Data frameworks in metrology

Industrial sensors cybersecurity

IN
MEASUREMENT
WE TRUST

François Massé
Ineris
France

Introduction

Operators of industrial facilities have to :

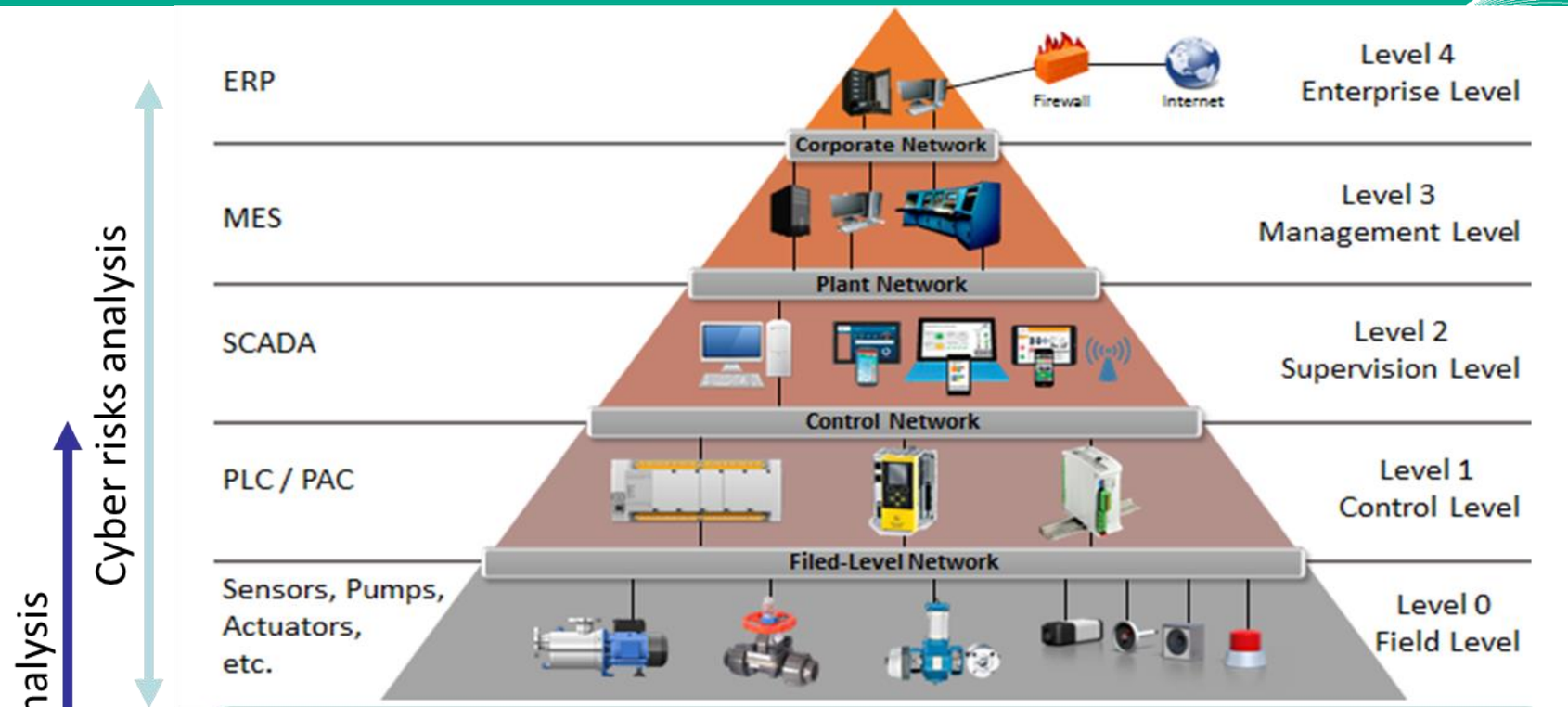
- Assess the risk their installation poses for people and environment
- Protect themselves against financial losses
- Provide essential services to the economy and the community

Reliability and dependability of industrial control and safety systems limits the impact of failures on theses objectives

Deliberate attacks on these systems can also have availability or safety consequences

The ICS cybersecurity relies on the architecture and security management of the overall ICS and on the management of vulnerabilities of its components

What is an industrial control system?



Why is the vulnerability of ICS increasing?

- Increase of Attack surface
- Increase of vulnerabilities
- Increase of the threat

What are the possible consequences?

Impact on

- Availability: accessibilty of information and ressources
- Integrity: modification of information
- Confidentiality: access to information by unauthorised parties

What about the sensors?

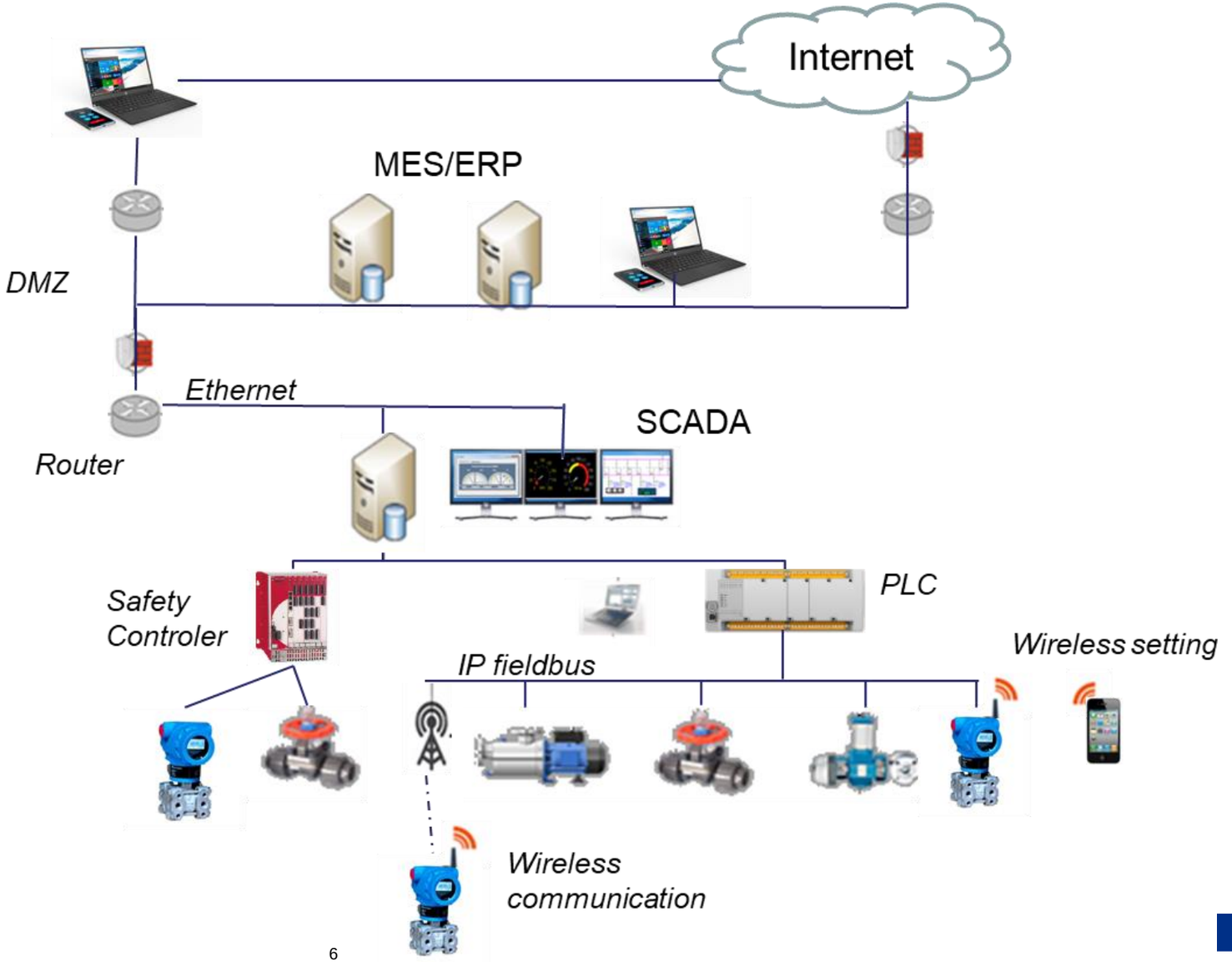
ICS cybersecurity is mainly focused on SCADA and PLC

Sensors are vulnerable as well:

- Use of IP communication
- Use of wireless communication
- Use of wireless setting (I.E Bluetooth communication interfaces)

With possible consequences as:

- loss of communication with PLC or supervision
- modification of transmitted data (e.g. attack man in the middle)
- modification of sensor settings (measurement scale, alarm thresholds, etc.)



How to protect sensors ?

As a supplier, hardening the sensors and applying cybersecurity standard (IEC 62443-4-1/2 as well as functional safety standards (IEC 61508)

- Apply a security lifecycle
- Apply technical Hardening measure like
  - securing the interfaces (strong authentication, encryption...),
  - Defensive coding (consistency checks, prevention of memories defects…))
- Test security features
- Perform a vulnerabilities watch and alert
- Secure production chain and updates

As an integrator, reduce the attack surface and increase intrusion detection

- Disable unused services and interface
- Use Whitelisting
- Redundancy of sensors and control of consistency of measures by Scada or PLCs
- Avoid Wireless communication for critical measure (availability and response time are never guaranteed)

Thank you for your attention

François Massé
Ineris
Francois.masse@ineris.fr