Analysis of cybersecurity threats in Industry 4.0: the case of intrusion detection

Juan Enrique Rubio
Rodrigo Roman
Javier Lopez

University of Malaga

NICS

CRITIS 2017

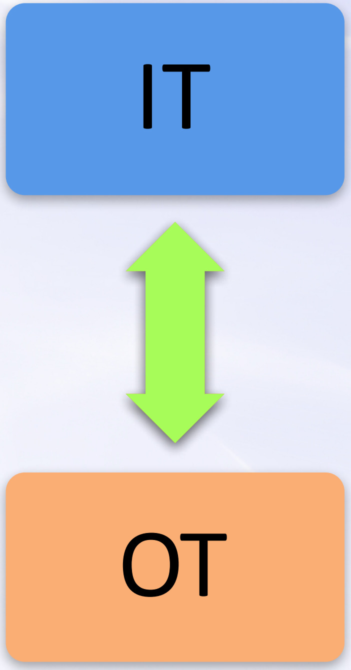
Outline

1. **Introduction**
2. **Cyber-security threats of Industry 4.0 enabling technologies**
3. **Cyber-security issues in Industry 4.0 innovative services**
4. **Intrusion Detection in Industry 4.0**

INTRODUCTION

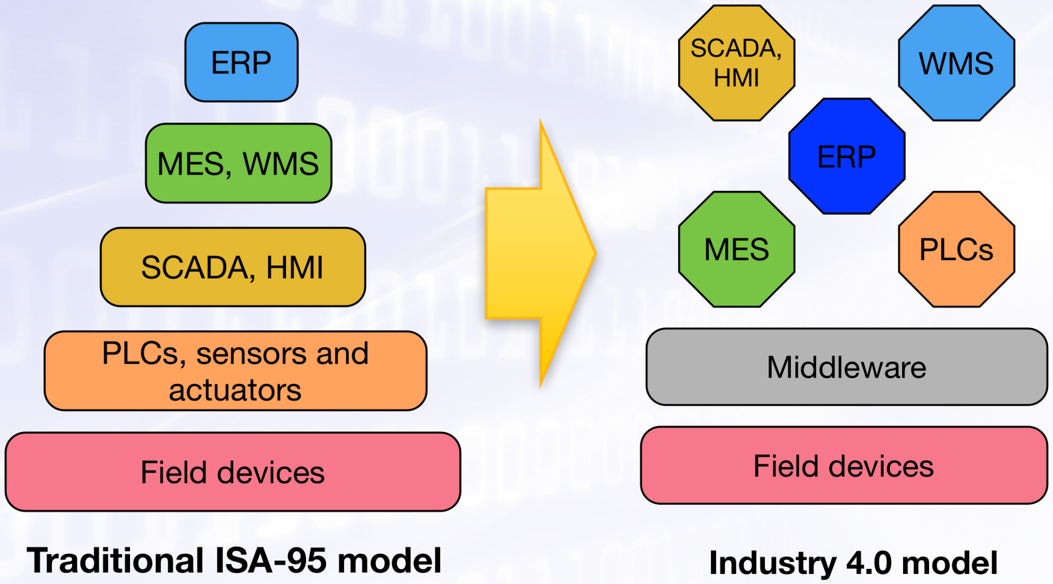
IT and OT integration

- SCADA systems (Supervisory Control and Data Acquisition) are now present in most critical infrastructures.
- Traditionally, these systems and industrial networks (**Operational Technology**) had to be isolated from other environments.
- However, at present, they have been interconnected with external networks (**Information Technology**).



Towards Industry 4.0

- Digitization of all components within the industry to make the productive processes digitally connected and distributed, providing a highly integrated value chain



Interoperability

Virtualization

Decentralization

Real time

Service Orientation

Modularity

Interactivity

Industry 4.0 innovative services and security

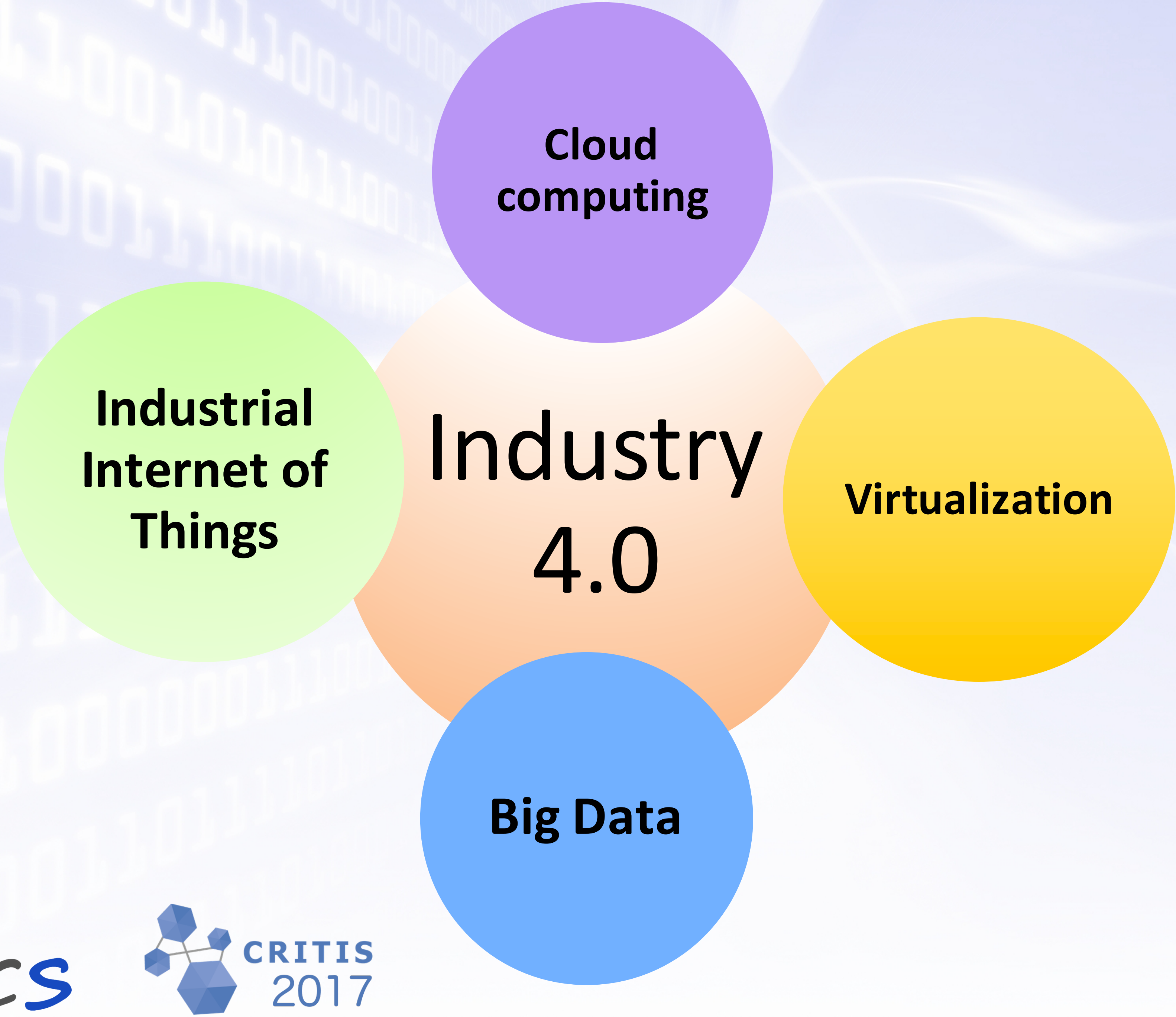
- Creation of innovative services:
  - ❑ Novel cooperative infrastructures
  - ❑ Cloud manufacturing
  - ❑ Agents for decision making
  - ❑ Advanced interactions
  - ❑ …

- The increase in security threats caused by the Industry 4.0 technologies and its innovative services must be addressed

- It is essential to study the requirements of intrusion detection systems in the upcoming industrial context

CYBER-SECURITY THREATS OF INDUSTRY 4.0 TECHNOLOGIES

Introduction: the Industry 4.0 concept

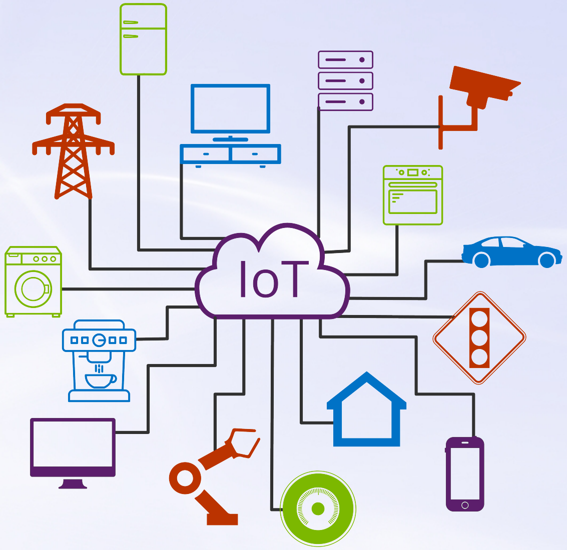


Cyber-security threats of Industry 4.0 enabling technologies

Industrial Internet of Things

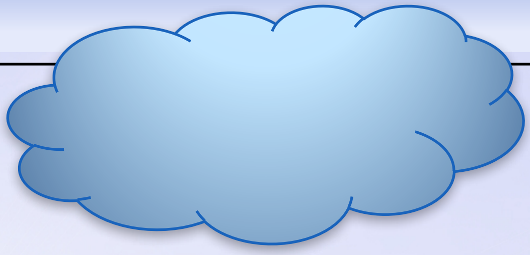
- ○ Massive interconnection of machines, operators and the product itself

- The main concern are the attacks perpetrated against their availability, due to the scarcity of resources (CPU, memory or battery)



Cyber-security threats of Industry 4.0 enabling technologies

Cloud computing



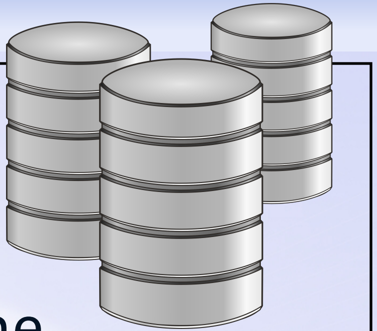
- ○ Processing of information retrieved by IIoT devices, cloud-based manufacturing

- The most common attack goes against its availability, by means of a Denial of service (DoS) attacks against the infrastructure

- Confidentiality problems arise when putting trust in the service provider, who has total access to the stored data

Cyber-security threats of Industry 4.0 enabling technologies

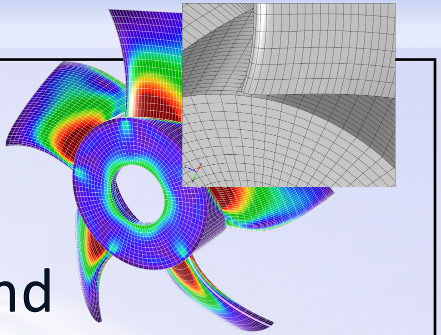
Big Data



- ○ Data analytics with the information extracted from the industrial network to optimize operations and identify anomalies
- Difficult to ensure the security of all components and nodes
- Confidentiality and Integrity of data are threatened if appropriate measures are not applied, which is frequent in this context to improve efficiency

Cyber-security threats of Industry 4.0 enabling technologies

Virtualization



- ○ Virtual representations of machines for simulations and AR/VR devices to interact with the production chain

- The main challenge is the secure information exchange between the physical assets and their virtual representations

- Authentication issues exist with the dissemination of information over multiple vulnerable platforms (e.g., smartphones)

CYBER-SECURITY THREATS IN INDUSTRY 4.0 INNOVATIVE SERVICES

Cyber-security threats in Industry 4.0 innovative services

Novel infrastructures

- Decentralized architecture where any element cooperates with any other
- Attacks could be launched from any element of the infrastructure, blurring the authentication barriers between the different subsystems

Retrofitting

- Integration of Industry 4.0 technologies to legacy systems
- New ways for attacks against legacy systems, exposing their information

Industrial data space

- Secure exchange of information between industrial partners
- Extraction of competitive intelligence

Cyber-security threats in Industry 4.0 innovative services

Cloud manufacturing

- Product customization in the cloud
- Availability and confidentiality of business data affected

Agents

- Workflow planners or self-organising assembly systems
- Compromised agents to influence decisions and the overall workflow

Other enhanced interactions

- Digital twins and advanced HMIs
- They can be manipulated to launch other attacks and extract information

Cyber-security threats in Industry 4.0 innovative services

	Novel infrastructures	Retrofitting	Industrial Data Space	Cloud manufacturing	Agents	Other interactions
Availability	Wide attack surface	Single point of failure	Cascade effects	Wide attack surface	Agents as malware	Denial of service
Confidentiality	Global data in local context	Exposure of sensing layer	Information leakage	Business process leakage	Agent data in local context	Information leakage
Integrity	Behaviour manipulation	Cross-cutting attacks	Cascade effects	Manipulation of components	Tampered data/agents	Disrupt decision making processes
Authentication	Complexity and misconfiguration	Fake legacy/sensing layers	Bigger scope of attacks	Management issues	Attacks from/to agents	Privilege escalation

INTRUSION DETECTION IN INDUSTRY 4.0

Intrusion Detection in Industry 4.0

- Requirements for the design, deployment and management of intrusion detection systems (IDS):

✓ Coverage

- All interactions and elements of an Industry 4.0
- Easily upgradable with new detection algorithms.

✓ Holism

- Users, configurations, potential points of failure and cascade effects are taken into account
- They must be familiarized with the cooperative nature

NICS CRITIS 2017

Intrusion Detection in Industry 4.0

- Requirements for the design, deployment and management of intrusion detection systems (IDS):

  - ✓ Intelligence
    - Behavioral analysis and information correlation to consider the existence of more advanced attacks
  - ✓ Symbiosis
    - Close interaction with other protection mechanisms, such as prevention systems and forensics, as well as the Industry 4.0 services

- The state of the art on IDS for the current industrial ecosystems do not fully cover the previously mentioned requirements

Conclusions

- We have introduced the Industry 4.0 enabling technologies and provided an overview of their threats

- The main threats arisen as consequence of the integration of these novel technologies in the industrial ecosystems have been studied

- Based on this, we have identified a set of requirements for future intrusion detection mechanisms in the industry.

NICS CRITIS 2017

Thanks

Analysis of cybersecurity threats in Industry 4.0: the case of intrusion detection

Juan Enrique Rubio
Rodrigo Roman
Javier Lopez

NICS

CRITIS 2017