
Safety & Security:
Two sides of the same coin
Xavier Pi
BARCELONA Nov 2014
ISACA
Trust in, and value from, information systems

SESSION OBJECTIVES

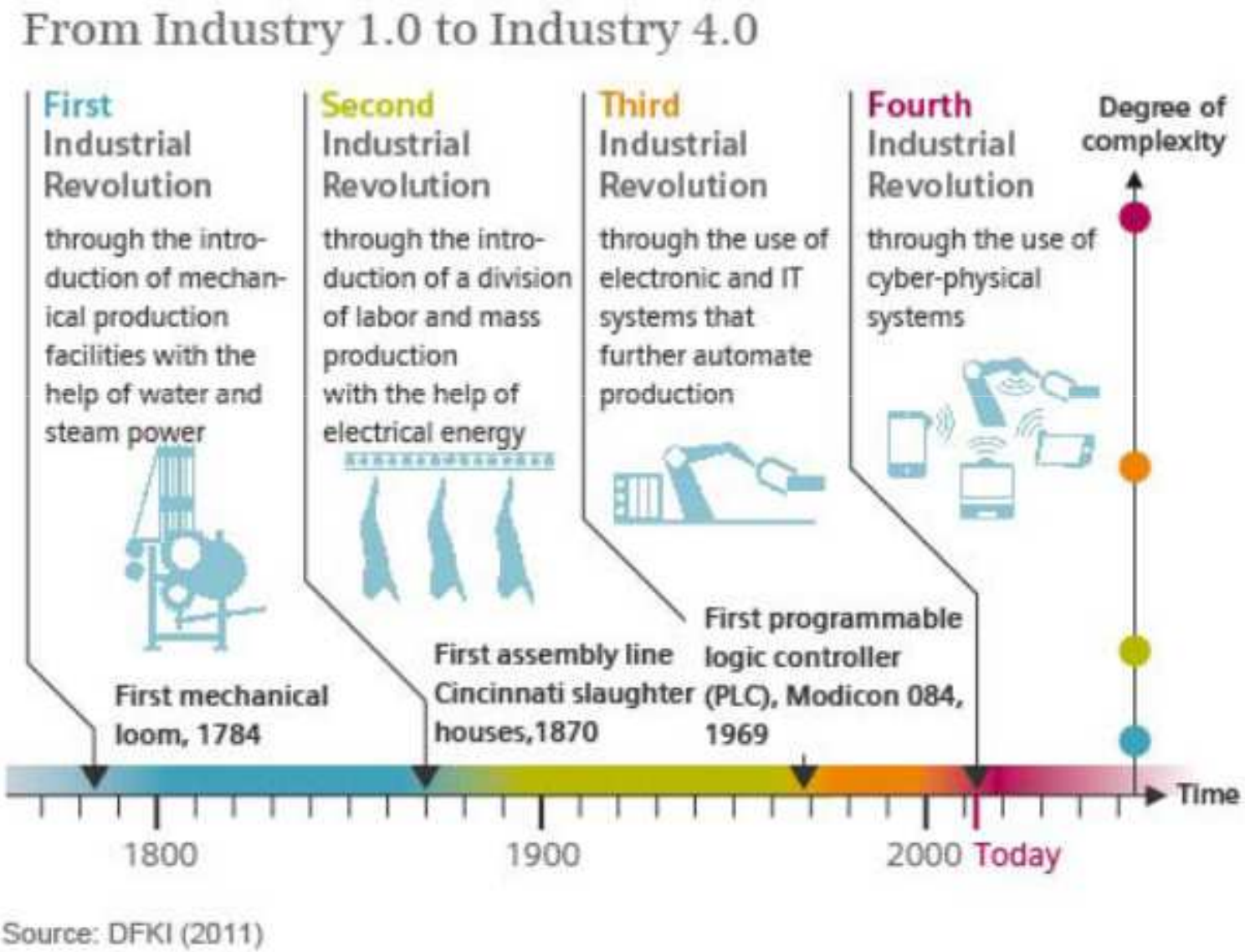
- **Explore the new industrial trends about safety and security**
- **Consider the hypothesis of a central role of Embedded Systems**
- **Consider a unified Safety & Security framework for industry**

ISACA
Trust in, and value from, information systems

INTERNET OF THINGS (ITO) AND CYBER-PHYSICAL SYSTEMS (CPS)

- **The Industry has recently (2013) formalized the term “Industry 4.0” based on IoT and CPSs**
- **The reference document is “Recommendations for implementing the strategic initiative industrie 4.0” from *acatech* (German National Academy of Science and Engineering)**

THE 4TH INDUSTRIAL REVOLUTION



CITIZEN EMPOWERMENT

- 1st revolution: No citizen empowerment.
- 2nd revolution: Emerges DIY (Do it Yourself) culture with magazines and games like Meccano
- 3d revolution: Several citizen empowerments processes: PC (lot of magazines in “80-90s”), Internet, mobile devices (faster and faster)
- 4th revolution: Knowledge Society, Makers and Open movements

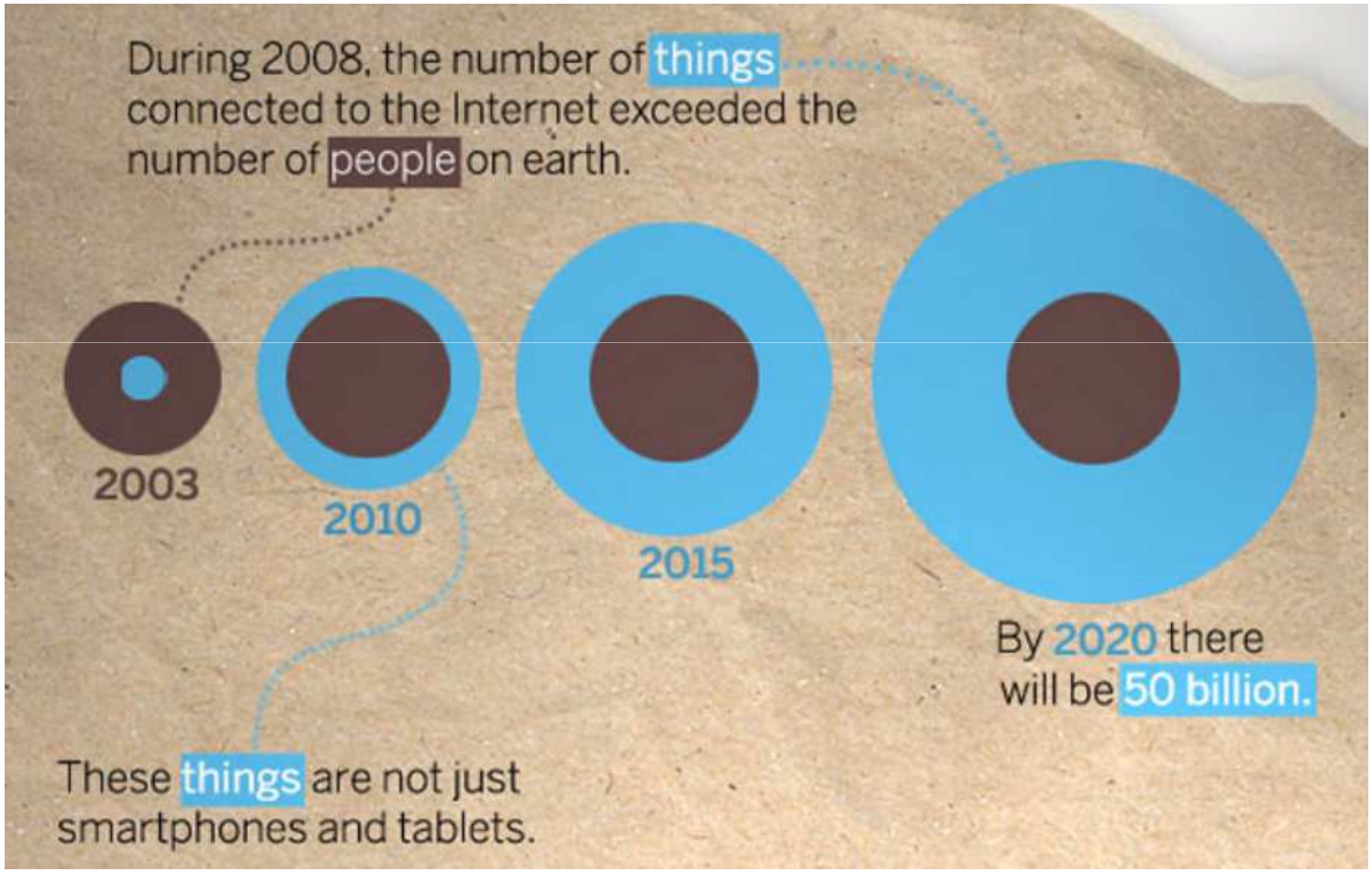
ISACA
Trust in, and value from, information systems

THEORETICAL BASIS OF IOT

- **IoT defined in 1999 by Kevin Ashton seminal paper "That 'Internet of Things' Thing“ published for the RFID Journal.**
- **Original idea: All objects in the world with minuscule identifying devices or machine-readable identifiers**
- **Today IoT is a network centric idea related to services and involves from devices to the Cloud**

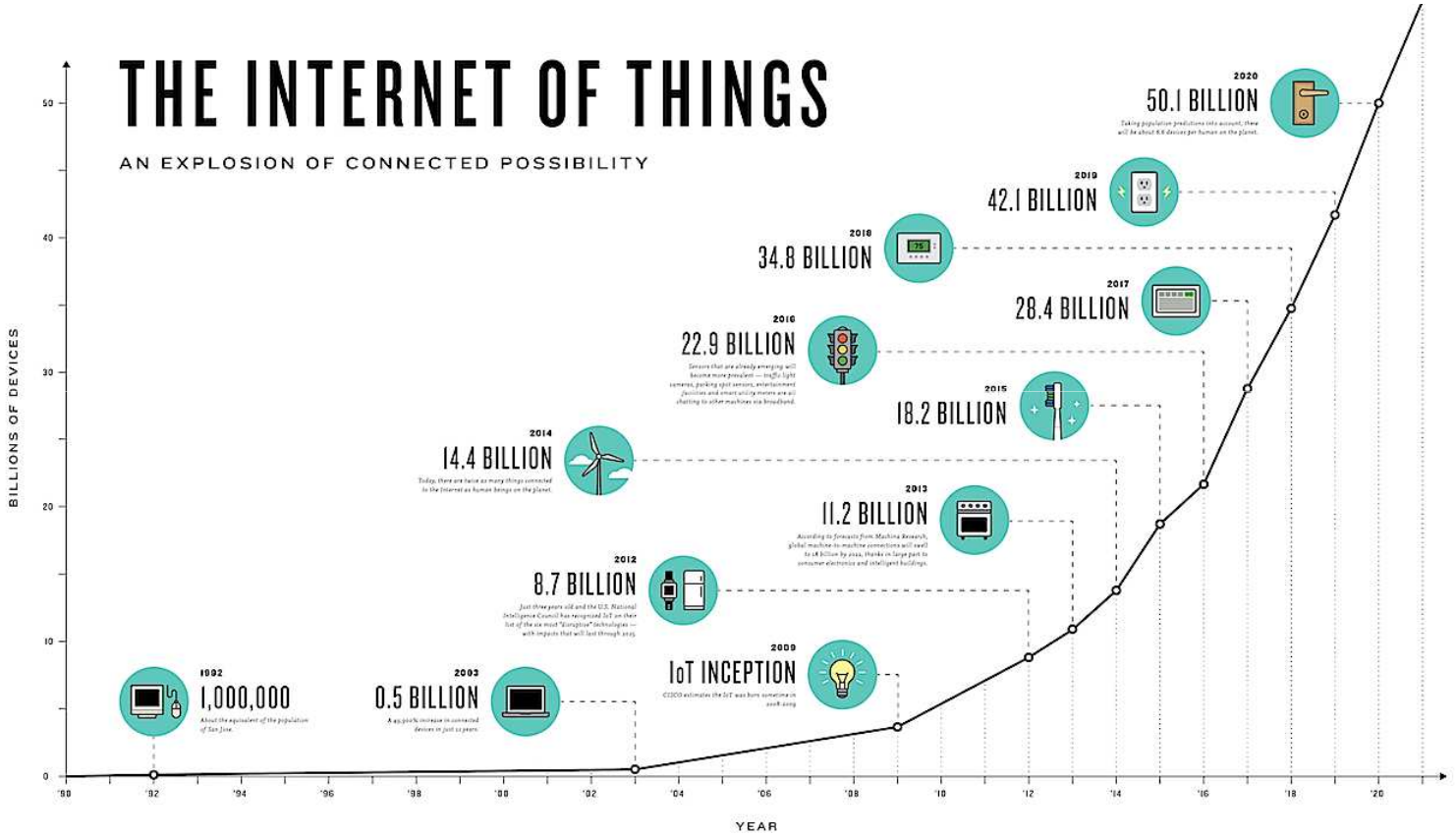
ISACA
Trust in, and value from, information systems

CISCO SYSTEMS VISION OF IOT



Source: CISCO

EXPONENTIAL GROWTH



Source: The Connectivist

ISACA
Trust in, and value from, information systems

THEORETICAL BASIS OF CPS

- **Defined as a “marriage between physical world and computational world”**
- **The Cyber-Physical Systems where identified by Hellen Gill at the NSF (US National Science Foundation) in 2006 as a key area of research.**
- **Enters the Industry in 2007 with Wayne Wolf article “The Good News and the Bad News”**

ISACA
Trust in, and value from, information systems

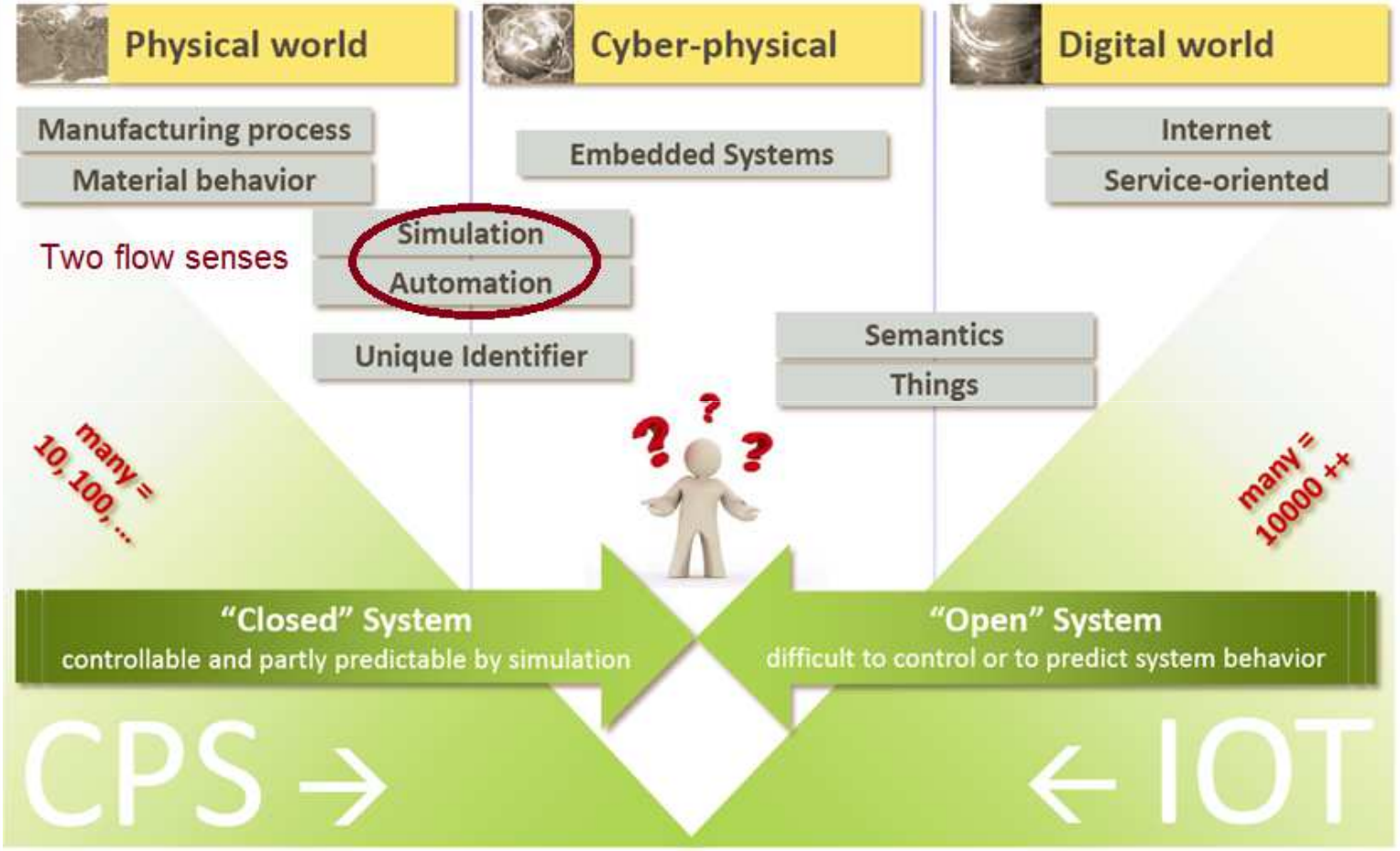
THE ROAD TO IOT AND CPS

- **1926** Nikola Tesla "Teleautomation"
- **1948** Norbert Wiener "Cybernetics"
- **1961** Charles Stark Draper "Apollo Guidance Computer" one of the first embedded systems
- **1988** Mark Weiser "Ubiquitous computing"
- **1999** Kevin Ashton "Internet of Things"
- **2006** Helen Gill "Cyber-physical systems"

Source: Jeshcke

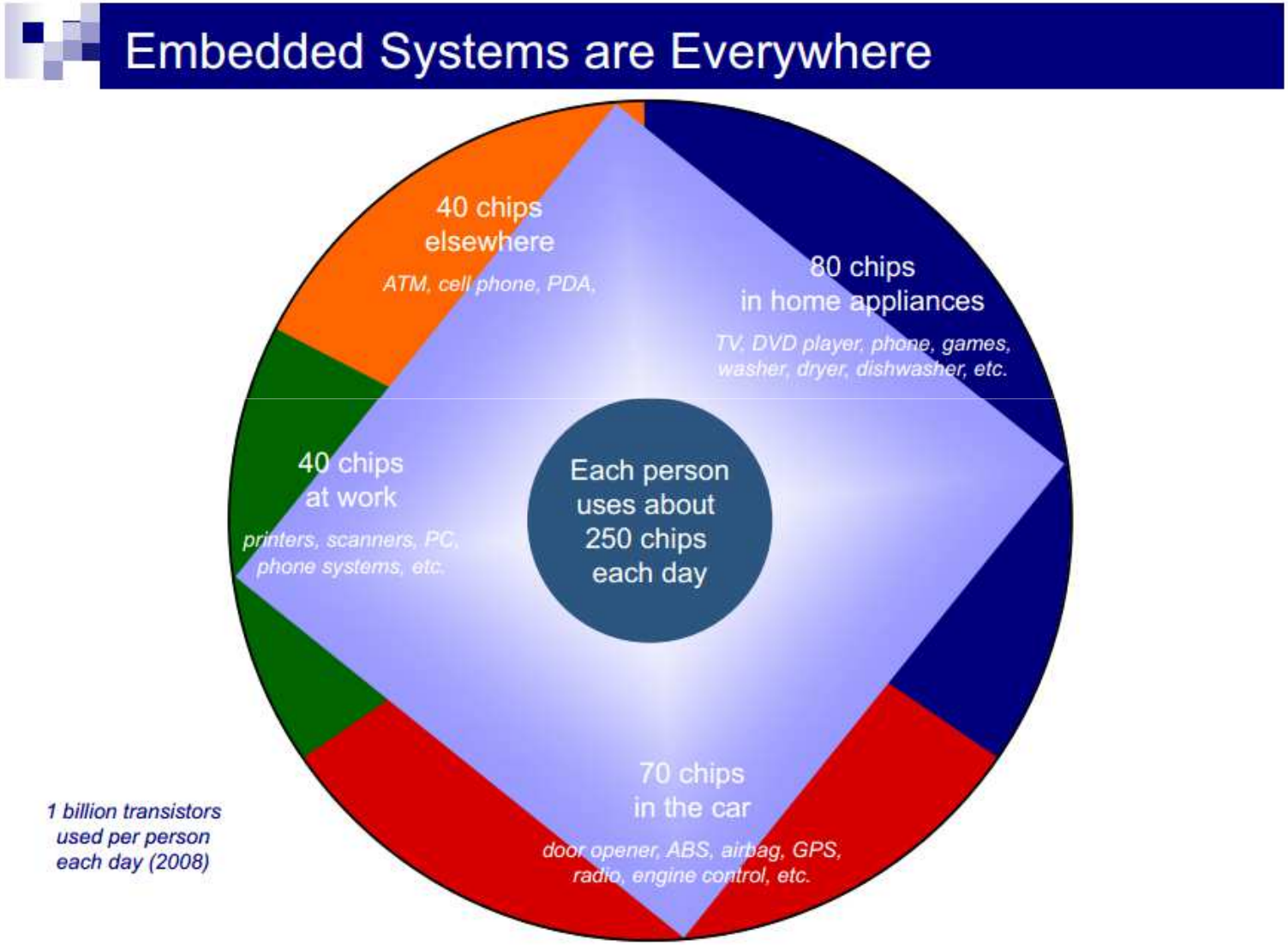
ISACA
Trust in, and value from, information systems

IOT AND CPS



Source: Jeshcke

EMBEDDED SYSTEMS



ISACA
Trust in, and value from, information systems

IOT AND CPS AND EMBEDDED SYSTEMS

- **Several researchers claim for a new emergent knowledge field (IoT & CPS), in which a lot of formalization work must be done**
- **Turing Prize (2007) Joseph Sifakis have predicted that in 2015 will be a strong impact from CPS over society and their citizens:**
- **EMBEDDED SYSTEMS REVOLUTION?**

ISACA
Trust in, and value from, information systems

VALUE CHAINS IN INDUSTRIAL AREAS

Complete value chains can be identified in industrial regions (Barcelona Case Study)

THE SMALLEST STAND ALONE INDUSTRIAL COMPUTER

DM3730 / AM3703 ARM Cortex A8 CPU 1GHZ / 512 Megabytes RAM + 512 Megabytes FLASH

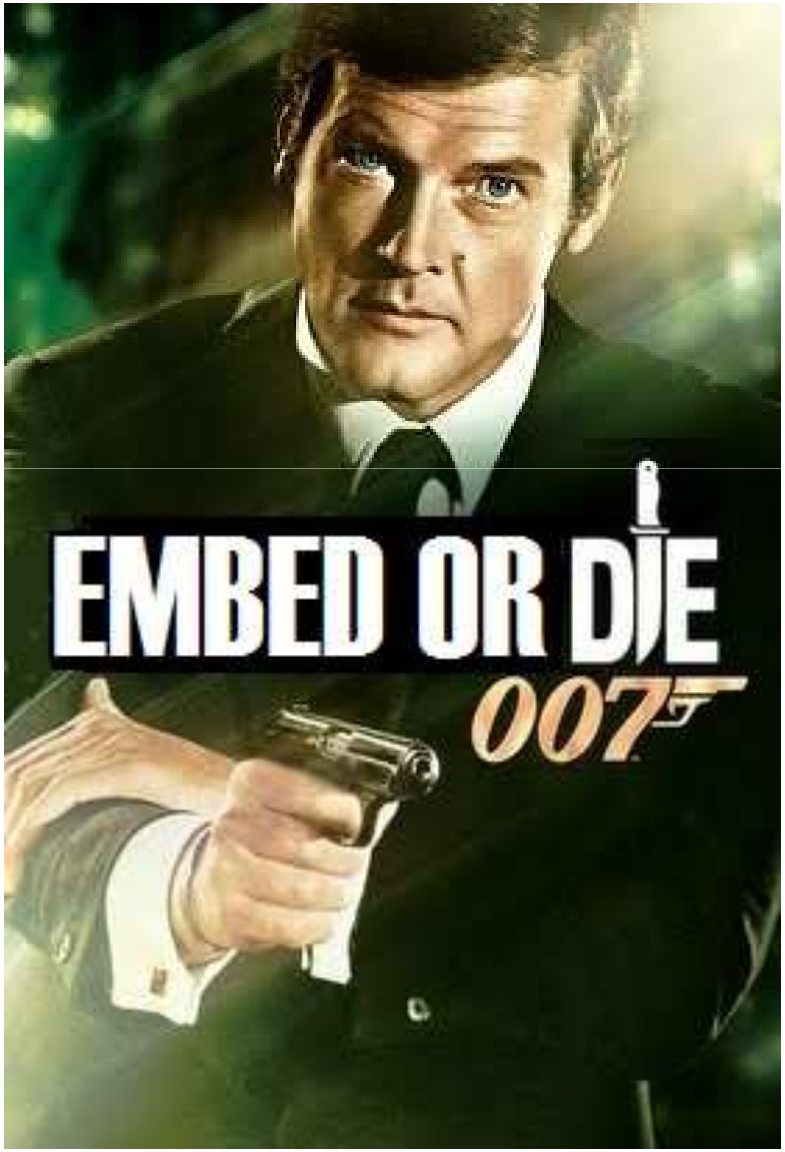
The IGEP COM MODULE is an industrial processor board. It can be used as a computer-on-module for your product but also as a stand alone computer without the need of a baseboard.You don't need anything else than a USB cable to power the IGEP COM MODULE and communicate with it by using Ethernet over USB gadget implemented on the Linux kernel. The IGEP COM MODULE provides a lot of features in a small size. You can build your project anywhere you want.

www.isee.biz

ARM processors are under huge demand: 20 million units are produced every day due to mobile devices market

ISACA
Trust in, and value from, information systems

REVOLUTION? WHAT MUST THE INDUSTRY DO?



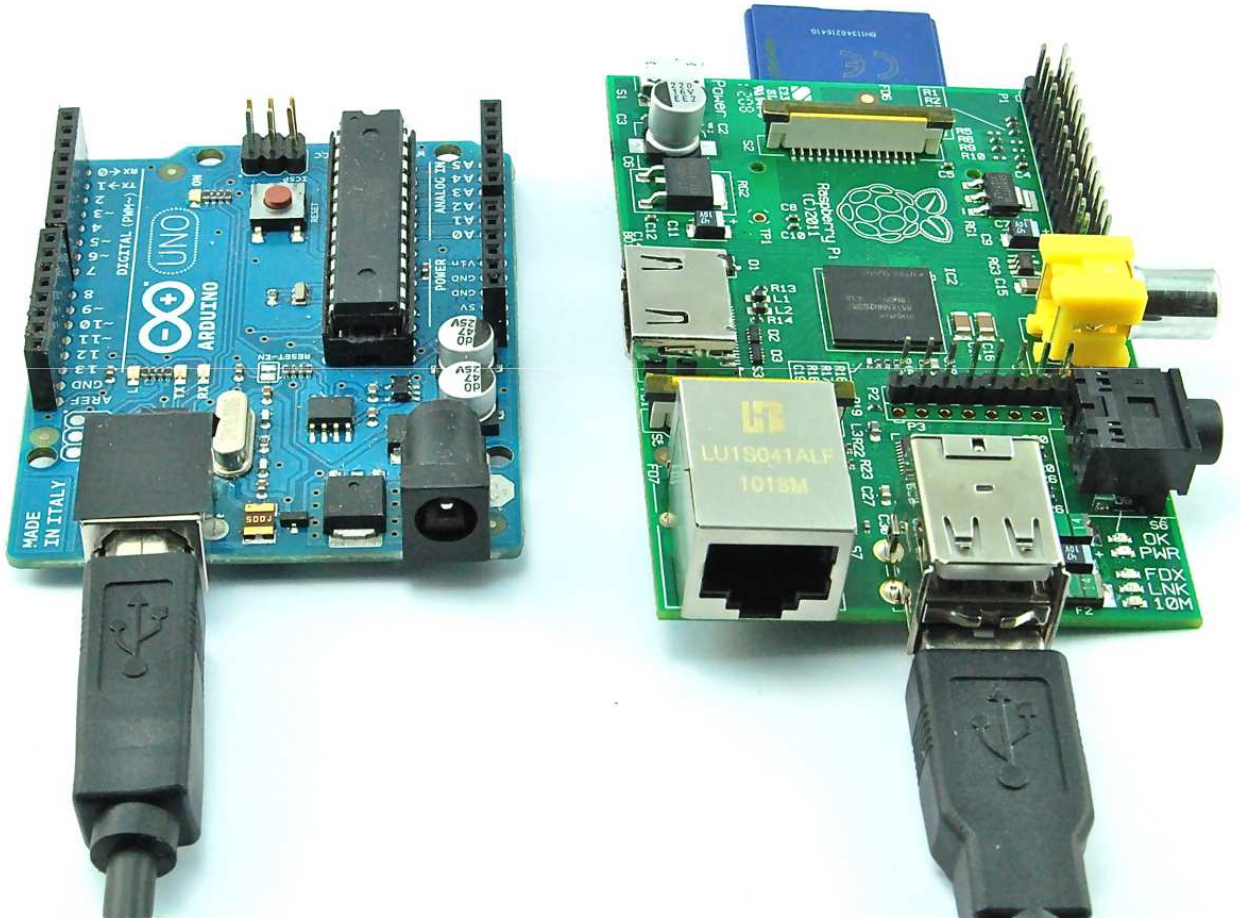
Source:
Embedded Systems WG

WHAT ABOUT CITIZENS? ARDUINO AND RASPBERRY PI

- **Arduino is a project born in Ivrea in 2005, Olivetti's historical headquarters, that consists of a small controller conceptually similar to an industrial PLC (Programmable Logic Controller). It is the *Open Source Hardware* world reference.**
- **Raspberry Pi is a project born in the University of Cambridge in 2009, that consists of a small card with a full fledged Linux computer.**

ISACA
Trust in, and value from, information systems

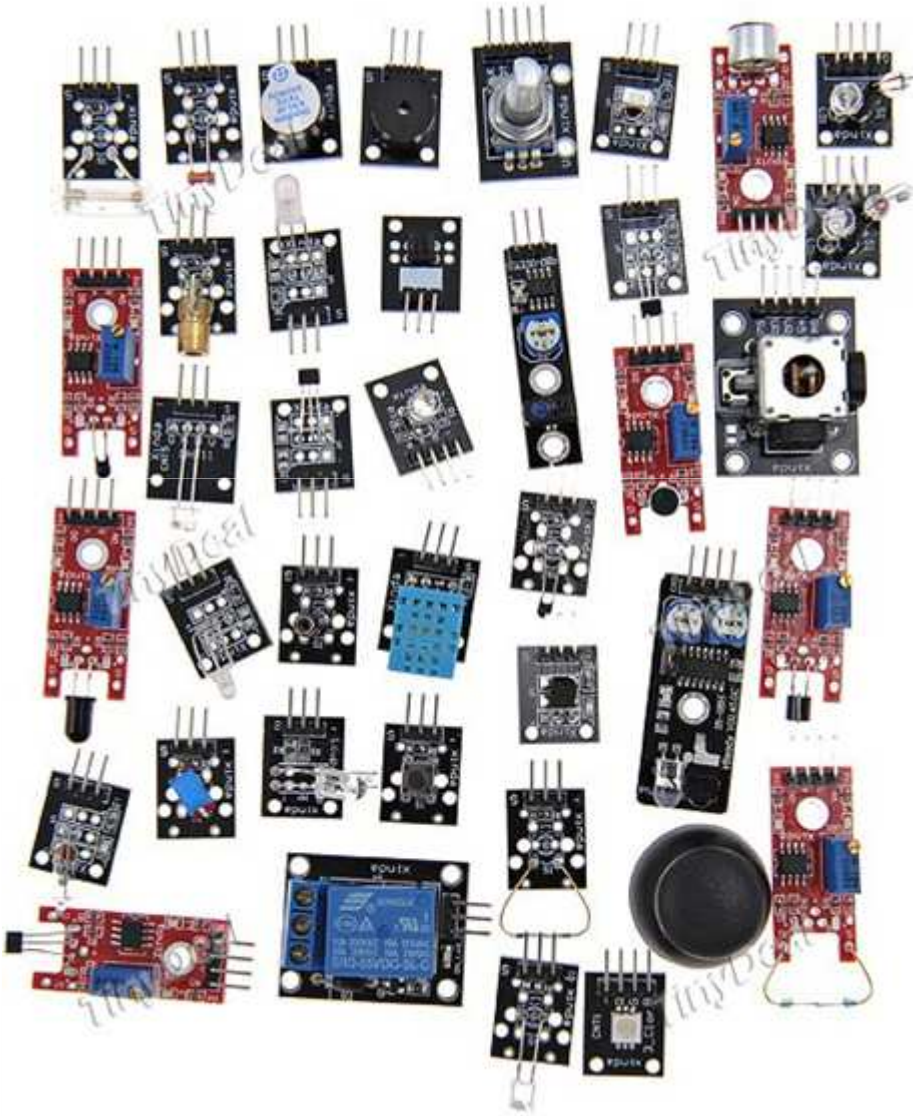
POPULAR EMBEDDED SYSTEMS SUCH AS ARDUINO AND RASPBERRY PI



Low cost Embedded Systems (>2.5 milion sold each)

ISACA
Trust in, and value from, information systems

SENSORS (ARDUINO)



- **All kind of sensors for Arduino:**
  - Temperature
  - Pressure, humidity
  - Gas/smoke
  - Light
  - And more

Low cost “37-in-1 Sensor Module Kit for Arduino (ECT-219472)”

Citizen projects such as vegetable patches

ISACA
Trust in, and value from, information systems

CITIZENS ARE LEARNING TO DEAL WITH IOT AND CPS

Source: Barcelona City Council

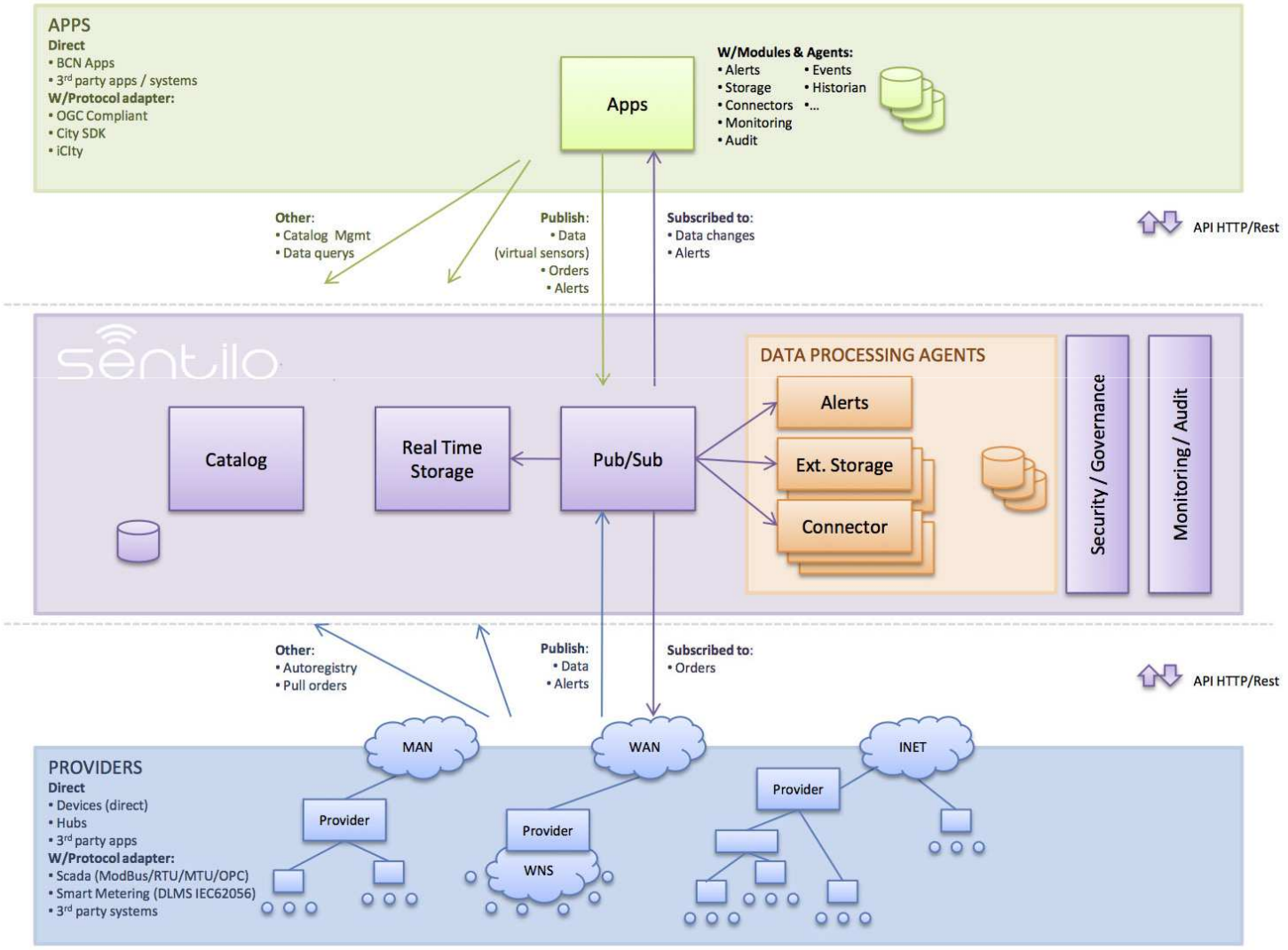
ISACA
Trust in, and value from, information systems

EMBEDDED SYSTEMS AND CITIZENS

- **Cities have been integrating Embedded Systems from decades, but initiatives such as CityOS or Sentilo (www.sentilo.io) are a qualitative jump**
- **Citizens are becoming an active agent of the transformation process to a new world.**
- **Where are the borders between hobbyists and professionals? Risk is the key.**
- **Are we prepared to afford the safety and security challenges?**

ISACA
Trust in, and value from, information systems

SENTILO BARCELONA SENSOR PLATFORM (CASE STUDY)



Source: Barcelona City Council

SAFETY AND SECURITY, TWO CULTURES ?

"Classical Safety-Oriented Dependability" versus "Classical Security"	
Safety	**Security**
Assumes trustworthy operators	Assumes fault free system
Assumes closed system	Assumes open connected system
Assumes time response from dedicated resources	Assumes shared generic platform

Source: Mazzini

- **Functional safety:**
  - *Part of overall safety to protect against incidents caused by incorrect functioning of components/systems*
- **Cybersecurity:**
  - *Part of overall security to Identify, protect (information), detect, respond, recover from attacks (NIST Framework)*

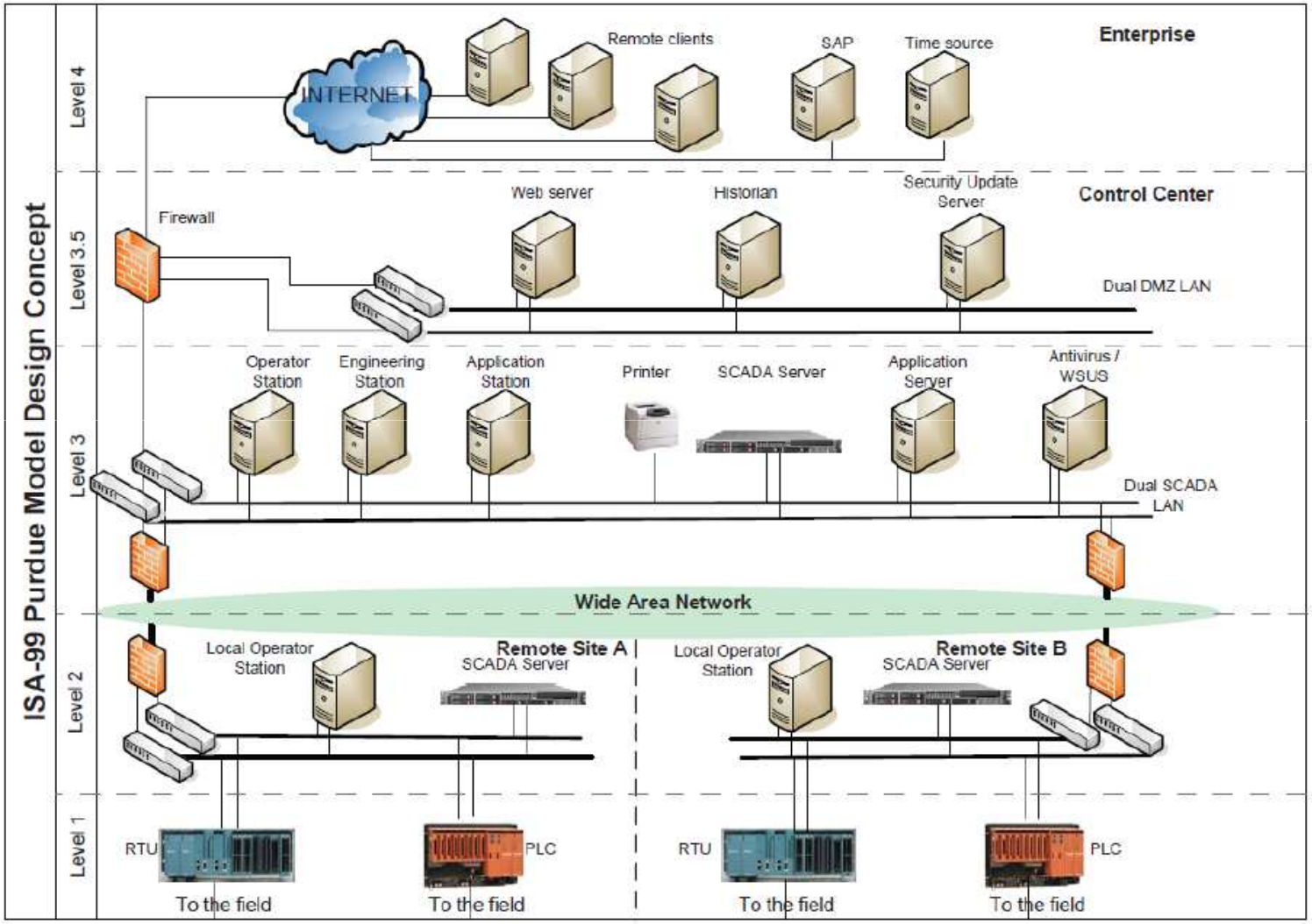
ISACA
Trust in, and value from, information systems

CONVERGENCE ?

- **The convergence of safety and security is happening everywhere in mission-critical embedded systems domains and today's methodologies are inadequately prepared for it.**
- **IEC 62443 and IEC 61508 are reference standards for cybersecurity and functional safety respectively.**
- **Until 2010 both communities are gone by their own**

ISACA
Trust in, and value from, information systems

IEC 62443 (FORMERLY ISA-99)



SCADA Network, in accordance with ISA-99 [ISA / IEC 62443]

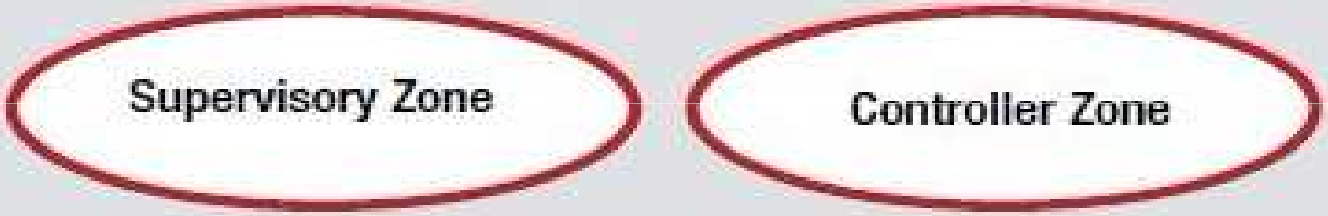
Source: Yokogawa

IEC 62443 ZONES AND CONDUITS

Security Zone Definition

"Security zone: grouping of logical or physical assets that share common security requirements". [ANSI/ISA99.01.01–2007-3.2.116]

A zone has a clearly defined border (either logical or physical), which is the boundary between included and excluded elements.



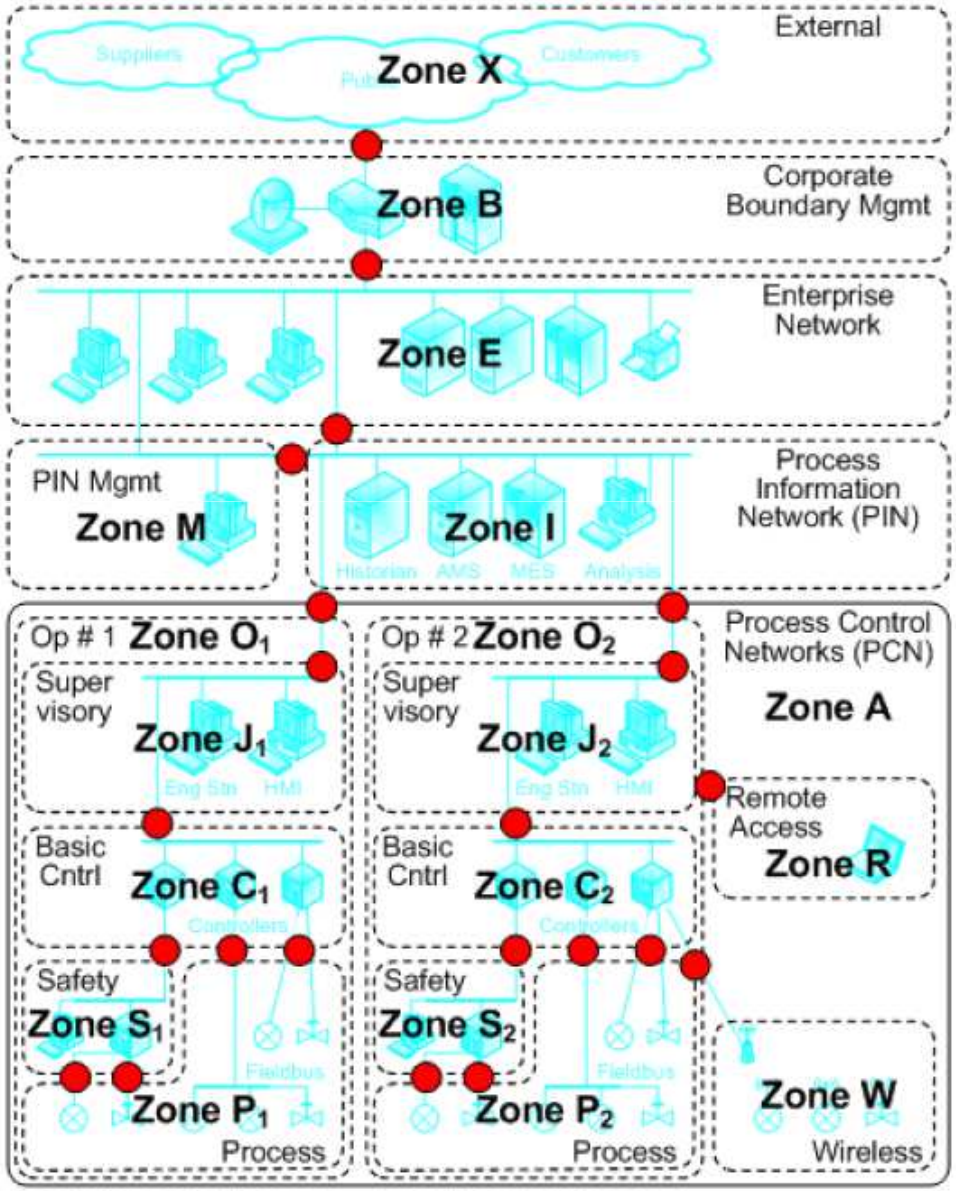
Conduit Definition

A conduit is a path for the flow of information between two zones.

- It can provide the security functions that allow different zones to communicate securely.
- Any transfer of electronic data between zones must have a conduit.

Source: Tofino

IEC 62443 CONDUITS



Source: Honeywell

ISA 99 / IEC 62443 SEGURITY LEVELS

Security Levels (SL)

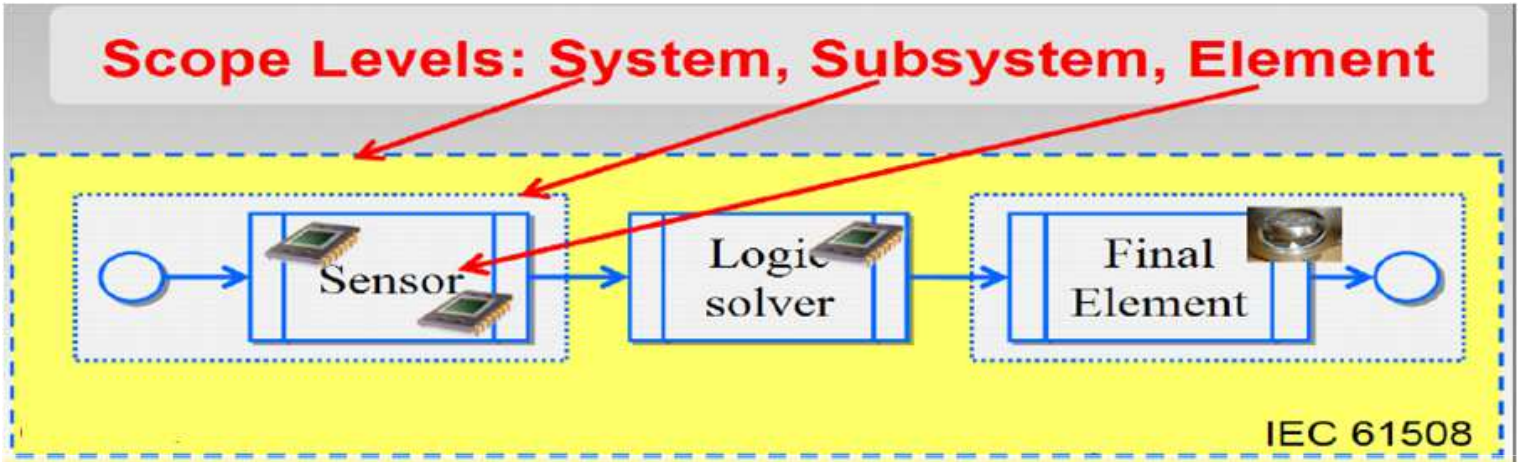
- SL 1 – PROTECTION AGAINST CASUAL OR COINCIDENTAL VIOLATION (I.e. changing a setpoint to a value outside engineering defined conditions, interception of a password send over the network in clear text.)
- SL 2 – PROTECTION AGAINST INTENTIONAL VIOLATION USING SIMPLE MEANS (I.e. virus infection, exploiting commonly known vulnerabilities of DMZ hosts)
- SL 3 – PROTECTION AGAINST INTENTIONAL VIOLATION USING SOPHISTICATED MEANS (I.e. exploits in operating systems, protocols. Attacker requires advanced security knowledge, advanced domain knowledge, advanced knowledge of the target system. I.e. password cracking.)
- SL 4 – PROTECTION AGAINST INTENTIONAL VIOLATION USING SOPHISTICATED MEANS WITH EXTENDED RESOURCES (Similar to SAL 3 but attacker now has extended resources to their disposal. I.e. StuxNet attack)

Source: Honeywell

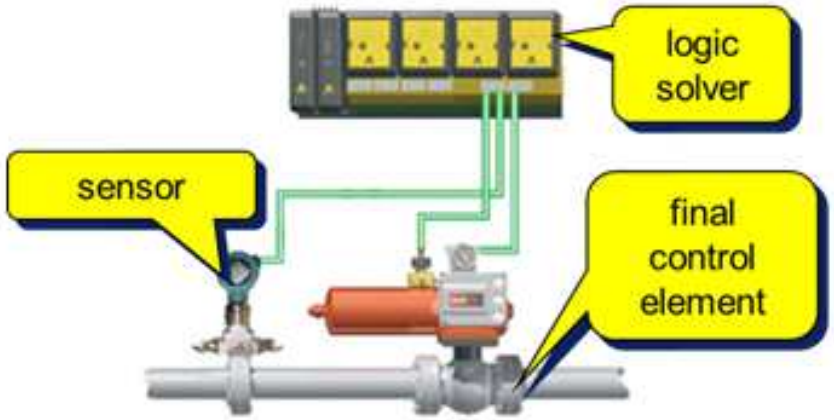
GENERAL PURPOSE VS INDUSTRIAL AUTOMATION PRIORITIES

Source: Yokogawa

IEC 61508 CONCEPTS



- **System**
  - *Subsystems (serial and/or parallel)*
    - *Elements (serial and/or parallel)*



ISACA
Trust in, and value from, information systems

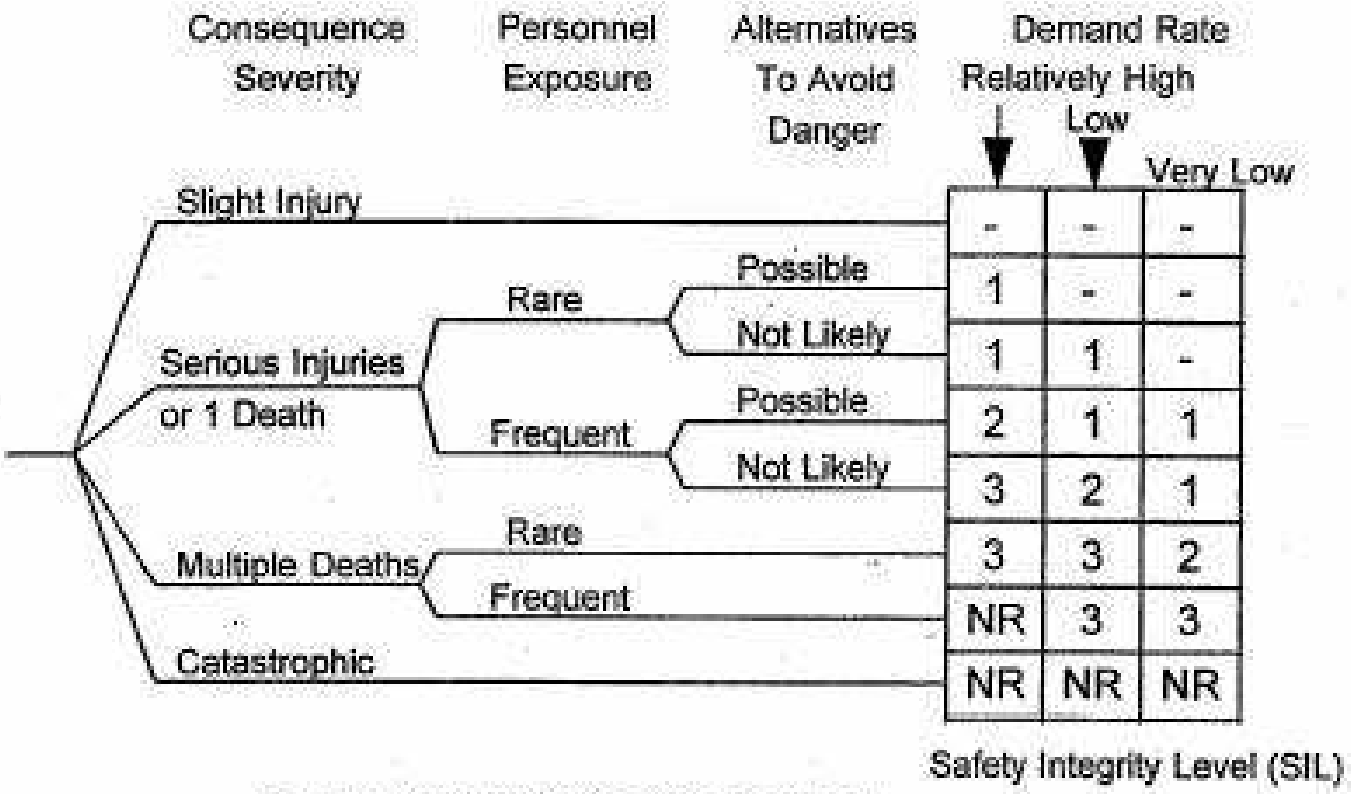
IEC 61508 SIL LEVELS

SIL: *"The Safety Integrity Level is a measure for the effectiveness of the risk reduction that each individual Safety Function is expected to provide"*

Safety Integrity Level	Risk Reduction Factor	PFD_{AVG} : Average Probability of Failure on Demand (Demand Mode)
SIL 4	100,000 – 10,000	$>=10^{-5}$ to $<10^{-4}$
SIL 3	10,000 - 1,000	$>=10^{-4}$ to $<10^{-3}$
SIL 2	1,000 - 100	$>=10^{-3}$ to $<10^{-2}$
SIL 1	100 to 10	$>=10^{-2}$ to $<10^{-1}$

Source: Exida

CONNECTING RISK ANALYSIS WITH SIL



IEC 62061 - ISO 13849-1 MIX FOR MACHINERY

EN IEC 62061

Determining the required SIL

Risk assessment and definition of the required safety integrity level (SIL)

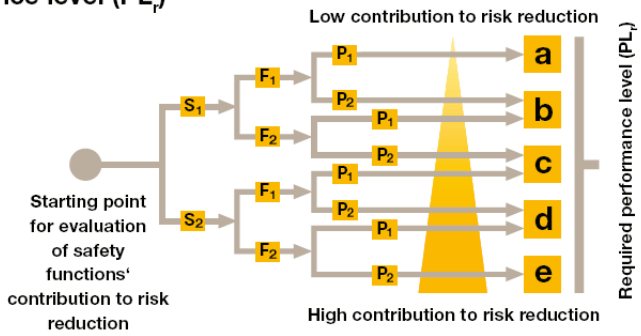
Consequences and severity	Se	Frequency and duration	Fr	Probability of hazardous event	Pr	Avoidance	Av	Class Cl 3-4	5-7	8-10	11-13	14-15
Death, losing an eye or arm	4	≤ 1 hour	5	Very high	5			SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, losing fingers	3	> 1 h – ≤ 1 day	5	Likely	4				OM	SIL 1	SIL 2	SIL 3
Reversible, medical attention	2	> 1 day – ≤ 2 weeks	4	Possible	3	Impossible	5			OM	SIL 1	SIL 2
Reversible, first aid	1	> 2 weeks – ≤ 1 year	3	Rarely	2	Possible	3				OM	SIL 1
		> 1 year	2	Negligible	1	Likely	1					

☐ OM = other measures required

EN ISO 13849-1

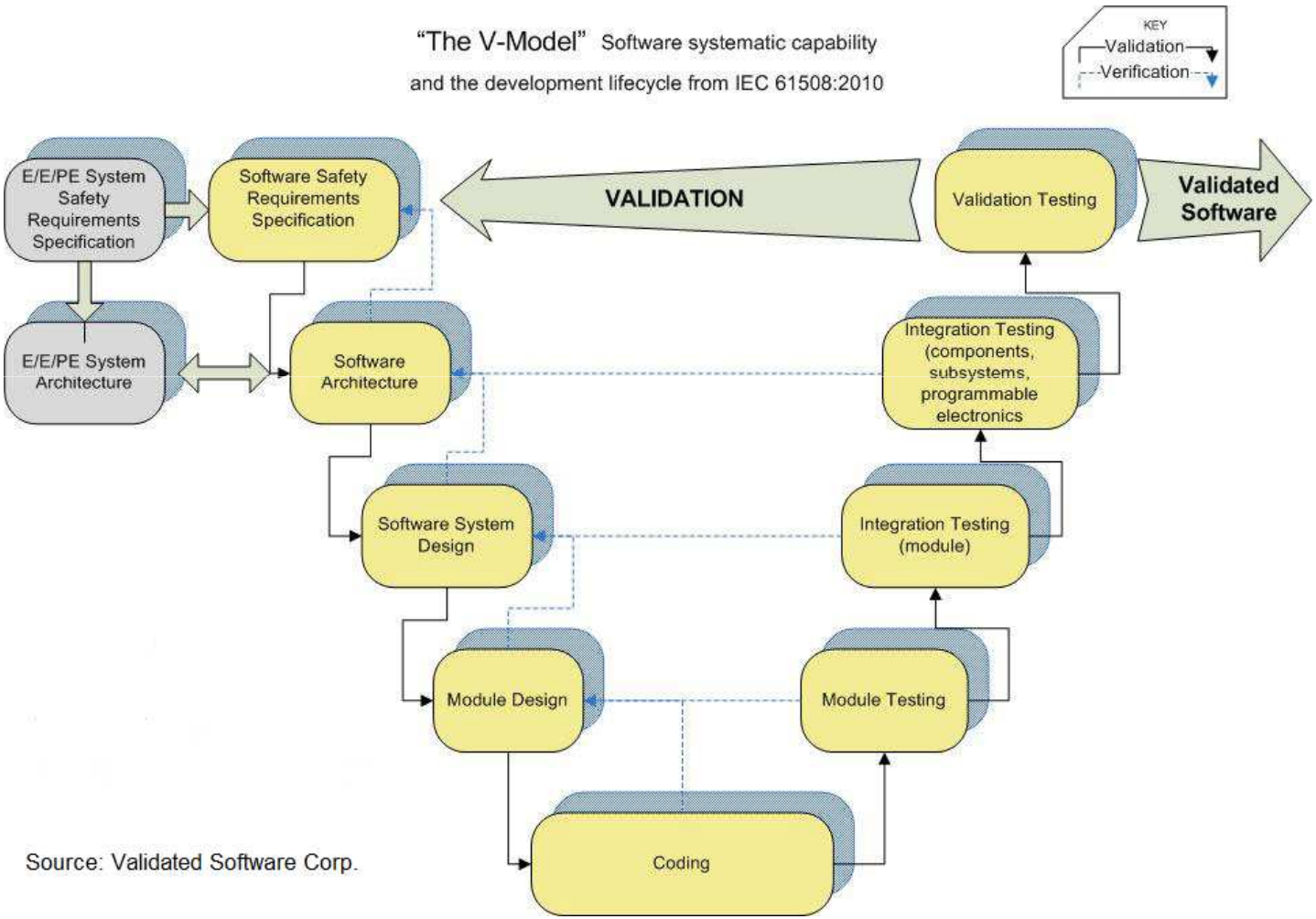
Determination of the required performance level (PL_r)

- **S – Severity of injury**
  - S_1 = Slight (normally reversible injury)
  - S_2 = Serious (normally irreversible injury including death)
- **F – Frequency and/or exposure to a hazard**
  - F_1 = Seldom to less often and/or the exposure time is short
  - F_2 = Frequent to continuous and/or the exposure time is long
- **P – Possibilities of avoiding the hazard or limiting the harm**
  - P_1 = Possible under specific conditions
  - P_2 = Scarcely possible

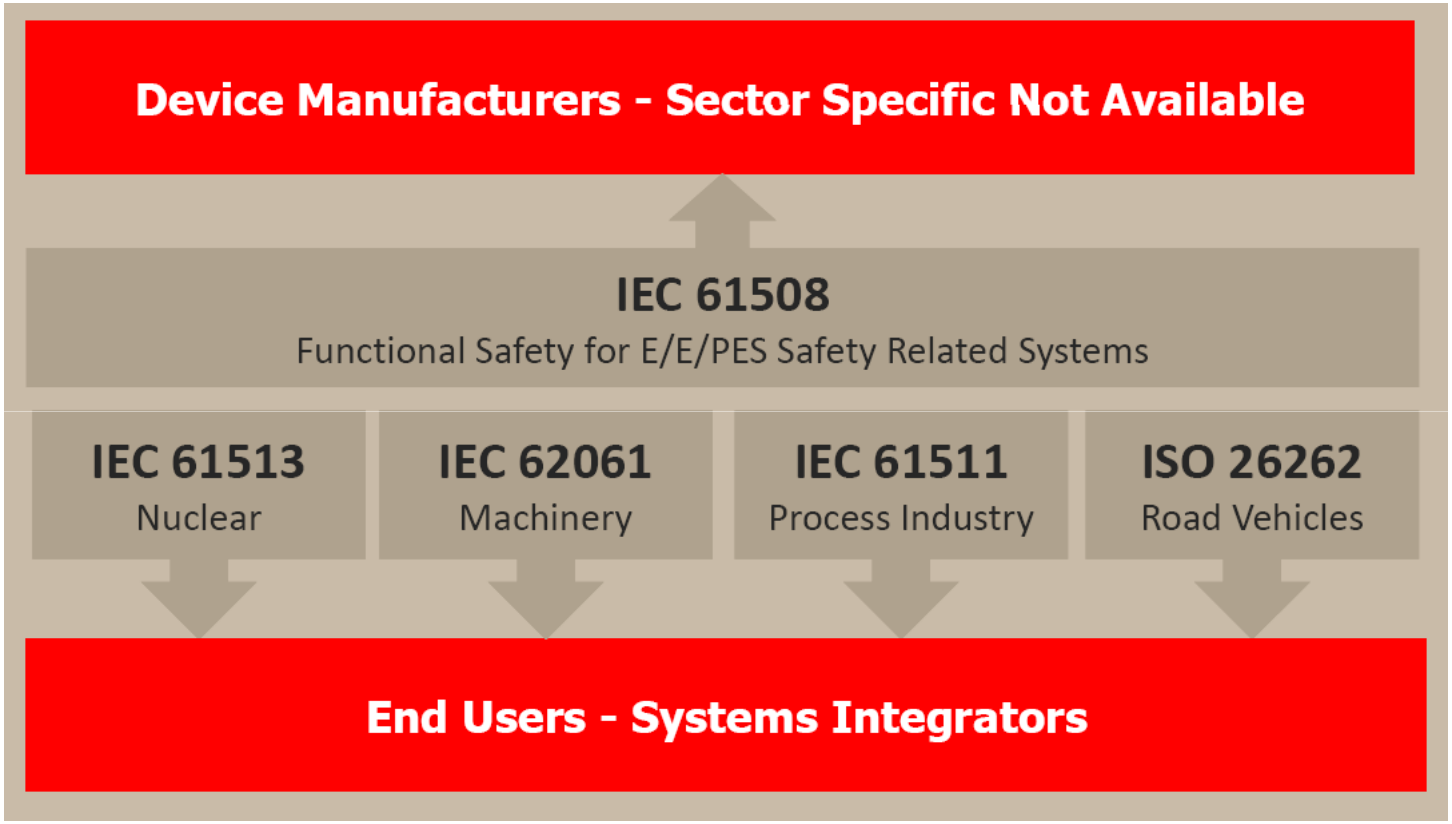


Determination of the PL_r

IEC 61508 AND V-MODEL (SW & HW)



IEC 61508 AND DERIVED STANDARDS



- Related standards: DO-254 (aerospace), EN 50128 (railway)

Source: Exida

ISACA
Trust in, and value from, information systems

IEC 61508 CHANGES IN 2010

- **In 2010 IEC 61508 was changed and updated with no minor changes:**
  - New terminology
  - Better classification of failures
  - System, subsystem and element scopes

- **Cybersecurity was introduced as relevant aspect to the process safety, but it is not mandatory. Anyway it is an important step.**

ISACA
Trust in, and value from, information systems

IEC 61508 ABOUT IEC 62443

- **IEC 61508-1:2010:**

7.5.2.2 If security threats have been identified, then a vulnerability analysis should be undertaken in order to specify security requirements.

NOTE Guidance is given in IEC 62443 series.

ISACA
Trust in, and value from, information systems

IEC 62443 ABOUT IEC 61508

- **IEC 62443-4-1:**

- **Foreword:**

  IEC 61508 can be considered contributing source to this standard.

ISACA
Trust in, and value from, information systems

MESSAGES FROM THE INDUSTRY

- **Organizations like TÜV or companies like Exida raises that safety functions performed by programmable electronic systems (embedded systems) are increasingly responsible for mitigating the risks that installations and systems present to people and the environment.**

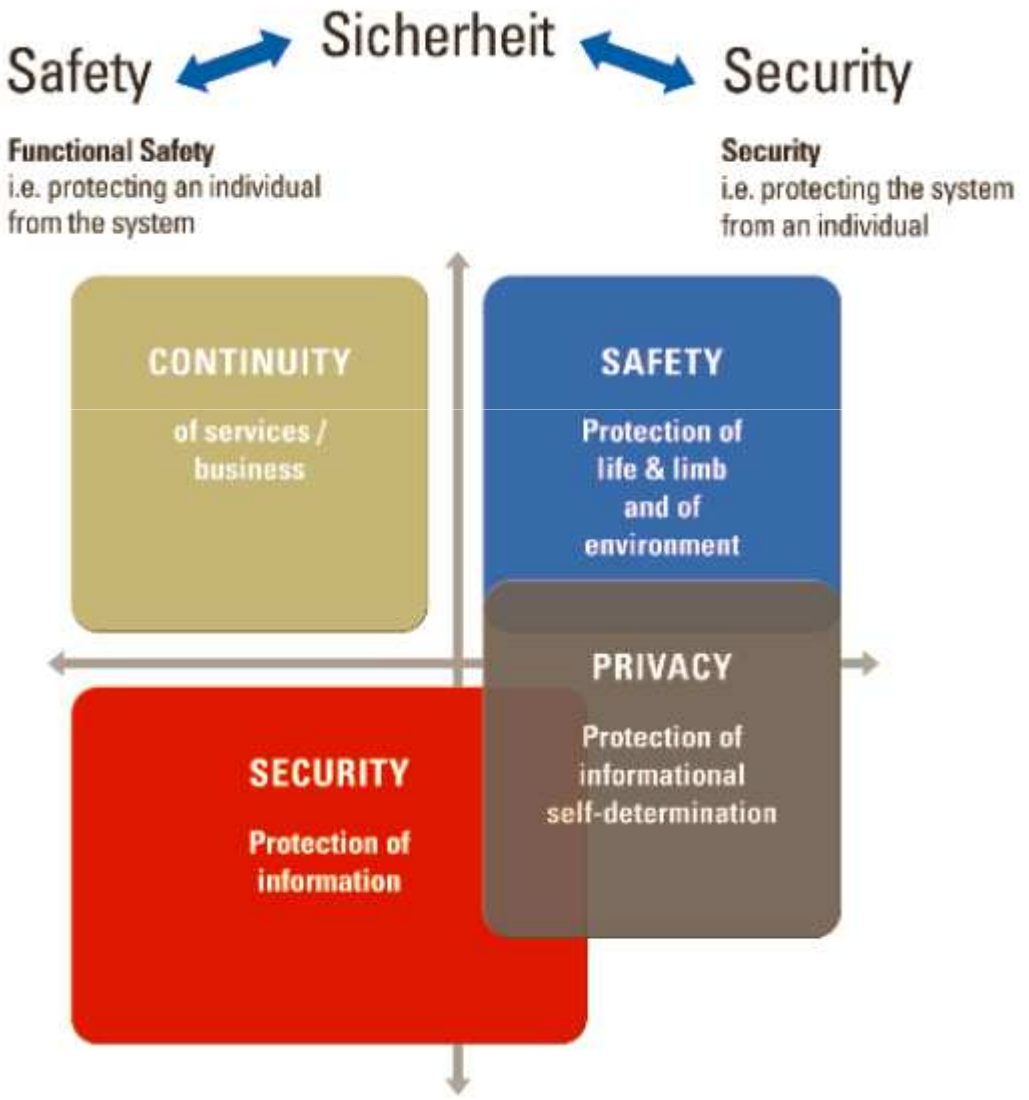
ISACA
Trust in, and value from, information systems

MESSAGES FROM THE INDUSTRY

- **Since “Stuxnet” it has become clear that the safety functions of these electronic controls must be effectively protected against unauthorized access and malicious attacks**
- **Functional Safety & IT Security: Two sides of the same coin**

ISACA
Trust in, and value from, information systems

TÜV COMBINED IEC 62443 AND IEC 61508 CERTIFICATION PROPOSAL



MESSAGES FROM THE ACADEMIA

- **Curtis G. Northcutt, researcher at MIT raises the following question:**

“Is it possible that an attacker altered the values of my signals to put me into another valid state such that now the output of the CPS does not match the inputs of the system, but the state still ‘appears’ to be valid?”

ISACA
Trust in, and value from, information systems

MESSAGES FROM THE ACADEMIA

- **The robustness algorithm provides an answer to this question by yielding a set, the robust zone, which contains all numbers of compromised signals such that no matter what the attacker changes, thus they cannot hide their alterations in the system and we guarantee that we can detect them.**

ISACA
Trust in, and value from, information systems

MESSAGES FROM THE EUROPEAN UNION

- **ECSEL european project is the continuation of the ARTEMIS project for Electronic Components and Systems (including Embedded Systems) for the 2014-2020 period.**
- **Its iniciative global budget is 1.215 billion €**
- **In its documentation the words multi-disciplinary, inter-disciplinary cross-disciplinary, multi-domain or multi-??? appear frequently**

ISACA
Trust in, and value from, information systems

CROSS-??? APPROACH IS A CHALLENGE ITSELF

- **Multidisciplinarity concerns are also developed by Rockwell Automation under the term *convergence* that includes technologic and human multiculturality issues.**
- **Rainer Stetter, director of the ITQ Mechatronics Institute pointed the difficulties of introducing the software dimension in teams with classical mechanical engineering roots.**
- **Safety & security communities have walked by their own historically**

ISACA
Trust in, and value from, information systems

CROSS-???? APPROACH IS A CHALLENGE ITSELF

- **The Bologna Declaration, made in 1999 and basis of the European Higher Education Space (EHEA) refers to the "Trends in Learning Structures in Higher Education" report.**
- **Two ideas appear:**
  - Multi layer system of national *diplómes* (multi country)
  - The emergence of new multidisciplinary institutions
- **C.P. Snow "Two Cultures" debate is still open but multilayer knowledge professionals demand is growing**

ISACA
Trust in, and value from, information systems

CROSS-???? APPROACH AND EMPATHY

- **In the Goleman's Emotional Intelligence competencies catalog there is the empathy competency**
- **Empathy is the "ability of share and understand mental states and emotions of other ones".**
- **Is empathy enough to afford the multi-inter-cross-??? challenges that are coming now ?**

ISACA
Trust in, and value from, information systems

EMULSIVITY

- **We propose a new emotional intelligence competency called *emulsivity*, defined as the "ability to maintain states of empathy steadily over time"**
- **It can be used to manage hybrid models, even with contradictions**
- **The word emulsivity comes from the term emulsion, that can be defined as a "stable mixture of substances, which by nature tend to repel"**

ISACA
Trust in, and value from, information systems

EMULSIVITY AND THE *ALLIOLI* APPROACH

- **An example of emulsion that can be used as a metaphor is *allioli***
- **There are many popular contests that consist of obtain *allioli* using manual and traditional techniques.**
- **Know-how and endeavour are shown by the participants in order to reach the emulsion.**
- **Emulsivity is a competency that can be learned and trained.**

ISACA
Trust in, and value from, information systems

AN OPTIMISTIC INTERPRETATION

- **THERE ARE ENCOURAGING SIGNALS COMING FROM THE INDUSTRY AND THE ACADEMIA CONVERGENT TO BUILD CONSISTENT MULTIDISCIPLINARY FRAMEWORKS IN ORDER TO AFFORD THE UPCOMING SAFETY & SECURITY CHALLENGES**

ISACA
Trust in, and value from, information systems

Thank you!!

Questions ?

Xavier Pi

Embedded Systems Working Group Chair, Industrial Policy & Technology Innovation Commission

COEIC.com

xpi@enginyers.net

ISACA

Trust in, and value from, information systems