

**6th Japan-EU
Symposium on
ICT Research and
Innovation**

October 7th, 2016
10:00 – 13:00

marc.duranton@cea.fr

**ADVANCED TECHNOLOGIES FOR A
HYPER-CONNECTED SOCIETY
INCLUDING SECURITY ASPECTS**

マーク デュラント
Marc Duranton



The World's Most Innovative Research Institutions

BY DAVID EWALT



TOP 25 INSTITUTIONS | 2015 RANKINGS



1	Alternative Energies and Atomic Energy Commission	FRANCE
2	Fraunhofer Society	GERMANY
3	Japan Science & Technology Agency	JAPAN
4	U.S. Department of Health & Human Services	USA
5	National Center for Scientific Research	FRANCE
6	Korea Institute of Science & Technology	SOUTH KOREA
7	National Institute of Advanced Industrial Science & Technology	JAPAN
8	U.S. Department of Energy	USA

Silicon Valley's hoodie-wearing tech entrepreneurs are the poster kids of innovation. But the innovators who are really changing the world are more likely to wear labcoats and hold government-related jobs in Grenoble, Munich or Tokyo. That's the conclusion of Reuters' Top 25 Global Innovators – Government, a list that identifies and ranks the publicly funded institutions doing the most to advance science and technology.

Topping the list is France's [Alternative Energies and Atomic Energy Commission \(CEA\)](#), for its research into areas including renewable power, public health, and information security. Rounding out the top three: Germany's Fraunhofer Society and Japan's Science and Technology Agency.

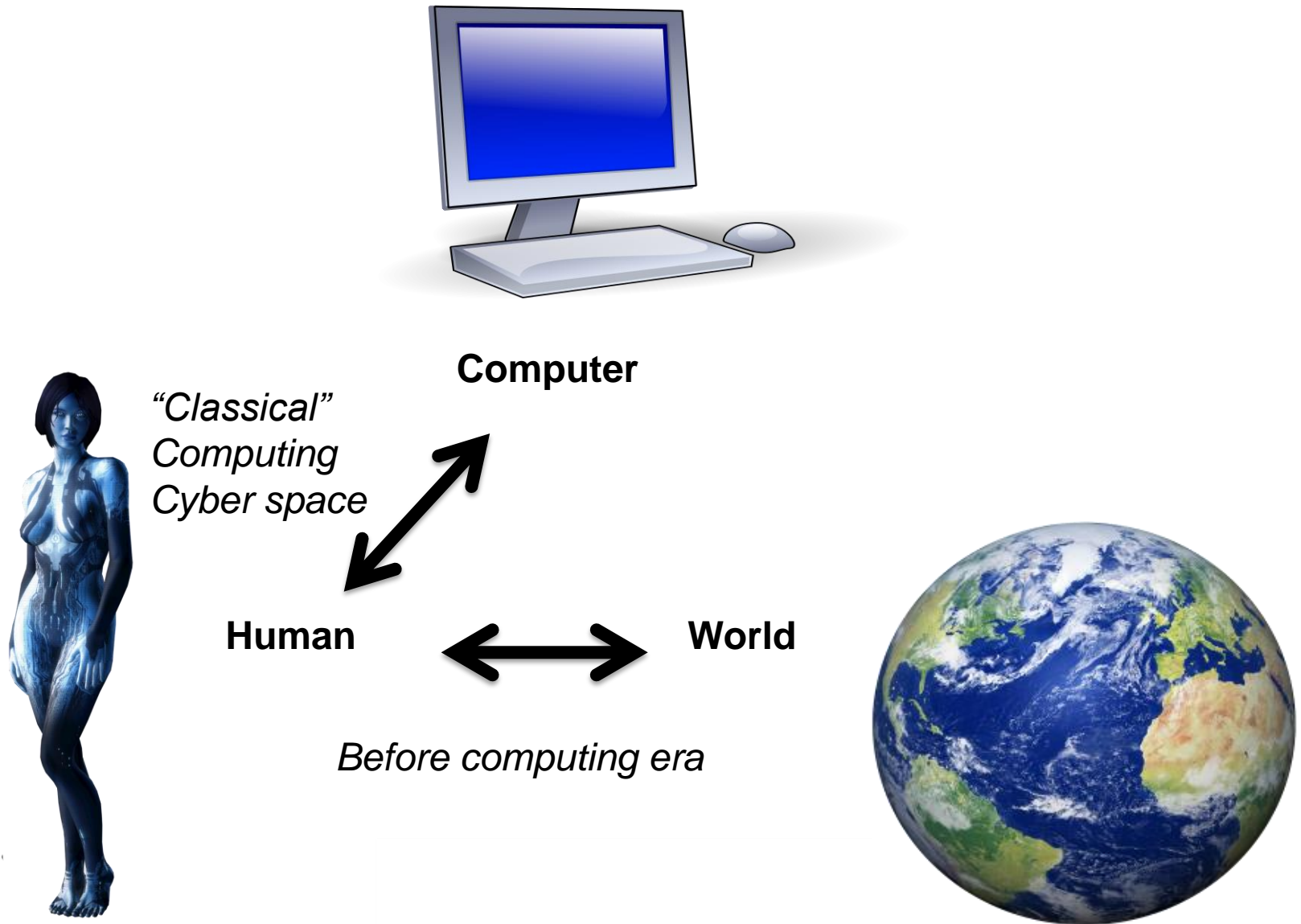


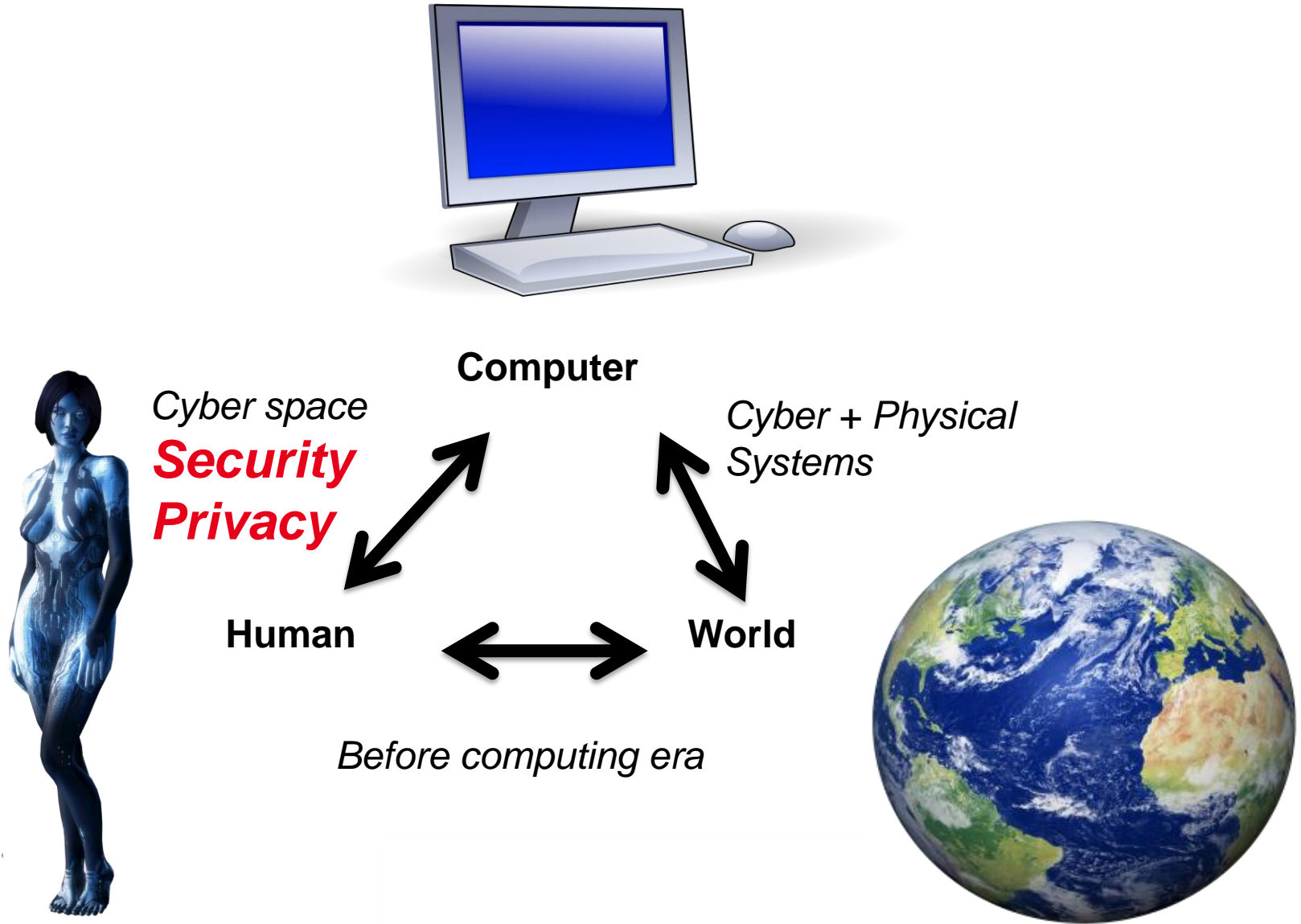
HiPEAC is coordination and support action on High Performance and Embedded Architecture and Compilation

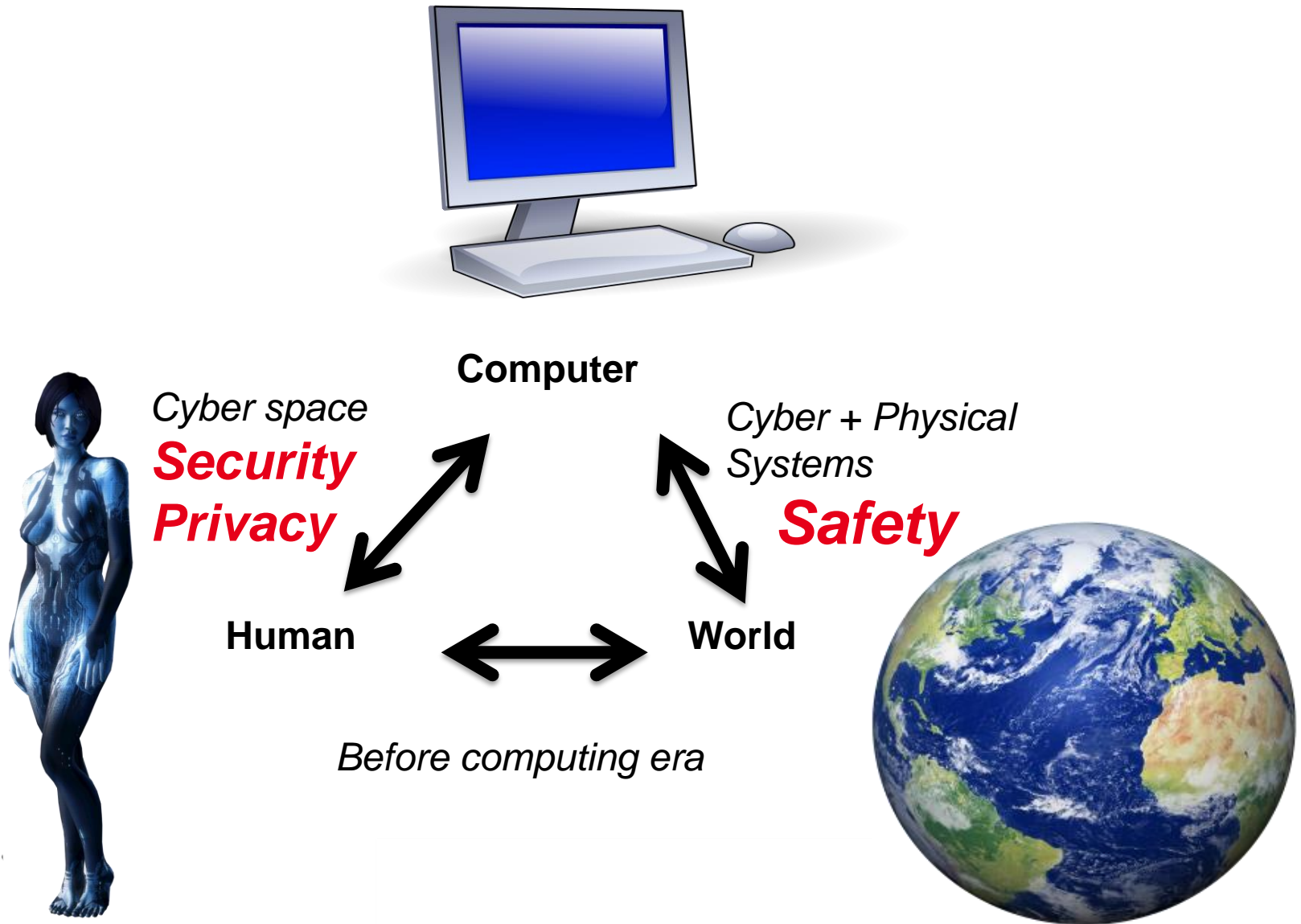
Created in 2004 as Network of Excellence, HiPEAC gathers over 450 leading European academic and industrial computing system researchers from nearly 320 institutions in one virtual center of excellence of 1700 researchers.



<http://www.hipeac.org/vision/>







New era of cyber and physical entanglement

Applications are delocalized,
distributed on
collaborating devices

Smart Computing Distribution



Machine to
Machine
Interactions
(often **black boxes**
to each other)
Interoperability

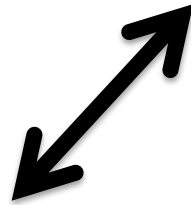


Computer

Constraints imposed
by the real world e.g.
time, ...

mixed-criticality

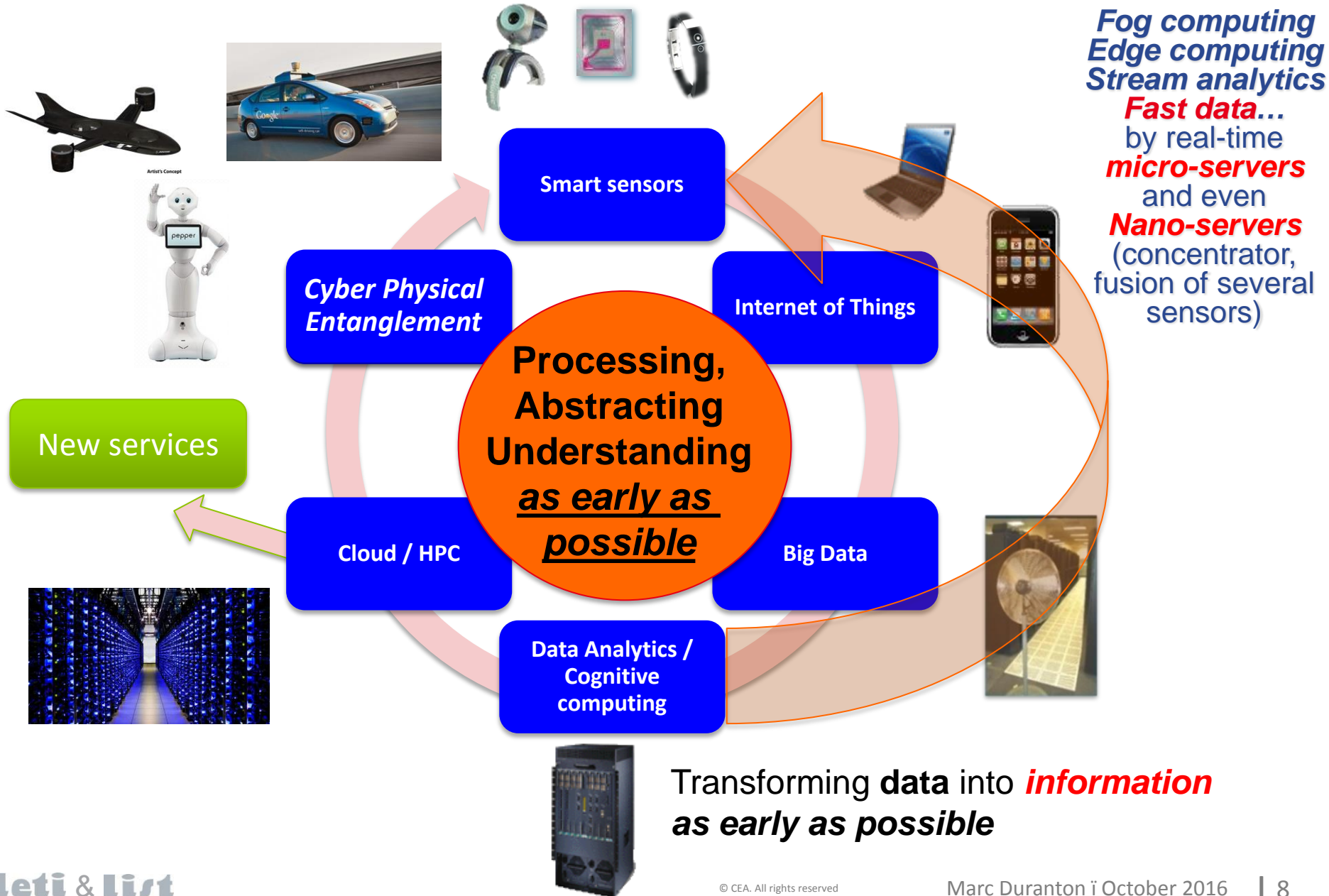
Human



World



Smart Computing Distribution





System should be autonomous to take good decisions in all conditions

Should I brake?

Transmission error
please retry later

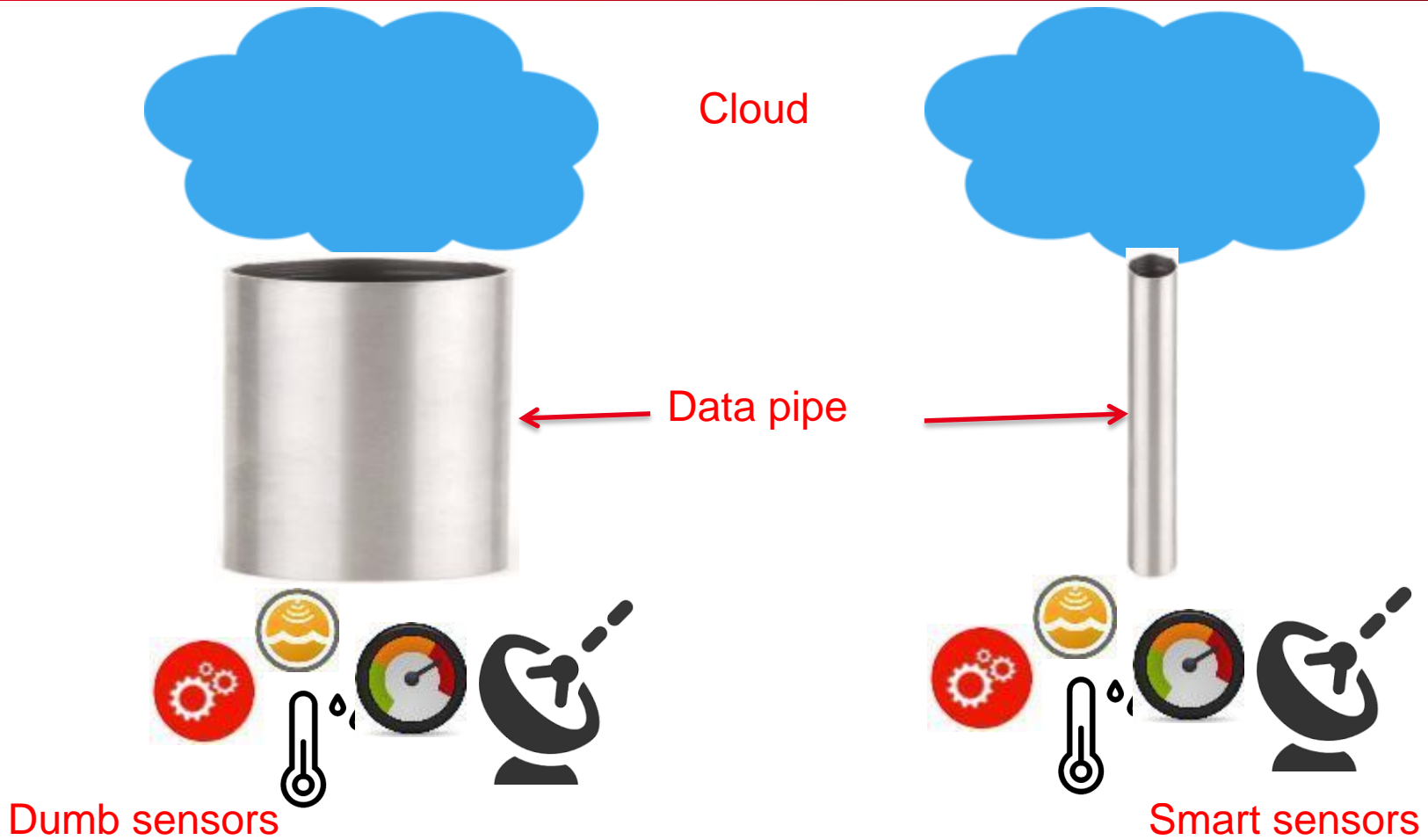


Safety will impose that basic autonomous functions should not rely on “always connected” or “always available”



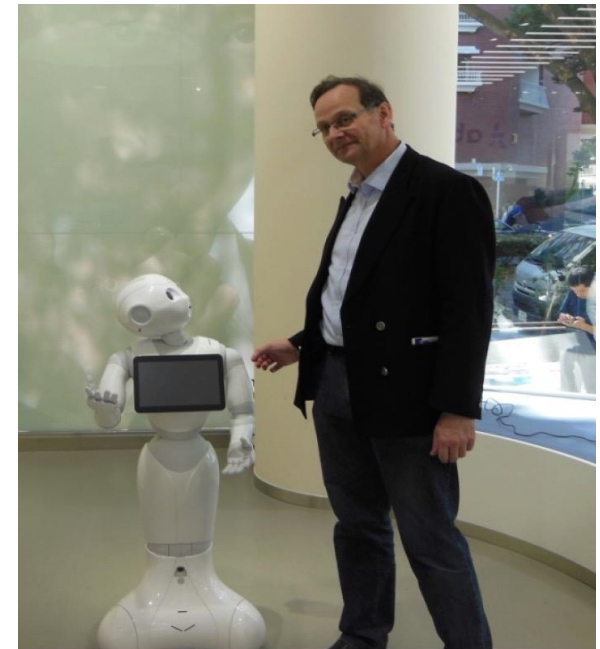
Example: detecting elderly people falling in their home

Privacy will impose that some processing should be done locally and not sent to the cloud.



Analytics and Big Data applications cannot always be done in the cloud. Streaming and distributed data analytics requires ***new tools to extract knowledge from data as early as possible.***

- We are entering the “*Centaur era*”
 - from the man/machine collaborating teams in chess
- IPA- Intelligent Personal Assistant (Siri, Cortana, Google Now, Alexa, ...)
- Intelligent building, smart-cities
- Self-driving cars (level 1 to 3)
- Home robots
- ...



- **Artificial Intelligence** is changing the man-machine interaction – natural interfaces, “intelligent” behavior
- The new systems should makes intelligent and **trustable decisions**



- Today security / privacy issues make the newspaper headlines

Hackers C

By Philip E. Ross
Posted 23 Jul 2015 | 1

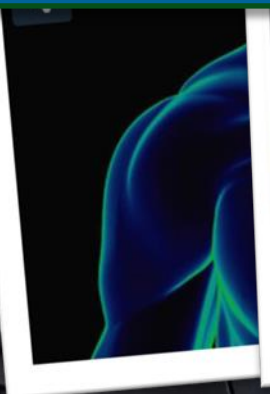


Massive adoption of IoT by citizens relies on confidence in terms of security and privacy



A Polish teenager allegedly turned the tram's personal train set, triggering chaos and derailed people were injured in one of the incidents.

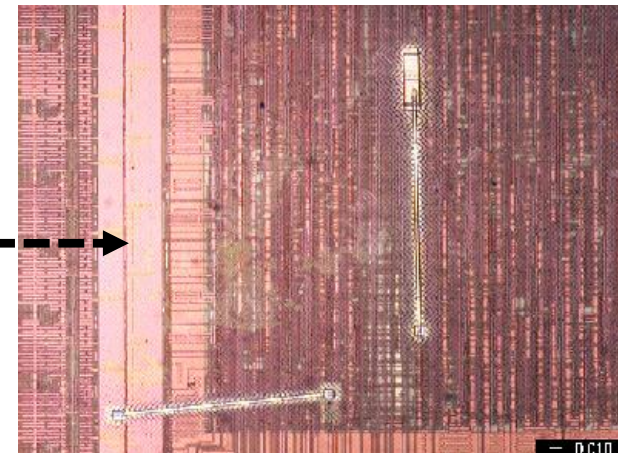
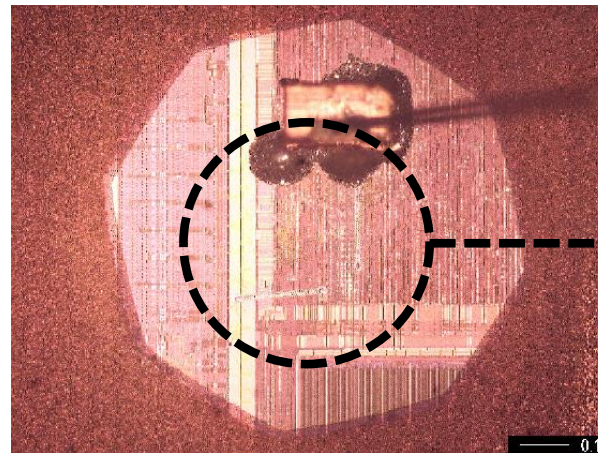
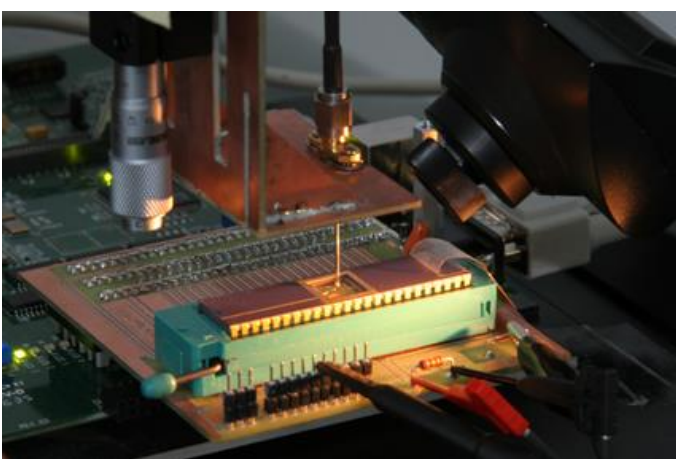
The 14-year-old modified a TV remote control's points, *The Telegraph* reports. Local police said depots to gather information needed to build the he modified track setting for a prank.



A smart refrigerator on display at the International Consumer Electronics Show (CES) last week in Las Vegas.

■ Systems must be *secured-by-design*

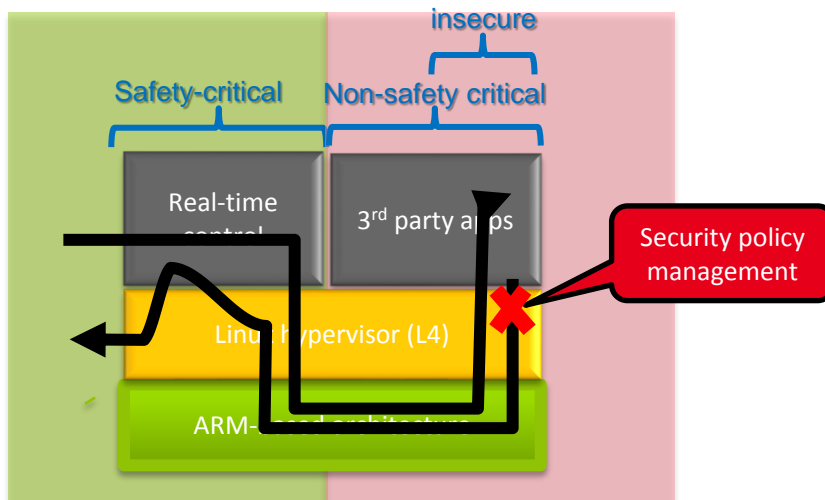
- Memory dump , reverse engineering, side channel analysis, bus probing...
- Security should be considered at all levels, *SW and HW*



■ “Trustworthy computing (with software) cannot exist until we have trustworthy hardware to build it on”

Dr. Dean Collins, Deputy Director, DARPA

- Systems (like smart cities, smart building, self-driving cars) will have to handle both
 - **Safety critical applications**, with strong constraints (latency, timing, ...)
 - **Best effort “classical” computing**
 - **Imported “insecure” applications** (black boxes)



Mixed-criticality
systems

- How to trust that the remote computing platform will not misuse your data?

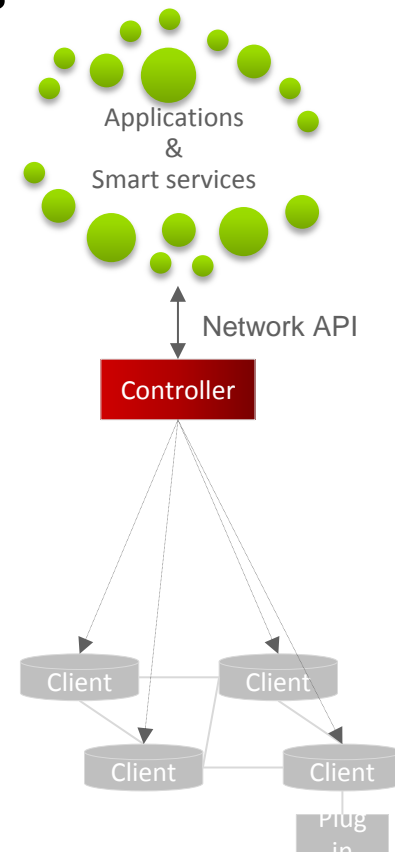
·
·
·
Homomorphic encryption !

- **How to trust that the remote computing platform will not misuse your data?**
- An **homomorphic encryption** system is a cryptosystem which, on top of allowing to encrypt and decrypt data, allows to perform (any) **calculations in the encrypted domain**.
- In essence, the « cryptocomputer »:
 - Keeps its algorithm private.
 - Can insert any (cleartext domain) data into the calculation.
 - Has access to **neither intermediate nor final calculations results**.
- Such (secure) cryptosystems have been shown to exist in 2009.

- Although theoretically efficient, the first systems were totally impractical.
- Now, thanks to the progress on algorithms, parallel compiler and new hardware,
- ***They are practically possible!***

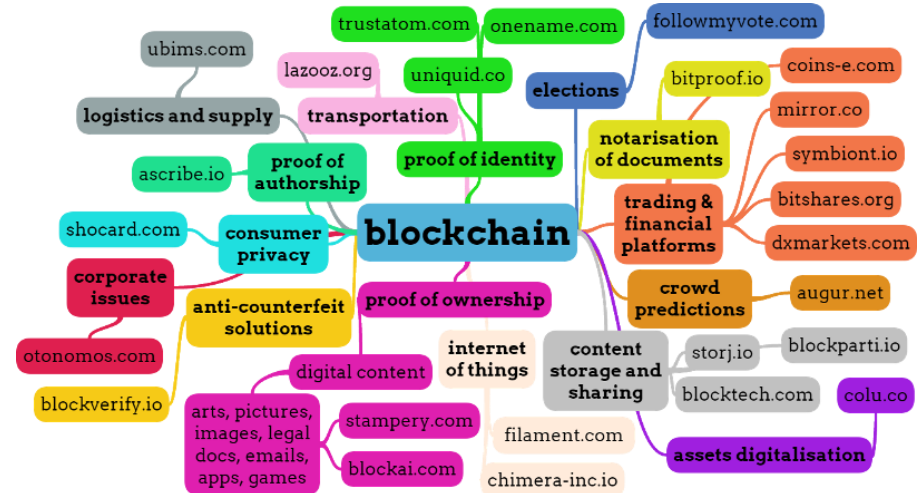
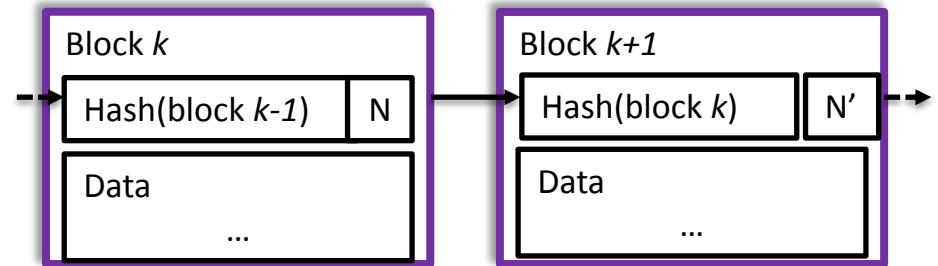


- More **intelligent** (Cognitive) **detection and counter-measure**
 - Intrusion Detection System (IDS) that detects attacks by difference from normal behavior
 - Reconfigure the network automatically in reaction to cyberattacks
 - **Adaptive resilience** to threats from inside and outside the network
- Hide user's data "statistically": ***differential privacy***
- ***User empowerment***: helping device owner to manage data privacy



A decentralized, deregulated record of data with integrity properties

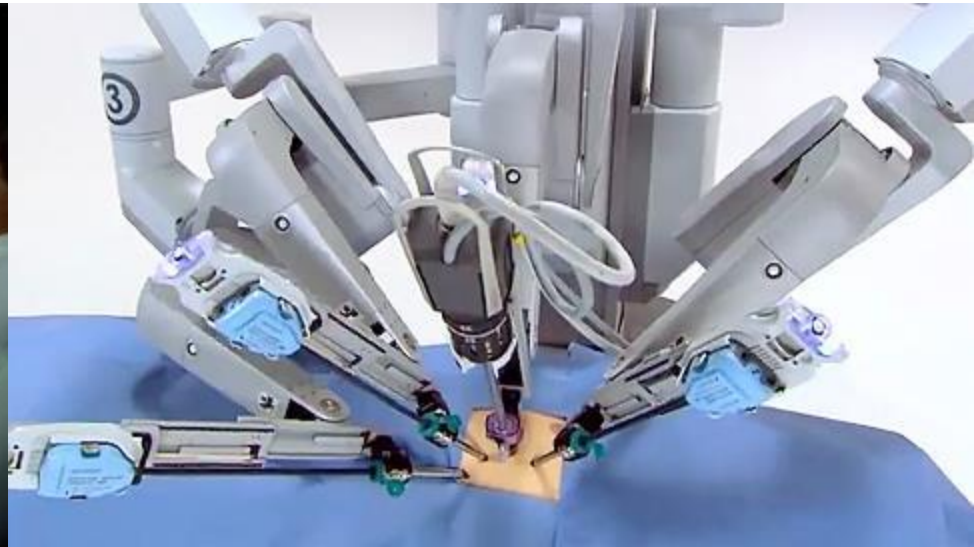
- Decentralized trusted authority
- Bitcoin is an application of blockchain
- We should work on **BlockChain of Things** (BoT)



- Trust is the key element for the success of IoT and CPS
- For Cyber-Physical Systems, *safety* is another key topic for having trustability

SAFETY
is
EVERYONE'S
RESPONSIBILITY!

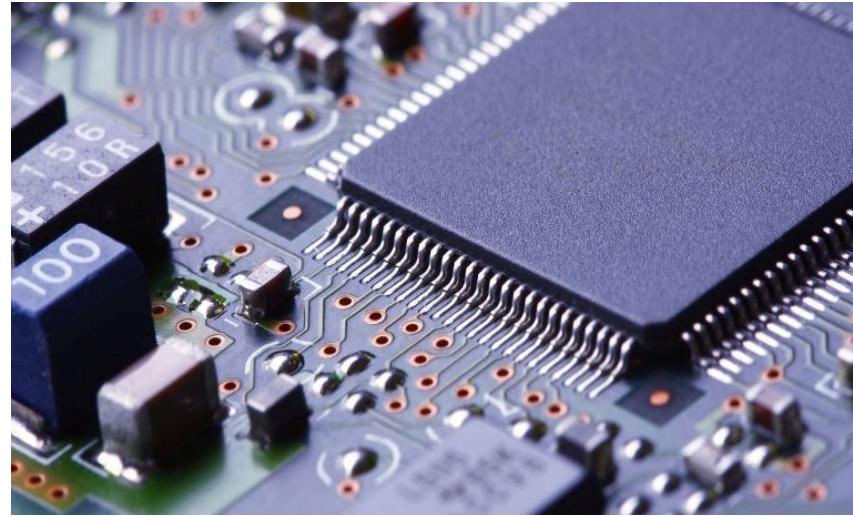




- Beyond predictability by design and beyond worst-case execution time (WCET)
- Capability to build ***trustable systems from untrusted components***
- Mastering trustability for complex distributed systems, composed of black or grey boxes

"People who are really serious about software should make their own hardware" Alan Kay

Current systems are ***not*** necessary ***efficient*** for new hyper-connected Cyber-Physical applications



PC era -> Intel x86 Smartphone era -> ARM

Cyber and Physical entanglement era -> result of combined Japan and EU efforts?

In embedded systems market, almost 90% of the market is on selling hardware (from Global Markets insight).



- Japan and the European Union are two key players in the ICT field, enabling Smart and Hyper-connected Society
- Scale of today's global challenges requires that we ***work together*** more closely and effectively to build ***Simple Efficient and Trustable Systems***
 - In conformity with the mutual interests and the research orientation of the EU and Japan
- Acceptance of the hyper connected society will require that the systems should be trusted

Together, make it happen!



- Constraints of the era of cyber and physical entanglement:
 - *Mixed criticality*
 - *Safety*
- *Interoperability*
- *Smart Computing Distribution:*
 - Transforming data into *information as early as possible*
 - Embedded intelligence needs local high end computing
- **Security and Privacy: *Simple Efficient and Trustable Systems***
 - “Trustworthy computing (with software) cannot exist until we *have trustworthy hardware* to build it on
 - *Homomorphic encryption, Adaptive resilience, Differential privacy*
 - *Block chain and smart contracts: Blockchain of Things*
- *Building trustable systems from untrusted components*
- “People who are really serious about software should make their own hardware”



Thank you for your attention
どうもありがとうございます

marc.duranton@cea.fr



leti

Centre de Grenoble
17 rue des Martyrs
38054 Grenoble Cedex

list

Centre de Saclay
Nano-Innov PC 172
91191 Gif sur Yvette Cedex

