PANEL ON SYSTEMS/INTELLI

TRENDS IN INDUSTRIAL AND CYBER SYSTEMS

28TH JUNE, 2018 – INTELLI 2018

VENICE, ITALY

TRENDS IN INDUSTRIAL AND CYBER SYSTEMS

- Moderator: João Reis

- Panelists
  - Dr. Petre Dini
    - IARIA, USA
  - Dr. Voicu Groza
    - School of Electrical Engineering and Computer Science (EECS), University of Ottawa, Canada
  - MSc. João Reis
    - Research Center for Systems & Technologies (SYSTEC), Faculty of Engineering University of Porto, Portugal

TRENDS IN INDUSTRIAL AND CYBER SYSTEMS

- Petre Dini
  - Physical vs. digital protection
  - Dangers in IoT-based Industry 4.0
  - Case study: Spoofing detection
- Voicu Groza
  - Vulnerabilities of Industry 4.0 Development
- João Reis
  - Machine Learning in Manufacturing

INDUSTRY 4.0

1.0 | **1784** | based on mechanical production equipment driven by water and steam power

2.0 | **1870** | based on mass production enabled by the division of labor and the use of electrical energy

3.0 | **1969** | based on the use of electronics and IT to further automate production

4.0 | **tomorrow** | based on the use of cyber-physical systems

Technology

- Digital networking production facilities
- Fast pace of technological change and innovative technologies

Customers

- Customised solutions
- Wide diversity of customers and markets
- New services

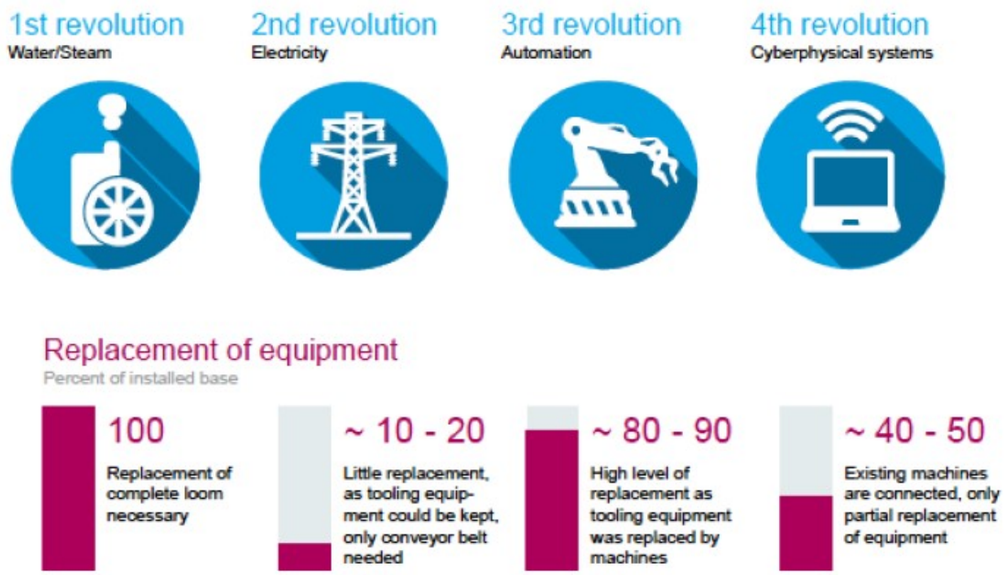
People

- Training and qualifications
- Interaction between human beings and technology

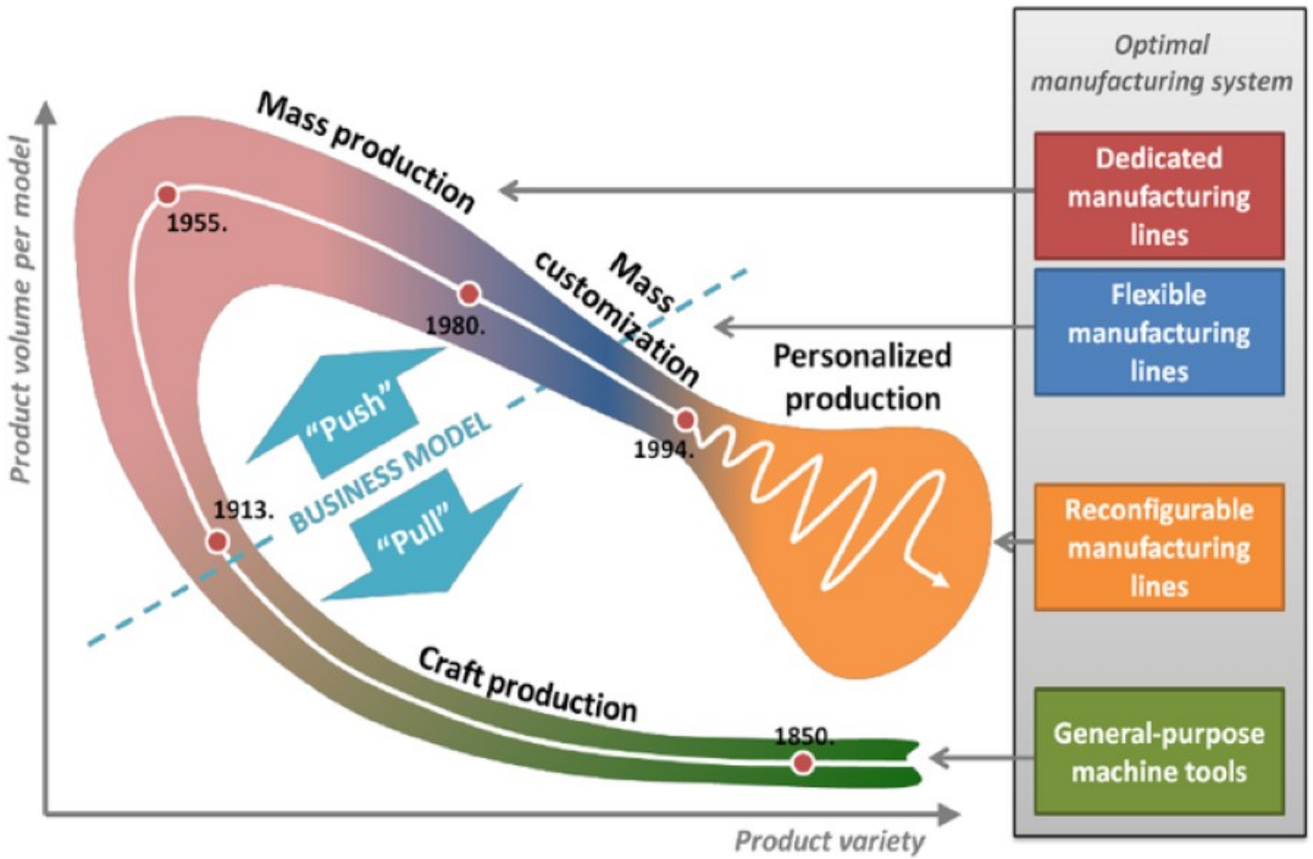
INDUSTRY 4.0

What's so different about industry 4.0?

- It's not about replacing the existing assets, it's about mastering disruptive technologies



FROM CRAFT PRODUCTION TO PERSONALISED CUSTOMISATION



Trends

Customer specific production:

- Individualised products
- Mass production but individual design
- Small lot sizes, one piece flow

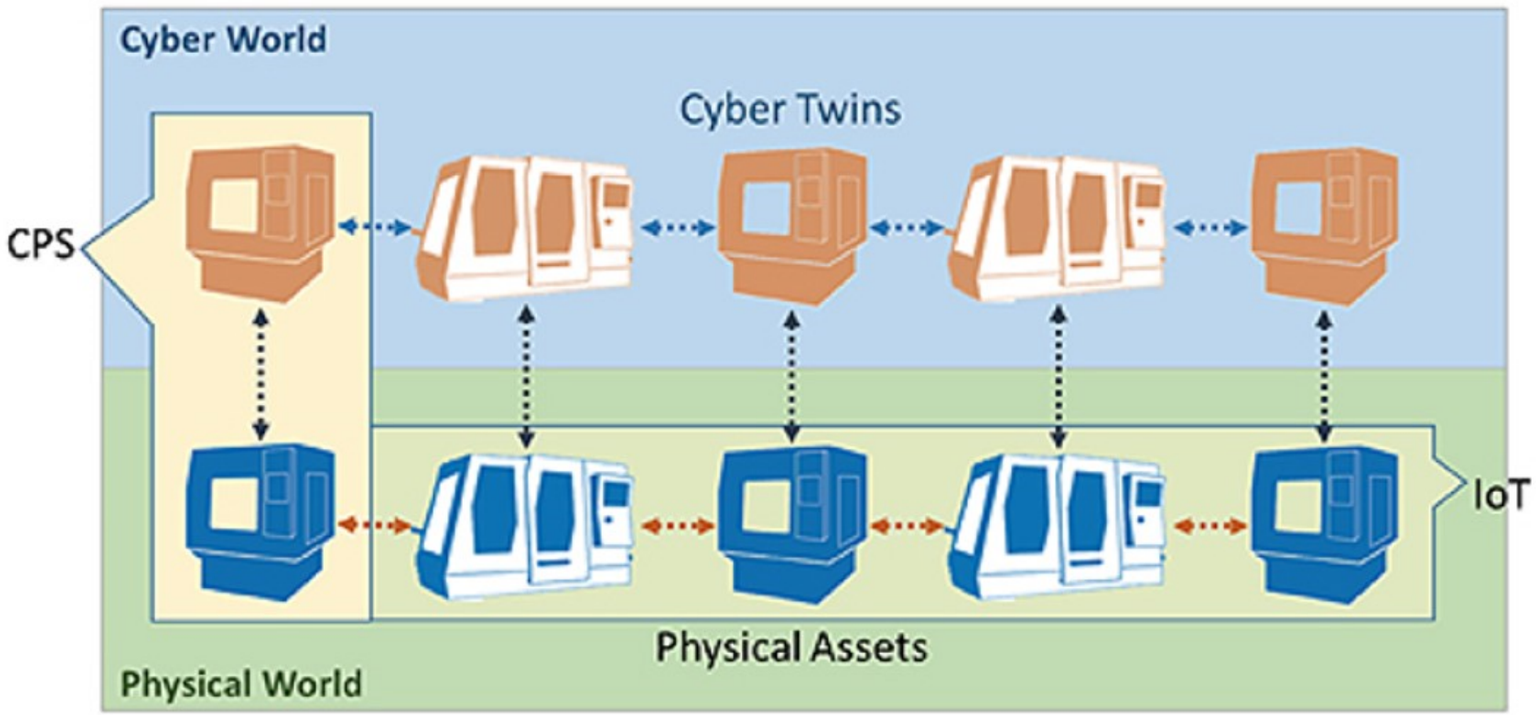
Sustainability:

- High efficiency and near-to-zero emission
- Reusability of machines and equipment
- Avoid waste

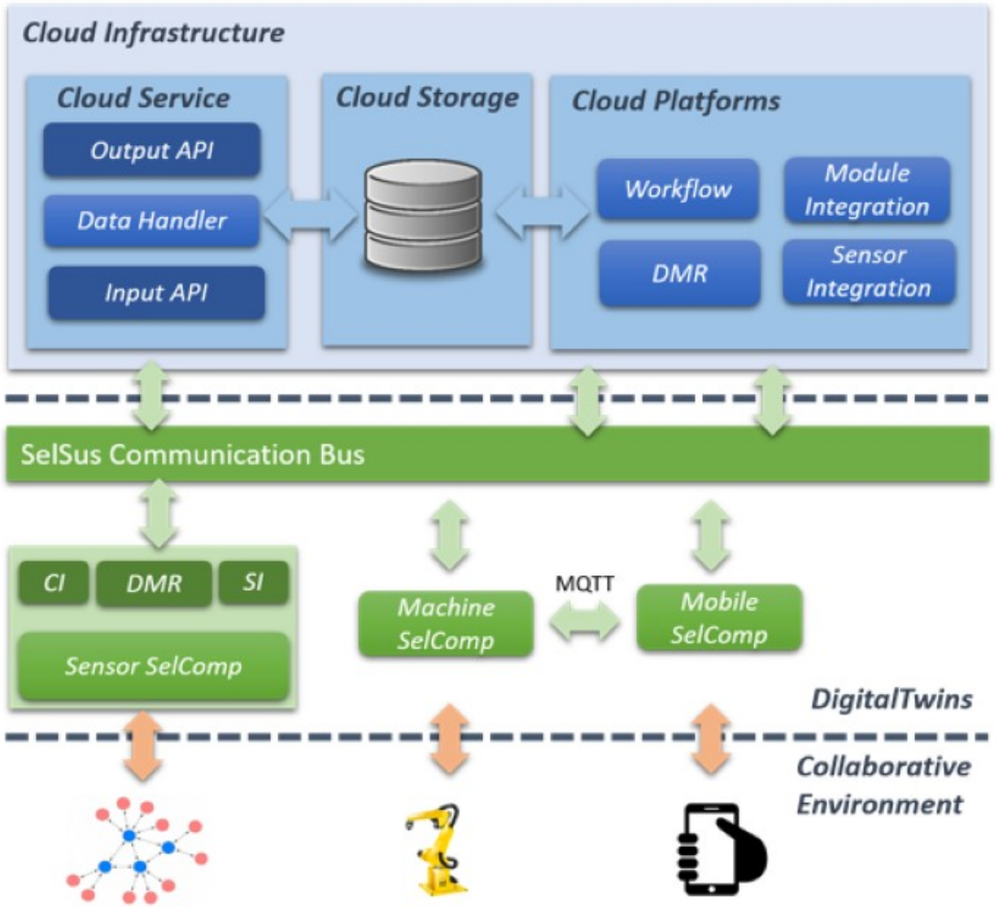
Digitisation and networking:

- Digital & virtual factory
- Integrated value chains
- Constant change

CYBER-PHYSICAL SYSTEM



CYBER-PHYSICAL SYSTEM



PANEL ON SYSTEMS/INTELLI

MACHINE LEARNING IN INDUSTRY

28TH JUNE, 2018 – INTELLI 2018

VENICE, ITALY

SYSTEC

RESEARCH CENTER
FOR SYSTEMS & TECHNOLOGIES

U.PORTO

FEUP FACULDADE DE ENGENHARIA
UNIVERSIDADE DO PORTO

JOAO REIS, GIL GONÇALVES

RESEARCH CENTER FOR SYSTEMS & TECHNOLOGIES (SYSTEC)

FACULTY OF ENGINEERING UNIVERSITY OF PORTO

PORTUGAL

MACHINE LEARNING IN INDUSTRY

- Do Machine Learning algorithms really work?
- Do we really know what is going on in the algorithms?
- It is really necessary a so large amount of data?
- Could these algorithms be transferred to industry?

ALPHAGO

A DOCUMENTARY • SPRING 2017

MACHINE LEARNING IN INDUSTRY

- Do Machine Learning algorithms really work?
  - Yes
- Do we really know what is going on in the algorithms?
- It is really necessary a so large amount of data?
- Could these algorithms be transferred to industry?

MACHINE LEARNING IN INDUSTRY

- Do Machine Learning algorithms really work?
- Do we really know what is going on in the algorithms?
  - No
- It is really necessary a so large amount of data?
- Could these algorithms be transferred to industry?

KEITH RANKIN

441

Intelligent Machines

The Dark Secret at the Heart of AI

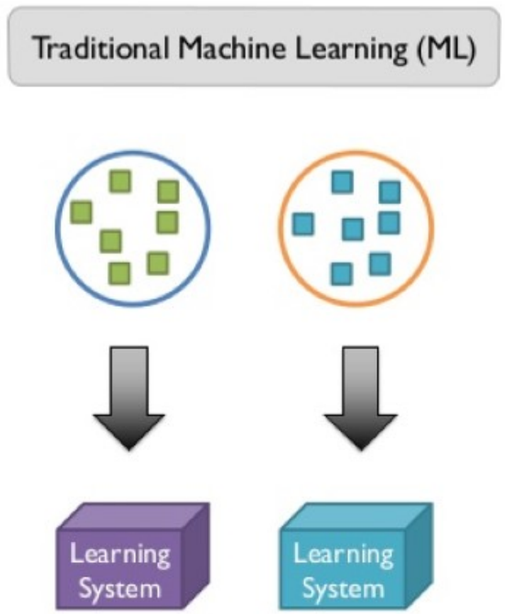
No one really knows how the most advanced algorithms do what they do. That could be a problem.

by Will Knight April 11, 2017

Last year, a strange self-driving car was released onto the quiet roads of Monmouth County, New Jersey. The experimental vehicle, developed by researchers at the chip maker Nvidia, didn't look different from other autonomous cars, but it was unlike anything demonstrated by Google, Tesla, or General Motors, and it showed the rising power of artificial intelligence. The car didn't follow a

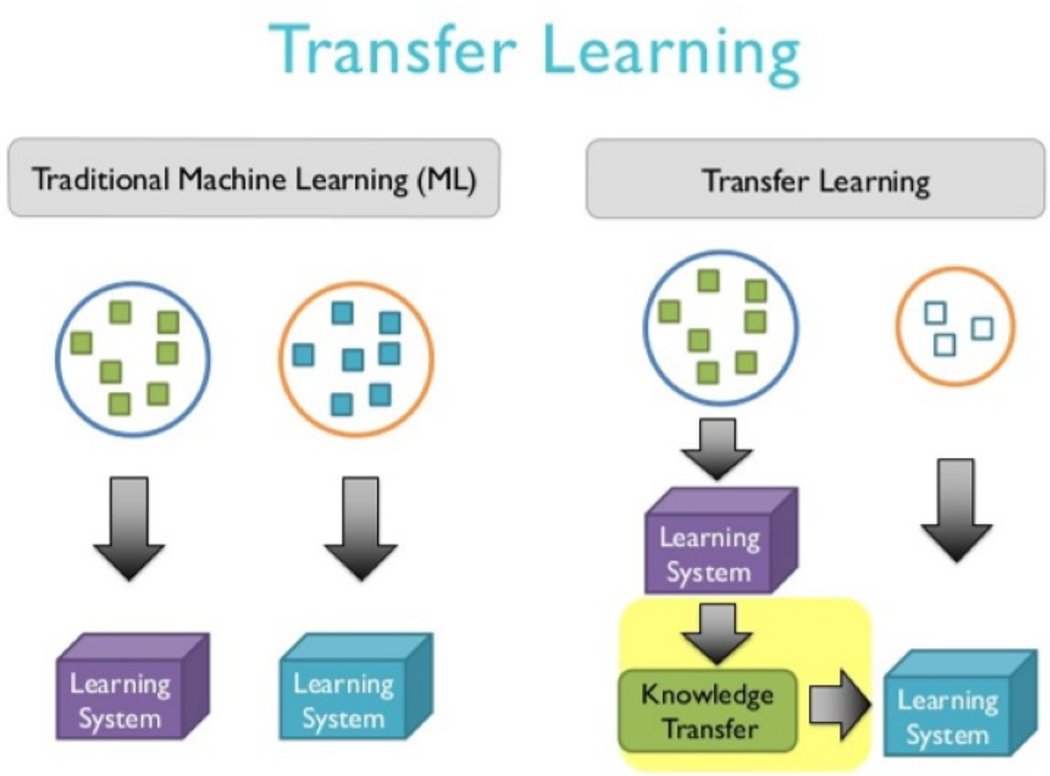
MACHINE LEARNING IN INDUSTRY

- Do Machine Learning algorithms really work?
- Do we really know what is going on in the algorithms?
- It is really necessary a large amount of data?
  - Yes and No
- Could these algorithms be transferred to industry?



MACHINE LEARNING IN INDUSTRY

- Do Machine Learning algorithms really work?
- Do we really know what is going on in the algorithms?
- It is really necessary a large amount of data?
  - Yes and No
- Could these algorithms be transferred to industry?



MACHINE LEARNING IN INDU

- Do Machine Learning algorithms really work?
- Do we really know what is going on in the algorithms?
- It is really necessary a large amount of data?
  - Yes and No
- Could these algorithms be transferred to industry?

The Download

What's up in emerging technology

DeepMind's latest AI transfers its learning to new tasks

By using insights from one job to help it do another, a successful new artificial intelligence hints at a more versatile future for machine learning.

Backstory: Most algorithms can be trained in only one domain, and can't use what's been learned for one task to perform another, new one. A big hope for AI is to have systems take insights from one setting and apply them

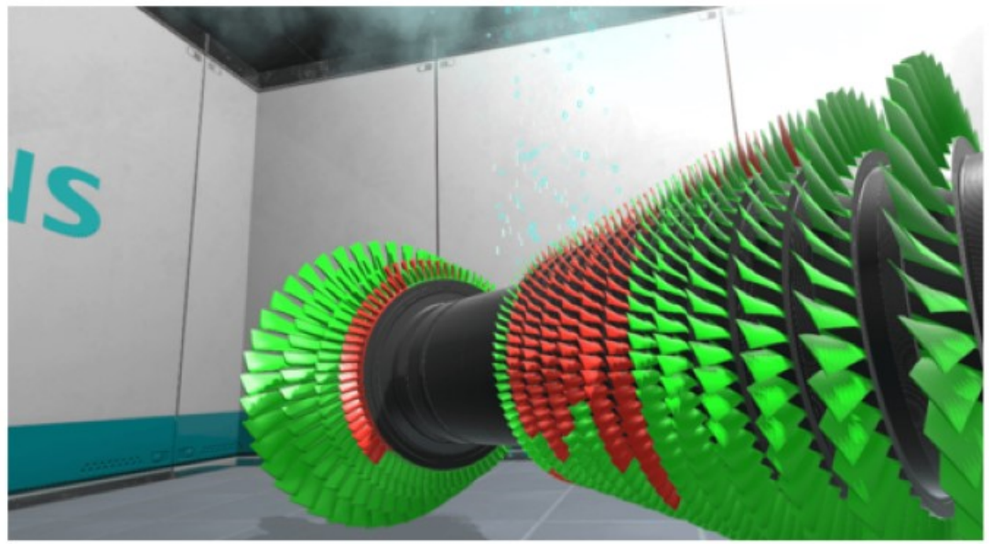
MACHINE LEARNING IN INDUSTRY

- Do Machine Learning algorithms really work?
- Do we really know what is going on in the algorithms?
- It is really necessary a so large amount of data?
- Could these algorithms be transferred to industry?

MACHINE LEARNING IN INDUSTRY

- Siemens has been using neural networks to monitor its steel plants and improve efficiencies
- Investment around $10 billions in US software companies
- Launched MindSphere (2016) - Cloud Platform with IBM's Watson Analytics
- Monitor, record, and analyze everything in manufacturing from design to delivery to find problems and solutions

SIEMENS



"Even after experts had done their best to optimize the turbine's nitrous oxide emissions, our AI system was able to reduce emissions by an additional 10 to 15%."

Click2Make → Product-as-a-Service technology

MACHINE LEARNING IN INDUSTRY

- In 2015 GE launched its Brilliant Manufacturing Suite for customers to track and process everything in the manufacturing process to find possible issues before they emerge and to detect inefficiencies.
- **Goal:** Link design, engineering, manufacturing, supply chain, distribution and services into one globally scalable using Predix, their industrial internet of things platform.
- GE spent around $1 billion developing the system, and by 2020 GE expects Predix to process one million terabytes of data per day.
- Their first "Brilliant Factory" was built in 2015 in Pune, India with a $200 million investment, leading to an improvement of equipment effectiveness at this facility by 18 percent.
- Wind generator factory in Vietnam increasing productivity 5%
- Jet engine factory in Muskegon had a 25% better on-time delivery rate. Decreased unplanned downtime by 10-20% by equipping machines with smart sensors to detect wear.

MACHINE LEARNING IN INDUSTRY

- In 2015 Fanuc acquired a 6 percent stake in the AI startup Preferred Network for $7.3 million to integrate deep learning to its robots.
- In early 2016 it announced a collaboration with Cisco and Rockwell Automation to develop and deploy FIELD (FANUC Intelligent Edge Link and Drive)
- Just a few months later Fanuc partnered with NVIDIA to use their AI chips for their "factories of the future."

FANUC

MACHINE LEARNING IN INDUSTRY

- One use of AI they have been investing in is helping to improve human-robot collaboration.
- getting near robotic arms while they worked was a major health hazard requiring safety barriers between people and machines
- KUKA claims their LBR iiwa *"is the world's first series-produced sensitive, and therefore HRC-compatible, robot."*
- Its use of intelligent control technology and high-performance sensors means it can work right beside a human without the risk of accidentally crushing a person.
- BMW is using these Robotic Arms

KUKA

Panel on SYSTEMS/INTELLI

Trends in Industrial and Cyber Systems

Built-in Protection

Petre Dini, IARIA, USA

petre@iaria.org

Thursday, June 28th

June 24-28, 2018 - Venice, Italy

PHYSICAL/DIGITAL FACETS

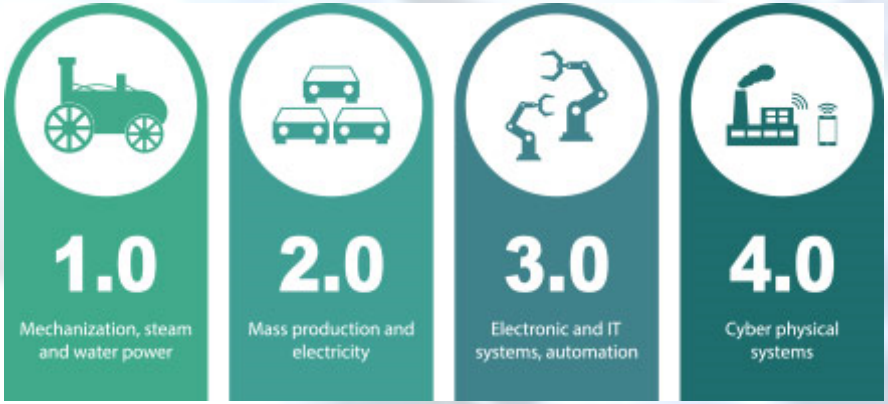
1. Physical vs. Digital Protection
2. Dangers in IoT-based Industry 4.0
3. Case Study: Spoofing Detection

Physical vs. Digital Protection

Hammer, Bits, Wireless

1001(?)11000(??)10101111

Internet of Things, Big/Huge Data, Industry 4.0, IIoT (Industrial Internet of Things)



https://www.vksapp.com/resources/use-cases/industrial-revolution-iot-iiot-industry-40?gclid=EAIaIQobChMI2LDNrorK2wIVg_5kCh0aFgqfEAAYAiAAEgJEN_D_BwE

Dangers in IoT-based Industry 4.0

Techniques/Logistics

- Cloud/Distribution (execution, storage, control)
- Datacenter's Location (physically protected/not-protected)
- Obscurity/unknown Location/Server (of /storage/execution)

IIOT

Remote Access

- Good on TV channels
- Risky in Industrial systems

Acting on

- pre-settings
- current values
- implicit/hidden peer-interactions

Protection *(no smart | with small computation power)*

- High speed/small communication window
- Setting (temporary) access roles
- Considering side effects

Case Study: Spoofing Detection

IEEE Communications Magazine
May 2018, vol. 56, no. 5, pp. 66-71

Theme: Spoofing | Safety and Security | Cloud/Fog Computing

Two many connected devices

- **Low QoE and QoS as Limited Power/Storage**
- **In Production: (i) Peer-robots can execute computationally intensive tasks (as Fog nodes), when robots are deployed in mobile applications**
- **In Cyber systems (e.g., drones/unmanned aerial vehicles): GPS spoofing is a major security attack (in this case, the Fog nodes execute tasks offloaded from users via wireless communication links)**

GPS spoofing send fake GPS data to receivers, so it is an easy-to-launch attack

- **case study: Department of Home Security (USA); Mexican drug traffickers used satellites signal deception technology to attack Border Patrol UAV via wrong GPS coordinates**
- **Solutions: many spoofing detection methods exist / at a cost and complexity**

Protecting Cyber/Industrial Systems

Challenges: A LOT

General Requirements

- Designing systems with the (self)-Protection as main requirement
- Building a Response Strategy to attacks
- Minimize the exposition to Critical Risks
- Protect Embedded Systems (more difficult to discover a threat)
- Protect Vital Infrastructure
- Protect Monitoring, Control and Decision Systems
- Protect human-related service delivery systems (water, health, food, etc.)

Thanks

Q&A

WWW.IARIA.ORG

uOttawa

L'Université canadienne
Canada's university

Panel on SYSTEMS / INTELLI

Trends in Industrial and Cyber Systems

Vulnerabilities of Industry 4.0 Development

Dr. Voicu Groza

School of Electrical Engineering and Computer Science

Université d'Ottawa | University of Ottawa

Industry 4.0 …

… promises major improvements in the industrial processes

- by connecting local and global networks for information exchange amongst smart machinery
- while integrating possibly all stages of the value chain.

Devil’s Advocate Questions

- Efficiency of the new applications
- Implementation’s cost
- Impact on work: employees retraining
- Preparedness of organization's decision makers

Industry 4.0 Challenges

Small and medium-sized enterprises (SMEs) concerns:
high investment and conversion costs

To evaluate the application of Industry 4.0:
IoT gateways & I4.0 starter kits +

Thanks

Q & A

More Q’s … than A’s