Industry4.0 – All Inclusive

«IoT, CPS e le nuove frontiere della intelligenza artificiale»

Modulo 4
CPS: progettazione ed implementazione

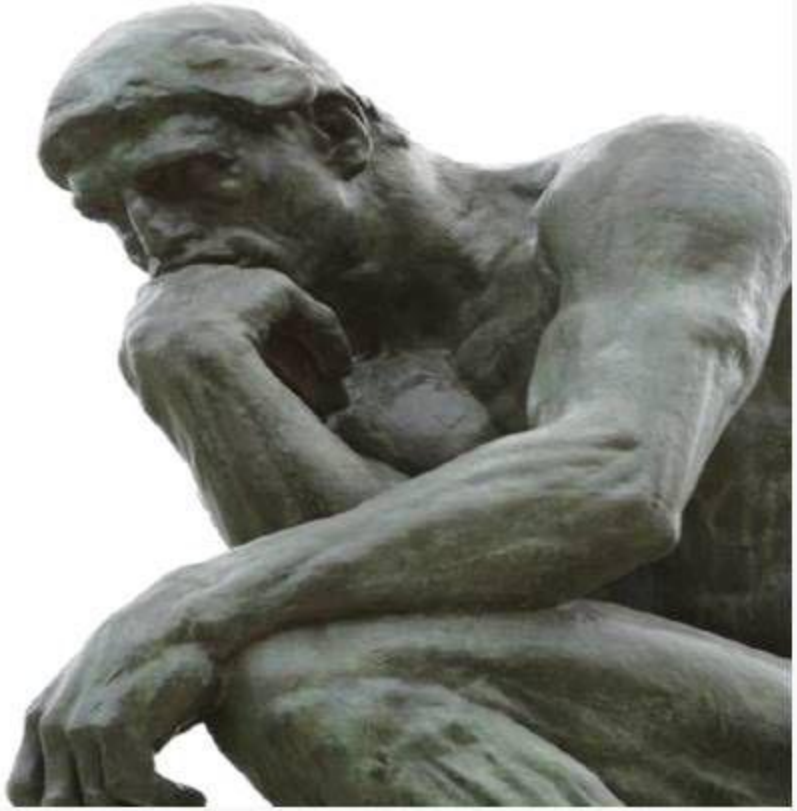
Alessandro Vizzarri

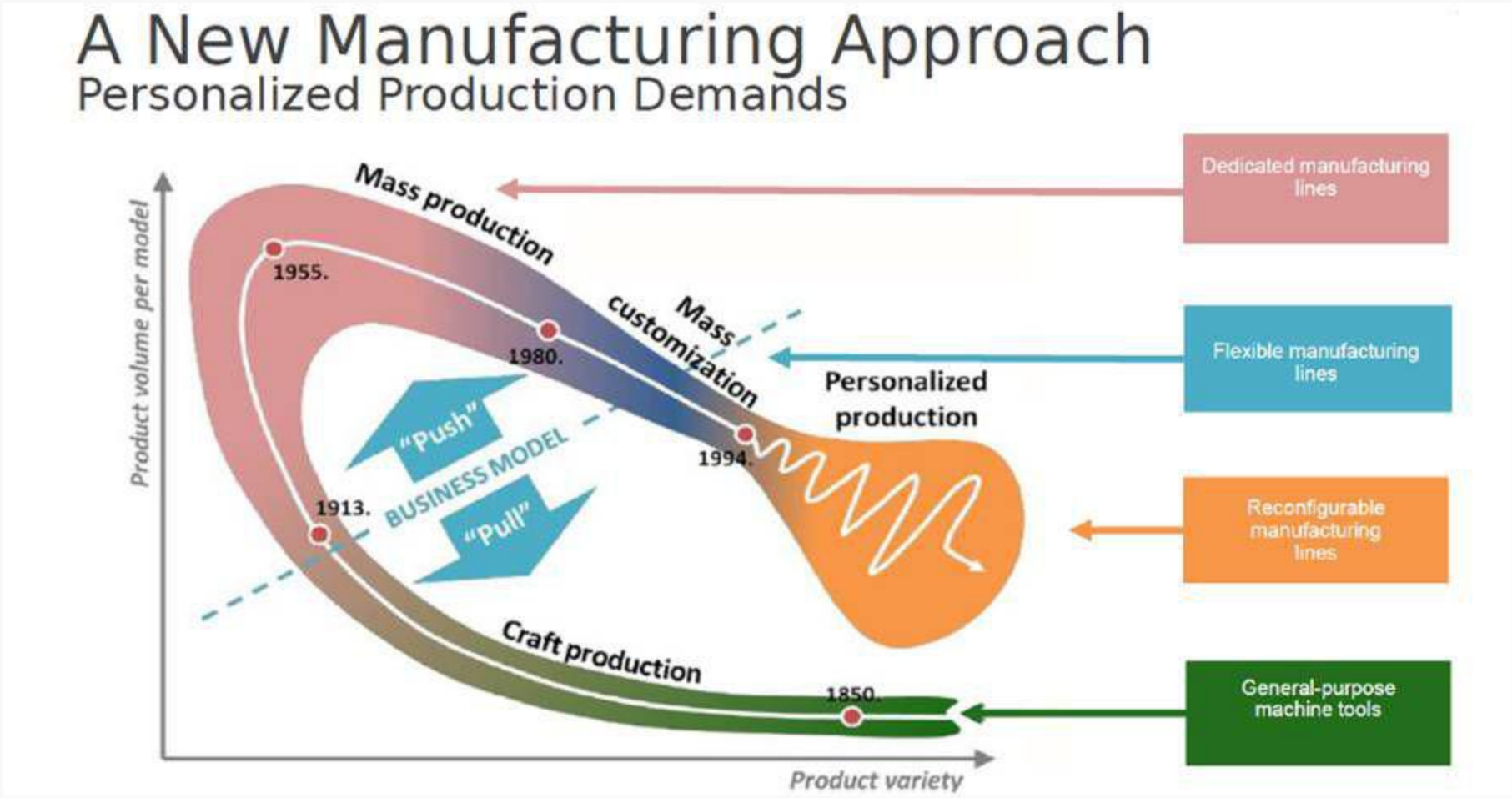
Dipartimento di Ingegneria dell'Impresa "Mario Lucertini"

Università di Roma "Tor Vergata"

Re-Thinking

- Products
- Value Add
- Business Model
- Business Processes





SOURCE: "Design of reconfigurable manufacturing systems", Journal of Manufacturing Systems, 2013 – Prof. Yoram Koren

Key Automation Trends

INVESTMENT OPTIMIZATION	AUTOMATION HIGH DENSITY	MATERIAL MANAGEMENT	INTEGRATED PRODUCT-PROCESS	ZERO DEFECTS
				
• Maximize Overall Equipment Effectiveness • Enhanced Virtual Commissioning • Minimize Production Cost	• Minimize Floor Space per Vehicle • Maximize Machine Modules Reuse • Minimize Plant Facility Construction Costs	• Transportation Cost • Minimize Path per Kitting • Minimize man hours/kitting • Minimize Implementation Time and Cost • Minimize Non-Value Added Activities	• Product-Process standard template • Non-Model Specific Architecture • Minimize Startup Time • Advanced Joining Technologies for Dissimilar Materials	• Minimize Scrap and Rework Costs • Minimize Defect Rates

(Fonte: Ing. Roberto Sabella, Quadrato della Radio, 2017)

Digital Factory Elements

Virtual industrialization

Virtual plants and products to prepare physical production via simulation, verification and physical mapping

Smart Robots & Machines

Multipurpose «intelligent» robots able to adapt, communicate, and interact with each other and with humans based on remote control

New quality of connectivity

Connection of digital and real worlds with constant exchange of information between machines, work pieces, systems and human beings

Big data and analytics

New methods to handle huge amounts of data and tap into the potential of cloud computing

Cyber-physical systems and marketplace

IT systems built around machines, storage systems and supplies linked up as CPS

Factory efficiency

Preventive and predictive maintenance; energy efficiency; decentralization and remotization; process reengineering

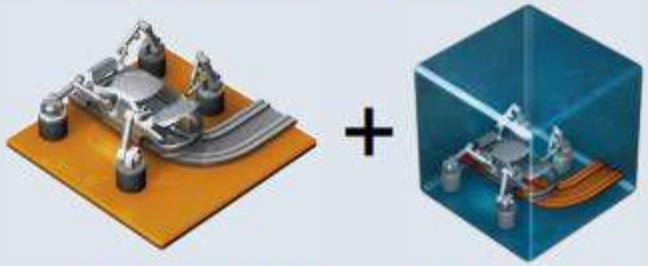
(Fonte: Ing. Roberto Sabella, Quadrato della Radio, 2017)

Progettazione di sistemi CPS

SIEMENS

Cyber-physical systems
have all the information as a digital model

Cyber-physical system (CPS)



Physical production facility + Digital model

Contains all the information on …

- Software / Informatics
- Mechanics,
- Electrics, Electronics
- Automation, HMI
- Safety, security
- Maintenance
- Location, identity…
- Status
- SW version
- Interfaces
- …

The digital model is always up-to-date and is extended over the entire lifecycle

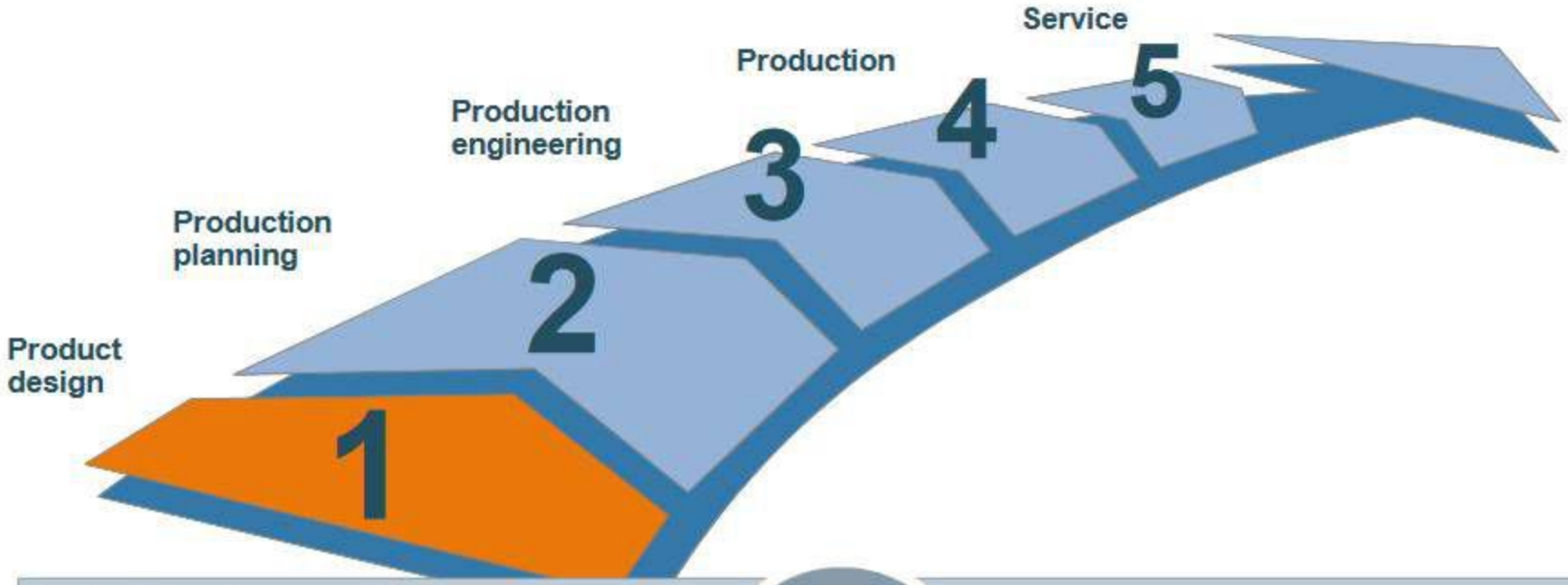
Product design → Production planning → Production engineering → Production execution → Services

(Fonte: Siemens, 2015)

Progettazione di sistemi CPS

The Future of Manufacturing
1. Faster development of product design through PLM software

SIEMENS



(Fonte: Siemens, 2015)

Progettazione di sistemi CPS

SIEMENS

Digitalization is Transforming the Manufacturing Industry

Smart Model
The product model sets the objectives needed to produce itself

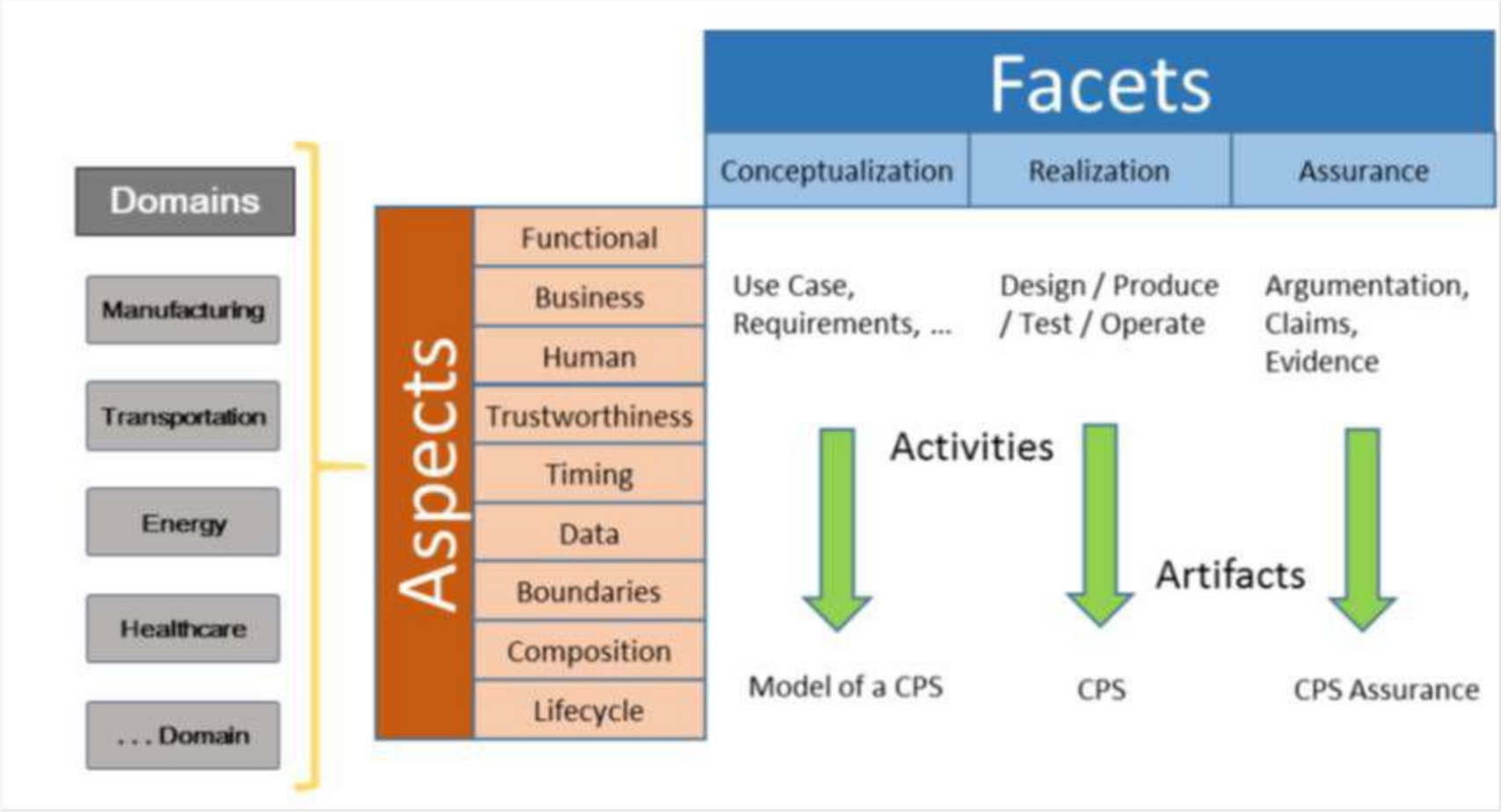
Digital Twin
Full digital product definition that simulates reality

Optimized, Distributed Production
Autonomous production with embedded intelligence.

(Fonte: Siemens, 2015)

Definizione di Internet of Things (IoT)

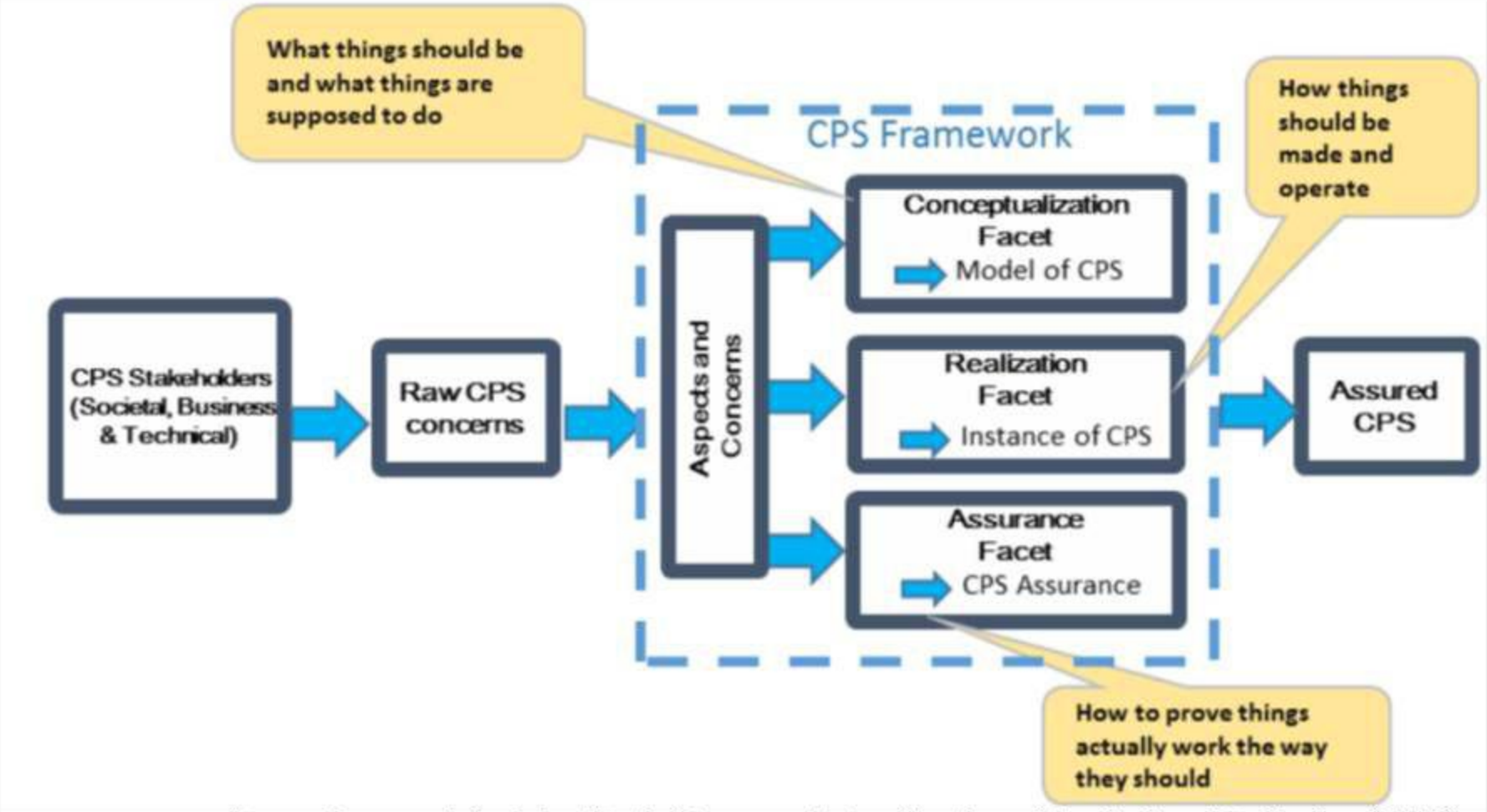
- CPS: il framework di riferimento



(Fonte: Framework for Cyber Physical Systems - National Institute of Standards and Technology (NIST), 2016)

Definizione di Internet of Things (IoT)

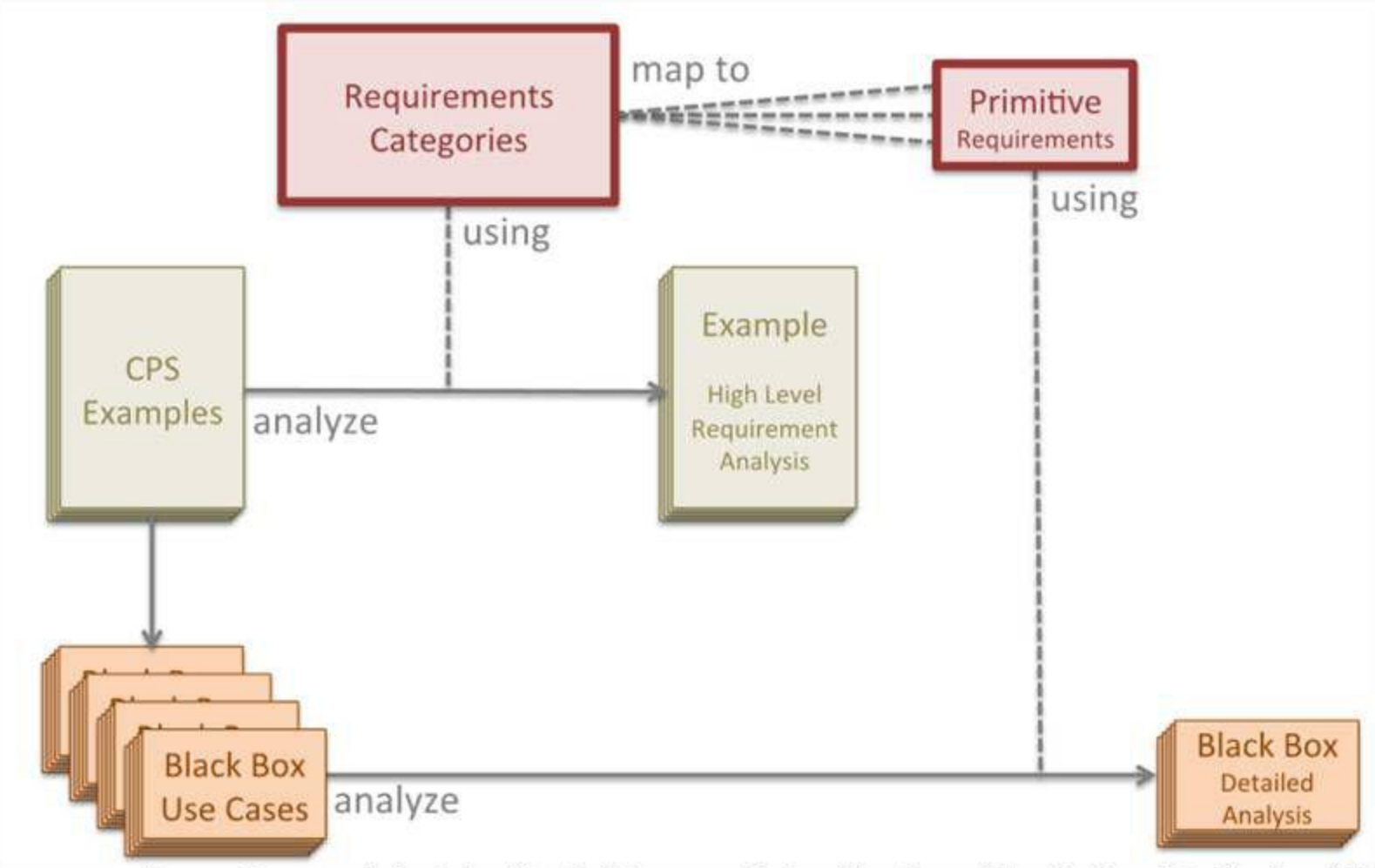
- CPS: il framework di riferimento Inter-CPS



(Fonte: Framework for Cyber Physical Systems - National Institute of Standards and Technology (NIST), 2016)

Definizione di Internet of Things (IoT)

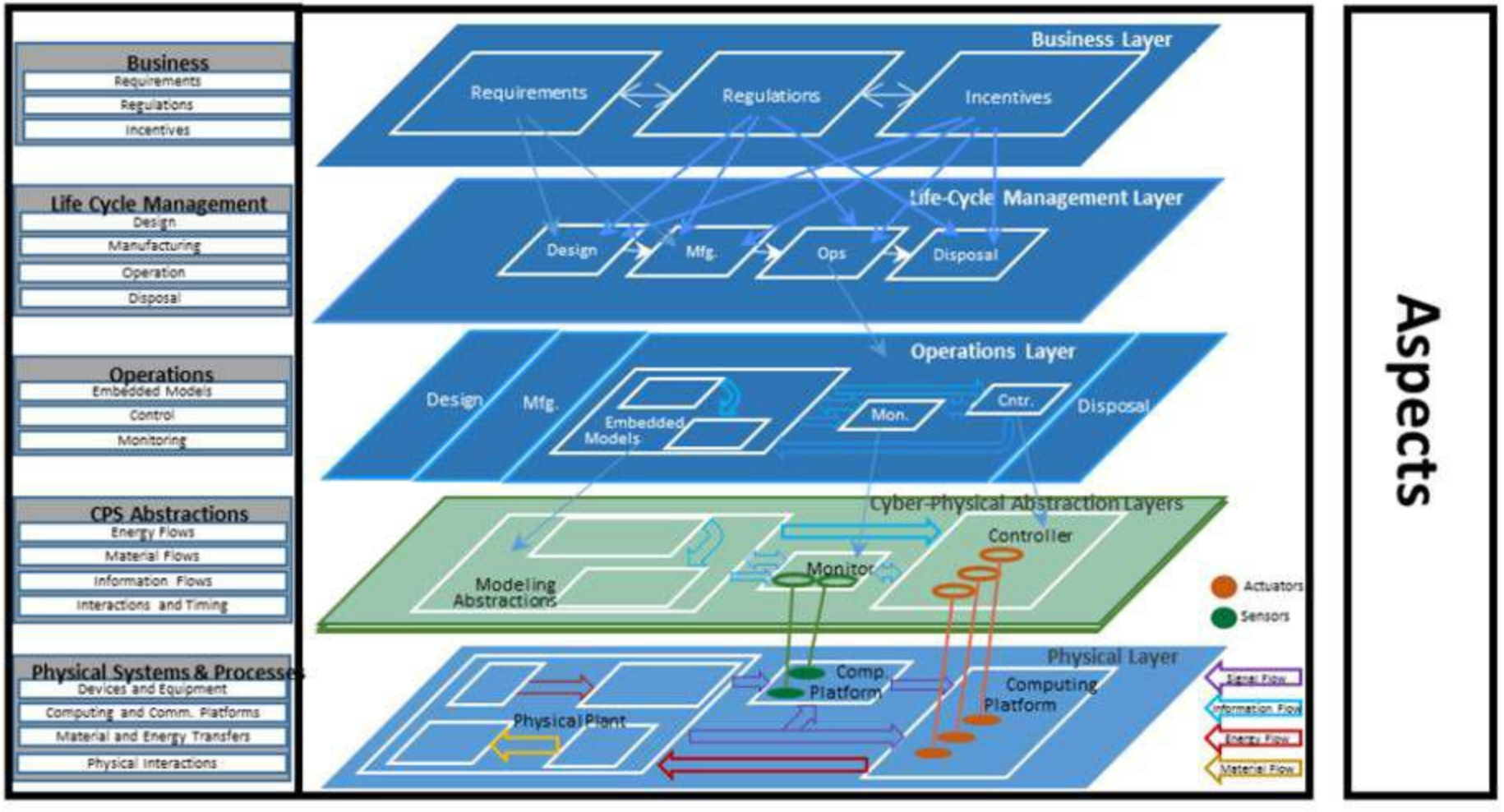
- CPS: il workflow



(Fonte: Framework for Cyber Physical Systems - National Institute of Standards and Technology (NIST), 2016)

Definizione di Internet of Things (IoT)

- CPS: i diversi livelli coinvolti



Fonte: Framework for Cyber Physical Systems – NIST, 2016

CPS & Sicurezza

- Gli attackers possono essere in grado di lanciare singoli attacchi per controllare i sistemi CPS
- Esempio: ***resonance attacks***. L'Attacker impone una nuova frequenza di oscillazione ai sensori/attuatori per poterli controllare
- Fino ad oggi la sicurezza ha riguardato:
  - i sistemi IT aziendali (con aggiornamenti software e patch)
  - i sistemi di controllo SCADA (focus sulla reliability: protezione del sistema da attacchi casuali)
- Perciò emerge che:
  - Aggiornamenti software e patch previsti per i sistemi IT non sono sufficienti
  - Soluzioni specifiche del prodotto (es. SCADA) non sono più sufficienti
- Occorre:
  - Maturare una ***visione complessiva della cyber-security***
  - Adottare un approccio basato su ***Prevention → Detection&recovery → Resilience***
  - Esempi: ridondanza e/o diversità a livello di sistema o applicazione, ridondanza fisica e/o analitica, predizione, adattatività, rischedulazione,