Co-funded by the
Erasmus+ Programme
of the European Union

Cyber Physical System (CPS) and Data Security

Module II: Digital Factory Modeling: How to formulate a virtual world

Prof.Dr.Athakorn Kengpol, KMUTNB

Curriculum Development
of Master's Degree Program in
Industrial Engineering for Thailand Sustainable Smart Industry

Content

- **Learning Outcome**
- **Definition**
- **Evolution**
- **Difference from software and embedded systems**
- **Heterogeneity and modelling, long term goal**
- **Upgradation**
- **Scientific and technical challenges**
- **Challenges for CPS software design**
- **Expectations and design challenges of CPS**
- **Institutional, societal, and other challenges**
- **Application**
- **Security and Privacy Issues in Cyber-Physical Systems**
- **Activities** (Lab sheet)
- **Summary**
- **Learning Outcome**

Co-funded by the
Erasmus+ Programme
of the European Union

Learning Outcome

Formulate a data model representing data streamlining in a production line of an existing traditional factory using a data flow diagram

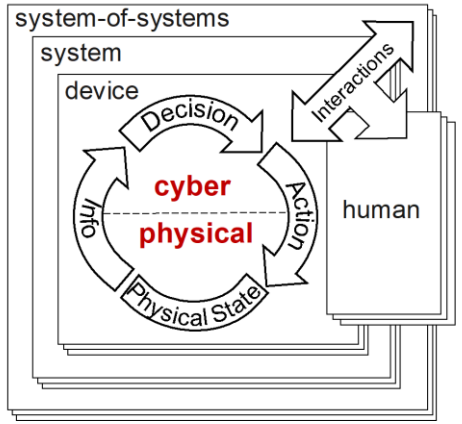
Co-funded by the
Erasmus+ Programme
of the European Union

Definition

Digital Factory

A cyber physical system (CPS) is a complex system that integrates computation, communication, and physical processes. **Digital manufacturing** is a method of using computers and related technologies to control an entire production process. **Industry 4.0** can make manufacturing more efficient, flexible, and sustainable through communication and intelligence; therefore, it can increase the competitiveness. Key technologies such as the Internet of Things, cloud computing, machine-to-machine (M2M) communications, 3D printing, and Big Data have great impacts on Industry 4.0. Therefore, **CPS** is the way to **streamlining process** in a production line of an existing traditional factory using a data flow diagram for Digital factory is important.

- *Cyber-physical systems are physical, biological, and engineered systems whose operations are integrated, monitored, and/or controlled by a computational core. Components are networked at every scale.*



The Framework for Cyber-Physical Systems was released by the NIST CPSPWG on May 26, 2016

Co-funded by the Erasmus+ Programme of the European Union

Definition

What are Cyber Physical Systems?

https://www.youtube.com/watch?v=FxRJFLWbyjM

Co-funded by the
Erasmus+ Programme
of the European Union

Definition

What are Cyber Physical Systems?

https://www.youtube.com/watch?v=C53GIimgLCA

Co-funded by the Erasmus+ Programme of the European Union

Definition

What are Cyber Physical Systems?

- Cyber – computation, communication, and control that are discrete, logical, and switched
- Physical – natural and human-made systems governed by the laws of physics and operating in continuous time
- Cyber-Physical Systems – systems in which the cyber and physical systems are tightly integrated at all scales and levels Change from cyber merely appliquéd on physical
- Change from physical with off-the-shelf commodity “computing as parts” mindset
- Change from ad hoc to grounded, assured development

https://www.sciencedirect.com/science/article/pii/S2095809918306120X

Co-funded by the Erasmus+ Programme of the European Union

Definition

Why Cyber Physical Systems?

- **Embedded computers allow us to add capabilities to physical systems.**

  eg: Computer - controlled automotive engines are fuel-efficient and low-emission.

- **By merging computing and communication with physical processes, CPS brings many benefits:**

  Safer and more efficient systems

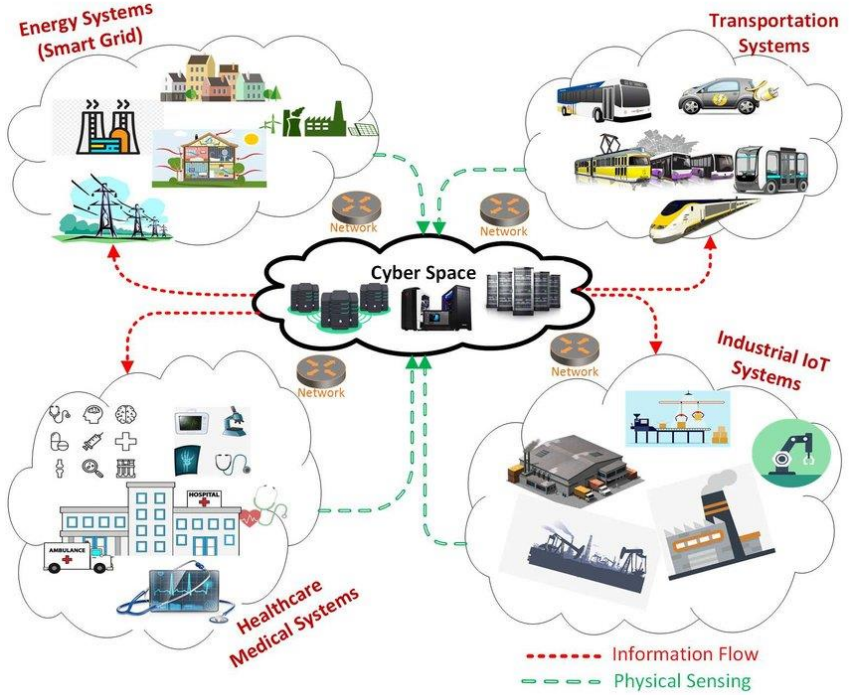
  Reduce the cost of building and operating systems

  Could form complex systems that provide new capabilities

- **Technological and Economic Drivers**

  The decreasing cost of computation, networking, and sensing provides the economic motivation.

  Environmental pressures make new technologies appear to improve energy efficiency and reduce pollution.



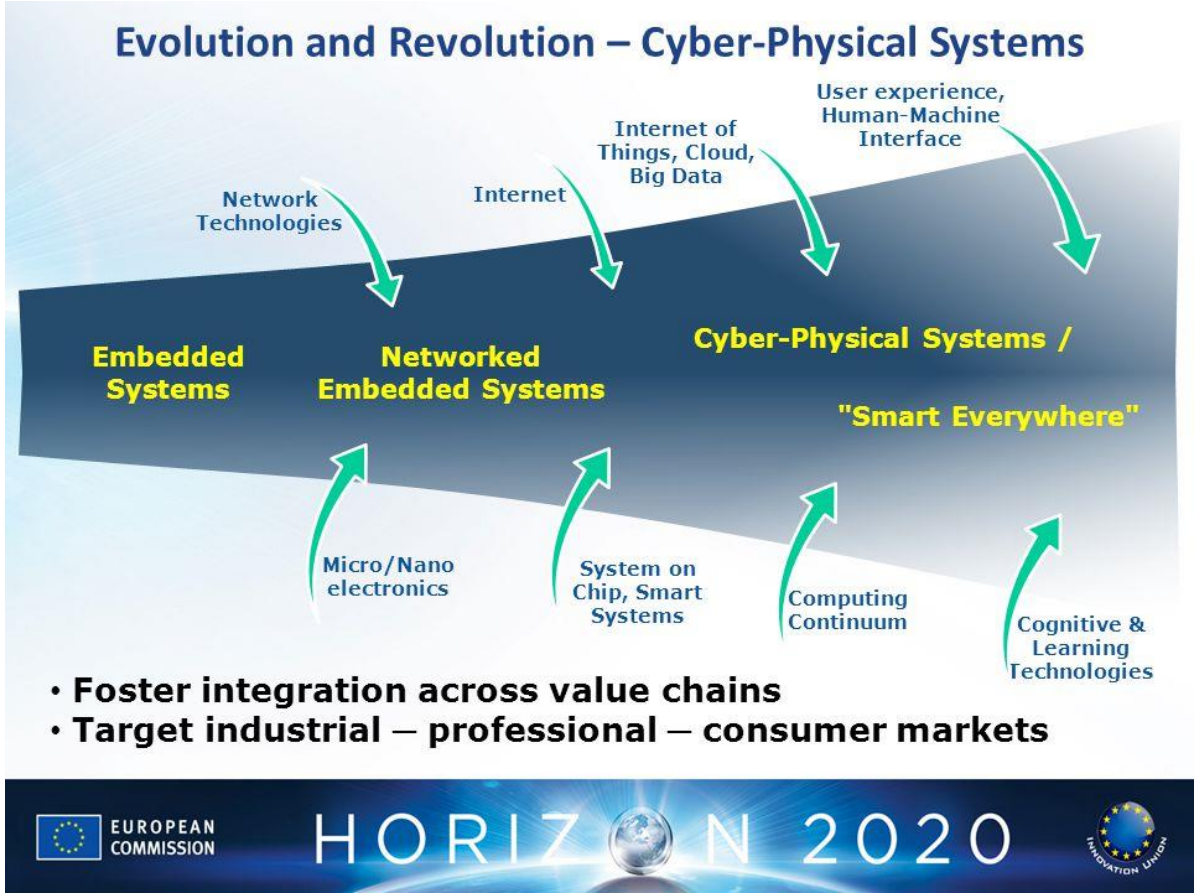
https://www.researchgate.net/figure/Application-Scenarios-of-cyber-physical-systems-describing-the-information-flow-and_fig2_329466954

Co-funded by the Erasmus+ Programme of the European Union

EVOLUTION OF CPS

Digital Factory

- **Two types of computing systems**
  - Desktops, servers, PCs, and notebooks
  - Embedded
- **The next frontier**
  - Mainframe computing (60’s-70’s)
    - Large computers to execute big data processing applications
  - Desktop computing & Internet (80’s-90’s)
    - One computer at every desk to do business/personal activities
  - **Embedded computing (21st Century)**
    - **“Invisible” part of the environment**
    - **Transformation of industry**



Co-funded by the Erasmus+ Programme of the European Union

https://www.slideserve.com/emily-jenkins/ict-1-smart-cyber-physical-s-ystems-in-h2020

EVOLUTION OF CPS

Digital Factory

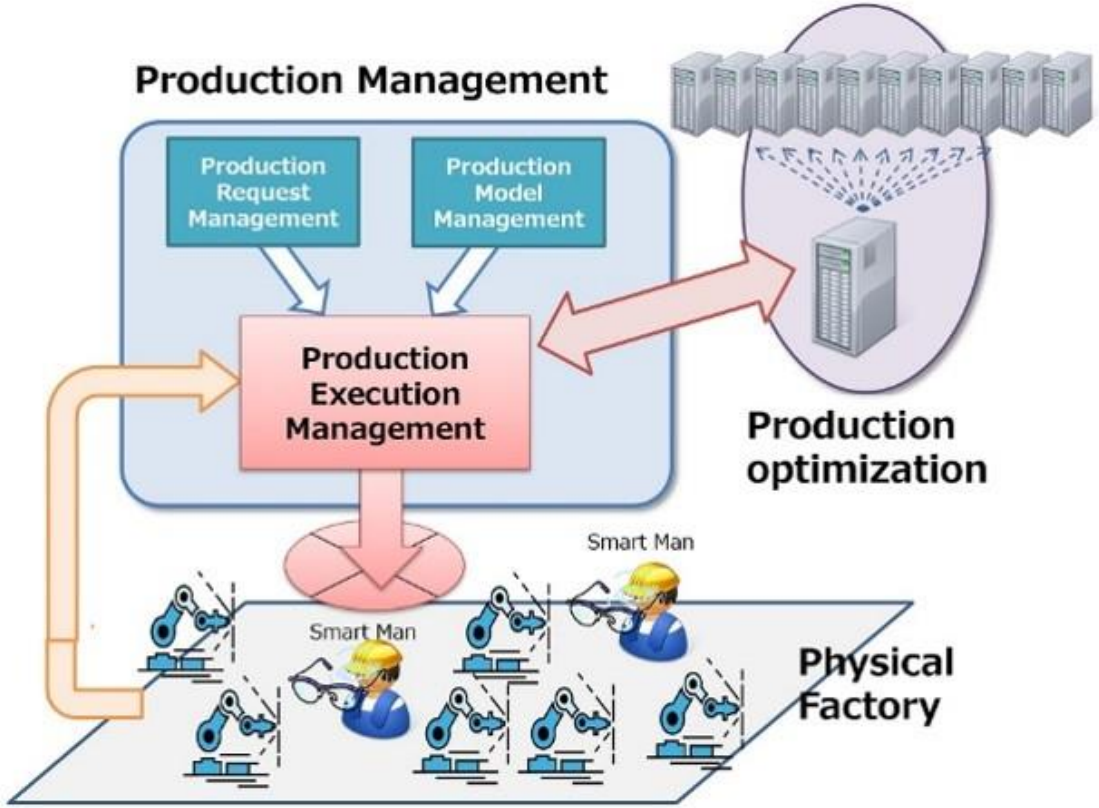
- Cyber-Physical systems, a key infrastructure to support smart manufacturing, are integration of physical, networking, and computation processes.
- In a physical systems, embedded sensors and other monitoring devices collect DATA to be fed into computation processes in a cyber system. In this system, there is infrastructure constructed digitally to map with the physical one (Digital Twin).
- After arrive at an optimal solution, the cyber system will feed information back to control the physical system through actuators.
- Networking technology allows the elements in both systems to be connected interactively with each other.

Co-funded by the
Erasmus+ Programme
of the European Union

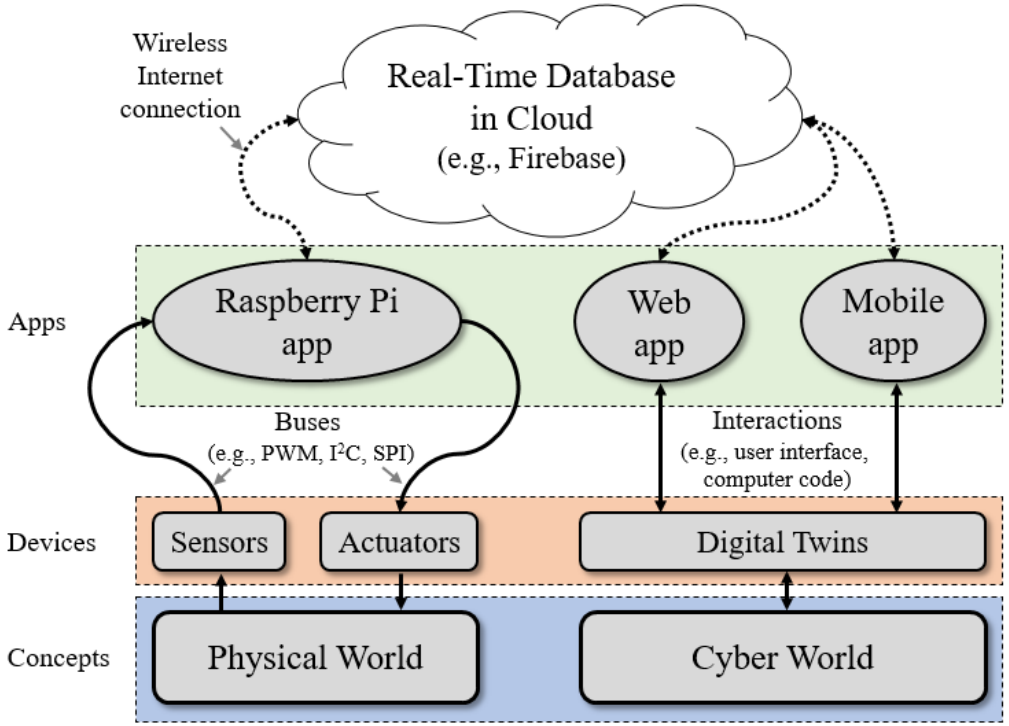
EVOLUTION OF CPS

Digital Factory

- **Relationship between the physical and cyber systems**



http://www.lexer.co.jp/en/product/iot



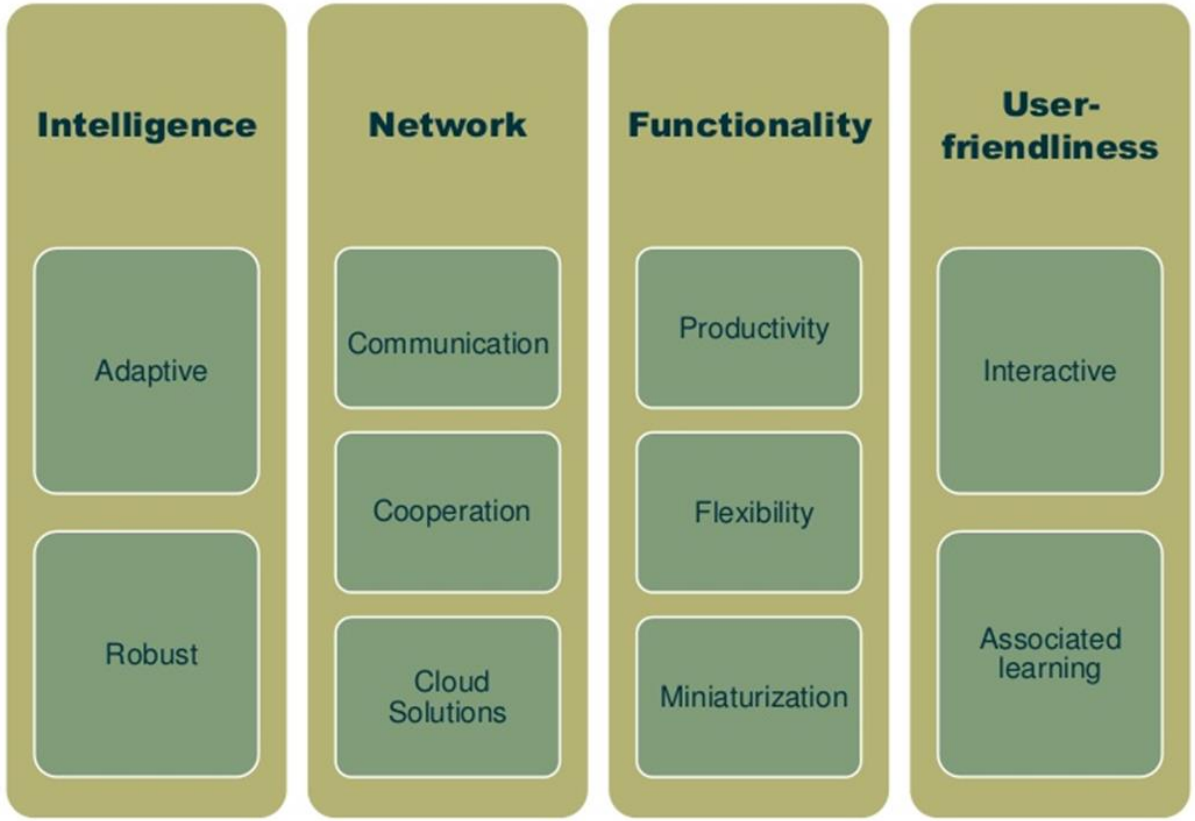
A Cyber-Physical System for Programming and Controlling IoT Systems

https://medium.com/@charlesxie/building-a-cyber-physical-system-to-simplify-iot-app-development-f3579b7916dc

Co-funded by the Erasmus+ Programme of the European Union

EVOLUTION OF CPS

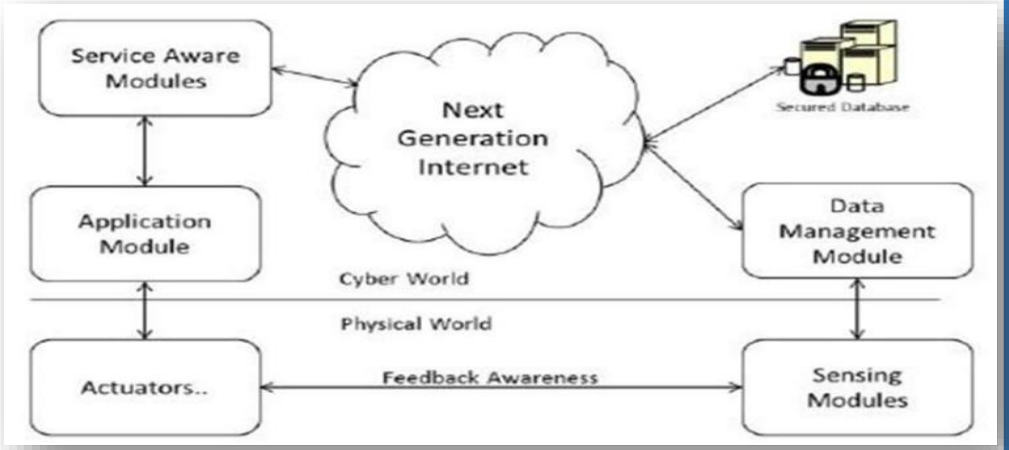
- **Characteristics of CPSs**



Co-funded by the Erasmus+ Programme of the European Union

EVOLUTION OF CPS

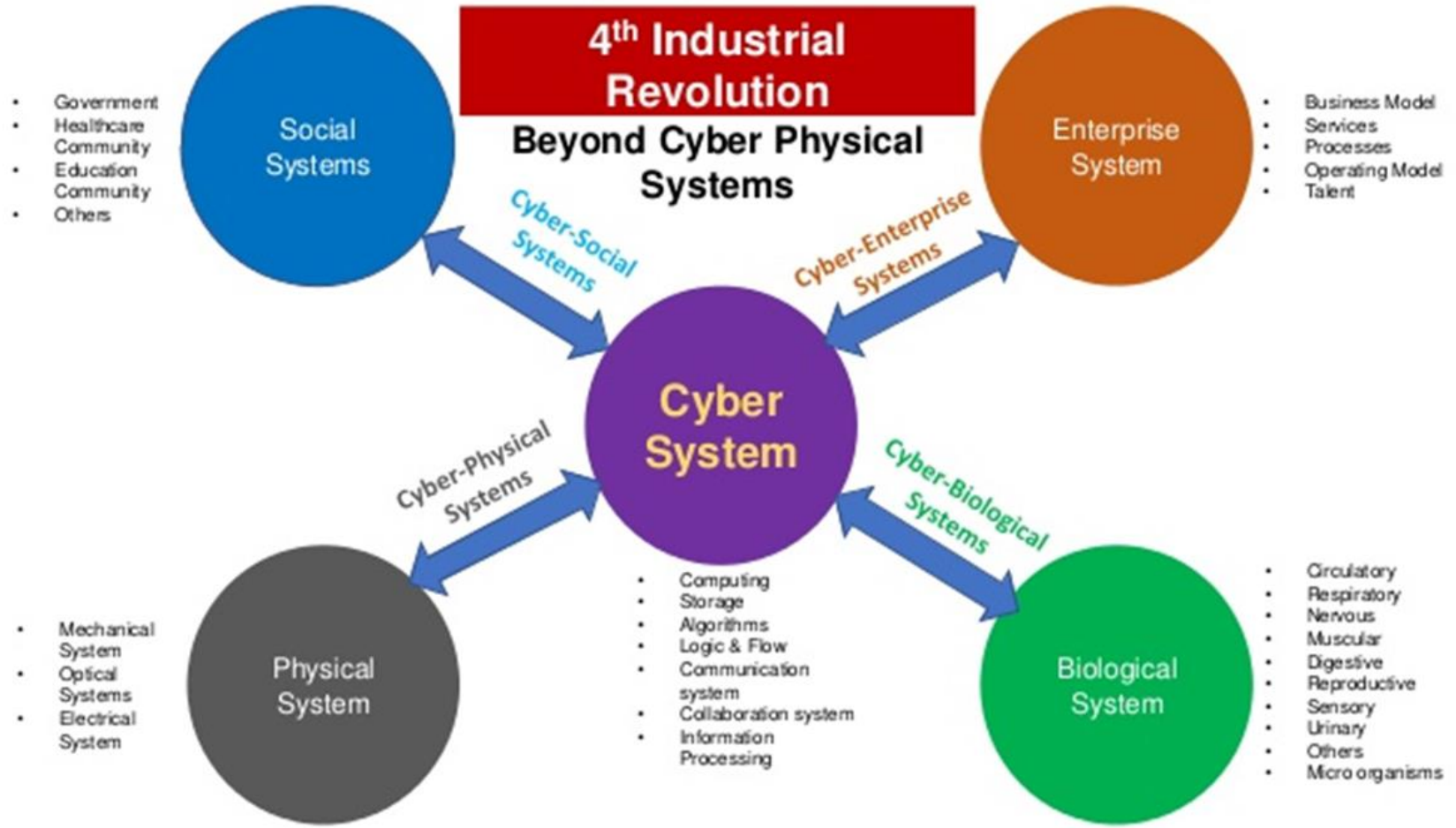
- **MODULES IN CPS**
  - **Sensing Module**
    - Data collection from physical world through sensors
  - **Data Management Module(DMM)**
    - Consists of the computational devices and storage media
  - **Next Generation Internet**
    - Enabling applications to select the path, or paths that their packets take between the source and destination
  - **Service Aware Modules (SAM)**
    - Sensed data is being recognized and sent to the services available
  - **Application Module (AM)**
    - Service are deployed and interact with NGI
    - Info is saved on database for QoS support.(NoSQL)
  - **Sensors and Actuators**
    - Actuator receives the commands from the Application Module, and executes



Co-funded by the Erasmus+ Programme of the European Union

EVOLUTION OF CPS

Digital Factory



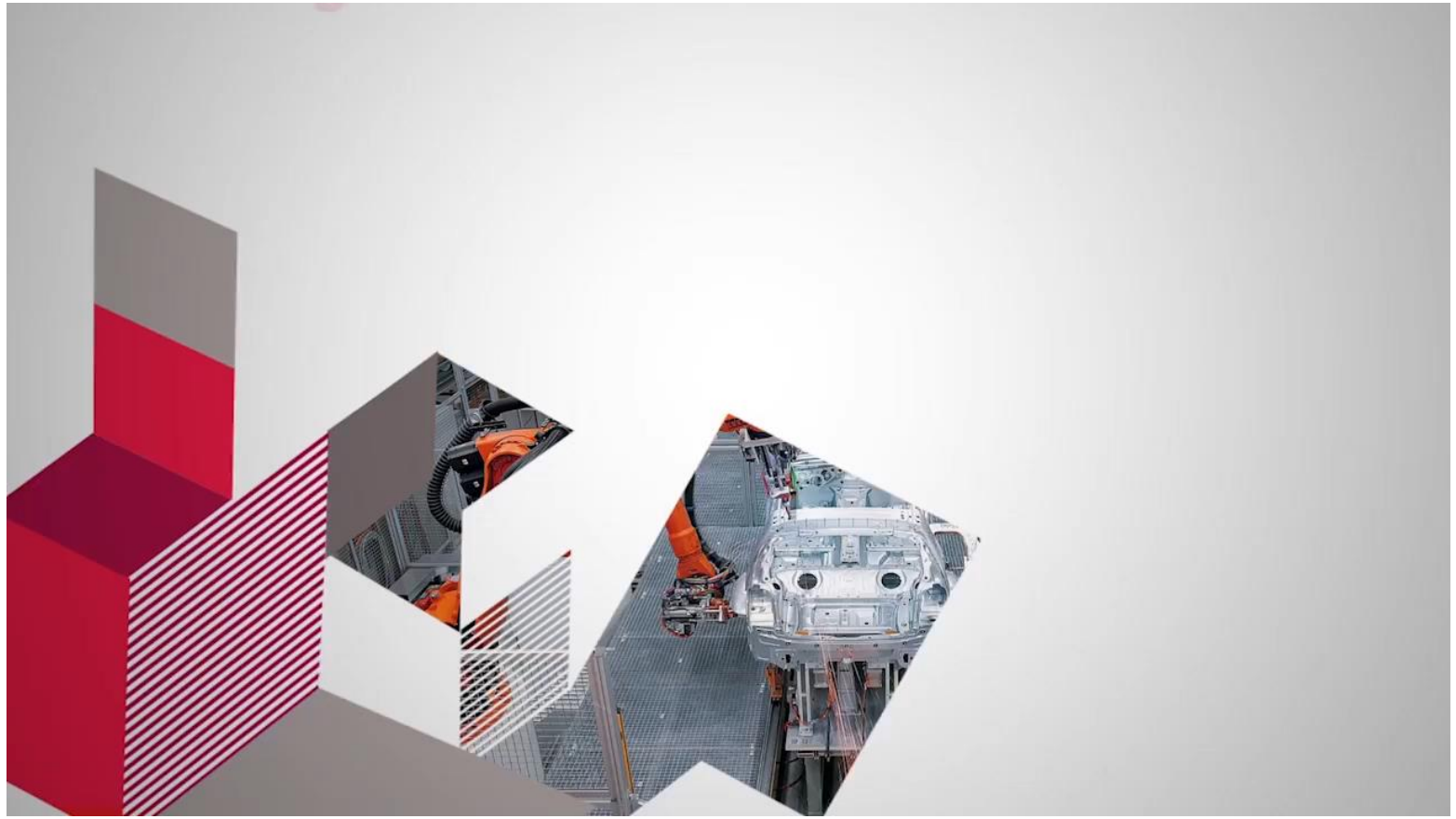
https://pt.slideshare.net/vsr0001/4th-industrial-revolution-is-beyond-cyber-physical-systems

Co-funded by the Erasmus+ Programme of the European Union

EVOLUTION OF CPS

Digital Factory

- **Industry 4.0 based on CPS**



https://www.youtube.com/watch?v=04GnNgWhv5c&t=12s

Co-funded by the
Erasmus+ Programme
of the European Union

CPS Difference from software and embedded systems

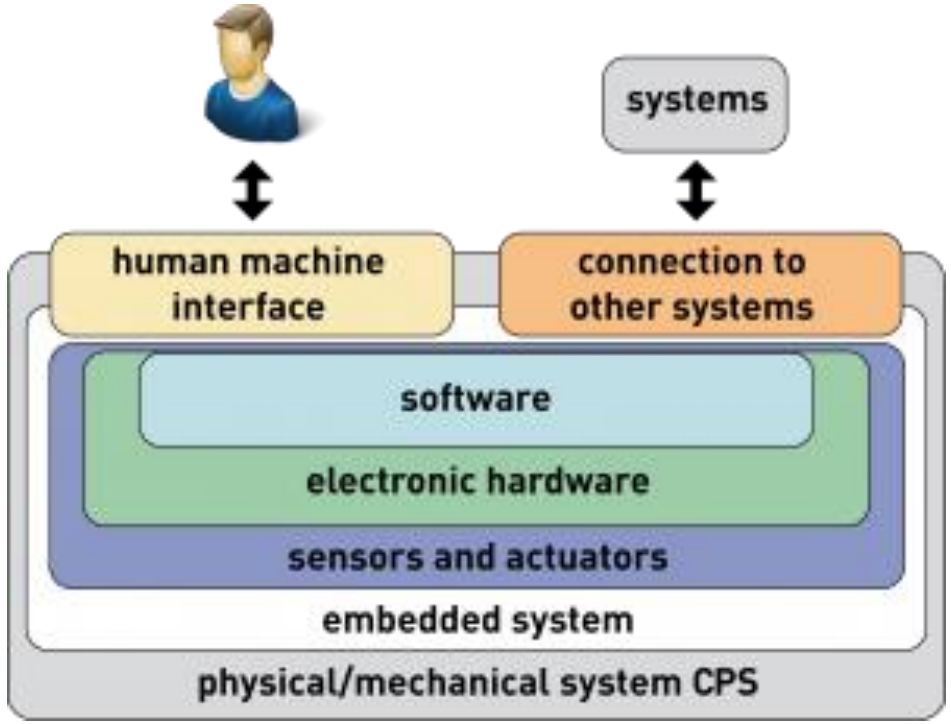
- **Where CPS Differs from General-Purpose Software Systems?**

Software Systems Problem:

- Software systems are sets of interacting sequences of state transformations with the end objective of transforming data

The CPS problem:

- CPS has the end objective of orchestrating physical processes. Timeliness, safety, reliability, security, privacy, and adaptability all take on a different character



http://addi-data.com/cps-cyber-physical-systems/

Co-funded by the Erasmus+ Programme of the European Union

CPS Difference from software and embedded systems

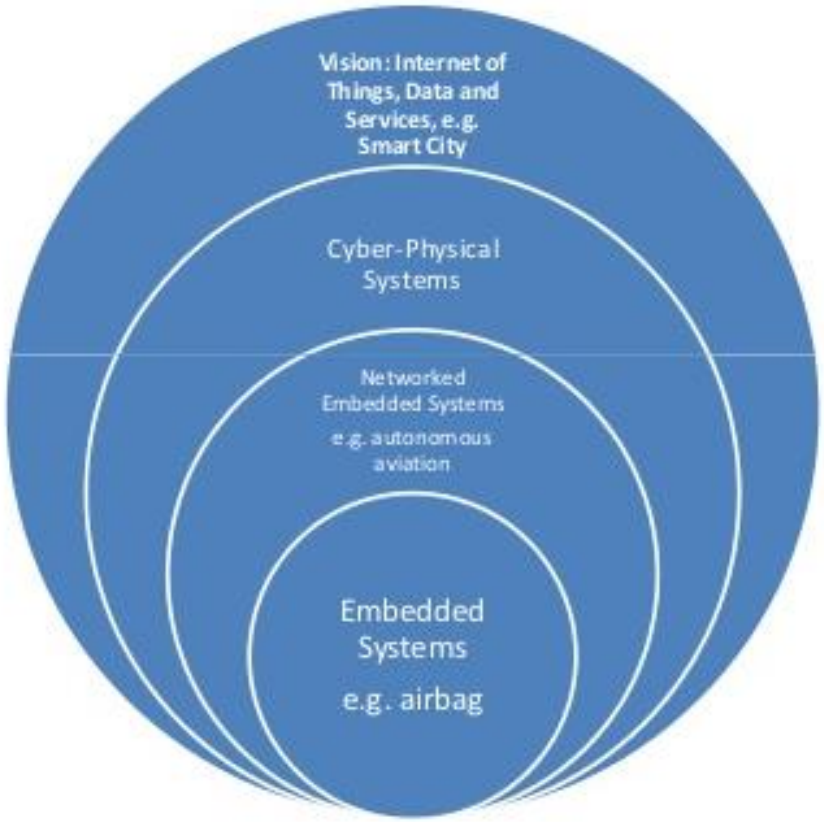
- **Where CPS Differs from Embedded Systems**

The embedded systems problem:

- Embedded software is software on small computers. The technical problem is one of optimization (coping with limited resources)

The CPS problem:

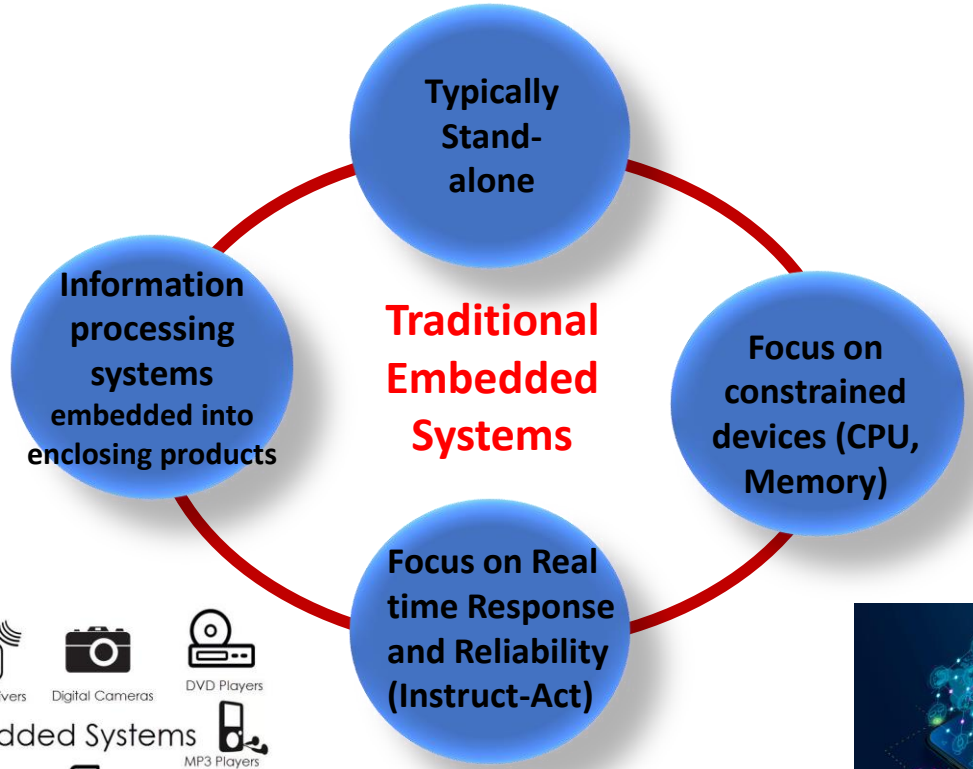
- Computation and networking integrated with physical processes. The technical problem is managing time and concurrency in networked computational systems

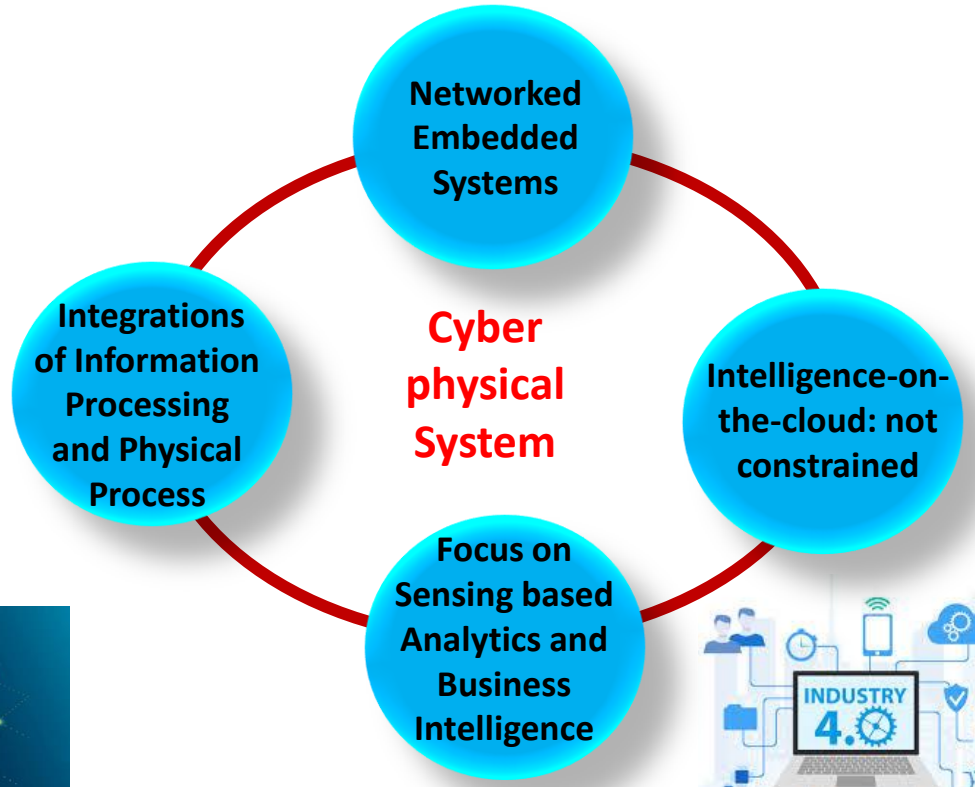


Co-funded by the Erasmus+ Programme of the European Union

CPS Difference from software and embedded systems

- **Traditional Embedded Systems vs. Cyber physical System**



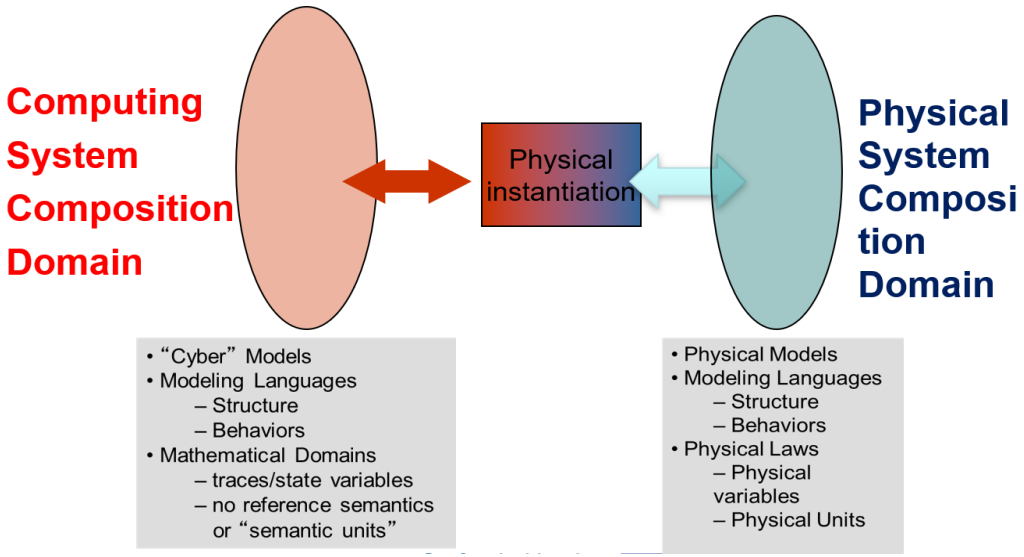


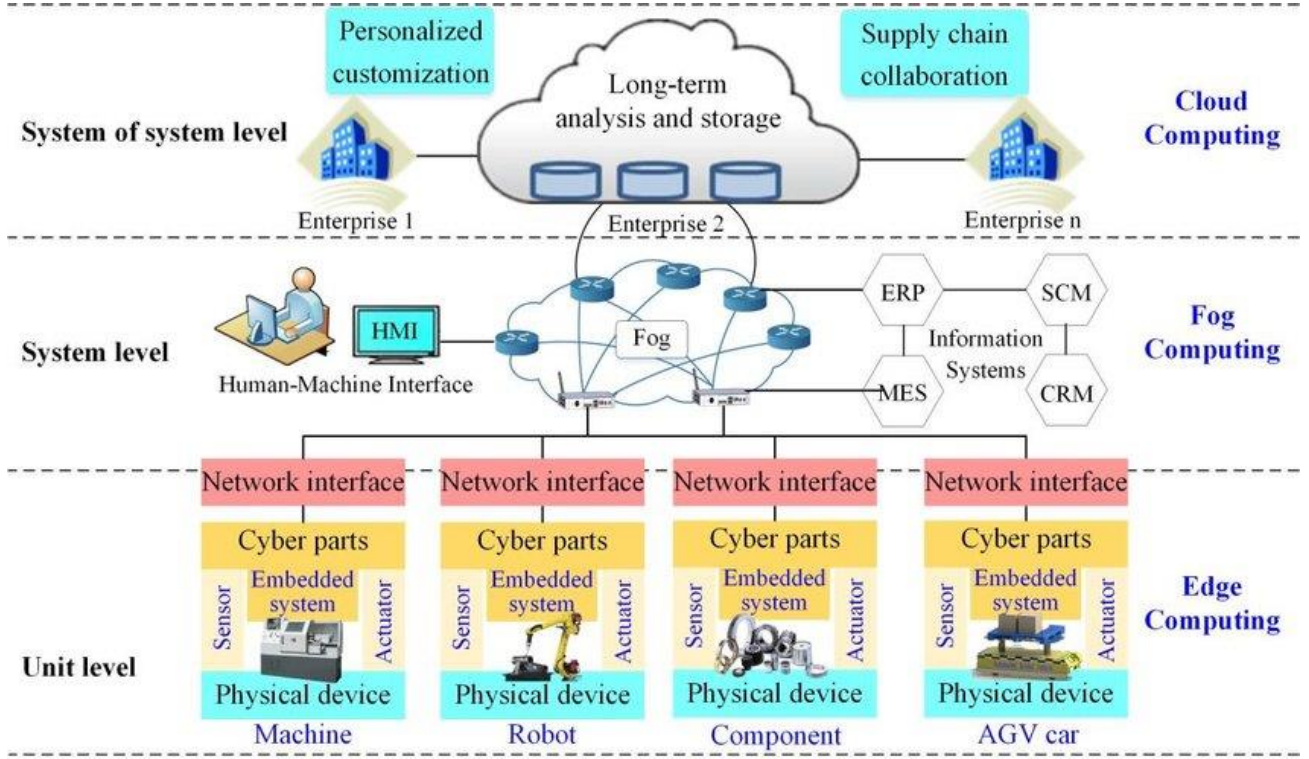
From Embedded ..... Towards CPS

Co-funded by the Erasmus+ Programme of the European Union

Heterogeneity and Modeling

Digital Factory





https://www.researchgate.net/figure/Modeling-of-various-levels-CPS-and-DT-in-manufacturing-based-on-edge-computing-fog_fig1_327856531

Co-funded by the Erasmus+ Programme of the European Union

Long-Term Goal OF CPS

- **Transform how we interact with the physical world just like the internet transformed how we interact with one another.**
  - *Convergence of embedded systems, control theory, hybrid systems, microcontrollers, sensor, actuators, wireless networks, wide area networks, distributed systems, operating systems, advances in structures*

- Building CPSs that integrate computational and physical objects requires **new systems science foundations.**
  - *Fusion of physical and computational sciences*

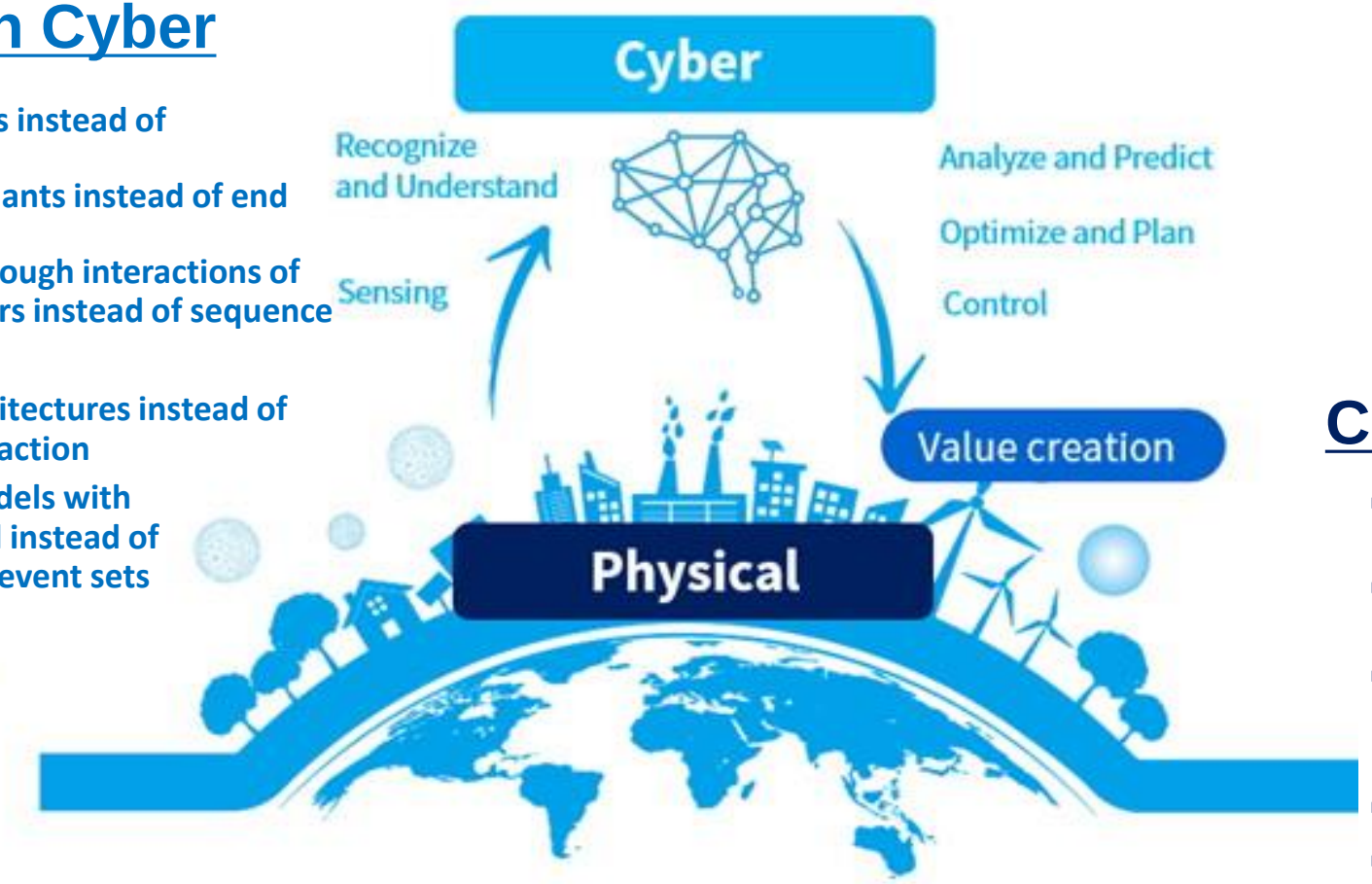
Co-funded by the
Erasmus+ Programme
of the European Union

Upgradation Interaction & Coordination

Digital Factory

Changes in Cyber

- Rich time models instead of sequencing
- Behavioral invariants instead of end results
- Functionality through interactions of ongoing behaviors instead of sequence of actions
- Component architectures instead of procedural abstraction
- Concurrency models with partially ordered instead of linearly ordered event sets



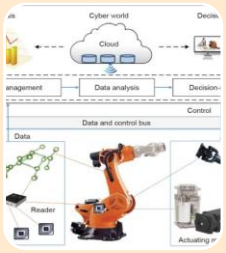
Changes in Physical

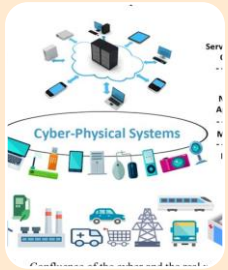
- Precise interaction and coordination protocols
- Hugely increased system size with controllable, stable behavior
- Dynamic system architectures (nature and extent of interaction can be modified)
- Adaptive, autonomic behavior
- **Self-descriptive, self monitoring system architecture for safety guarantees.**

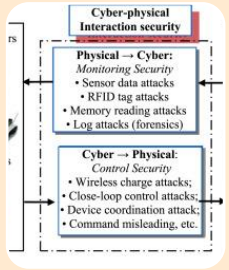
Co-funded by the Erasmus+ Programme of the European Union

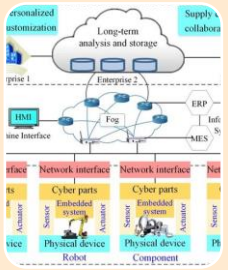
Scientific and technical challenges

Digital Factory









Integrating complex, heterogeneous large-scale systems

Interaction between humans and systems

Dealing with uncertainty

Measuring and verifying system performance

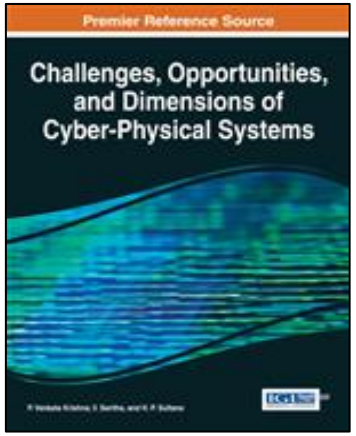
System design

Co-funded by the Erasmus+ Programme of the European Union

Design process of CPS

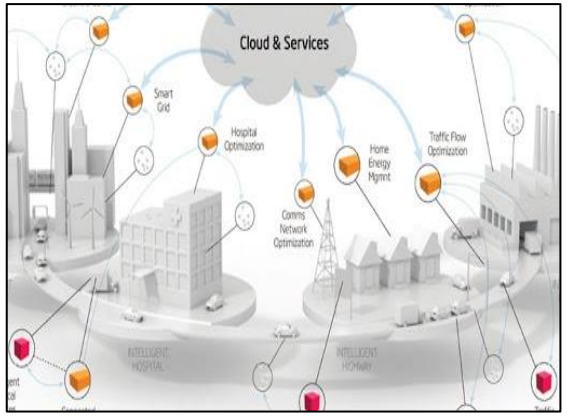
Digital Factory

Phase 1
- Application knowledge

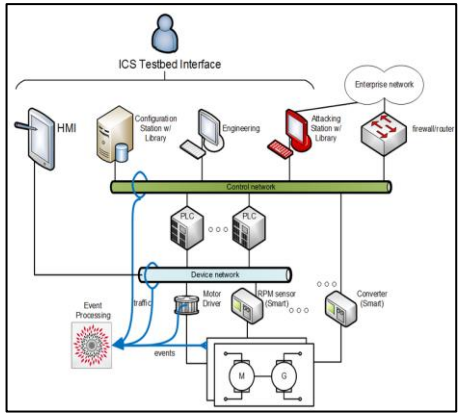


Phase 2
- Specification
- Hardware/Software components

Phase 3
- Design repository
- Application mapping



Phase 4
- Design
- Test

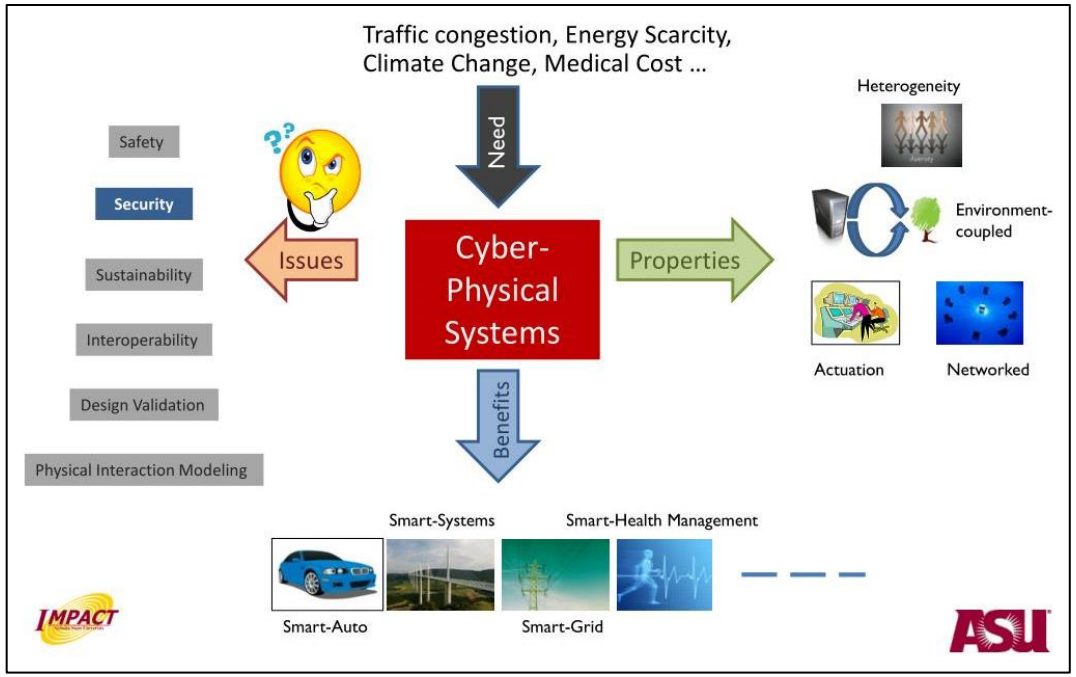


Co-funded by the Erasmus+ Programme of the European Union

Scientific and technical challenges

Digital Factory

- **Compositionality: system-level properties can be computed from local properties of components**
- **Composability: component properties are not changing as a result of interactions with other components.**
- **Heterogeneity CPS are heterogeneous in components and design requirements.**
- **CPS products make design flows product specific which is bad for design automation.**
- **COST: The cost of certification of complex systems is high.**
- **Security: issues. One side can be attacked through the other side.**

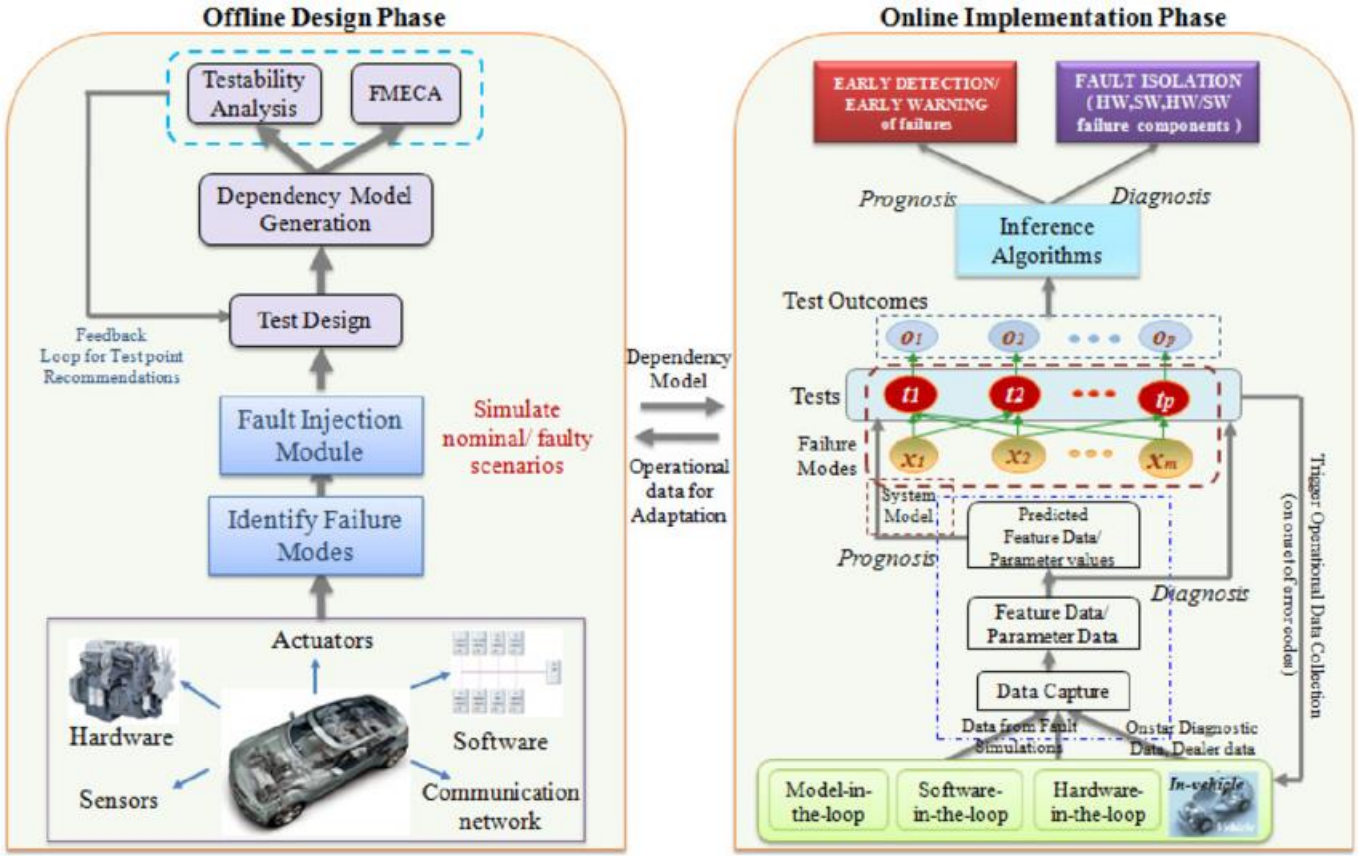


Co-funded by the Erasmus+ Programme of the European Union

Challenges for CPS software design

Digital Factory

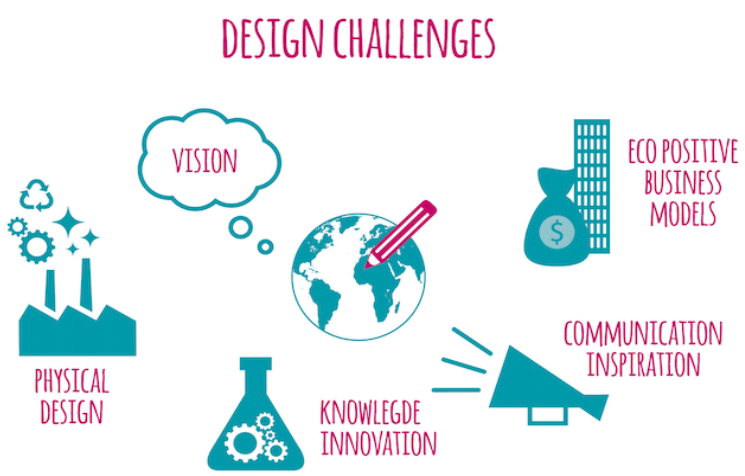
- Dynamic environments
- Capture the required behavior
- Validate specifications
- Efficient translation of specifications into implementations
- How can we check that we meet real-time constraints?
- How do we validate embedded real-time software? – large volumes of data – testing may be safety-critical

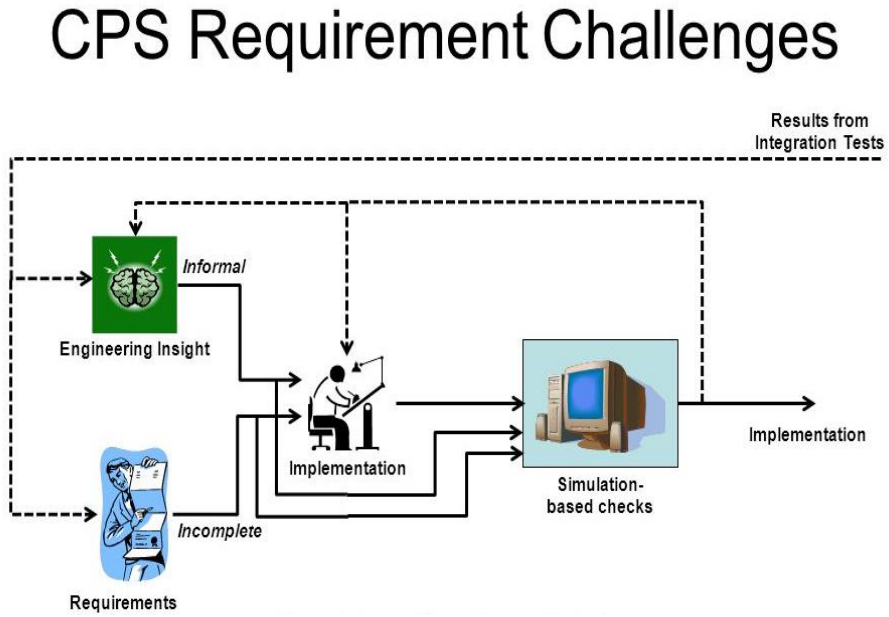


Co-funded by the Erasmus+ Programme of the European Union

Expectations and design challenges of CPS

- Dependability
- Efficiency
- Meeting real-time requirements
- Hardware properties, physical environment

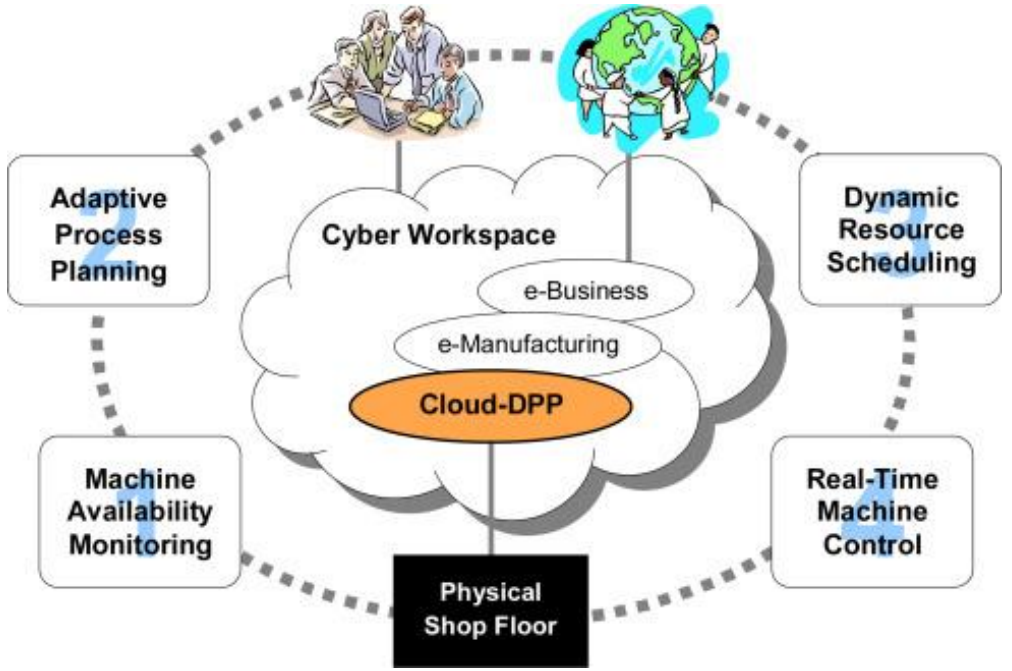




Co-funded by the Erasmus+ Programme of the European Union

Institutional, societal, and other challenges

- ❑ Trust, security, and privacy
- ❑ Effective models of governance
- ❑ Creation of CPS business models
- ❑ Understanding the value of CPS



Co-funded by the Erasmus+ Programme of the European Union

The Challenge of Physical World

Digital Factory

- **Physical world & Industry 4.0**

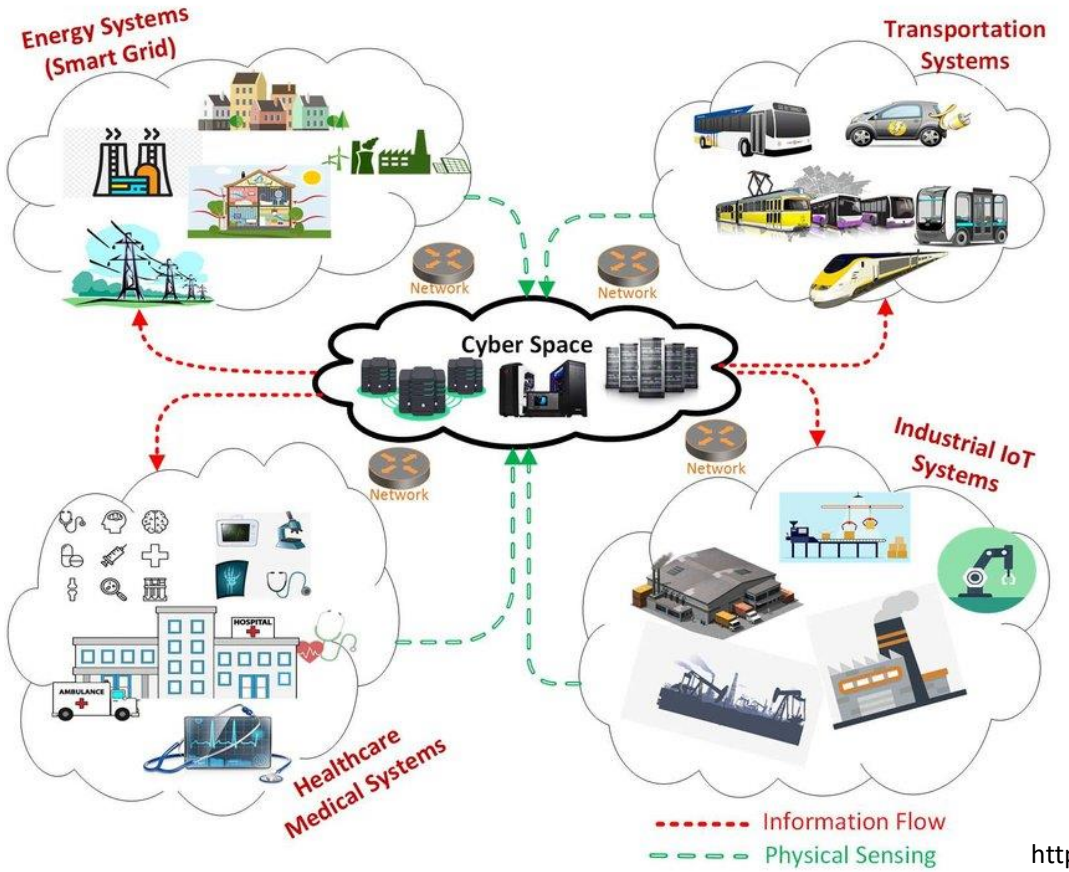
https://www.youtube.com/watch?v=ktcRXyE8SaY

Co-funded by the
Erasmus+ Programme
of the European Union

Application

Digital Factory

- **Applications of CPS**



https://www.researchgate.net/figure/Application-Scenarios-of-cyber-physical-systems-describing-the-information-flow-and_fig2_329466954

Co-funded by the
Erasmus+ Programme
of the European Union

Application

Digital Factory

- **Applications of CPS**

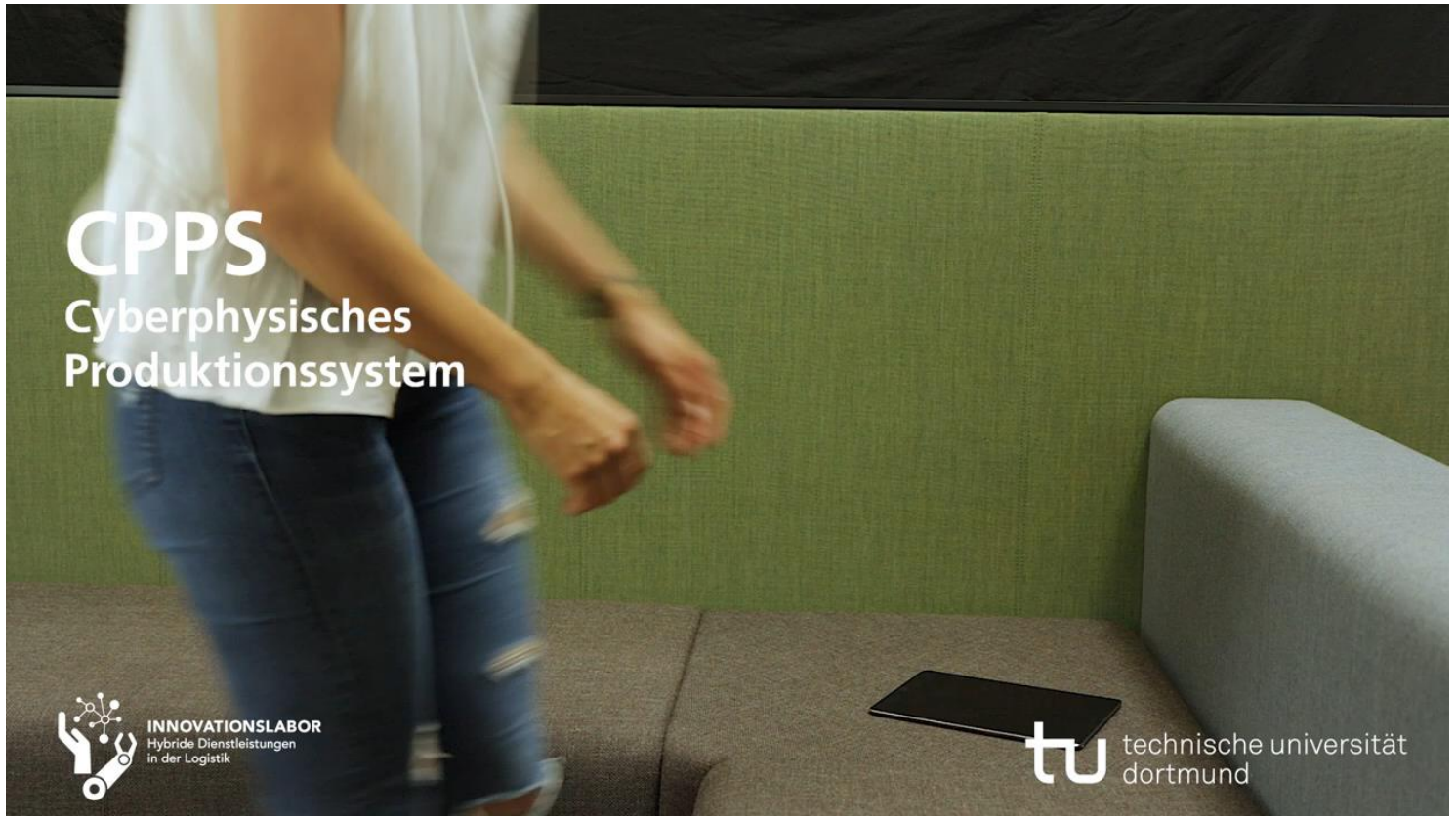
https://www.youtube.com/watch?v=wro3uoHR-ZY&t=13s

Co-funded by the
Erasmus+ Programme
of the European Union

Application

Digital Factory

- **Applications of CPS on production line**



https://www.youtube.com/watch?v=RNCgnZ4Z44I&t=36s

Co-funded by the
Erasmus+ Programme
of the European Union

Application

Digital Factory

- **Applications of CPS : Cyber Physical System based Proactive Collaborative Maintenance**

https://www.youtube.com/watch?v=sHiVEi1BZ0o

Co-funded by the Erasmus+ Programme of the European Union

Application

Digital Factory

- **Applications of CPS for Industry 4.0**

https://www.youtube.com/watch?v=hjKC-XhwU1E

Co-funded by the
Erasmus+ Programme
of the European Union

Application

- **Applications of CPS**

https://www.youtube.com/watch?v=raZIpxnjmJs

Co-funded by the
Erasmus+ Programme
of the European Union

Application

Digital Factory

- **CPS on Smart factory**

https://www.youtube.com/watch?v=Ropu4FwMEHo

Co-funded by the
Erasmus+ Programme
of the European Union

Application

- **Applications of CPS : The Internet of Things**

https://www.youtube.com/watch?v=5OQQZ9eWF-4&t=84s

Co-funded by the
Erasmus+ Programme
of the European Union

Application

Digital Factory

- **Applications of CPS**

Health Care and Medicine

Hospital : Real time monitoring and control can be achieved by Data Management Module and Service awareness module which also plays an important role in order to provide QoS monitoring. While designing a system for hospital, sensitive applications are queued on the top priority.

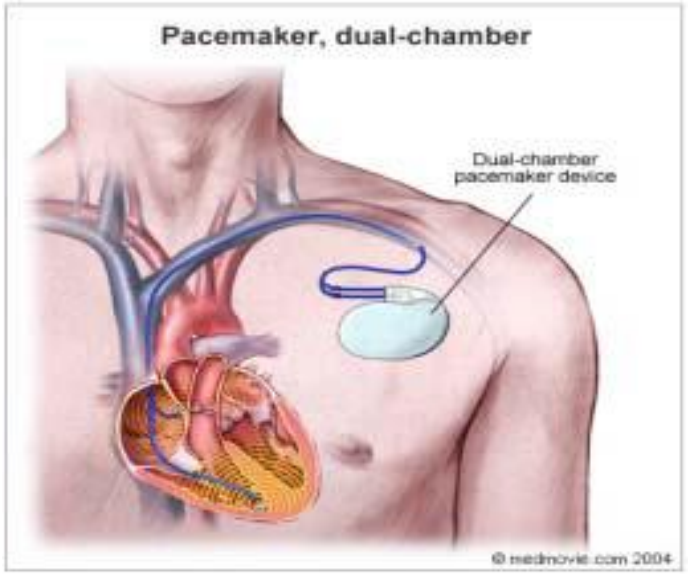
- **Home care: monitoring and control**

  Blood glucose monitors, infusion pumps, accelerometers

- **Operating Room of the Future**

  Robotic Microsurgery

- **Progress in bioinformatics: gene, protein expression, systems biology, disease dynamics, control mechanisms**



Co-funded by the Erasmus+ Programme of the European Union

Application

- **Applications of CPS**

Electric Power Grid

- ***Current picture:***

  Equipment protection devices trip locally, reactively

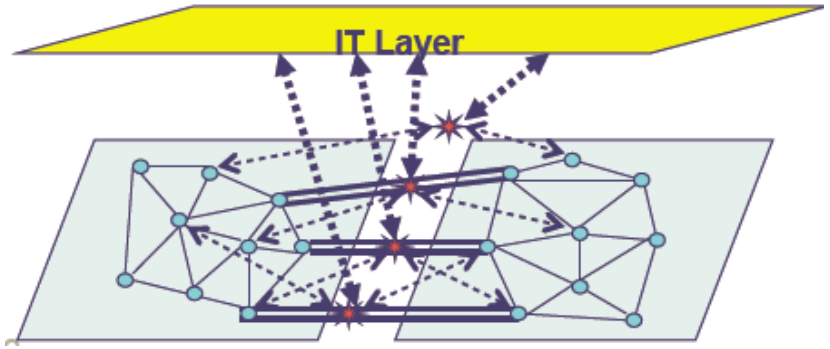
  Cascading failure

- ***Better future?***

  Real-time cooperative control of protection devices

  Self-healing, aggregate islands of stable bulk power

  Coordinate distributed and dynamically interacting participants



Co-funded by the
Erasmus+ Programme
of the European Union

Security and Privacy Issues in Cyber-Physical Systems

- **Differences between corporate IT security and CPS security**

  - ❑ **Software patching and frequent updates, are not well suited for control systems**
  - ❑ **While availability is a well studied problem in information security, real-time availability provides a stricter operational environment than most traditional IT systems**
  - ❑ **Large industrial control systems also have a large amount of legacy systems** (most of the efforts done for legacy systems should be considered as short-term solutions; underlying technology must satisfy some minimum performance)
  - ❑ **Network dynamic**

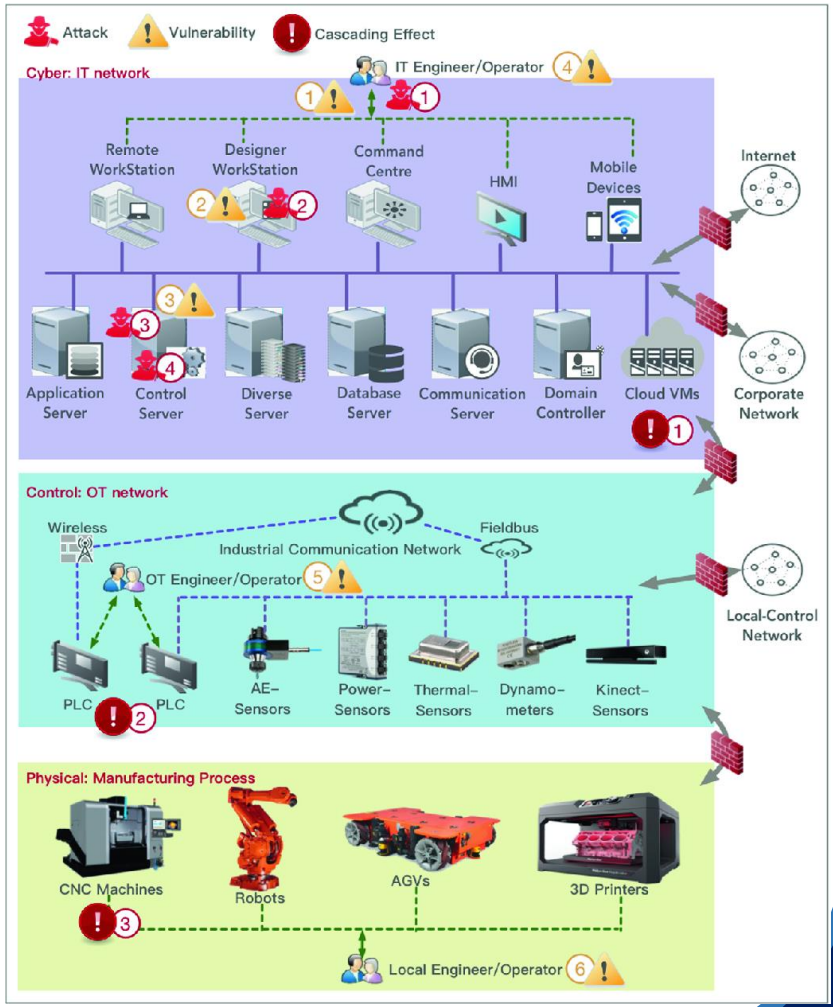
https://www.youtube.com/watch?v=_6IZ5yCYwx8

Co-funded by the Erasmus+ Programme of the European Union

Security and Privacy Issues in Cyber-Physical Systems

Digital Factory

- **New security problem in CPS/Control systems**
  - ❑ **Authentication, access control, message integrity, separation of privilege, etc. can all help**
    - Traditionally focused on information (security)
  - ❑ **How attacks affect the estimation and control algorithms?**
    - Ultimately, how attacks affect the physical world
  - ❑ **Intrusion Detection Systems (IDSs) have not considered algorithms for detecting deception attacks launched by compromised sensor nodes against estimation and control algorithms**
    - Dynamics of physical systems bring more challenges and set of problems
  - ❑ **Information awareness to operators of control systems**



Co-funded by the Erasmus+ Programme of the European Union

Security and Privacy Issues in Cyber-Physical Systems

- **Cyberspace and Cybersecurity**

https://www.youtube.com/watch?v=3Wq4S2pXD3c&t=133s

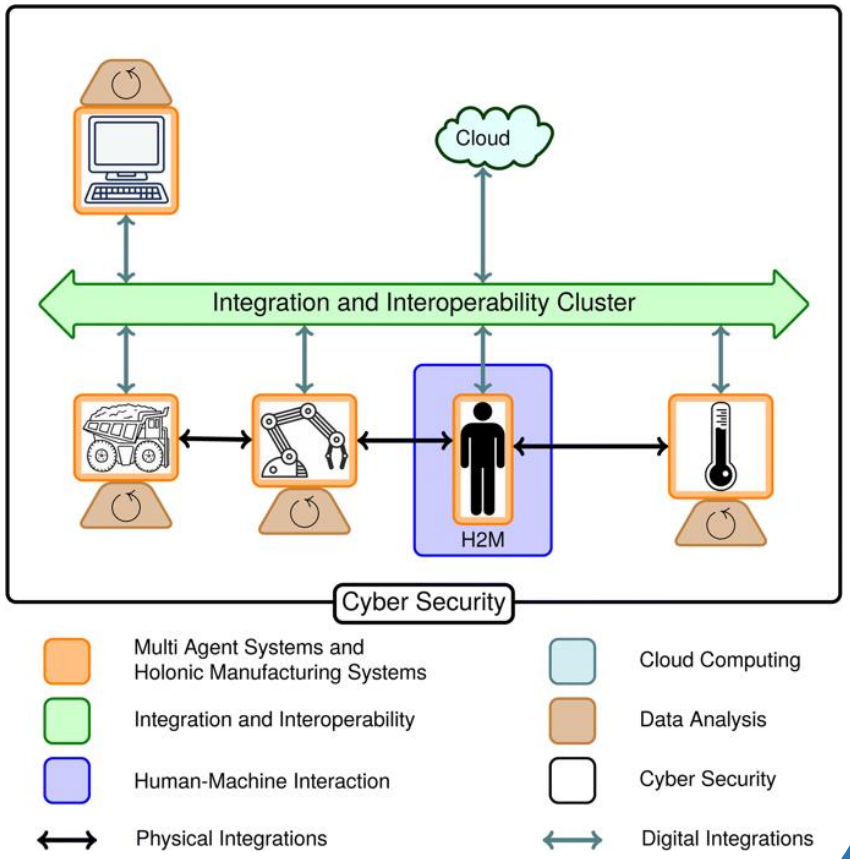
Co-funded by the Erasmus+ Programme of the European Union

Security and Privacy Issues in Cyber-Physical Systems

- **Countermeasures**

  - **Most of the effort for protecting control systems has focused on reliability (the protection of the system against random faults)**
    - urgent growing concern for protecting control

  - **systems against malicious cyber attacks**
    - Dimensions
    - Prevention
    - Detection and recovery
    - Resilience
    - Deterrence

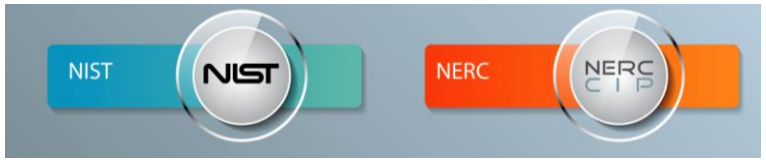


Co-funded by the Erasmus+ Programme of the European Union

Security and Privacy Issues in Cyber-Physical Systems

- **Prevention**
  - ❖ **cybersecurity standards**
    - ❑ **North American Electric Corporation (NERC) cybersecurity standards for electric systems.**
      - ***NERC*** *is authorized to enforce compliance to these standards, and it is expected that all electric utilities are fully compliant with these standards*
    - ❑ **NIST**
      - **SP 800-53*** the guideline for security best practices which federal agencies should meet
      - **Guide to Industrial Control System (ICS) Security**
    - ❑ **ISA (International Society of Automation)**
      - **ISA SP 99**: a security standard to be used in manufacturing and general industrial controls
    - ❑ **ETSI**
  - ❖ **SCADA - Supervisory Control And Data Acquisition**

    Standardization efforts with respect to access control and key management in wireless sensor networks



ISA 99 / IEC 62443 standard

ISA IEC

ICS/SCADA Security

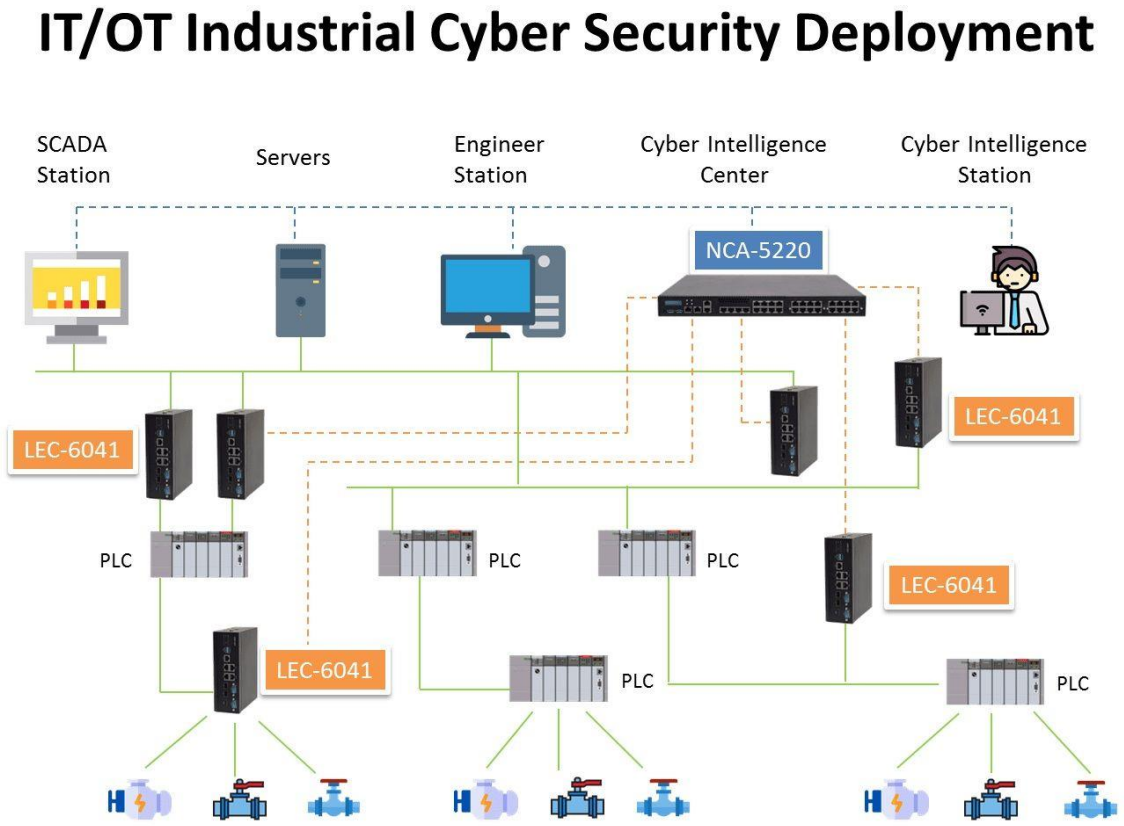
ETSI

* **NIST** Special Publication 800-53, *"Security and Privacy Controls for Federal Information Systems and Organizations,"*

Co-funded by the Erasmus+ Programme of the European Union

Security and Privacy Issues in Cyber-Physical Systems

- **Example of Prevention with SCADA**



Co-funded by the Erasmus+ Programme of the European Union

Security and Privacy Issues in Cyber-Physical Systems

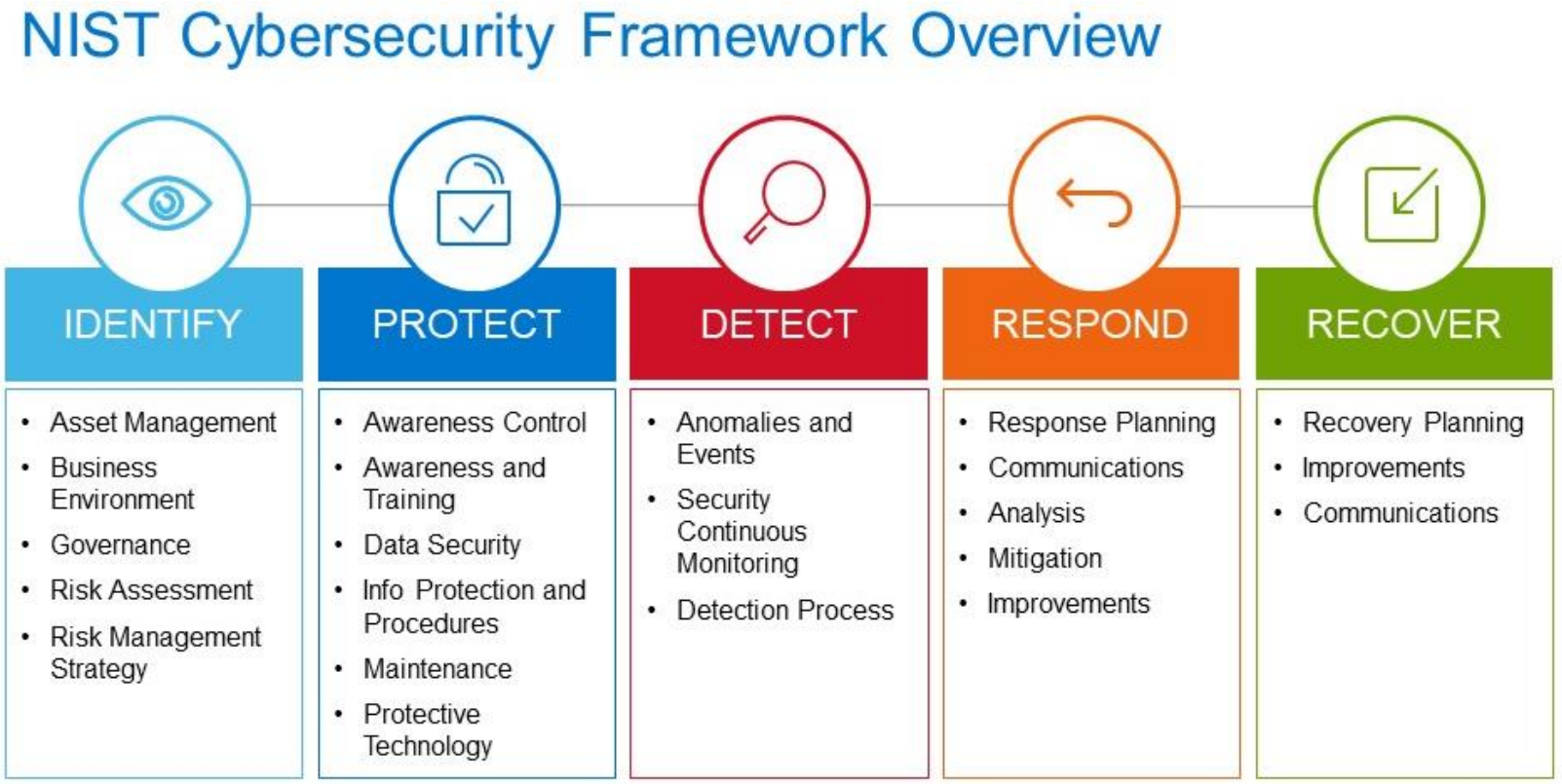
- **Detection and recovery**
  - **Utilizing our knowledge of the physical systems, control systems** can provide a paradigm shift for intrusion detection e.g. by monitoring the physical system for anomalies we may be able to detect attacks that are undetectable from the IT side, e.g. against resonance attack
  - **Identify deception attacks launched by compromised** controllers and/or sensors
  - **Implement a model-based detection scheme,** e.g. as game between the detector and the attacker
  - **Utilizing ideas from control theory** such as reconfiguration or fault-detection and isolation, to design autonomous and real-time detection and response algorithms for safety-critical applications that require real-time responses

https://www.slideshare.net/exigent/how-to-implement-nist-cybersecurity-standards-in-my-organization-125956627

Co-funded by the Erasmus+ Programme of the European Union

Security and Privacy Issues in Cyber-Physical Systems

- **Example of NIST Standard**

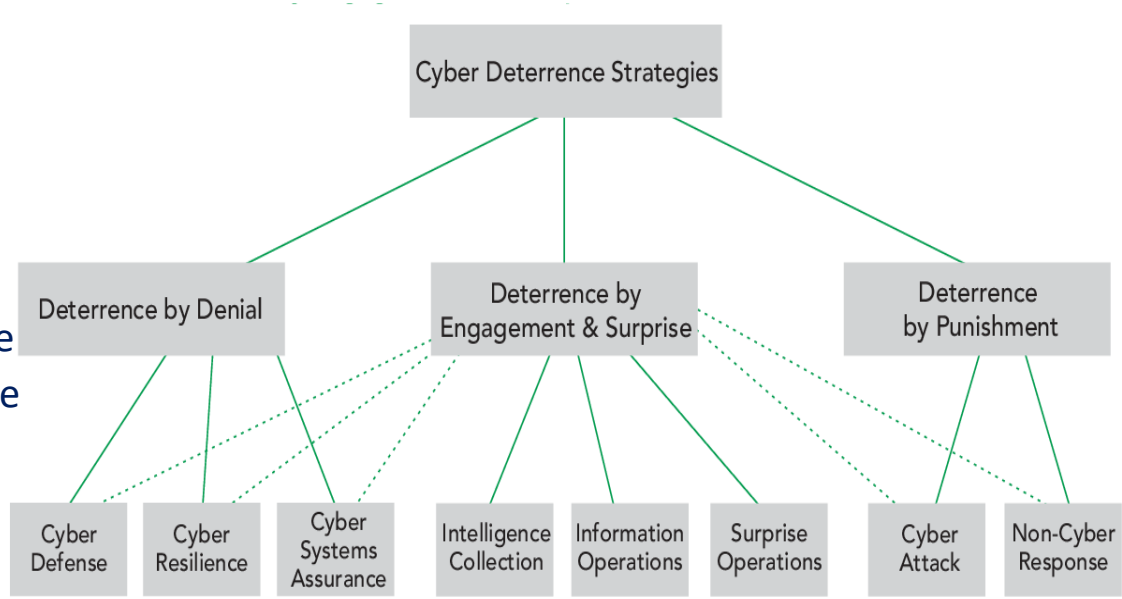


https://infocus.delltechnologies.com/michael_dulavitz/strengthen-security-of-your-data-center-with-the-nist-cybersecurity-framework/

Co-funded by the Erasmus+ Programme of the European Union

Security and Privacy Issues in Cyber-Physical Systems

- **Resilience and deterrence**
  - **Useful principles**
    - Redundancy as a way to prevent a single-point of failure
    - Diversity as a way to prevent that a single attack vector can compromise all the replicas (the added redundancy)
    - Principle of least-privilege, and the separation of privilege (also known as separation of duty) principle
  - **In CPS**, **physical and analytical redundancies** should be combined with security principles (e.g., diversity and separation of duty) to adapt or reschedule its operation during attacks
  - **Design novel robust control and estimation algorithms** that consider more realistic attack models from a security point-of-view, e.g. Game Theory
  - **Deterrence**

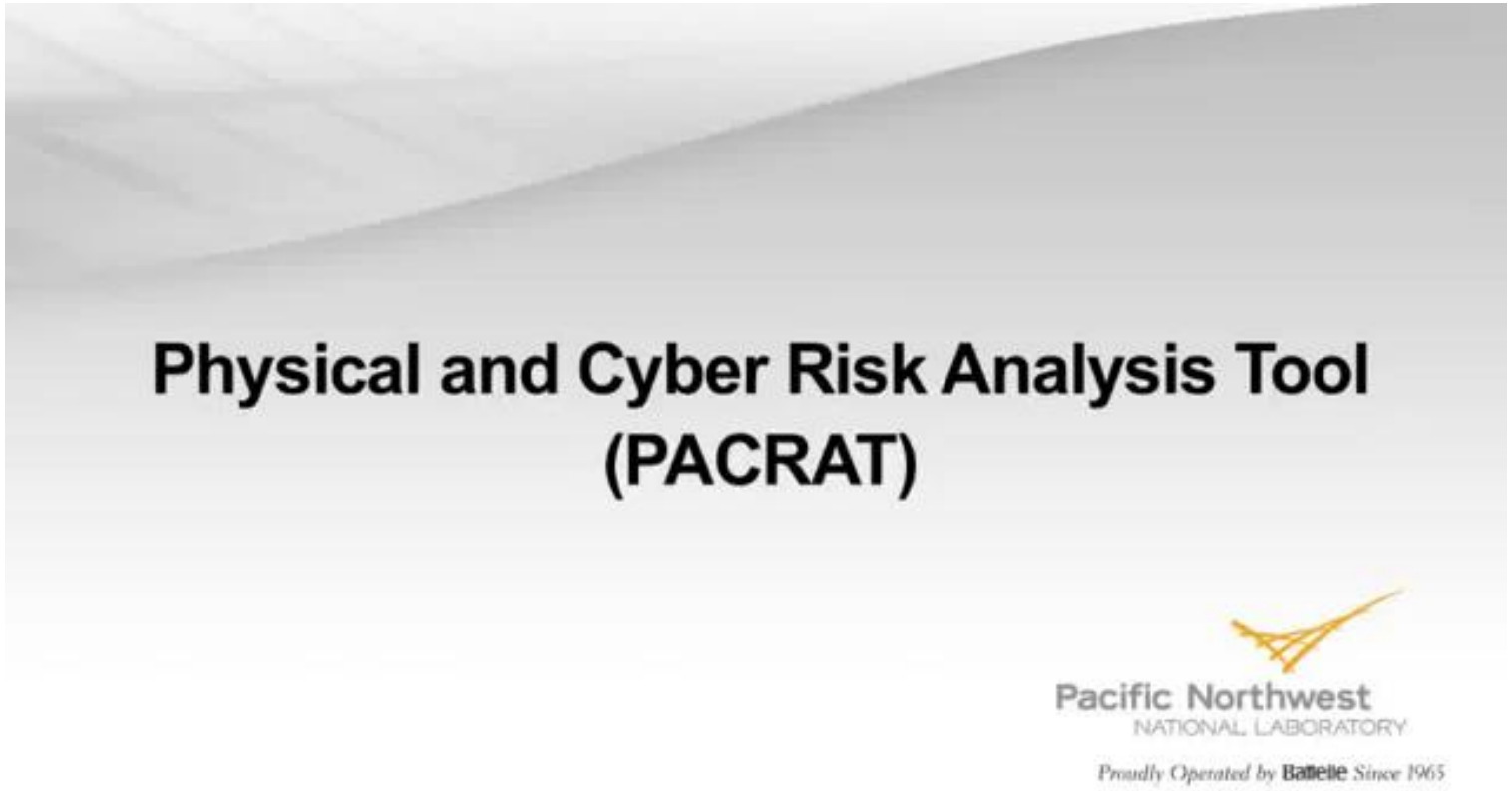


Co-funded by the Erasmus+ Programme of the European Union

Security and Privacy Issues in Cyber-Physical Systems

Digital Factory

- **Physical Protection & Cyber Security**



https://www.youtube.com/watch?v=Hh5NEpJZGZw&t=22s

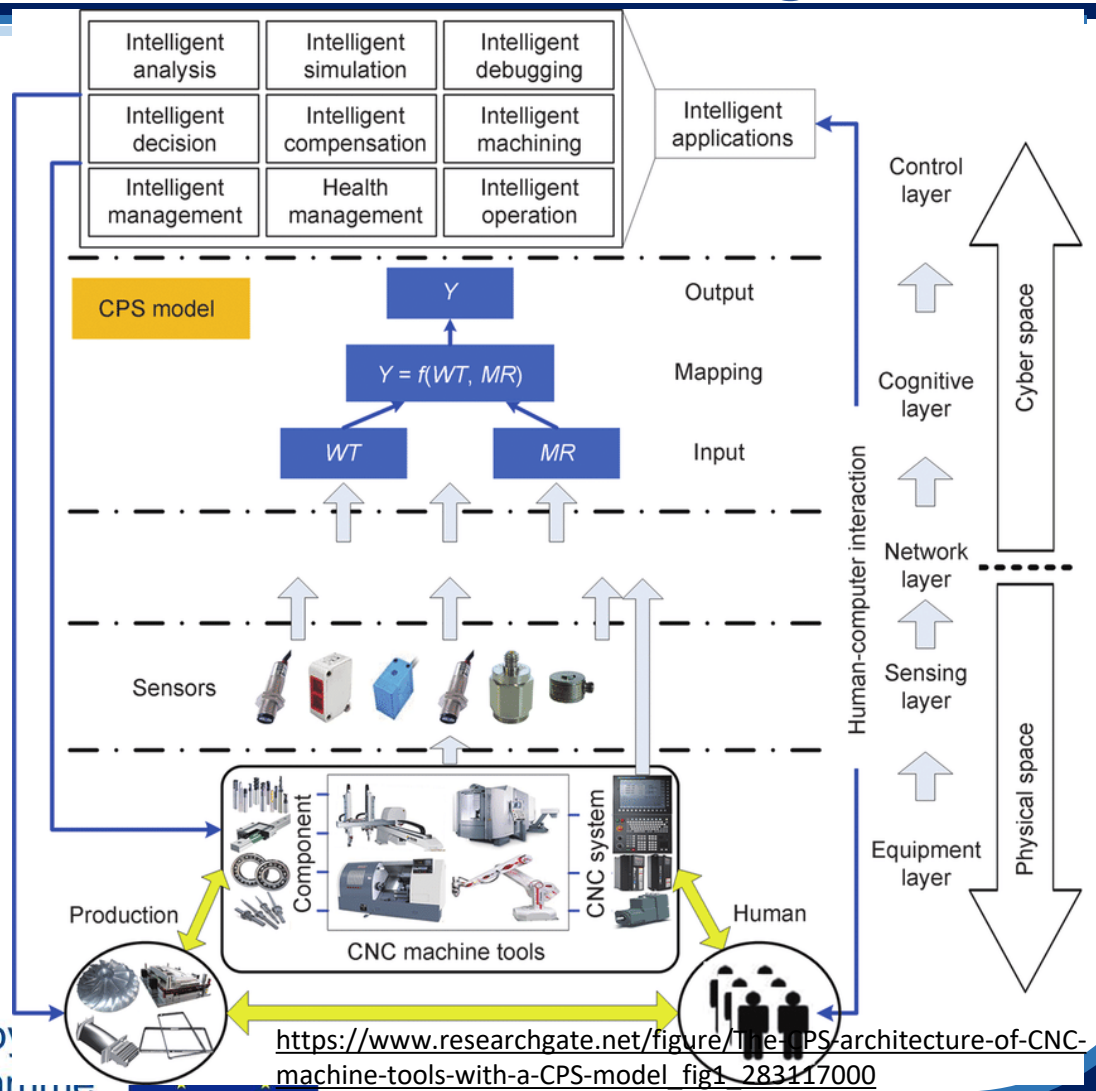
Co-funded by the Erasmus+ Programme of the European Union

Activities (Example)

Digital Factory

- **The-CPS-architecture-of-CNC-machine-tools-with-a-CPS-model**

https://www.researchgate.net/figure/CPS-enabled-Smart-Machine-Tools-After-the-smart-design-CPS-enabled-smart-machine-tools_fig3_322673524



https://www.researchgate.net/figure/The-CPS-architecture-of-CNC-machine-tools-with-a-CPS-model_fig1_283117000

Co-funded by the Erasmus+ Programme of the European Union

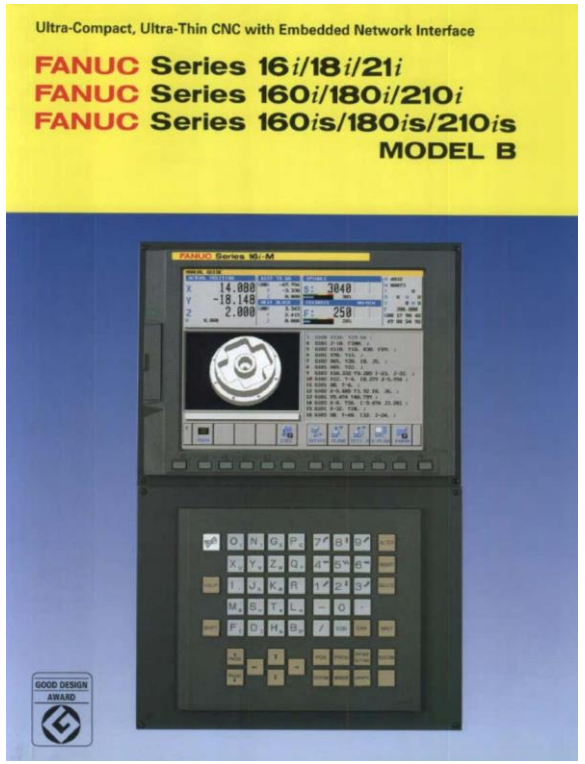
Activities (Lab sheet)

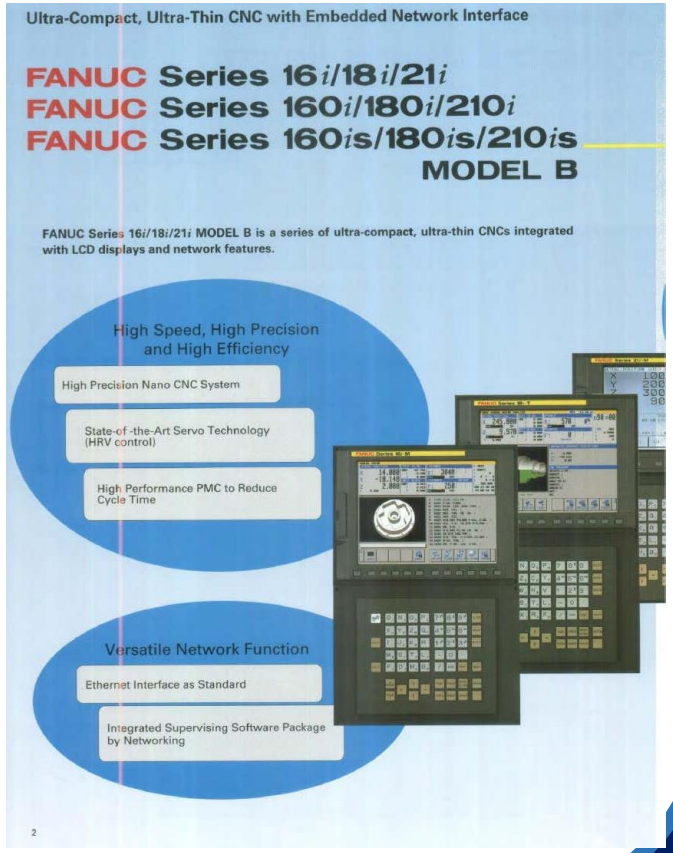
Digital Factory

- Design and development of a system for CNC turning to be in the form of Cyber-Physical Production Systems by writing architecture, data flow diagram and some available services. Streamlining process in the production line of CNC turning. Use data below:

CNC (Fanuc 18i)

- CNC/PMC
- FOCAS 1 Driver
- Sockets
(164.41.17.20:8193)



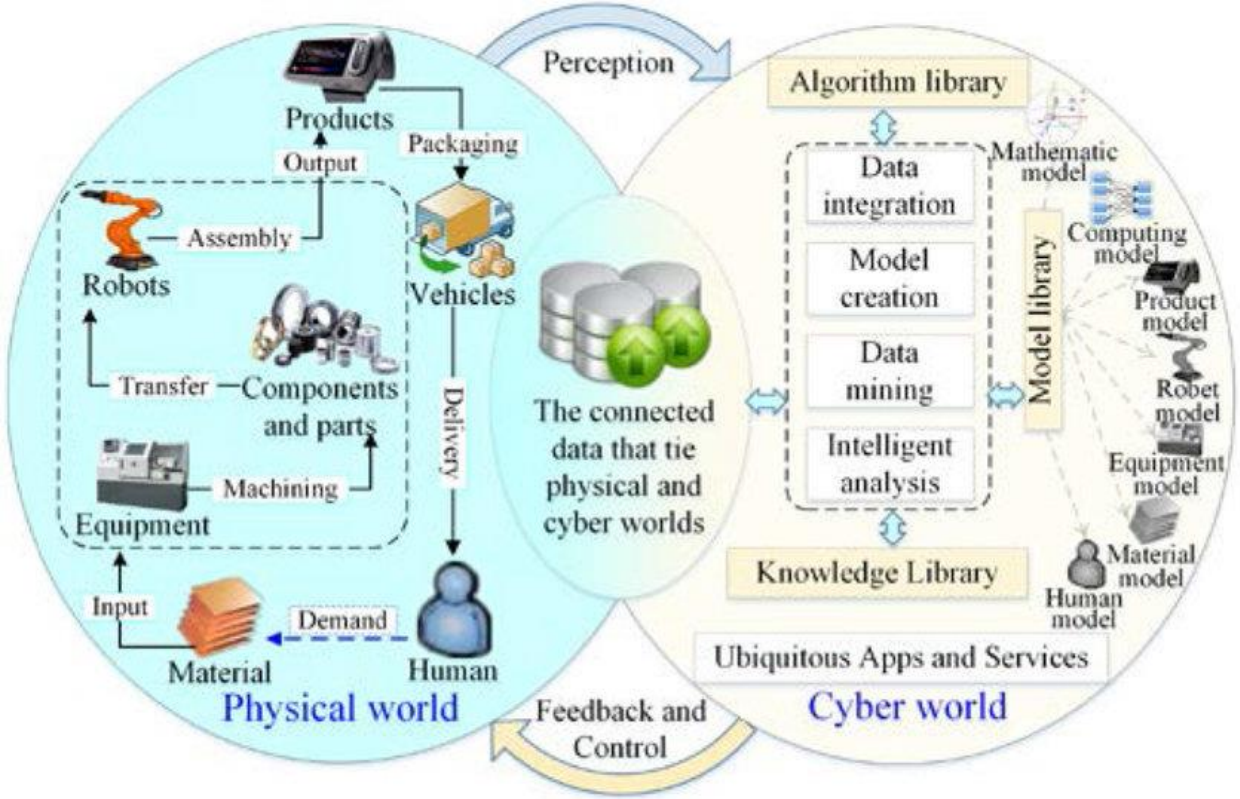


Co-funded by the Erasmus+ Programme of the European Union

Summary

Digital Factory

- **Cyber-physical systems** are everywhere, from semi-autonomous vehicles to wearable devices. These types of systems blend human and compute power, and integrating mechanical systems with human physical interaction giving both a form of **"super powers"**. Opportunities to specialize in cyber-physical systems are growing as quickly as the technology itself, from large corporations to individual makers ...
- CPS is the way to **streamlining process** in a production line of an existing traditional factory using a data flow diagram.



https://www.researchgate.net/figure/Manufacturing-cyber-physical-integration-and-fusion-supported-by-CPS-in-SoSM_fig6_318694164

Co-funded by the Erasmus+ Programme of the European Union

Learning Outcome

Digital Factory

Formulate a data model representing data streamlining in a production line of an existing traditional factory using a data flow diagram

Co-funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

Thank you