STORMSHIELD

Network Endpoint Data

Agenda & contacts

Vincent Nicaise

Industrial Partnership and Ecosystem Manager

Vincent.nicaise@stormshield.eu
+33 6 37 68 22 58

Olivier Puchadez

Sales Manager Strategic Markets

olivier.puchadez.stormshield.eu
+33 6 47 09 02 83

Industrial cybersecurity awareness

Automation in our everyday lives

Challenges

Baku-Tbilisi-Ceyhan pipeline Turkey. Pipeline and pumping station destroyed (1 billion in lost equipment and revenue)

Water treatment plant, Maroochy Australia. 800 m^3 of waste water discharged into rivers and weirs

Material damage / personal injury

Loss of revenue

Environmental impact

Data theft

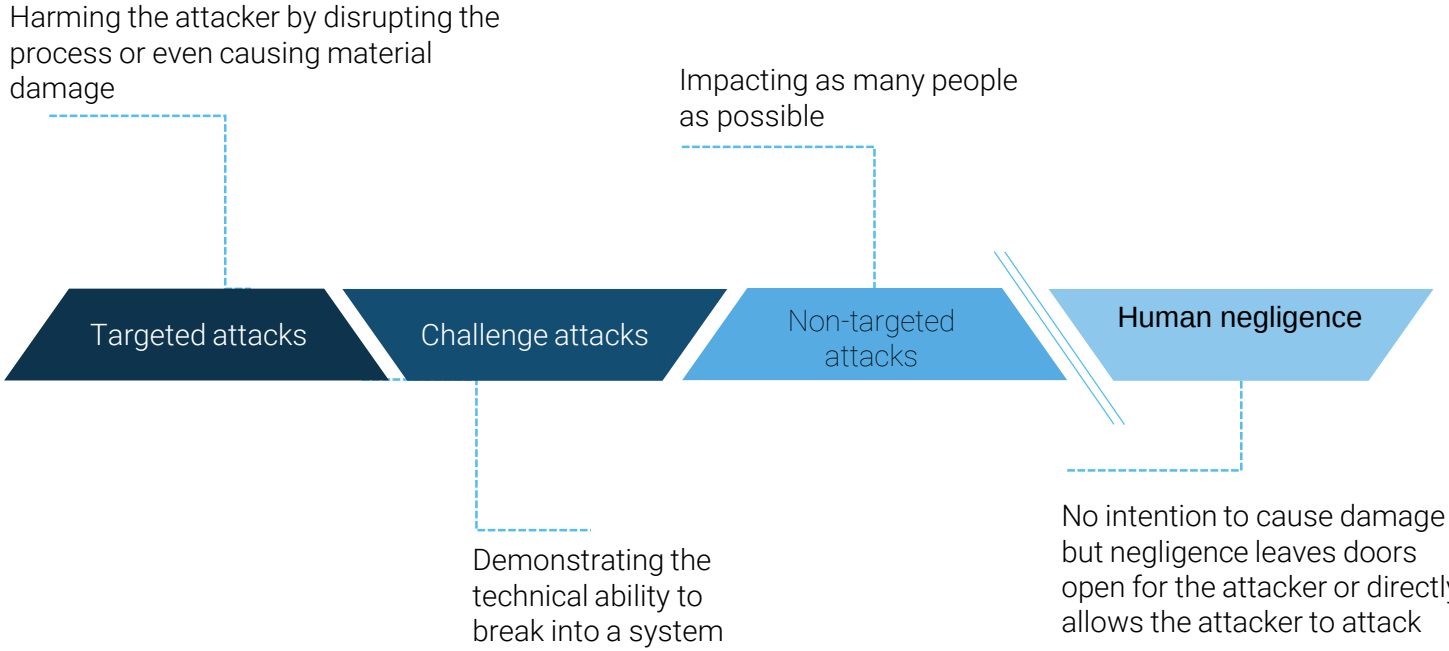
Public liability - Publicity

NotPetya: Several of Merck's factories paralysed. €135 million in losses.

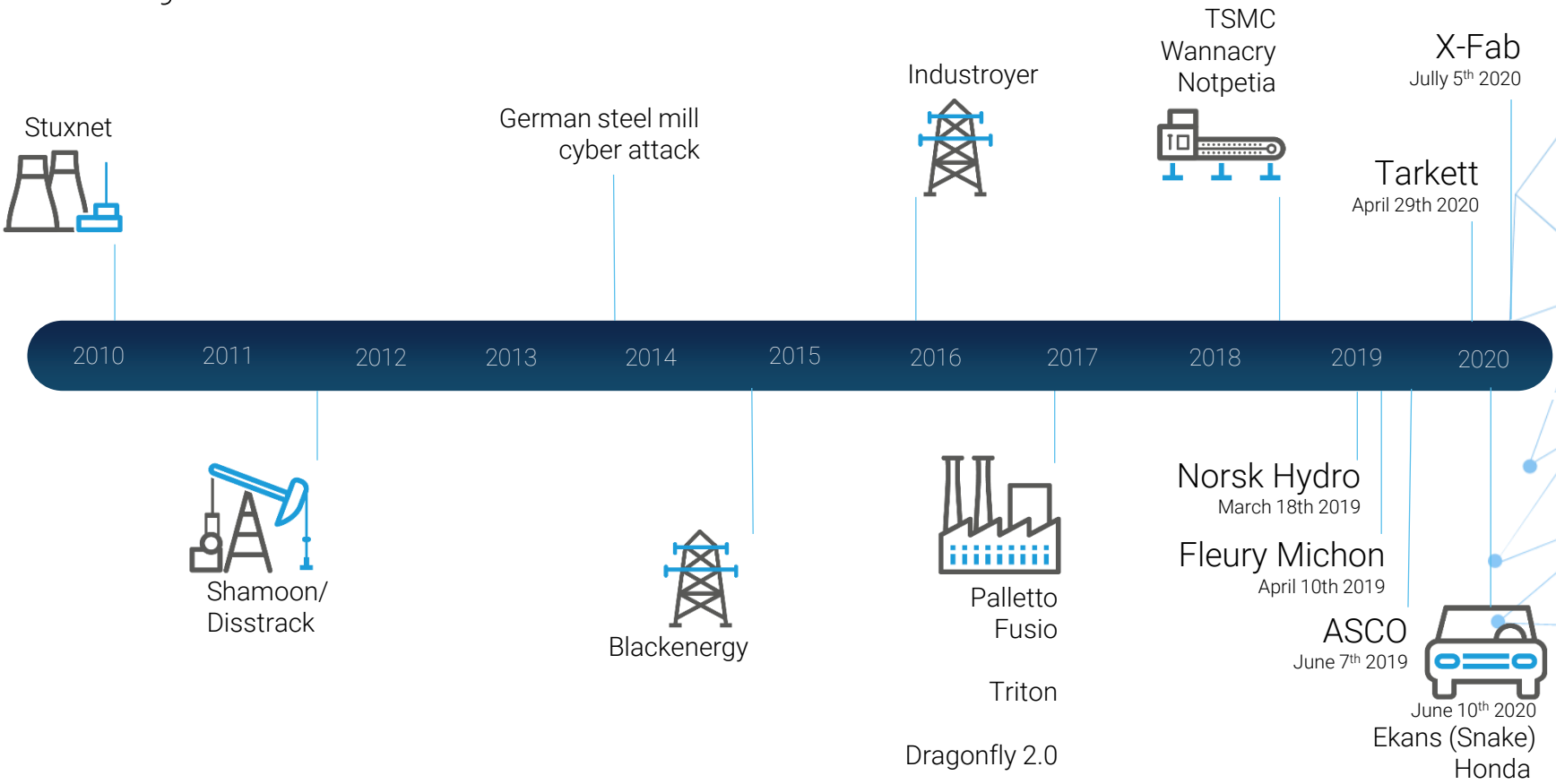
Wannacry: Renault. Several factories at a standstill including Sandouville - 3,400 employees
3 days of stoppage

Blackenergy - Ukraine, 30 substations paralysed, 230,000 people without electricity for 1 to 6 hours

Types of attack



Major OT attacks



OT environment

Differences between IT and OT

IT	Differences	OT
processing data	Systems objectives	managing installations (physical, material), regulating processes, obtaining and processing data
business constraints and confidentiality constraints	Functional aspects	business constraints and "real time" constraints, operational security (OS) constraints, 24/7 availability
Air-conditioned server rooms, office, home	Physical environment	production workshops: dust, temperature, vibrations, electromagnetism, nearby harmful products, outdoor environment, etc.
mostly in closed premises (office, home in the case of remote working)	Location	warehouses, factories, public roads, countryside (pumping stations, electricity substations, etc.), remote locations, offshore, etc.
about 5 years	Service life	10 to 40 years
Systems seasoned to cyber attacks	System	Real-time systems, built to endure operating conditions

Differences between IT and OT

People

IT: CISO, ISSD

OT: Factory manager, Production manager, software maintainer, etc.

Knowledge and skills

IT: manages the software and hardware components of the information system

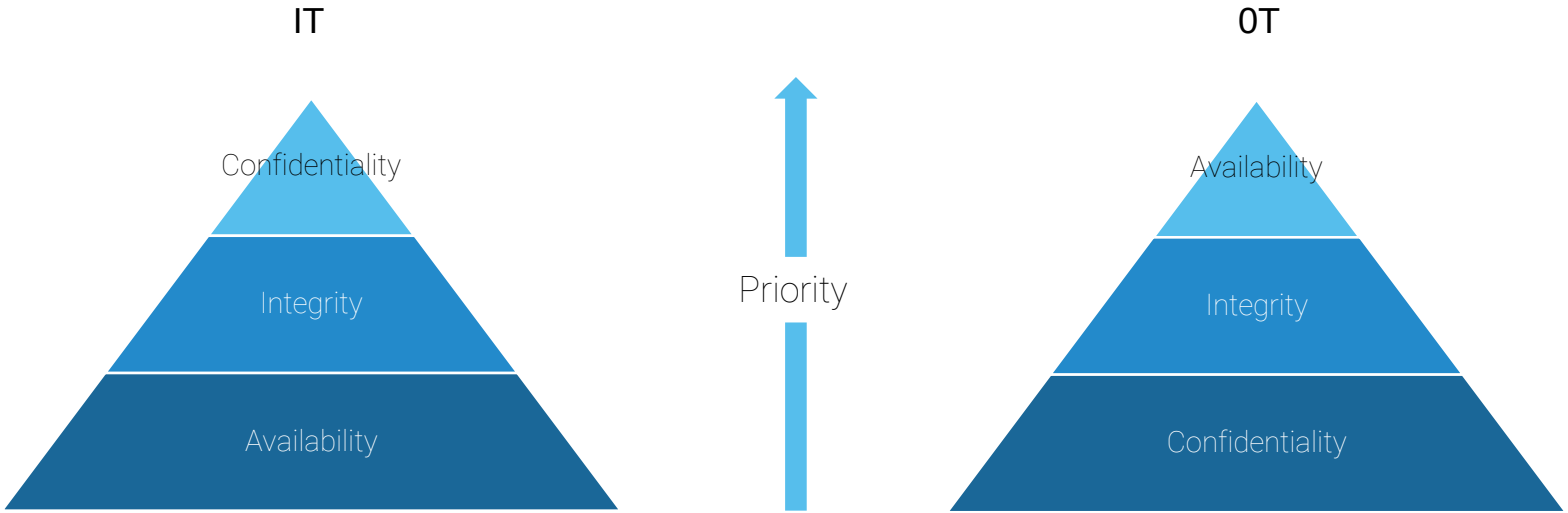
OT: organises, plans and monitors production targets

Need for convergence

IT: Better understanding of the environments and constraints of ICS

OT: Awareness of cyber issues and adaptation of your operations management

Cybersecurity objectives



Technical characteristics

Installations with a long service life

Profitability over several decades
Component obsolescence
Difficulties in sustaining maintenance

Vulnerable components

Few or no integrated cybersecurity mechanisms
Patch management complicated to implement

Continuous production

Material and economic considerations
24/7 availability
Reduced maintenance window

Diversity and technological stacking

Diverse requirements / manufacturers' specifications
Different integrators and batch management
Upgrading and extensions enabling product stacking (different generations and technologies)

Technical characteristics

Environmental constraints

Dust, humidity, heat, electromagnetic radiation, etc.

Real-time systems

Control of the PLC cycle time
Control of response times

Use of industrial protocols

Standard or specific
Few or no security mechanisms

Communication flow

Difficulty in controlling the flow matrices and the visibility of exchanges

Organisational characteristics

Demanding regulatory environment

Basic standards
Specification standards
Test method and analysis standards
Organisation standards

Sustainability of obsolete systems

Lower cost maintenance of Operational Conditions
Vulnerability management: installations in production and spare parts

Objectives and number of people involved

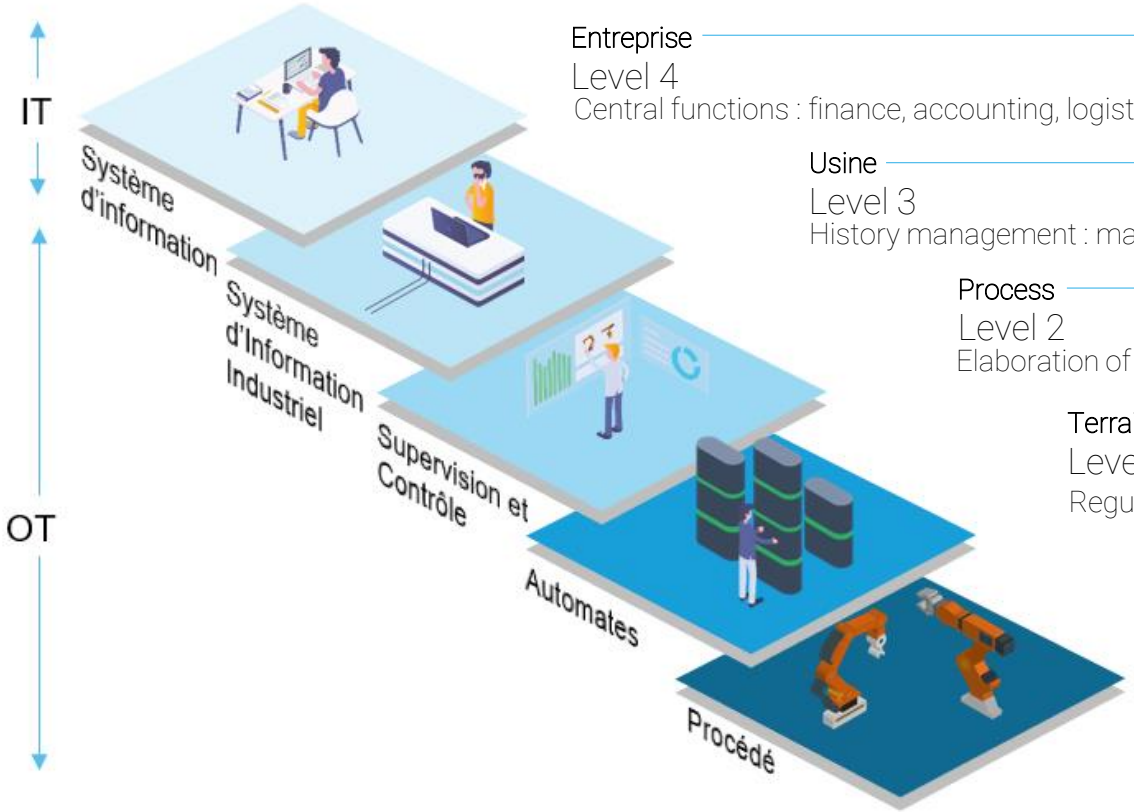
Round the clock shift teams
Operator, supplier, installer, integrator
Operator, software maintainer, etc.

Cost optimisation through outsourcing

Loss of control of the installation
Little or no awareness of cybersecurity in extension plans, upgrading, etc.

ICS components

ICS Architecture



Entreprise
Level 4
Central functions : finance, accounting, logistics

Usine
Level 3
History management : management of industrial processes

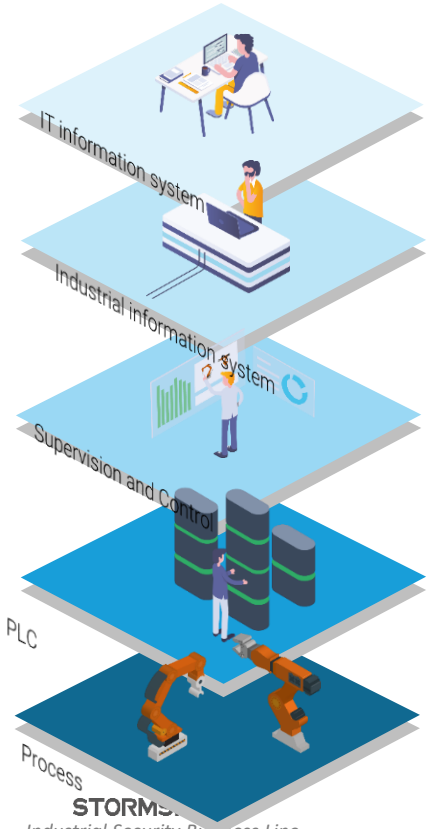
Process
Level 2
Elaboration of orders

Terrain
Level 1
Regulation and automatism

Level 0
Sensors and actuators

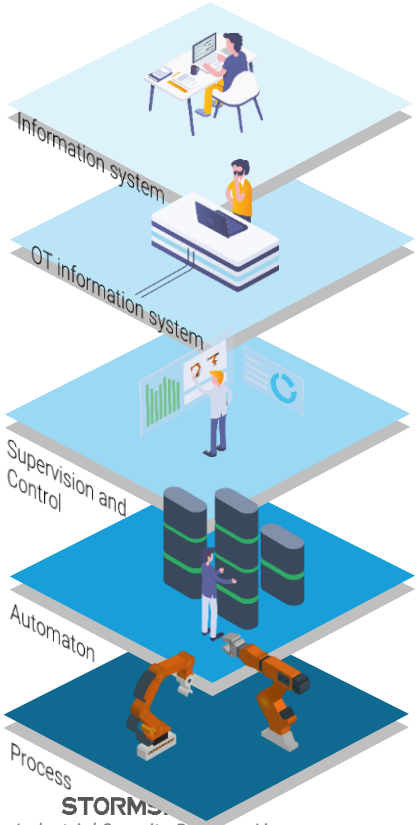
CIM Pyramid (Computer-integrated Manufacturing) – created in the 80's by the NIST
Organized in organisation levels

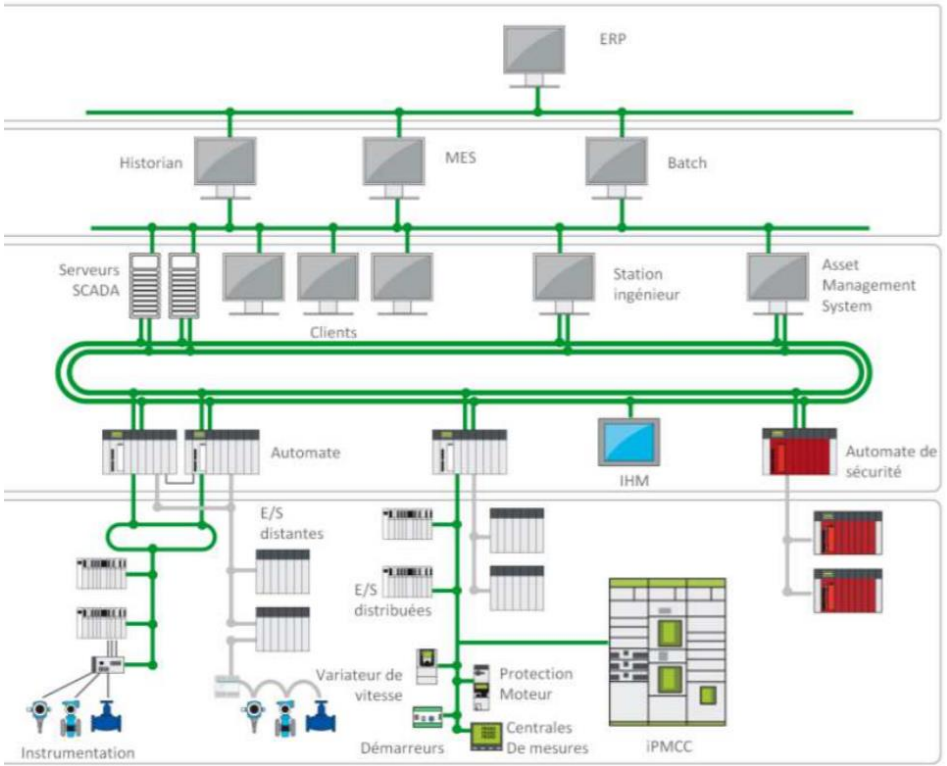
ICS Architecture



Functions	Type of datas	Type of application
Overall production planning	Files Databases (minutes, heures)	ERP
Manage production, scheduling and production monitoring, quality control and monitoring of resources	Files, databases(minutes, hours)	MES
Consolidate and interpret information from the field so that operators can know the state of the process and intervene	Files, Databases, (seconds)	SCADA, DCS, historian, cockpit, engineering station
Collect process data and modify (automatic, semi-automatic or manual) its operation by acting on the actuators	Words (milliseconds)	PLC, DCS, IHM, cockpit
Collecting data on the process state can act on the physical components of the installation	Bits (microseconds)	Embedded systems

Architecture ICS





ICS components

SENSORS

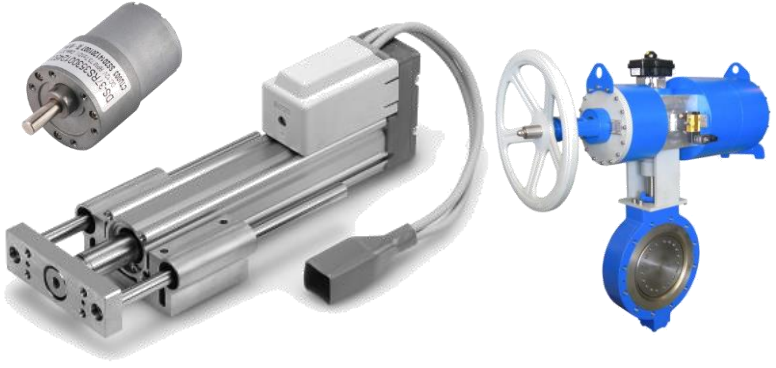
A sensor is an element of the operative part which will react to a physical phenomenon and send the signal to the control part.

Example : optical sensor, movement, contact, level…

ACTUATORS

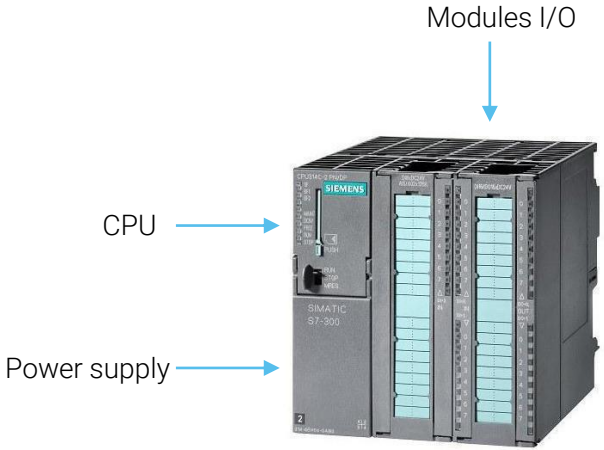
An actuator is an element of the operative part which will translate the signal sent by the control part into a physical action

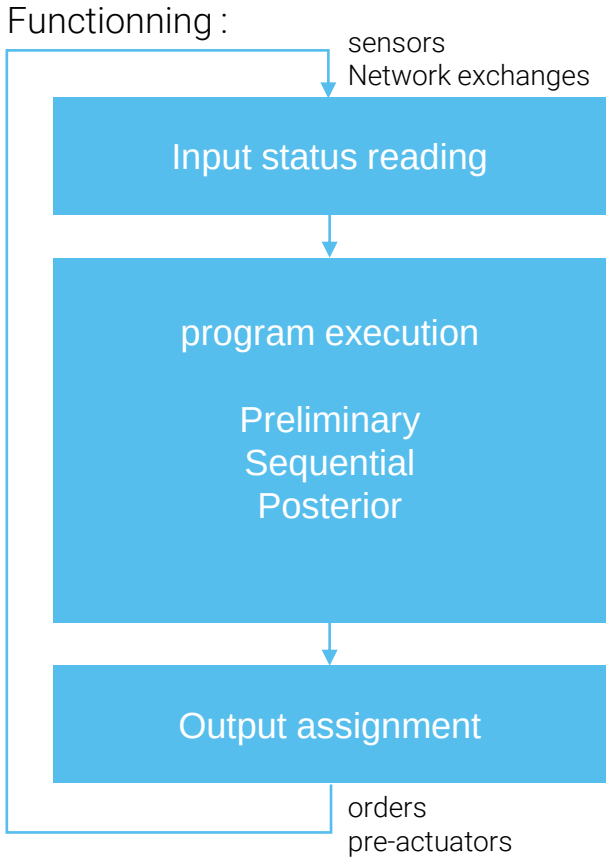
Exemple : an engine, a cylinder, a valve…



ICS components

PLC
Programmable electronic device used to control industrial processes by sequential processing.
It sends orders to the pre-actuators (operative part on the actuator side) from input data (sensors) (control part on the sensor side), instructions, and a computer program.





ICS components

Supervision

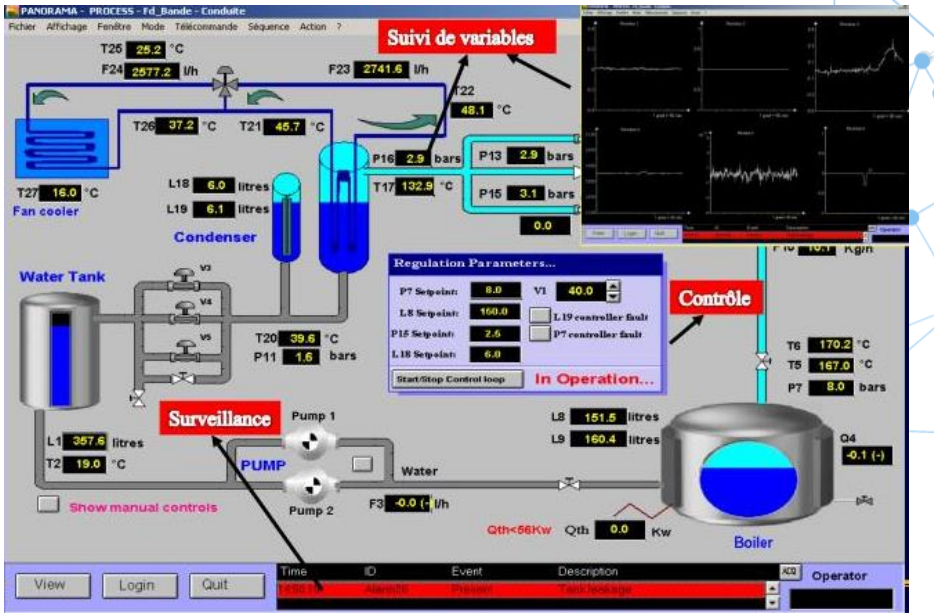
Industrial technique for monitoring and piloting computerized processes

Supervision concerns the acquisition of data (measurements, alarms, operating status feedback) and process control parameters.

It represents the process activity through an HMI.

Objectives

- Check the availability of services/functions
- Control the use of resources
- Check that they are sufficient
- Detecting and locating defaults
- Troubleshooting
- Preventing breakdowns/defects/overflows
- Predicting developments
- Monitoring of variables



ICS components

Historian

Real time industrial production data management solution. It connects to data sources (SCADA, MES…) to collect and record.

Objectives

- Check availability of services / functions
- Control the use of resources
- Check that they are sufficient
- Detect and locate defaults
- Default diagnosis
- Prevent breakdowns / faults / overflows
- Predict developments
- Variables tracking

ICS components

MES (Manufacturing Execution System)

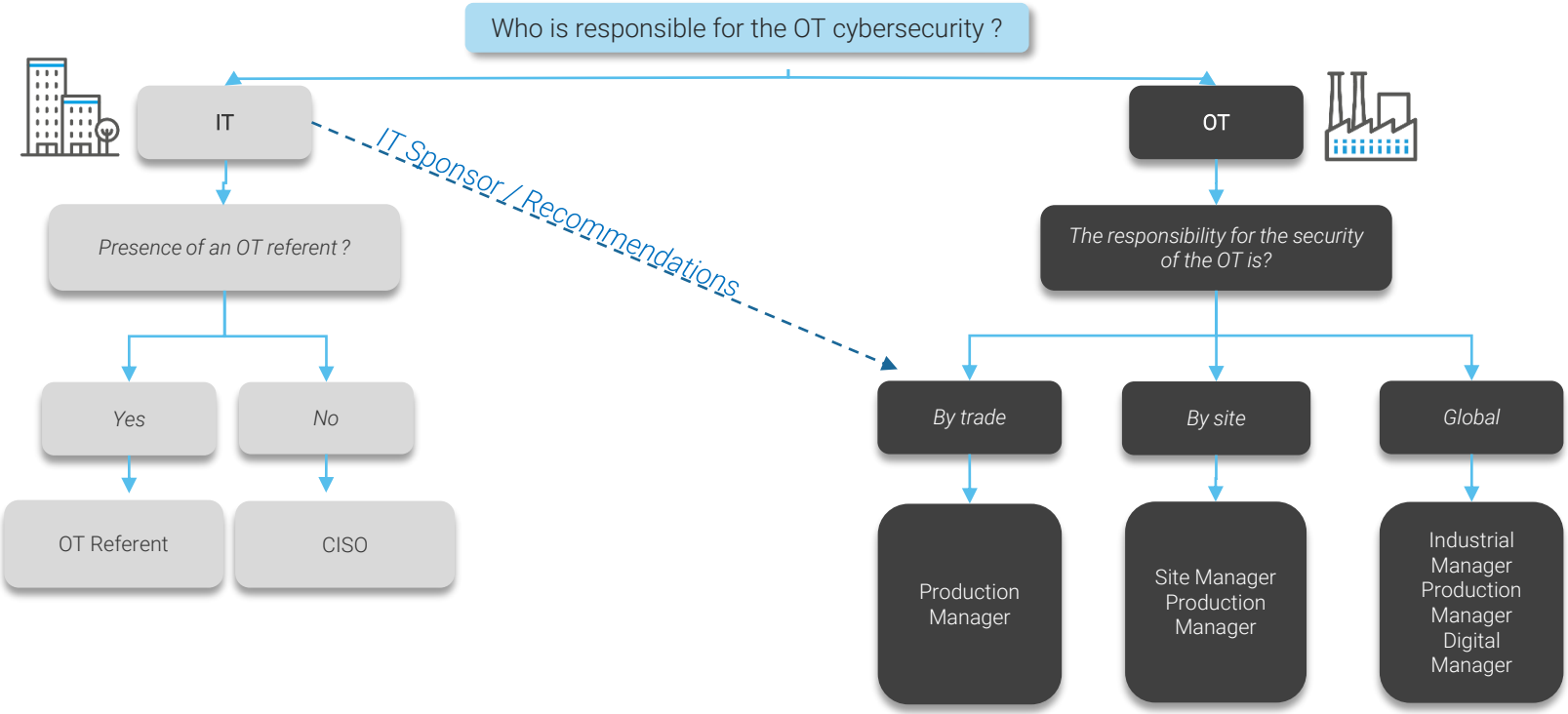
System that collects production data in real time for analysis with regard to traceability, quality control, production monitoring, scheduling and preventive and curative maintenance.

Functions :

- Data acquisition
- Scheduling
- Staff management
- Resource management
- Product and batch tracking
- Product traceability
- Quality control
- Process management
- Performance analysis
- Document management
- Maintenance management

How to manage an OT project

Identify the people



CONVICING ALSO :

- ✓ Safety officer
- ✓ Trade manager
- ✓ Site manager
- ✓ Operator

CONVICING ALSO :

- ✓ CISO
- ✓ Safety officer

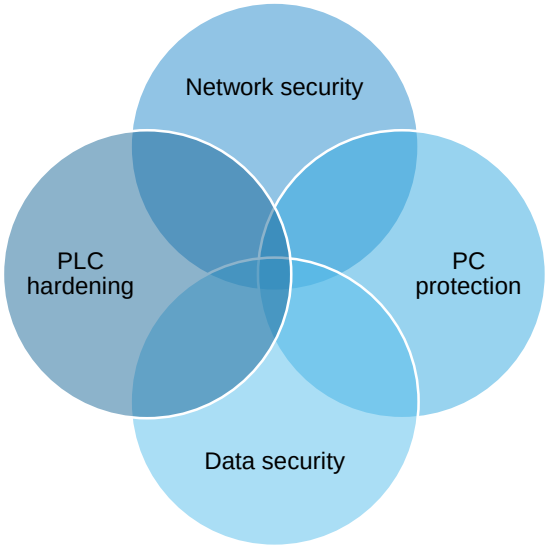
Identify needs and vulnerabilities

NETWORK SECURITY

- IT/OT segmentation
- Segmentation & filtering & NAT
- Remote maintenance/control
- Traceability of security events

NETWORK SECURITY

- Communication analysis and security close to the process



ENDPOINT SECURITY

- PC hardening
- USB key control
- Device Management
- Management of network connections

DATA SECURITY

- Data encryption of production information, PLC program…

Network security

Need / contexts	Risks	Cybersecurity solution	Stormshield advantages
IT and OT communicate with each other to optimize production, facility maintenance and service to users	OT attack coming from the IT	IT/OT segmentation / DMZ	French qualification and certification Spanish certification EAL3+ EAL4+
OT networks are often flat	Attacker movement and virus propagation facilitated	Internal OT segmentation & filtering & NAT	Transparent mode + IPS Flexible integration with hybride mode (transparent and routing segementation)
Manufacturers need to take control remotely of their distributed network Integrators maintain remotely their solution without cybersecuiryt best-practices	Access to the network from outside by employees or third party companies (e.g. integrator under maintenance contract)	Secure remote maintenance/control via VPN	VPN IPEC/SSL Industrial protocol analysis in the VPN Authentication through internal LDAP or external AD Easy VPN deployment and restoration through SMC
Detect an attack Post mortem analysis to trace the origin of an attack	Never knowing that an attack is in progress	Traceability and backup of security events	Transaction flow and security incident alarm Compatible with SIEM (Syslog/TLS, Netflow), Splunk, Logpoint, Prelude

PLC hardening

Need / contexts	Risks	Cybersecurity solution	Stormshield advantages
PLC to PLC network flows to conduct the process. PLC without integrated security Unsecured communications	An attacker modify the program or send a command not allowed and modifiy the process	Industrial protocol communication analysis close to the process to prevent an intrusion, a modification of function code, a neutralization of a PLC or system componen, an illegitimate communication	Analysis of 12 industrial protocol (covering 90% of the market) Personalised signature Minimum latence Setting up of a whitelisting of exchanges: only authorized flows are passing

PC protection

Need / contexts	Risks	Cybersecurity solution	Stormshield advantages
Due to operational constraints PCs have no security	Ransomware/malware Process takeover (for supervision or engineering PC)	PC hardening	Whitelisting of application Behavioural analysis OS protection
USB key are used for different purposes, on different PCs, sometimes for different customer	Infection by malware/ransomware Physical destruction Information theft	USB key control	Management of USB keys that are in the domain of trust
USB ports are used to connect non trusted equipments	Infection by malware/ransomware	Device Management	Device Whitelist/blacklist Port deactivation
PC can be connected to WiFi or third-party network	Access to the network (backdoor) Control of the PC Infection by malware/ransomware Process takeover (for supervision or engineenring PC)	Management of network connections	Network whitelist/blacklist Network contextualisation

Data Security

Need / contexts	Risks	Cybersecurity solution	Stormshield advantages
The plant uses critical and confidential data (PLC programs, production information…)	An attacker can steal and erase the data	Data encryption of production information, PLC program…	Data encryption Secure file modification workflow Management of the user for access to critical data Send encrypted data (intern and extern)
The plant send production data to the cloud and sometimes to US Cloud (Cloud ACT)	The data can be intercepted during sending. The data can be read by the US government (in case the data are stored in Google, Amazon…)	Encryption of data before sending to the cloud	Local data encryption and synchronization to the Cloud

OT cybersecurity
Use cases

Transportation sector

Securing the traffic management infrastructure of a major European city

Context :

- Evolution of RS232 in IP networks

Security deployed on roadway infrastructure :

- traffic regulation
- vehicle counting
- crossroads lights,
- variable displays…

Customer need :

- Segmentation : warn of an attack done by a person who opens a street cabinet
- Encrypted communications and secure maintenance between the central site and the street cabinets - VPN IPsec

Transportation sector

Equipment deployed :
2 clusters (SN710 et SN510) on the central site:
- Web trafic
- Connections with remote sites via private link

SNi40 Firewall for remote sites :
- 45 static points (street cabinets) + temporary sites connected in 4G (Hirschman routers)

Administration of the equipments via Stormshield Management Center

The Stormshield + for this project :
- Form factor box for deployment in an urban environment
- ANSSI qualification
- By-pass mode

Agri-food sector

Global player in the processing of agricultural products

Context :

- 25 production sites across Europe, North America and Asia
- Complete redefinition of the OT information system and deployment of security solutions

Customer need :

- IT/OT double-barrier firewall deployment
- DMZ implementation for historian and MES servers
- Analysis of industrial protocols
- Internal segmentation between different production units
- Centralized cybersecurity management for all plants

Agri-food sector

Challenges :

- IT historically secured with competing products
- Support of the OT team - need to convince the IT team
- International Deployment

Equipment deployed :

- 18 firewall
- 2 clusters
- 1 Security Management Center

The Stormshield + for this projet :

- Knowledge of the industrial environment and convincing speeches to OT teams
- Protocol analysis
- Product harderning
- ANSSI qualification

Water sector

Securing the distribution of drinking water for an entire French metropolis

Context :

- User customer of Stormshield IT solutions since 2013
- New OT need - trust in Stormshield
- Metropolis equipped with 30 water towers

Customer need :

- Double barrier
- Network segmentation
- Securing remote control and remote maintenance communications for 30 water towers
- Centralized security management
- Logging of security events and centralization to SIEM Logpoint

Water sector

Challenges :
High financial challenge - secured by entry-level firewalls

Equipment deployed :

- 30 x SN210 and 310 – remote sites
- 1 SN900 – central site
- Parc administration by Stormshield Management Center
- Stormshield Logpoint connector

The Stormshield + for this projet :

- ANSSI qualification
- Competitive entry-level firewall models

Thank you

Hope to hear you soon

STORMSHIELD

Get in Touch

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

+33 (0) 9 69 32 96 29

sales@stormshield.eu