



COMET CYB

A feedback on Industrial IoT: common use cases,
cybersecurity issues and solutions

02/12/2019 | Public



SPEAKER: SYLVAIN CASTILLO



Vice President

Security Architect

Information Security Auditor

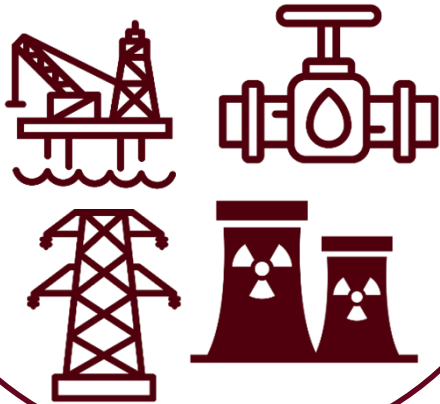
*In charge of the
Transformation department*

scastillo150@beijaflore.com

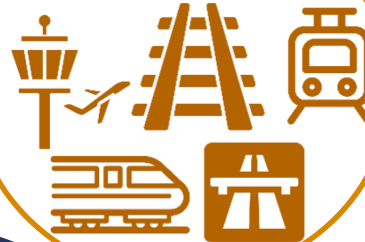
+33 6 01 39 51 77

5 MAIN FIELDS, 20+ CUSTOMERS, 1000+ INDUSTRIAL SITES

Energy - 37%



Transport - 10%



Defence - 23%



Industry - 23%



Pharmaceutical - 7%



AGENDA

01 STAKES, OBSERVATIONS AND RECOMMENDATIONS

02 IDENTIFICATION OF 4 RELEVANT USE CASES

03 MAJOR ISSUES RELATED TO INDUSTRIAL IOT

04 SECURITY COUNTER MEASURES FOR INDUSTRIAL IOT



01 - STAKES, OBSERVATIONS AND RECOMMENDATIONS

THE SECURITY MODEL OF INDUSTRIES MUST NOW CONSIDER IOT



IIOT IS AN EMERGING MARKET

IIoT market is highly fragmented and comprised of a large number of small startups. Most competitors' concerns is time to market, and do not consider cybersecurity stakes.



WITH A RISK OF UNCONTROLLED PROLIFERATION

IIoT solutions are usually made easy to deploy rather than secure. As businesses are proposed immediate benefits, this leads to isolated and non-controlled initiatives, with a risk of proliferation.



INDUSTRIES SHOULD ADAPT ITS GOVERNANCE AND ITS TOOLS TO KEEP CONTROL OF ITS INFORMATION SYSTEM

IIoT must be considered as part of the information system with an additional attack surface. A new governance, with IoT vulnerability management, hardening and audit must be defined. An IoT device management tool and an IoT dedicated network are required.



02 – IDENTIFICATION OF 4 RELEVANT USE CASES

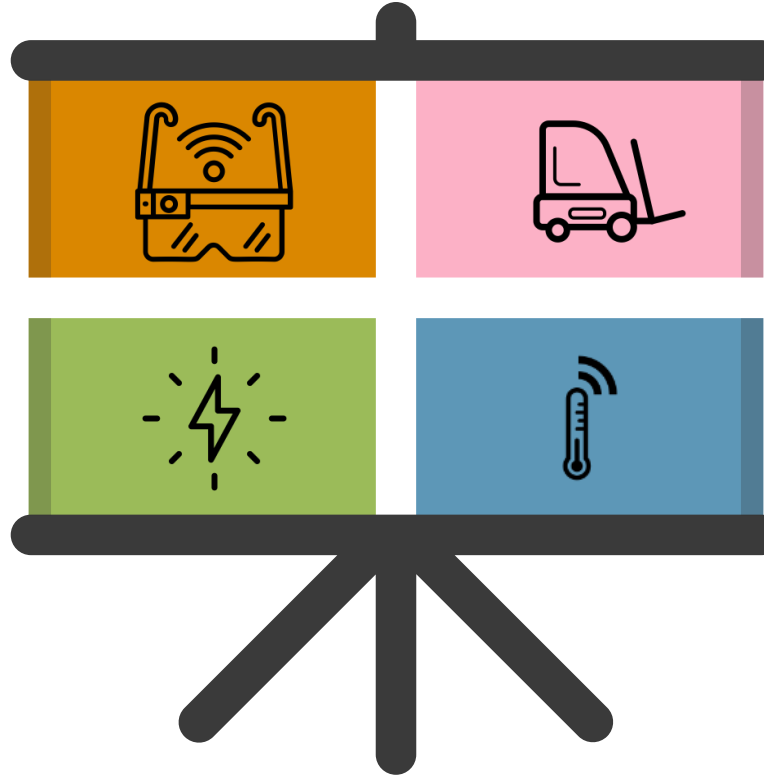
KNOW YOUR IIOT FEATURES BEFORE ENFORCE SECURITY MEASURES

SMART GLASSES FOR REMOTE ASSISTANCE

- The remote operator may see classified documents or information.

PREDICTIVE MAINTENANCE

- Process non-sensitive technical data to anticipate failures
- Vibrations analysis to anticipate failure probability
- overview of the electric consumption in a factory.



AUTOMATED GUIDED VEHICLE

- The AGV is an actuator and may be used to harm people by a malicious attacker.

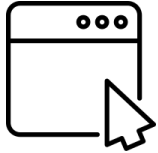
LOCALIZATION

- GPS or RFID positioning of tags stuck to pieces of equipment.
- Facilitates localization of mobile industrial assets.



03 – MAJOR ISSUES RELATED TO INDUSTRIAL IOT

MOST IIOT CAN BE MODELIZED USING A 3-LAYERS ARCHITECTURE



Application layer

The application layer is the central data aggregation and the management portion of the Industrial IoT ecosystem.
Used for data management, analytics and reporting purposes.



Network layer

The network layer serves as a communications aggregation, allowing devices to send data to the application layer.

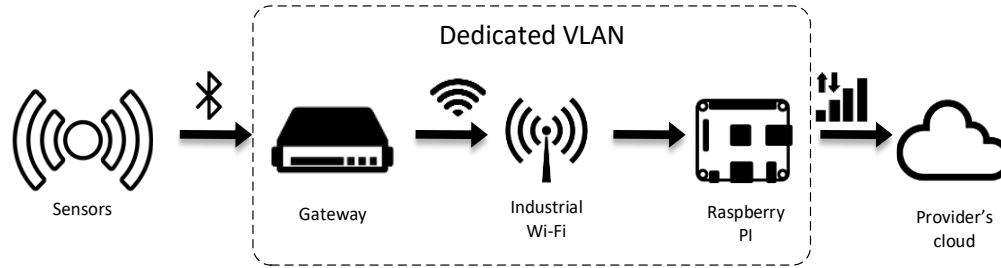


Device layer

The device layer is the physical part of the Industrial IoT ecosystem.
Various technologies (firmware, hardware) can be deployed.

1ST USE CASE: ANALYSIS OF THE ENERGY CONSUMPTION


TYPICAL ARCHITECTURE





CYBER SECURITY NEEDS





SECURITY MAIN RISKS

 Wi-Fi configuration is edited and the **VLAN is no longer logically insulated**: the Raspberry PI and the 4G modem could communicate with the Industrial network

 **Raspberry PI is compromised**: attacker exploits inherent vulnerabilities

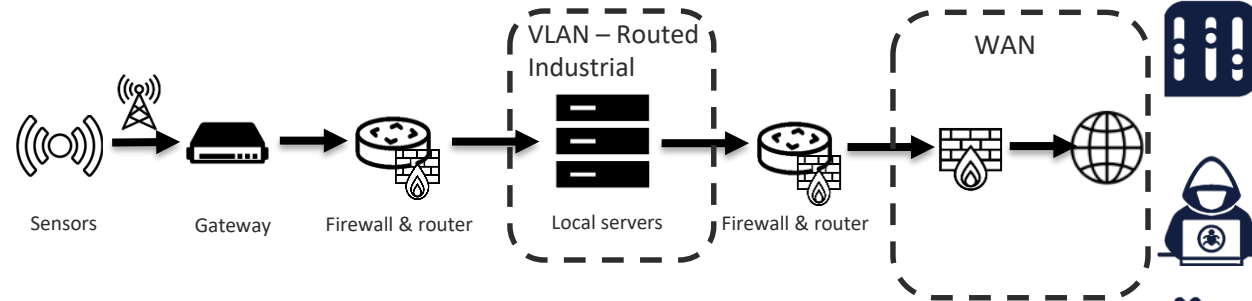
 Signal from the sensors is altered and values are changed: **make a bad decision**

 IIoT inherent vulnerabilities (**jamming the signal, create a breach in the network, use the device to run a DDOS attack, ...**)

 Payload coming from the outsourcer: **Sabotage**

2ND USE CASE: PREDICTIVE MAINTENANCE WITH LORAWAN

TYPICAL ARCHITECTURE



CYBER SECURITY NEEDS



SECURITY MAIN RISKS

A major part of the security **rely on the LoRaWAN gateway**. This gateway needs to be well configured and audited.

An attacker exploits the IoT to **gain access to the network**

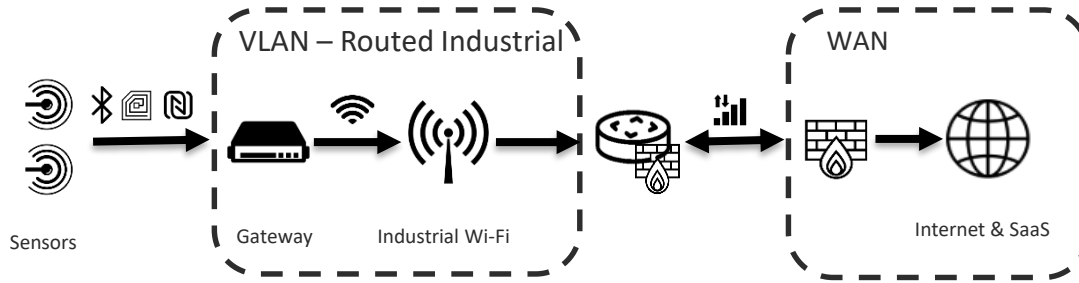
✕
... Signal from the sensors is altered and values are changed: **make a bad decision**

⚠️🔗 IIoT inherent vulnerabilities (**jamming the signal, create a breach in the network, use the device to run a DDOS attack, ...**)

🐞💻 Payload coming from the outsourcer: **Sabotage**

3RD USE CASE: SMART GLASSES FOR REMOTE ASSISTANCE

TYPICAL ARCHITECTURE



CYBER SECURITY NEEDS



SECURITY MAIN RISKS

There is a confidentiality issue regarding what is displayed on the glasses (e.g. classified industrial processes...) that may **disclosed by a malicious provider employee**.

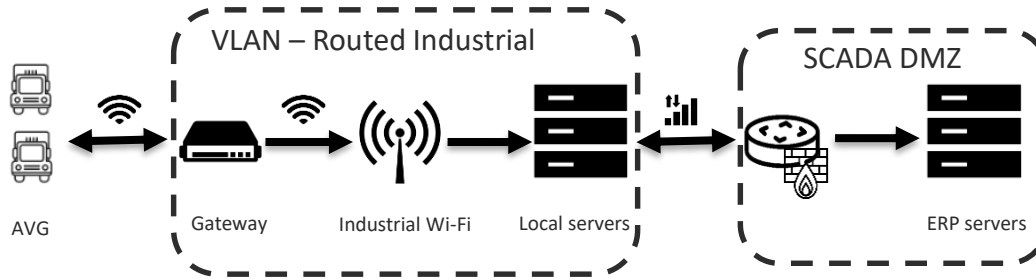
The **conversation being listened** by an attacker

✖
... An attacker **impersonating an employee** (Social engineering)

⚠️🔗 IIoT inherent vulnerabilities (**jamming the signal, create a breach in the network, use the device to run a DDOS attack, ...**)

4TH USE CASE: AUTOMATED GUIDED VEHICLE


TYPICAL ARCHITECTURE




CYBER SECURITY NEEDS




SECURITY MAIN RISKS

 AGV may **collide with somebody** or with a sensitive structure due to an attacker controlling it (human/operational risks).

 **Remote control** of AGV from the **network**

 **Remote control** of AGV from the Cloud Service **Provider's side**

 IIoT inherent vulnerabilities (**jamming the signal, create a breach in the network, use the device to run a DDOS attack, ...**)



04 – SECURITY COUNTER MEASURES FOR INDUSTRIAL IOT

BASIC SECURITY COUNTER MEASURES AT THE APPLICATION LAYER

ENROLMENT

All devices must be properly identified within applications to ensure the origin of the data.

Enrolment process needs to be controlled.

COMPLIANCE

The Industrial IoT application must be compliant with standards and laws, especially when using a SaaS application.

COMPLIANCE WITH PASSWORD POLICY

Industrial IoT applications passwords complexity must be compliant with the password policy

DEFAULT CREDENTIALS

No blank or default application password. Turnkey solutions have always default credentials, that should be revoked before the go live.



BASIC SECURITY COUNTER MEASURES AT THE NETWORK LAYER

ACCESS TO INTERNET

Forbid direct Internet access from Industrial IoT device
Limit modems (4G, 5G, etc.) as much as possible
If required, design a dedicated architecture

ACCESS FROM INTERNET

Use a bounce server for inbound network connection. Inbound connections must be avoided as much as possible

LOCAL NETWORK

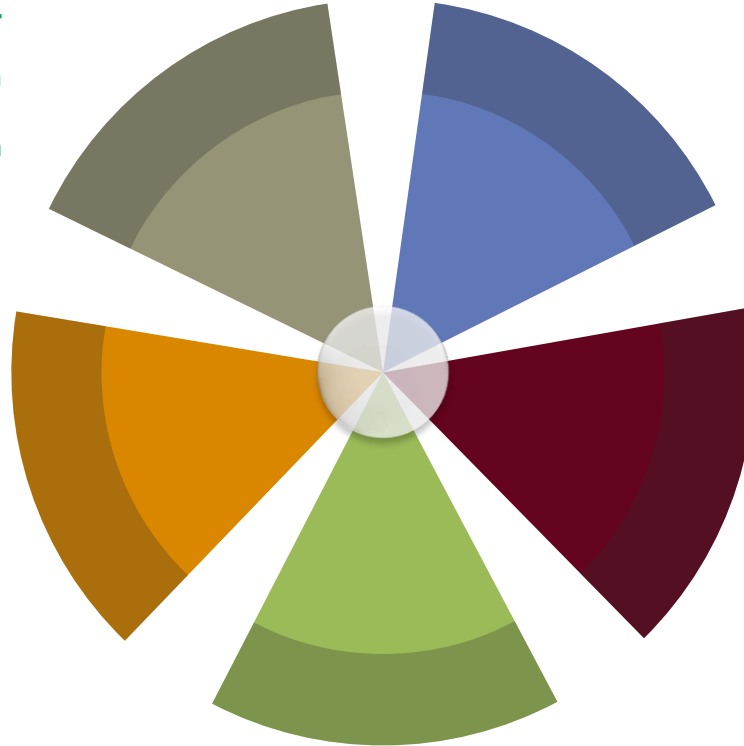
Industrial IoT devices must be authenticated on a local network

ENCRYPTION

Encryption between IoT device and IoT application must be at state of the art according to the cryptography policy if encryption is required

HOMEMADE PROTOCOLS LIMITATION

Use a mature and secure protocol, based on standards (e.g. TLS 1.2)



BASIC SECURITY COUNTER MEASURES AT THE DEVICE LAYER

COMPLIANCE WITH PASSWORD POLICY

Complexity of the passwords for Industrial IoT devices must be compliant with the policies

PATCH MANAGEMENT

Devices supporting security patches must be preferred (including the operating system and the firmware), and regular patches must be published and enforced where possible

DEFAULT PROVIDER CREDENTIALS

No blank or default device passwords

INVENTORY

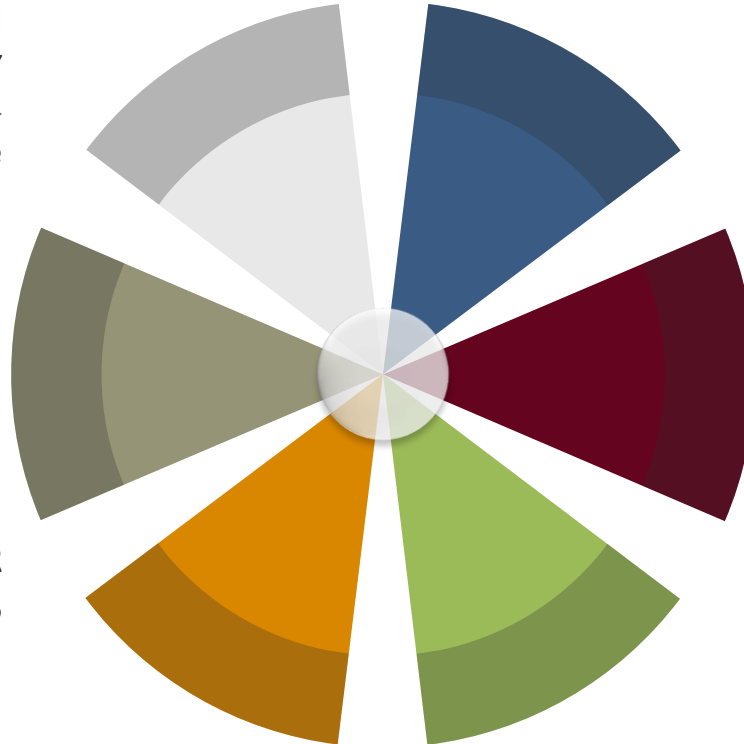
All Industrial IoT devices and sensors features must be inventoried by the provider

HARMFUL ACTUATORS

Physically isolate potentially harmful actuators from sensitive assets

DEVICE MANAGEMENT

All Industrial IoT must be managed through a device management tool





THANK YOU
FOR YOUR ATTENTION

SINCE 2000, BEIJAFLORE HAS BEEN BRIDGING THE GAP BETWEEN BUSINESS & TECHNOLOGY

STAFF

1100

160 in Brasil



Master's degree
From best engineering
and business schools

TURNOVER

2018

102 M€

+ 100
Key accounts



HOT TOPICS

BRASIL

Fast Expansion



Happy at work

ARTIFICIAL INTELLIGENCE

Focused R&D

CYBER SECURITY

LABS

#1 ISO 27001 certified consulting firm



BUSINESS
CONSULTING

CYBER RISK & SECURITY

IT ADVISORY



BANKING
& CAPITAL MARKETS



COMPETITIVE
STRATEGY



Siège social (Paris, France)

Pavillon Bourdan
11-13 avenue du Recteur Poincaré
75016 Paris

Belgium (Brussels)

IT Tower
Avenue Louise/Louizalaan 480
1050 Brussels

Brasil (São Paulo)

Rua Luigi Galvani, 70 – 7º andar
Ed. Alana II, Brooklin
04575-020
São Paulo – SP

Brasil (Rio)

Rua do Passeio, 70 – 6º andar
Centro
20021-290
Rio de Janeiro – RJ

Switzerland (Geneva)

Rue de la Corraterie 26,
1204 Genève

US (New York)

733 Third Avenue, Floor 15
New York, NY 10017