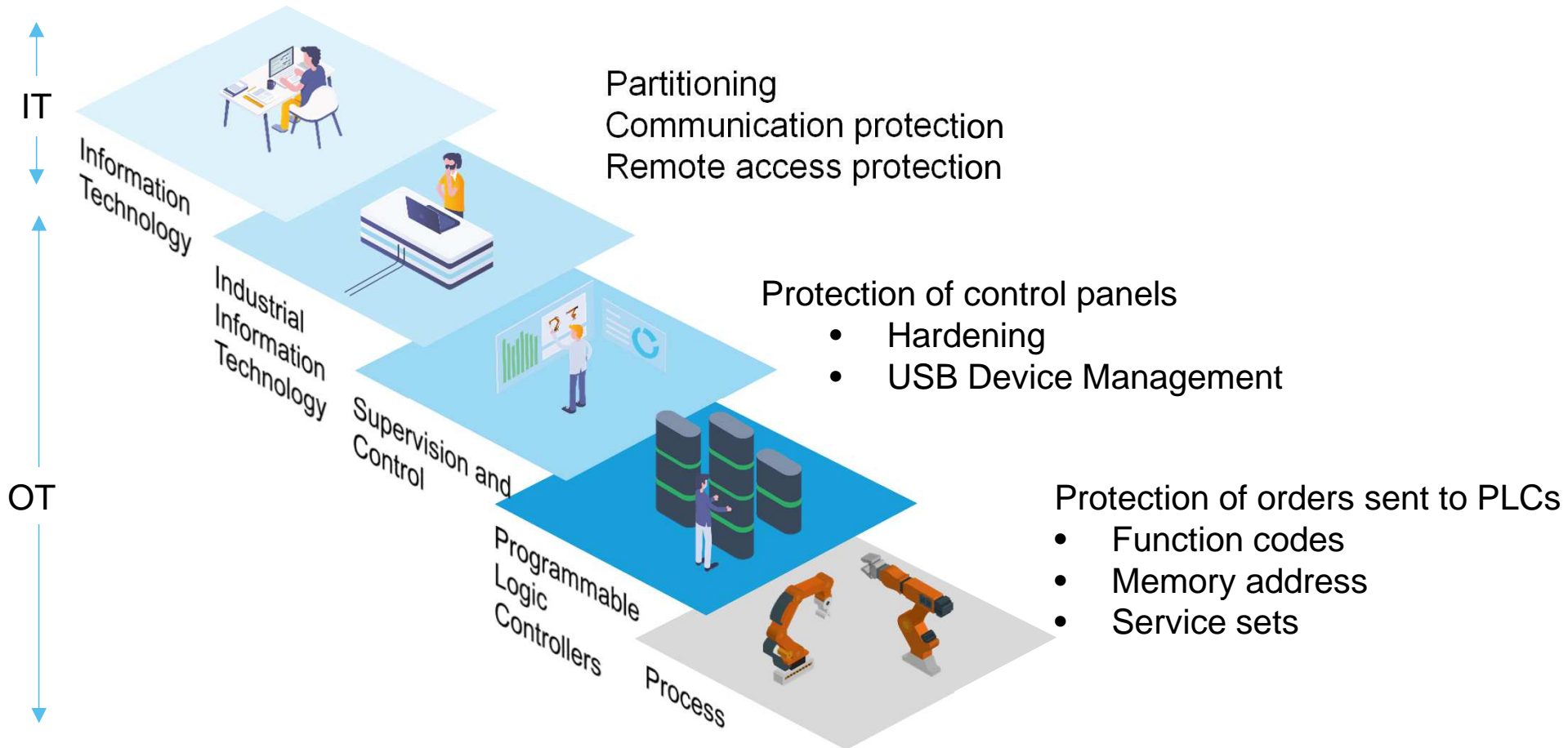


**STORMSHIELD**

ISBL - Industrial Security Business Line



# Our protection and detection capabilities



**STORMSHIELD**

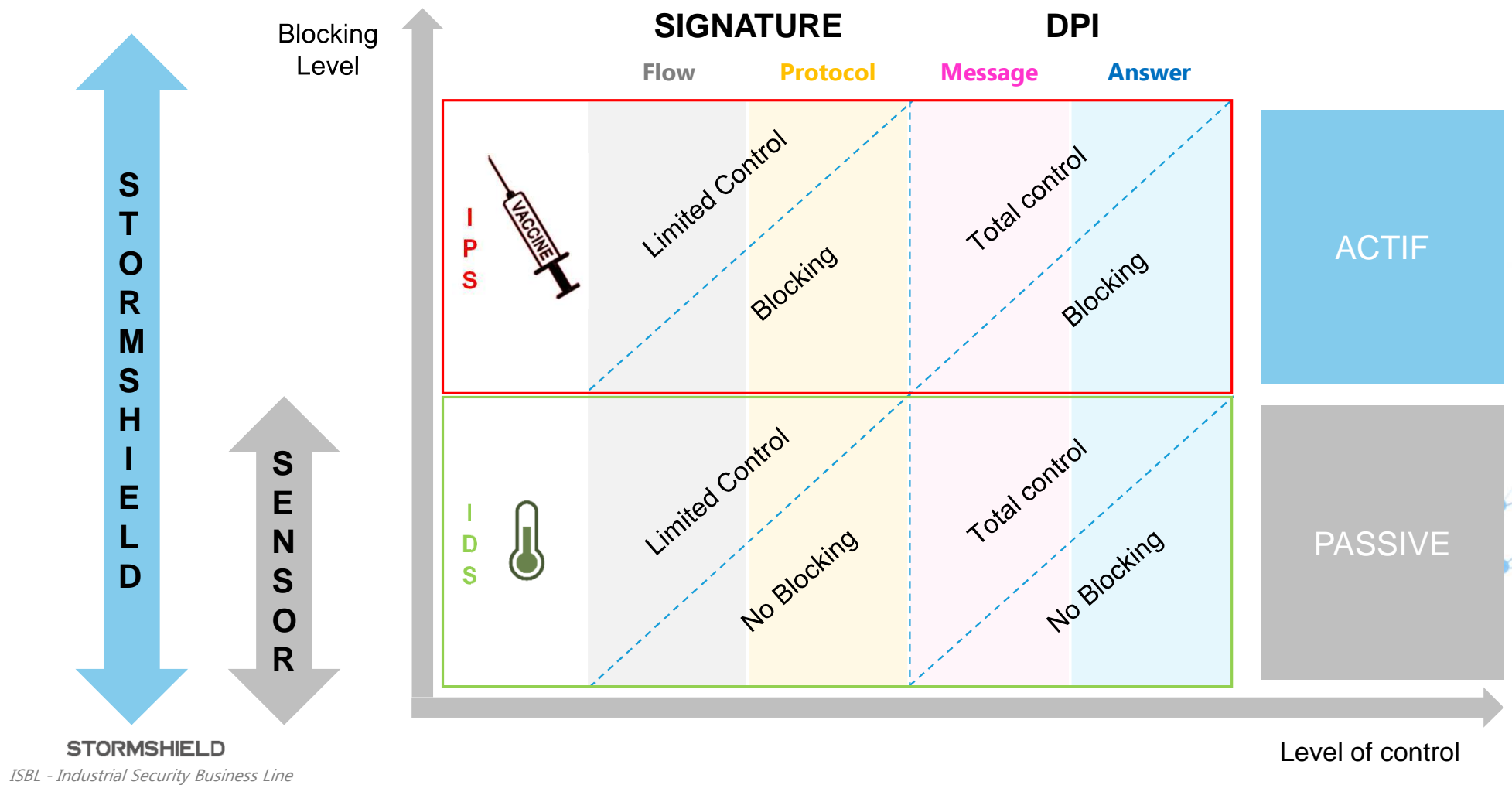
ISBL - Industrial Security Business Line

A high-angle, blue-tinted photograph of two men in business attire sitting at a table. The man on the left is looking up at the camera with a smile, while the man on the right is looking down at a document. On the table are two computer keyboards, a pen, and a document with a bar chart. The text 'Our detection capabilities' is overlaid in the center.

# Our detection capabilities

STORMSHIELD

# Firewall (IPS) vs. Sensor (IDS)

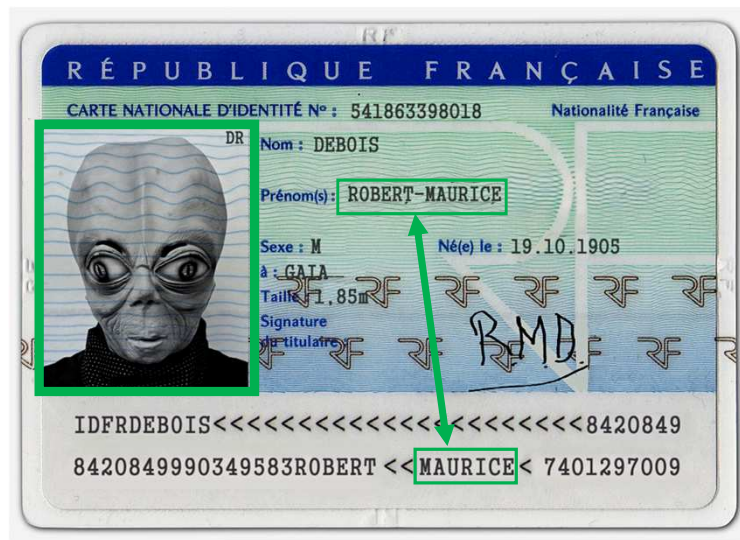


A high-angle photograph of two men in business attire sitting at a desk, looking at documents. The image is overlaid with a semi-transparent blue filter. The man on the left is smiling at the camera, while the man on the right is looking down at the papers. A computer keyboard is visible in the bottom left corner.

# **What is signature analysis?**

## **Analogy with the identity card**

# Analogy with the identity card



**Compliant**



**Non-compliant**

# What is a signature in the flow

- Example of a flow

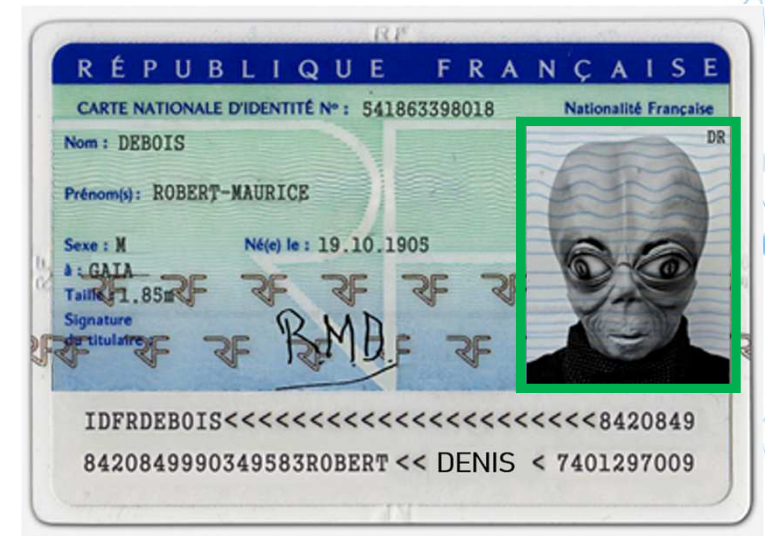
Header		Command	Parameters		
1 1 0 0	0 0 1 1	1 1 0 1	1 1 1 0	1 1 1 0	1 0 0 0

- Signature: **111101**      We are looking for a value no matter where it is located

Header		Command	Parameters		
1 1 0 0	0 0 <b>1 1</b>	<b>1 1 0 1</b>	1 1 1 0	1 1 1 0	1 0 0 0

Header		Command	Parameters		
1 1 0 0	0 0 1 1	1 1 0 <b>1</b>	<b>1 1 1 0</b>	<b>1</b> 1 1 0	1 0 0 0

Risk of **false positive** by detecting the signature in the wrong place



- The photo is on the identity card



# What is a signature in the protocol

- Example of flow for the COMET protocol

Header		Command	Parameters		
1 1 0 0	0 0 1 1	1 1 0 1	1 1 1 0	1 1 1 0	1 0 0 0

- Signature:

- Header :       xxxxxxx**11**     We look for the value 11 in the header
- Command :    **1101**       We look for the value 1101 in the command

Header		Command	Parameters		
1 1 0 0	0 0 <b>1 1</b>	<b>1 1 0 1</b>	1 1 1 0	1 1 1 0	1 0 0 0



- The photo is on the identity card.
  - But on the right



# **What is protocol analysis (DPI) ?**

## **Analogy with the identity document**



# RFC analysis (DPI) **per message**

- Example of flow for the COMET protocol

Header		Command	Parameters		
1 1 0 0	0 0 1 1	1 1 0 1	1 1 1 0	1 1 1 0	1 0 0 0

- The RFC of the COMET protocol tells us:
  - If command **1101** then the **length** of the **parameter field** is **12 bits**
- Configuration:
  - command: **1101**

Header		Command	Parameters		
1 1 0 0	0 0 1 1	<b>1 1 0 1</b>	1 1 1 0	1 1 1 0	1 0 0 0

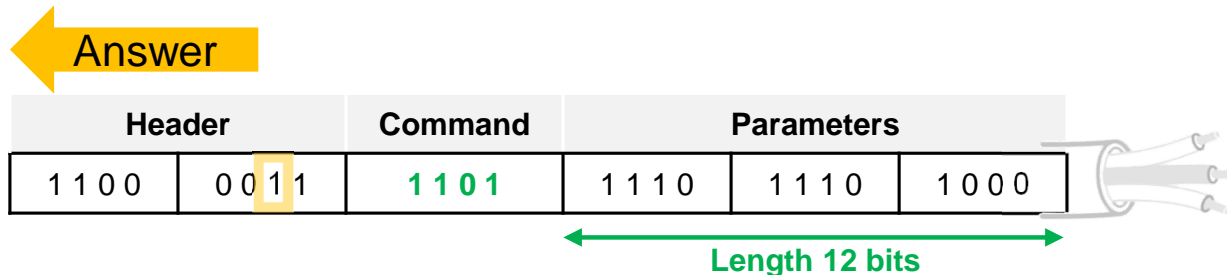
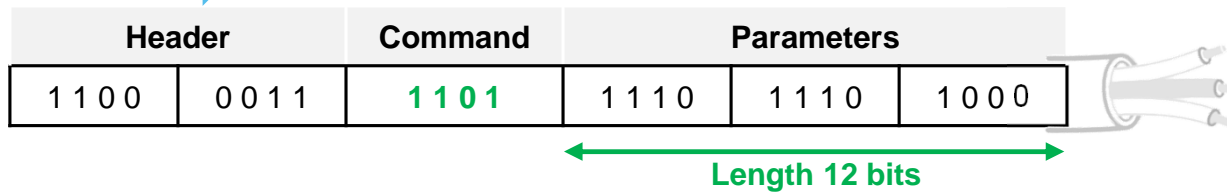
← length 12 bits →



- The photo is on the identity card
  - But on the right
- The first name is different on the MRZ band

## RFC analysis (DPI) **by Exchange [Stateful]**

- The RFC of the COMET protocol tells us
  - If **command 1101** then the length of the **parameter field is 12 bits**



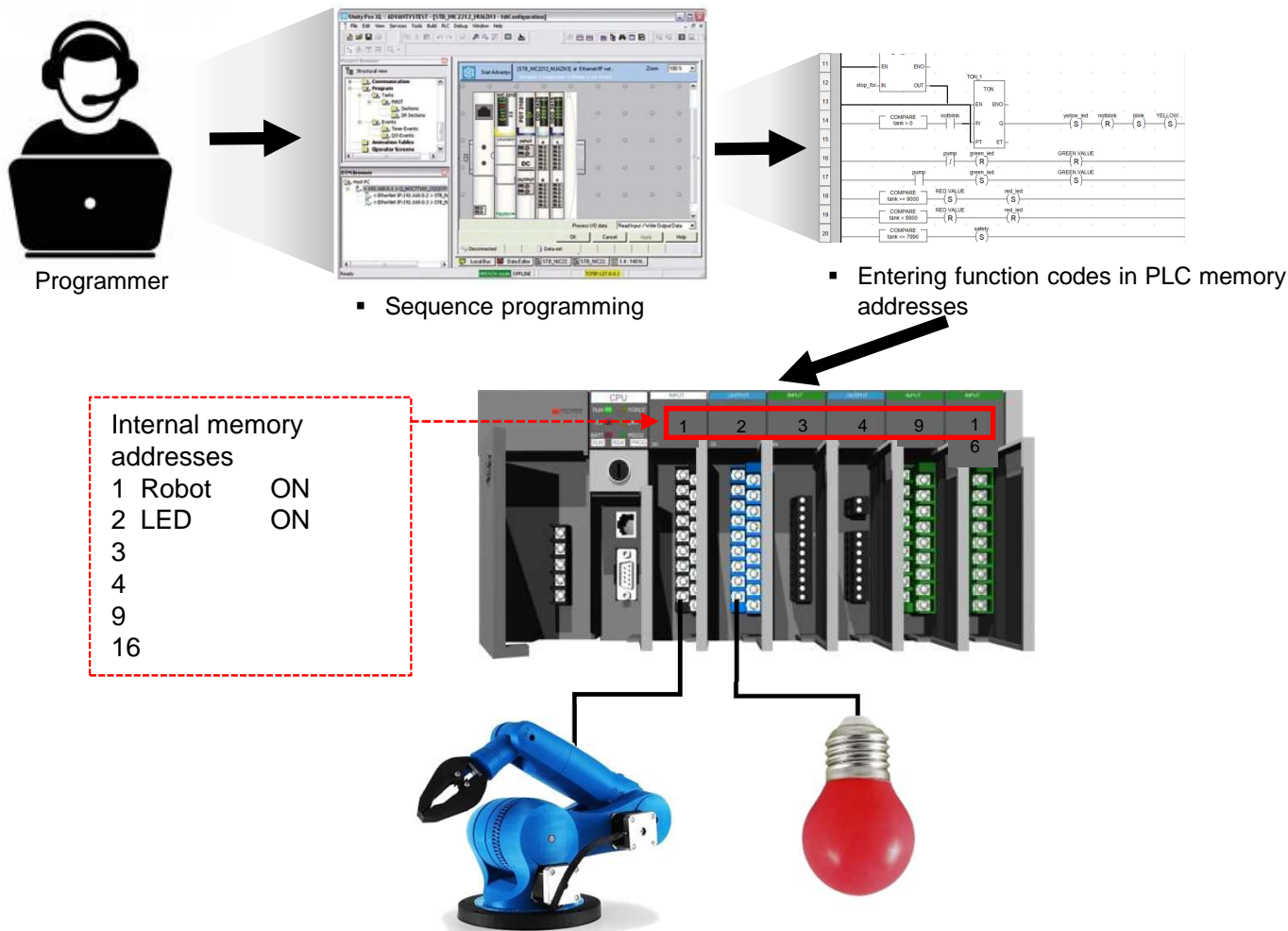
- The photo is on the identity card
  - But on the right
- The first name is different on the MRZ band
  - And on the VISA



# Securing communication in industrial environments

STORMSHIELD

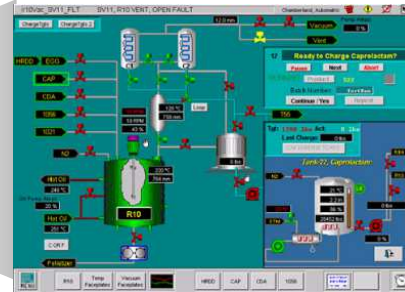
# Deep protection



# Deep protection



Operator



▪ IHM cockpit production line



Modbus, S7, OPC DA, ...

Gestion des codes de fonction Modbus

OPÉRATIONS PUBLIQUES

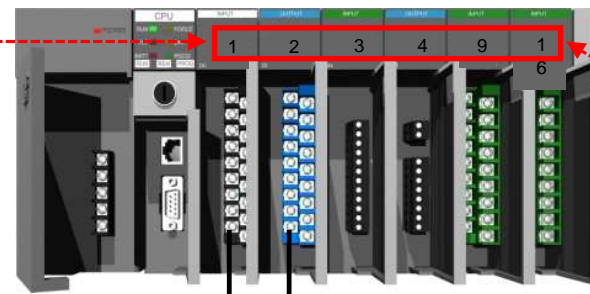
Modifier les opérations d'écriture | Modifier toutes les opérations

Code	Fonction	Action	Type
1	Lecture de N bits de sortie	Bloquer	Lecture
2	Lecture de N bits d'entrée	Bloquer	Lecture
3	Lecture de N mots de sortie	Analyser	Lecture
4	Lecture de N mots d'entrée	Bloquer	Lecture
5	Écriture d'un bit de sortie	Bloquer	Écriture
6	Écriture d'un mot de sortie	Analyser	Écriture
15	Écriture de N bits de sortie	Bloquer	Écriture

▪ Read and Write authorization

Internal memory addresses

- 1 Robot ON
- 2 LED ON
- 3
- 4
- 9
- 16



Gestion des Adresses Modbus

Recherche d'adresse ...

Adresse	Codes de fonction autorisés
9	6
16	6
1-16	3

- Authorization to **write** values to PLC memory zones 9 and 16
- Authorization to **read** values to PLC memory zones 1 to 16

STORMSHIELD

ISBL - Industrial Security Business Line

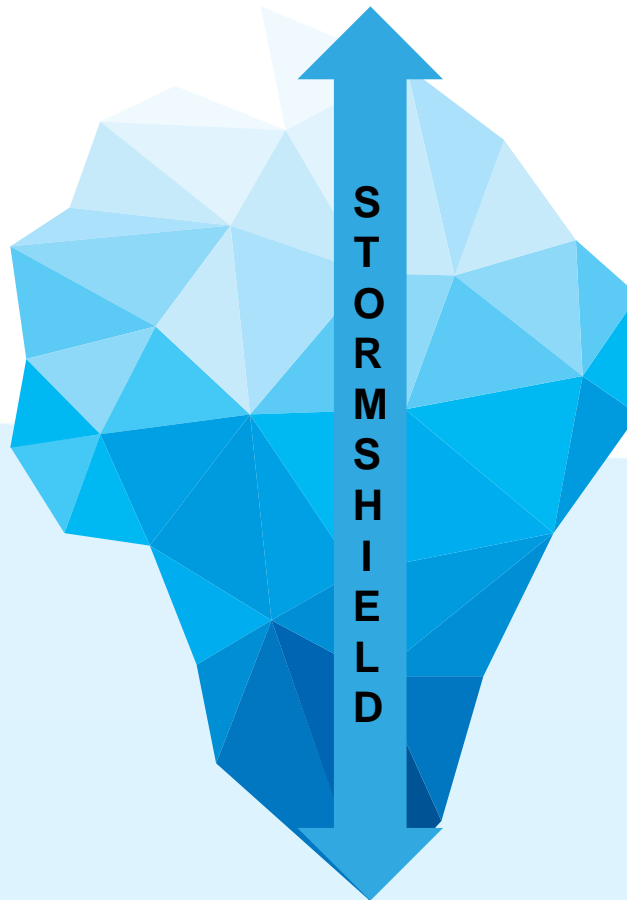
# SNS – Focus on IPS and personalized signature

## 20+ Standardised protocols

Modbus, OPC Classic, EtherNet/IP,  
CIP, BACnet/IP, IEC 60780-5-104, OPC  
UA, ICCP, IEC 61850, MQTT

## 700+ Owner Protocols

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



## DPI on 10+ Supported protocols natively on our FW

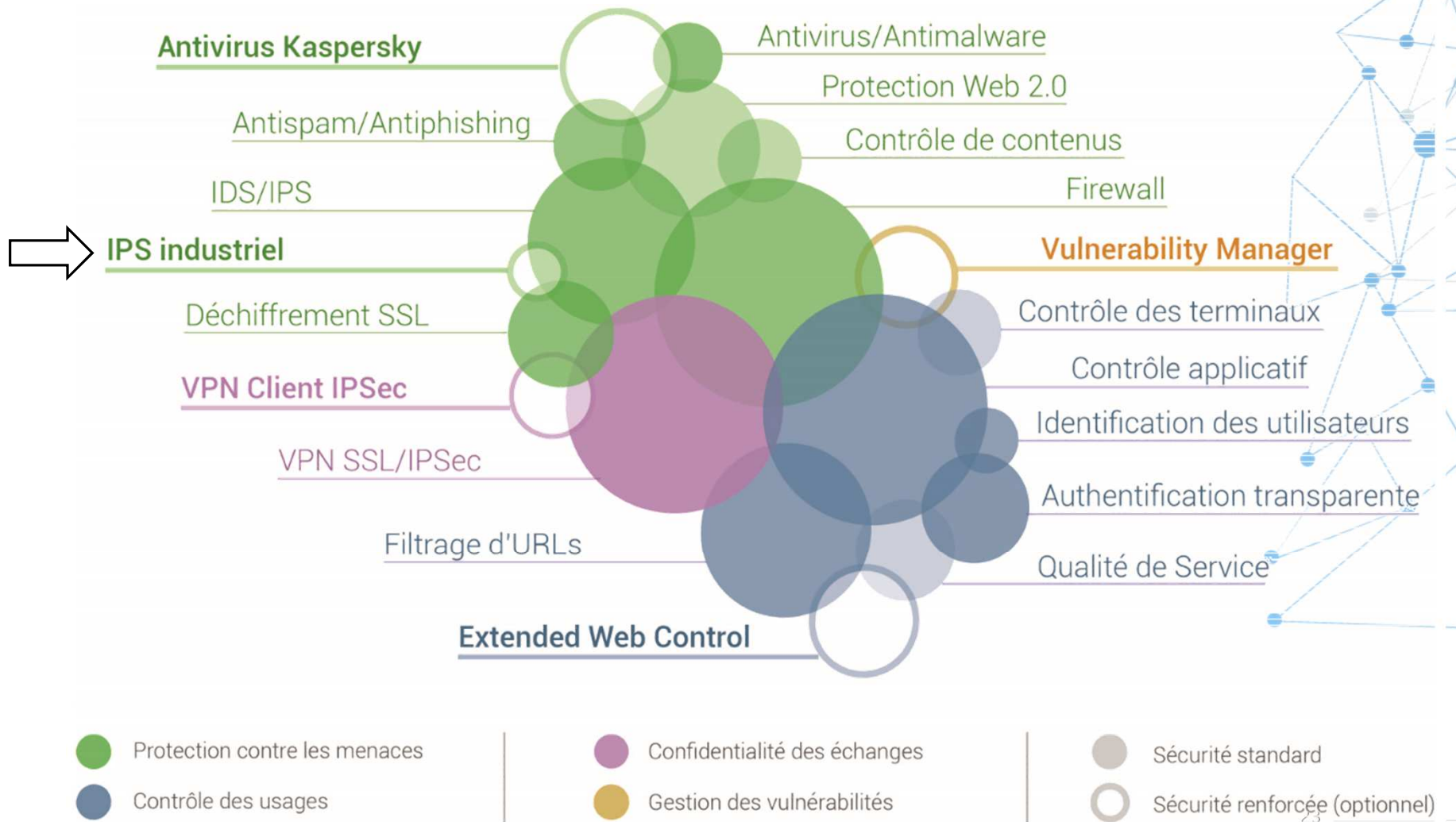
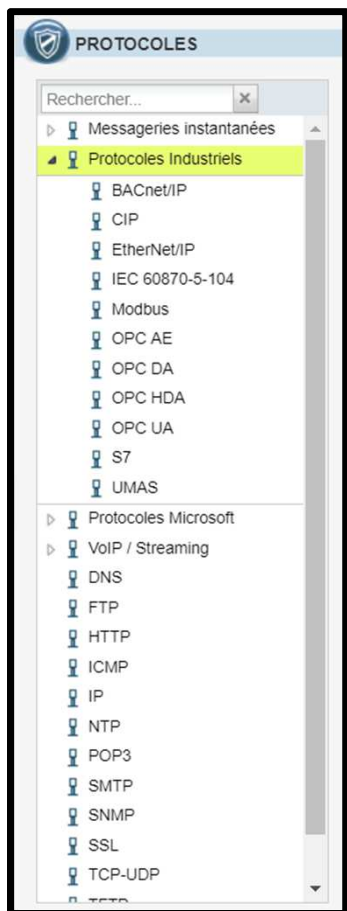
- |                                |                   |
|--------------------------------|-------------------|
| ✓ MODBUS                       | ✓ IEC 60780-5-104 |
| ✓ OPC Classique<br>(DA/HDA/AE) | ✓ OPC UA          |
| ✓ EtherNet/IP                  | ✓ UMAS            |
| ✓ CIP                          | ✓ S7              |
| ✓ BACnet/IP                    | ✓ DNP3            |

**STORMSHIELD**

ISBL - Industrial Security Business Line



# SNS – Features available throughout the range



**STORMSHIELD**

ISBL - Industrial Security Business Line

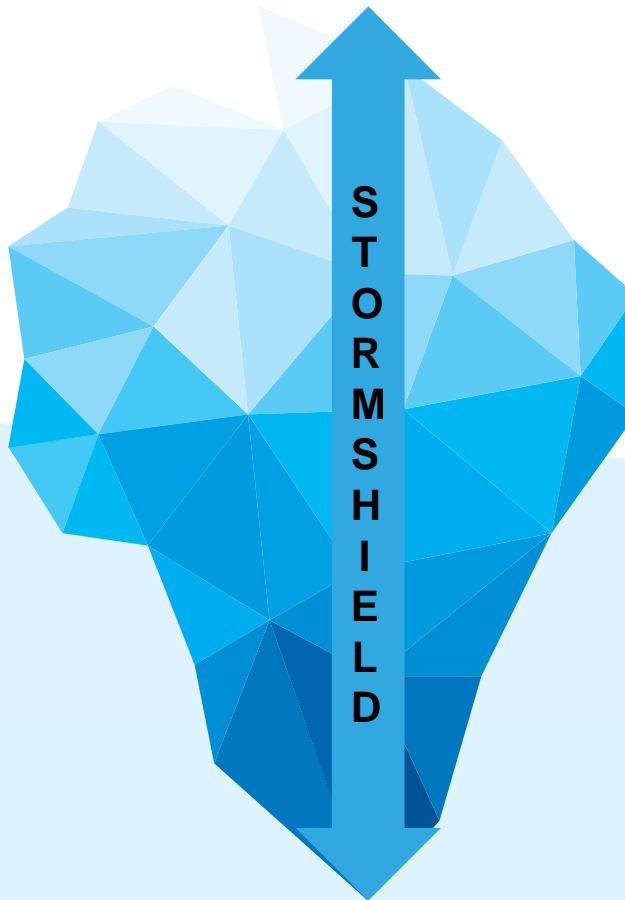
# SNS – Focus on IPS and personalized signature

## 20+ Standardised protocols

Modbus, OPC Classic, EtherNet/IP,  
CIP, BACnet/IP, IEC 60780-5-104, OPC  
UA, ICCP, IEC 61850, MQTT

## 700+ Owner Protocols

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



## DPI on 10+ Supported protocols natively on our FW

- |                                |                   |
|--------------------------------|-------------------|
| ✓ MODBUS                       | ✓ IEC 60780-5-104 |
| ✓ OPC Classique<br>(DA/HDA/AE) | ✓ OPC UA          |
| ✓ EtherNet/IP                  | ✓ UMAS            |
| ✓ CIP                          | ✓ S7              |
| ✓ BACnet/IP                    | ✓ DNP3            |

## Custom Pattern

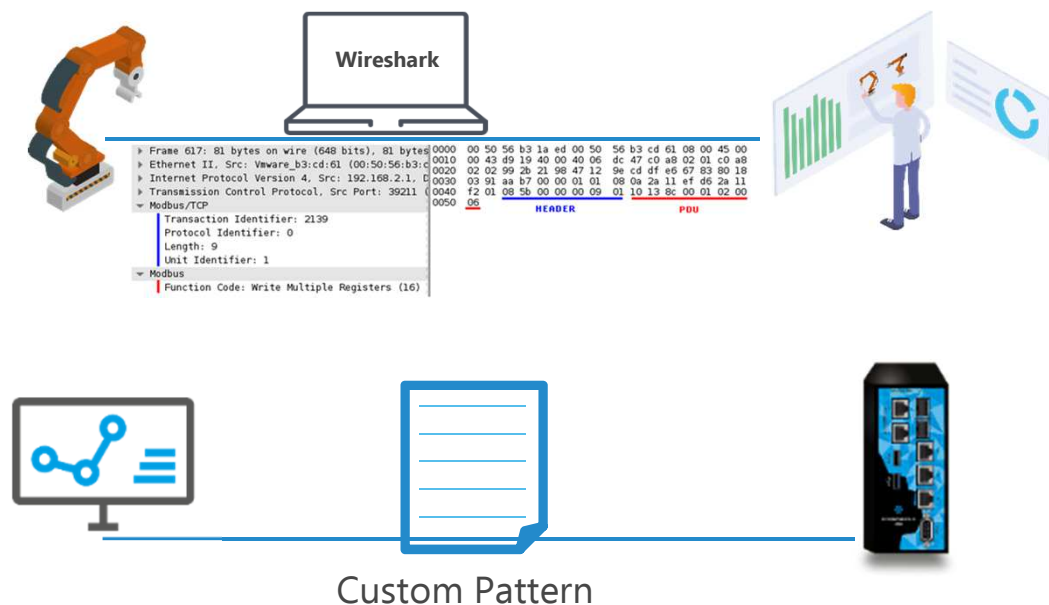
- ✓ To be adapted to the business context
- ✓ Comply with the protocol RFC
- ✓ Avoid handling errors

**STORMSHIELD**

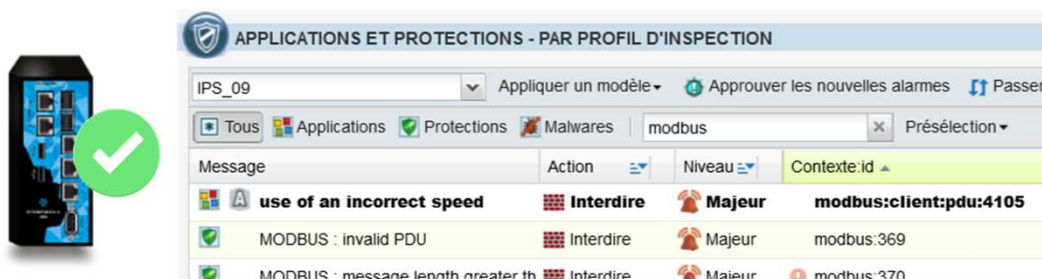
ISBL - Industrial Security Business Line



# SNS – Custom Pattern



Custom Pattern



**STORMSHIELD**

ISBL - Industrial Security Business Line

- ✓ Take a trace of the communication
- ✓ Custom pattern scripting and simplified implementation of the file on the FW

## Format du fichier :

[modbus:client:pdu.global]

Revision=1

[modbus:client:pdu.4097]

type=asq

severity=2

classification=1

action\_fw=pass,pass,pass,pass

level\_fw=major,major,major,major

description="Pump speed values out of range (greater or equal than 6)"

ldescr=""

1="^\x10\x13\x8c\x00\x01\x02\x00[\x06-\xff]"

on débute la description à partir du PDU

fromasqversion=1.0.0

Uptoasqversion=8.0.0

- ✓ FW adapted to the business context
- ✓ Able to protect the OT environment with a protocol that no longer complies with the RFC

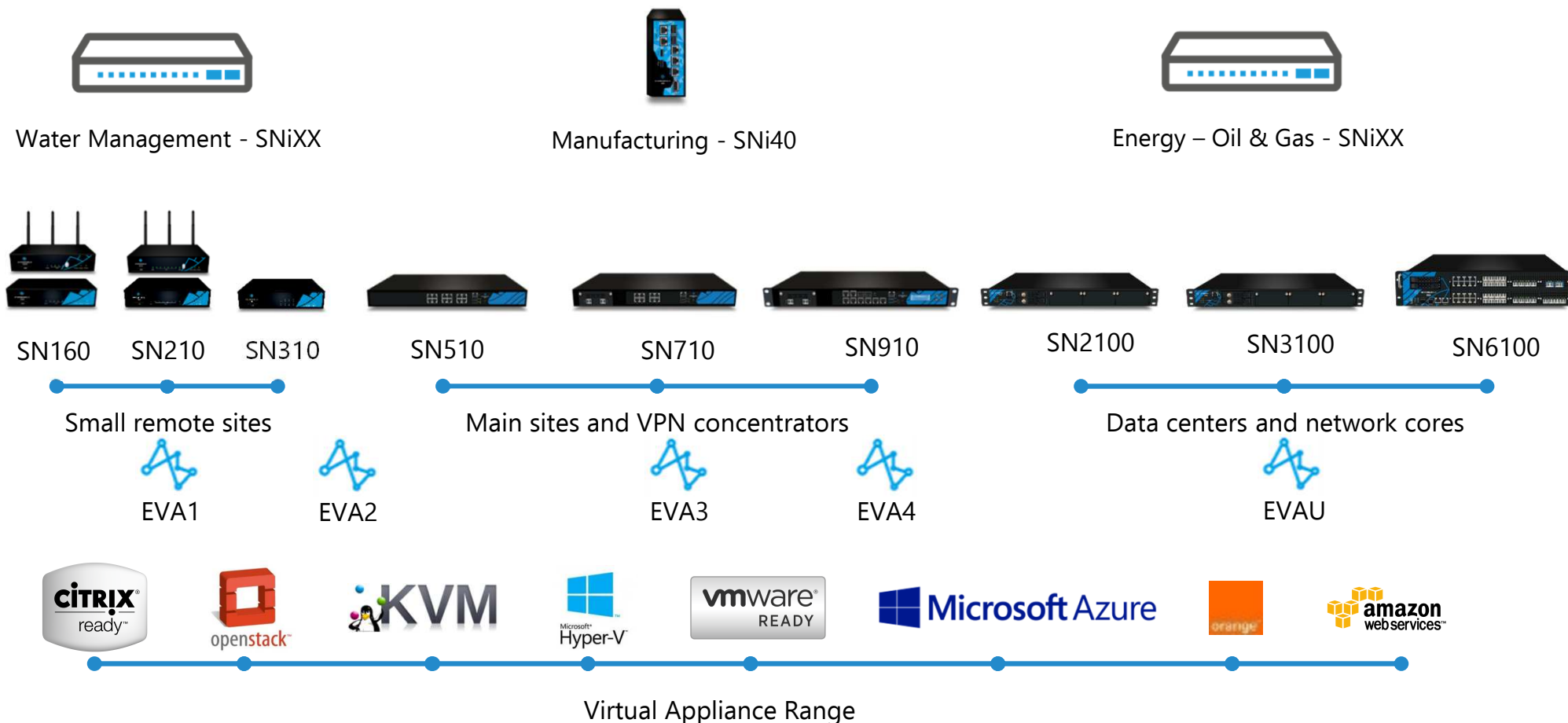


**Stormshield Network Security**

**Industrial network protection  
IT & OT**

STORMSHIELD

# SNS - End-to-end protection - convergence IT & OT



STORMSHIELD

CENTRALIZED ADMINISTRATION – SMC

# SNi40 : Industrial Firewall

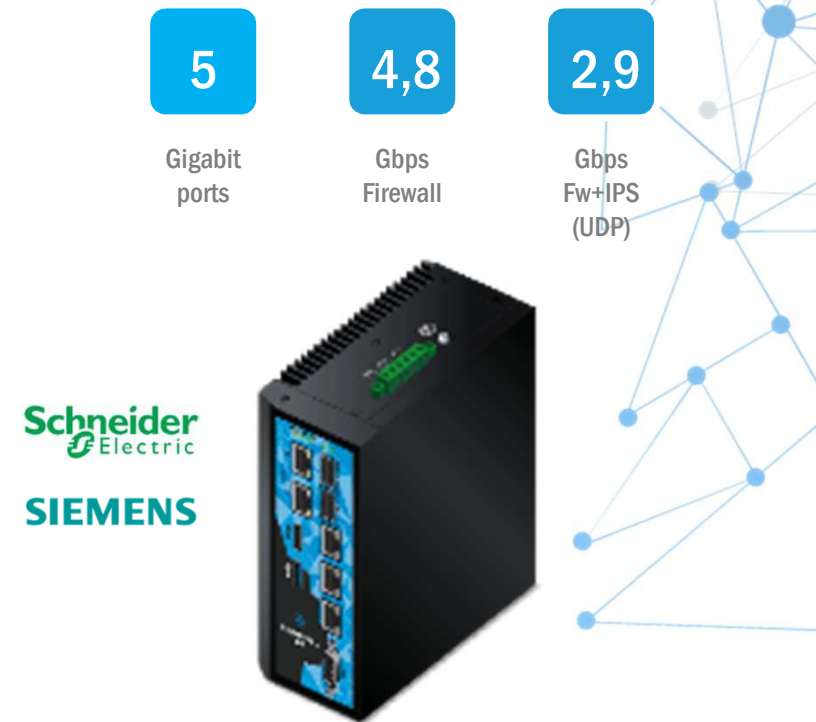
## SNi40

- Developed as part of the NG-IUTM project, Stormshield/Schneider Electric partnership sponsored by ANSSI
- Tested and validated by Schneider Electric and Siemens France
- Hardened equipment (IP30, -40 + 75°C)
- Redundant power supply : 24V (12-36V)
- **DPI on Industrial Protocols** : Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, IEC 60870-5-104, OPC (DA/HDA/AE), BACnet/IP
- **Safety mode** (By-Pass)
- **Certified** CSPN Industrial FW  
**Qualified** at the **STANDARD** level

### STORMSHIELD

ISBL - Industrial Security Business Line

FOR THE SECURISATION OF THE OT  
ENVIRONMENT WITH STRINGENT CONSTRAINTS

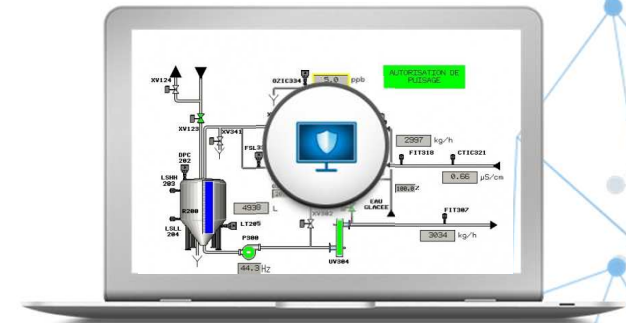
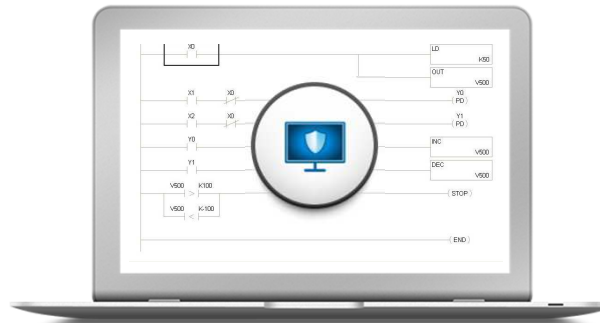


A high-angle, top-down photograph of two men in an office. The man on the left is leaning over a desk, smiling at the camera. The man on the right is also leaning over the desk, looking down at a document. The desk has a keyboard, a pen, and a document with a bar chart. The entire image is overlaid with a semi-transparent blue filter.

# Stormshield Endpoint Security

STORMSHIELD



# SES – The protector of industrial PCs



## STORMSHIELD

# SES – Points to remember

**Extend the security of your obsolete equipment,** that are no longer supported by Microsoft

End of life	SES : Extended support
April 2014	2021 
July 2015	2021 

**Signatureless protects against unknown threats,** oriented towards behavioural analysis without any connection to the Internet..

**Device control,** USB access management by authorizing or blocking ports and removable storage devices

**Postes de travail**  
Stormshield Endpoint Security



**Contextual policy,** Protection of the industrial workstation with a security policy that dynamically adapts to the context



**Low resource footprint,** on the protected system



**Qualification,** Common Criteria EAL3+ et FIPS 140-2



**Interoperability of business applications,** validated by 

**STORMSHIELD**

ISBL - Industrial Security Business Line



A high-angle photograph of two men in business attire sitting at a table, looking at documents. The man on the left is smiling at the camera. The man on the right is looking down at the documents. The entire image is covered with a semi-transparent blue filter. The word "Results" is centered in white text.

# Results

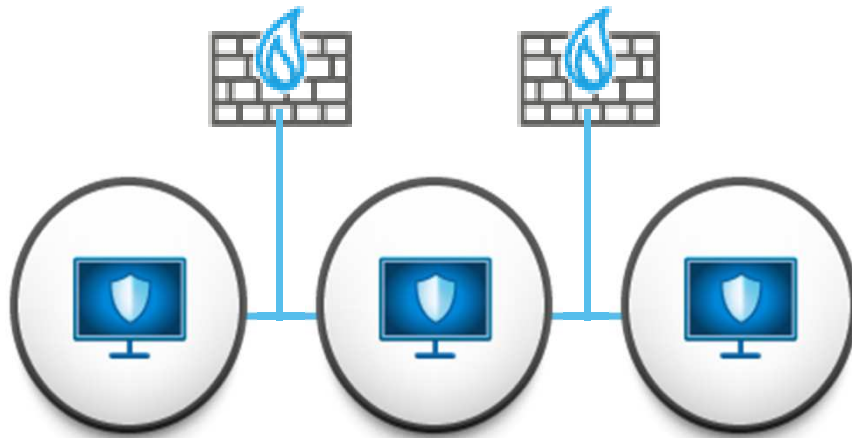
STORMSHIELD



# Stormshield at the Guiana Space Center



End to End protection deployed or being deployed for multiple projects



**STORMSHIELD**

*ISBL - Industrial Security Business Line*

# Thank you

We look forward to seeing you again



**STORMSHIELD**



## Get in Touch



22, rue du Gouverneur Général Éboué  
92130 Issy-les-Moulineaux FRANCE



+33 (0) 9 69 32 96 29



[Industrial.security.business.line@stormshield.eu](mailto:Industrial.security.business.line@stormshield.eu)

# Common Criteria & ANSSI: Certification vs Qualification

