IK4 IKERLAN
Research Alliance

Multicore, WCET and IEC-61508 certification of fail-safe mixed-criticality systems

WCET Workshop
Lund (7th July)

Jon Perez
jmperez@ikerlan.es

Outline

01 Context

02 Multicore is what you need / what you will have

03 The need and opportunity

04 Wind turbine and railway case studies

05 Conclusions and lessons learnt

IKERLAN

01

Context

Some Research Projects: Multicore & mixed-criticality

DREAMS

MultiPARTES

Contrex

CERTAINTY

PROXIMA

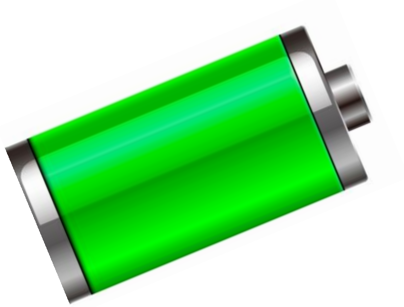
TACLe
Timing Analysis on Code-Level

EMC²

P-SOCRATES

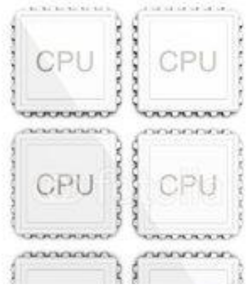
Keynote in a nutshell

Market Pull

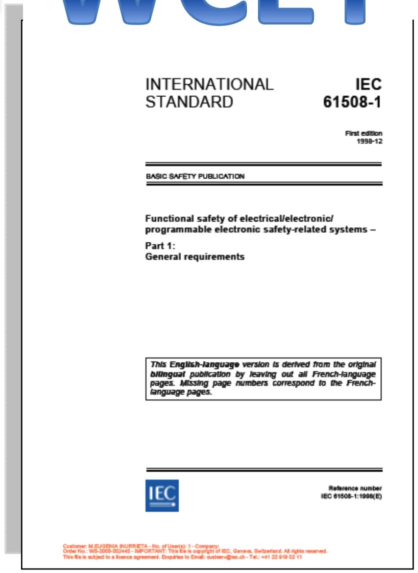


+

Technology Push



WCET



INTERNATIONAL STANDARD — IEC 61508-1

First edition 1998-12

BASIC SAFETY PUBLICATION

Functional safety of electrical/electronic/programmable electronic safety-related systems –

Part 1:
General requirements

This English-language version is derived from the original bilingual publication by leaving out all French-language pages. Missing page numbers correspond to the French-language pages.

IEC

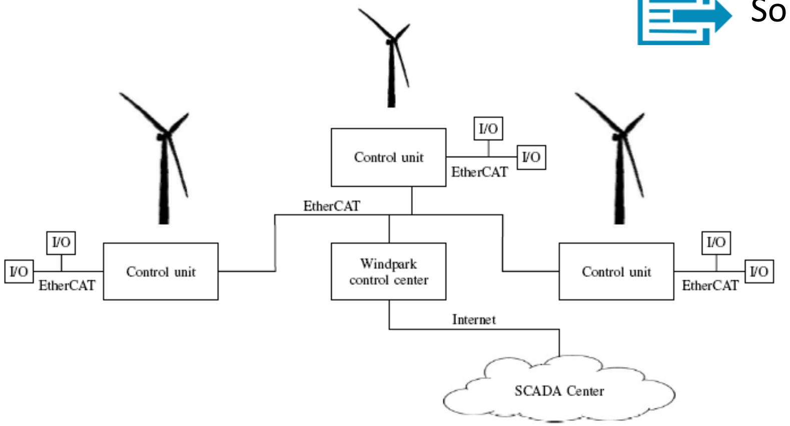
Reference number
IEC 61508-1:1998(E)

=

Product H2020

Off-shore Wind Turbine

- A modern off-shore wind turbine dependable control system manages [1,2]:
  - **I/Os**: up to three thousand inputs / outputs.
  - **Function & Nodes**: several hundreds of functions distributed over several hundred of nodes.
  - **Distributed**: grouped into eight subsystems interconnected with a fieldbus.
  - **Software**: several hundred thousand lines of code.



Source: www.alstom.com

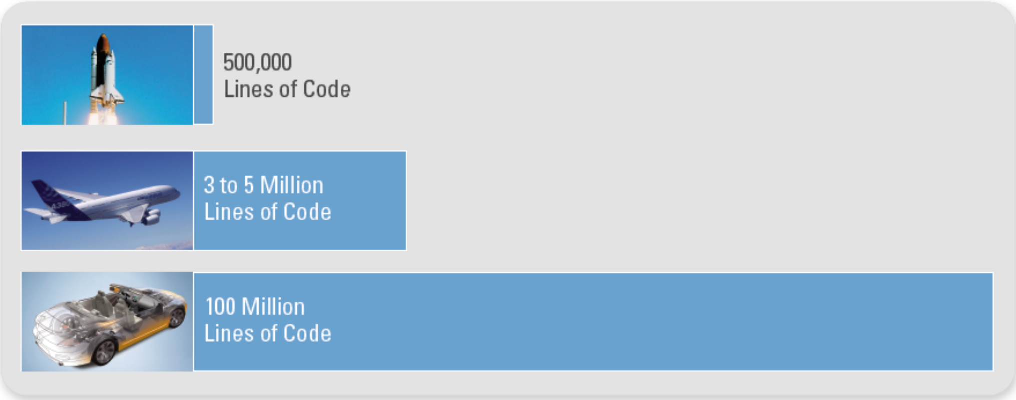
[1] Perez, J., et al. (2014). A safety concept for a wind power mixed-criticality embedded system based on multicore partitioning. Functional Safety in Industry Application, 11th International TÜV Rheinland Symposium, Cologne, Germany.

[2] Perez, J., et al. (2014). "A safety certification strategy for IEC-61508 compliant industrial mixed-criticality systems based on multicore partitioning." Euromicro DSD/SEAA Verona, Italy.

◊ Automotive domain:

- The software component in high-end cars currently totals around 20 million lines of code, deployed on as many as 70 ECUs [1].
- Automotive electronics accounts for some 30 % of overall production costs and is rising steadily [1].
- A premium car implements about 270 functions that a user interacts with, deployed over 67 independent embedded platforms, amounting to about 65 megabytes of binary code [2].

[3]



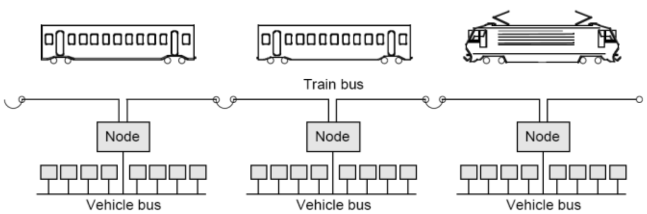
[4]

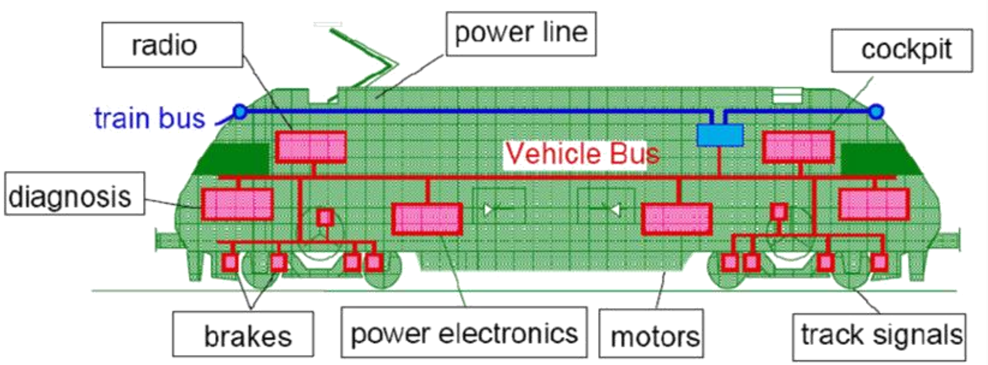
[1] Darren Buttle, ETAS GmbH, Germany, Real-Time in the Prime-Time, ECRTS (KEYNOTE TALK), 2012.
[2] Christian Salzmann and Thomas Stauner. Automotive software engineering. In Languages for System Specification, pages 333–347. Springer US, 2004.
[3] Leohold, J. Communication Requirements for Automotive Systems. 5thIEEE Workshop on Factory Communication Systems (WCFS). Wien, 2004.
[4] National Instruments, How engineers are reinventing the automobile,, http://www.ni.com/newsletter/51684/en/ , 2013.

Railway

◊ (On-board) railway domain:

- The ever increasing request for safety, better performance, energy efficient, environmentally friendly and cost reduction in modern railway trains have forced the introduction of sophisticated dependable embedded systems [1].
- The number of ECUs (Electric Control Units) within a train system is of the order of a few hundred [2,3].
- Groups of distributed embedded systems:
  - Train Control Unit.
  - Railway Signalling (e.g. ETCS).
  - Traction Control.
  - Brake Control.
  - Etc.





[1] The European Rail Research Advisory Council (ERRAC), Joint Strategy for European Rail Research 2020.

[2] Kirrmann, H. and P. A. Zuber (2001). "The IEC/IEEE Train Communication Network." IEEE Micro vol. 21, no. 2: 81-92.

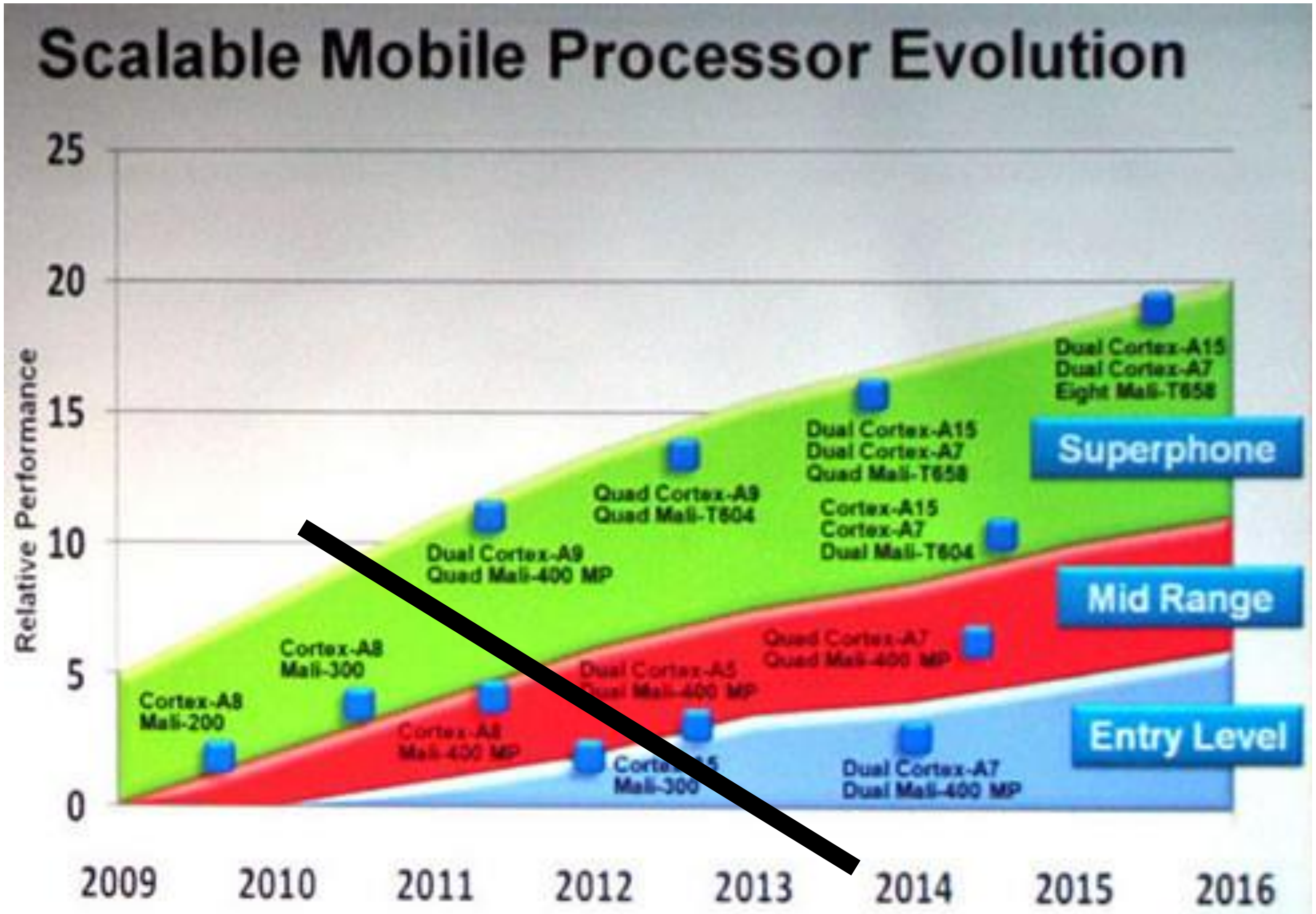
[3] F. Corbier, et al, *How Train Transportation Design Challenges can be addressed with Simulation-based Virtual Prototyping for Distributed Systems,* 3rdEuropean congress Embedded Real Time Software (ERTS), France, 2006.

IKERLAN

02

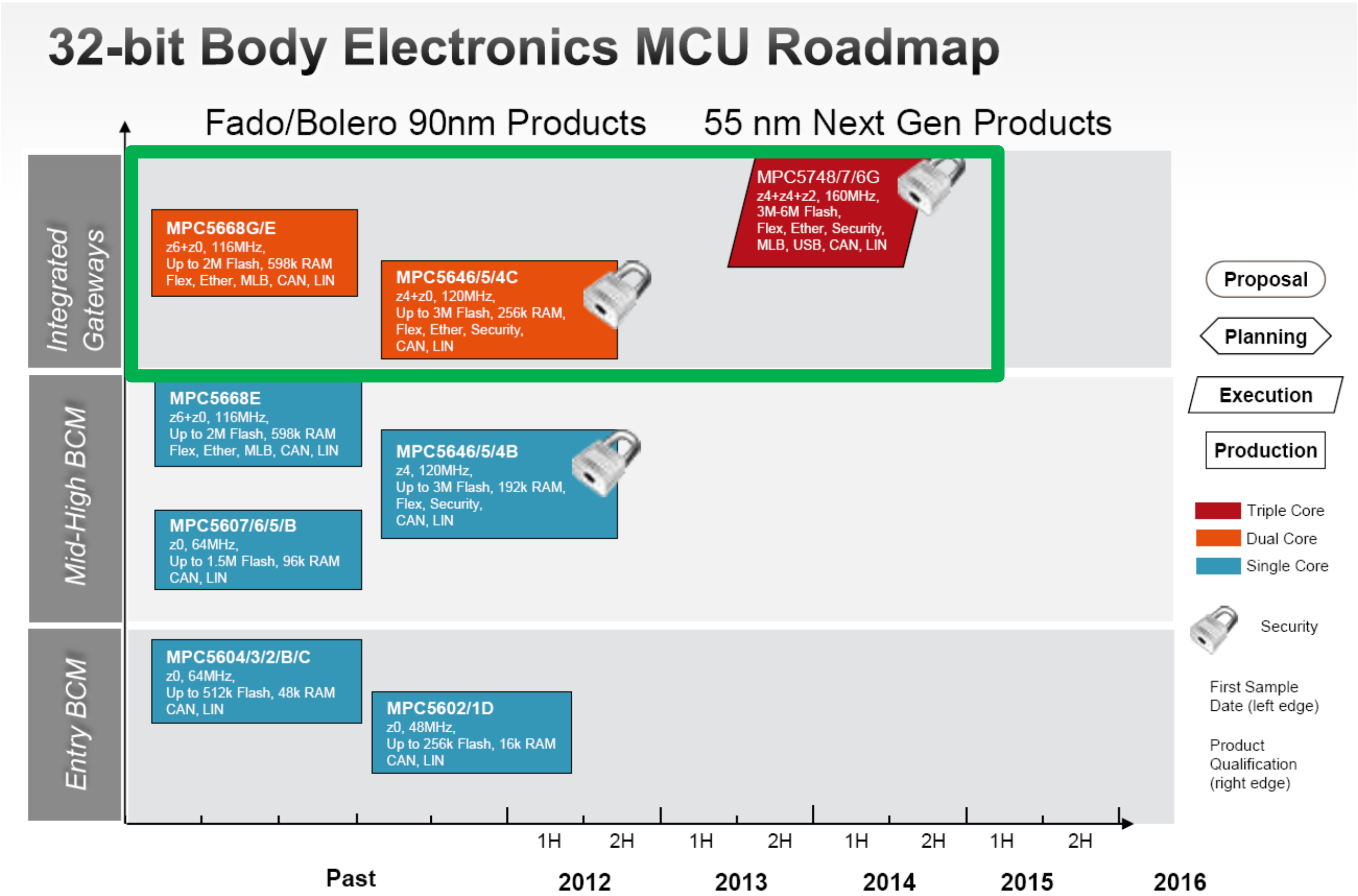
Multicore is what you need...
Multicore is what you will have...

Multicore & Mobile



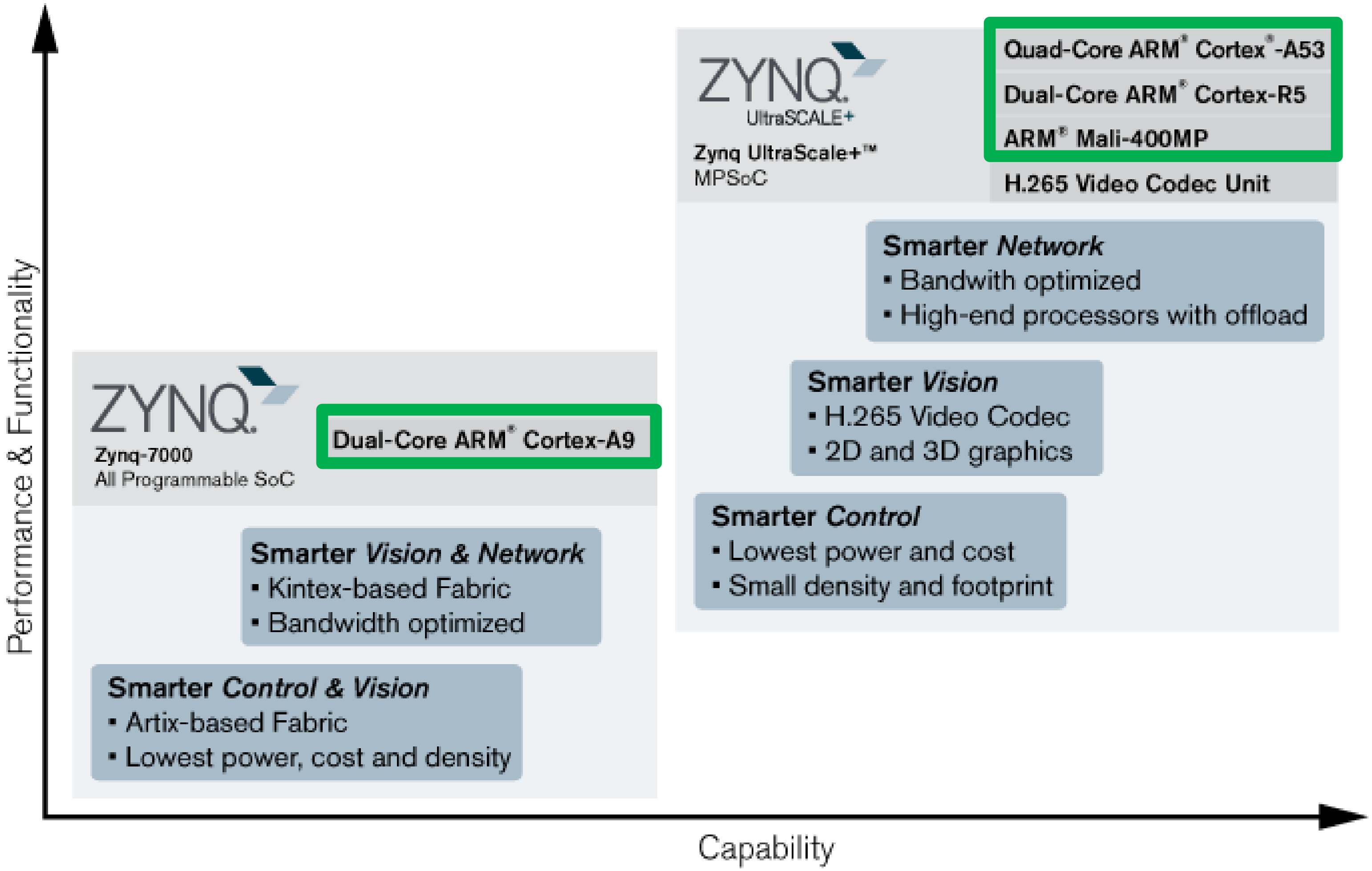
Source: www.arm.com

Multicore & Automotive



Source: www.freescale.com

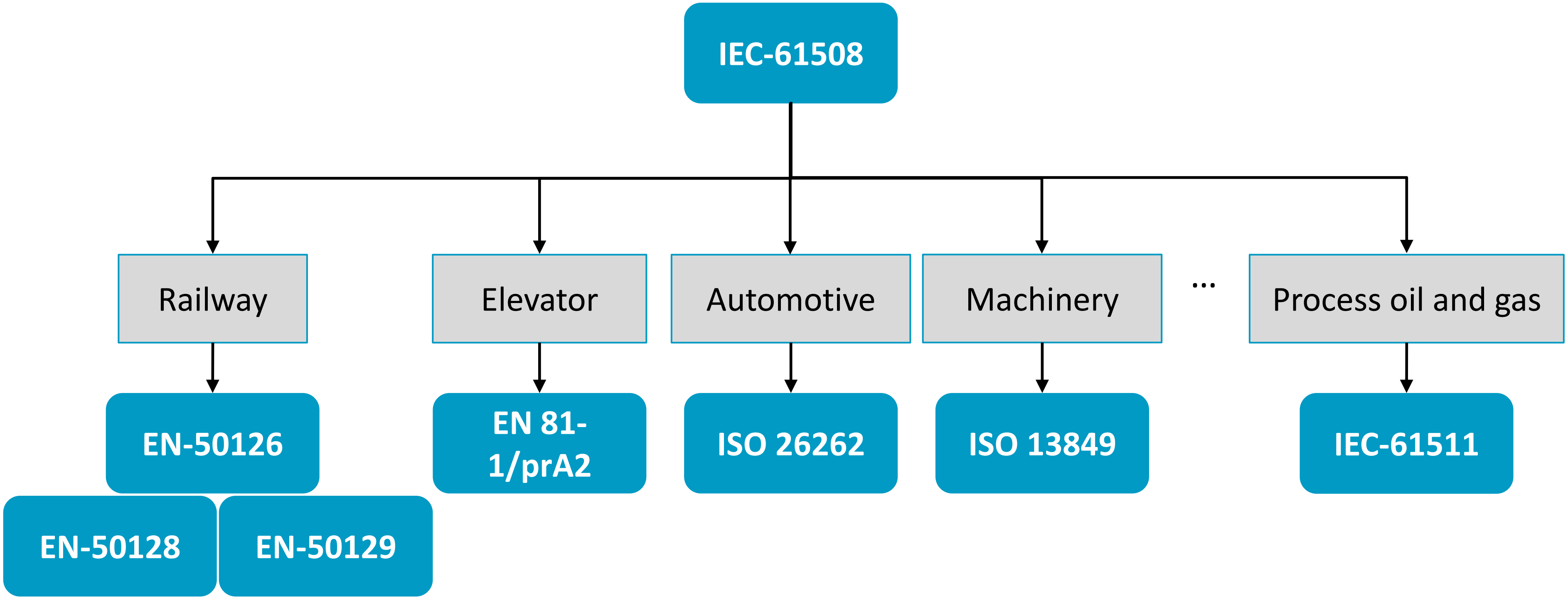
Generic purpose multicore



Source: www.xilinx.com

Safety certification (IEC-61508)

- IEC-61508: Functional safety of electrical / electronic / programmable electronic safety-related systems.



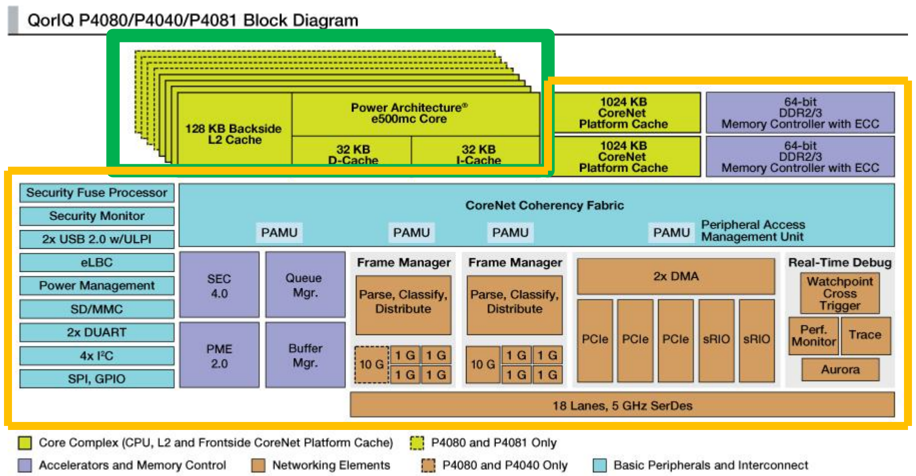
IEC-61508 safety standard & WCET

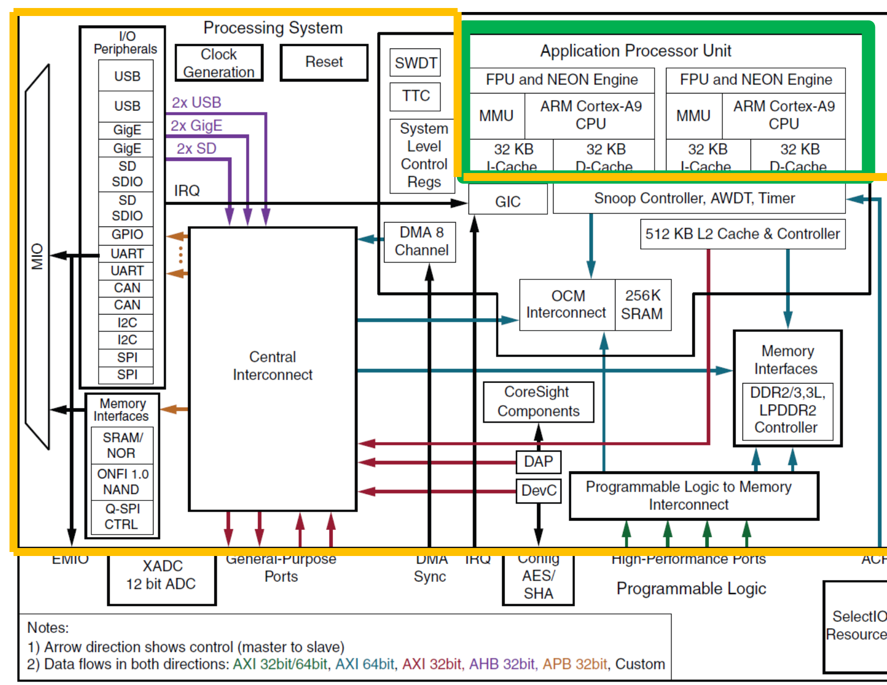
IEC-61508	ISO-26262
(7.4.2.2) The design method chosen shall possess features that facilitate the expression of: […] (4) **timing constraints**	(7.4.5) The software architectural design shall describe dynamic design aspects of the software components, including: [...] **the temporal constraints**
	(7.4.17) An **upper estimation** of required resources for the embedded software shall be made, including: (a) **the execution time**;
(IEC-61508-3 Annex F) Non-interference between software elements on a single computer: **F.5**: **cyclic scheduling** algorithm which gives each element a defined time slice supported **by worst case execution time** analysis of each element to demonstrate statically that the timing requirements for each element are met	(Annex D) Freedom from interference between software elements **D2.2:** With respect to timing constraints the effects of faults such as [...] **incorrect allocation of execution time** shall be considered and mechanisms such **as cyclic execution scheduling** can be considered.

Threats to be considered and managed

Threats to be considered and managed

◊ Worst Case Execution Time (WCET)





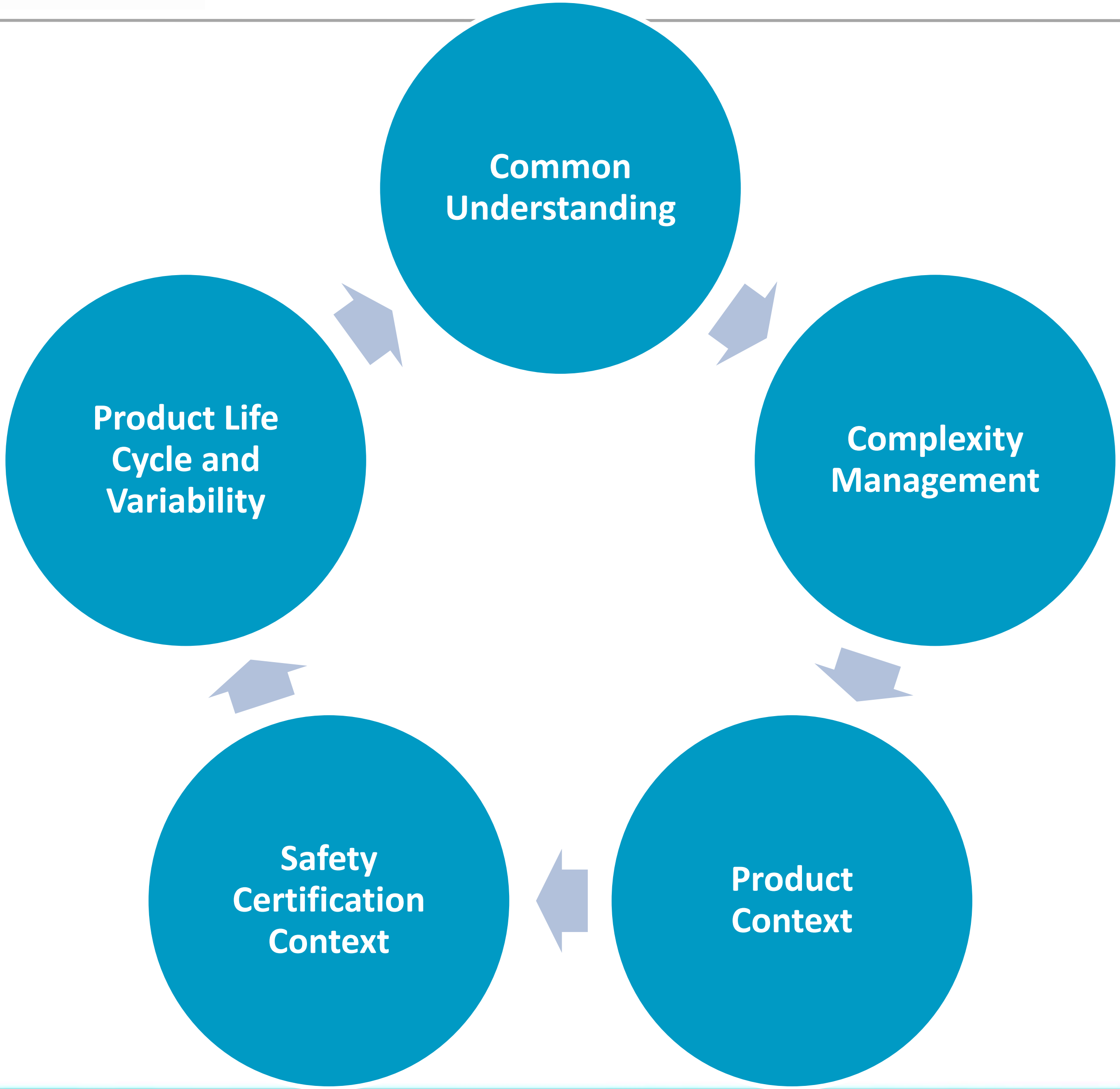
Source: www.freescale.com, www.xilinx.com

03

The need and opportunity

IK4 IKERLAN Research Alliance

Time to think.....



IKERLAN

03-A

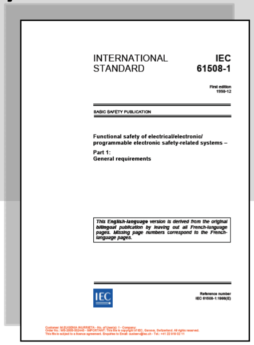
Common understanding

"What then is time? If nobody asks me, I know what time is, but if I am asked then I am at a loss what to say" (St. Augustine)

Basic Concepts / Different Terms

- Safety
  - Safety Critical
  - Mission Critical
- Temporal isolation
- Modular certification (?)
- Scheduling:
  - Vestas model
- Etc.

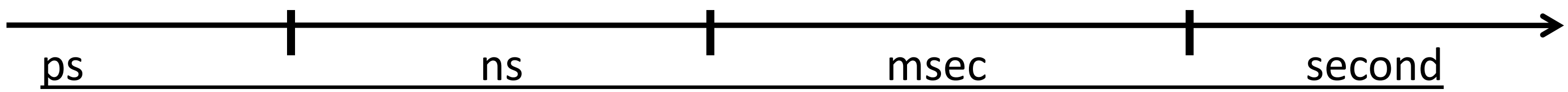
- Functional Safety
  - Fail safe / Fail operational
  - High demand / Low demand
- Temporal independence
- Compliant Item
- Scheduling (IEC-61508-3):
  - Deterministic scheduling methods
    - Time Triggered Architecture
    - Cyclic scheduling
- Etc.

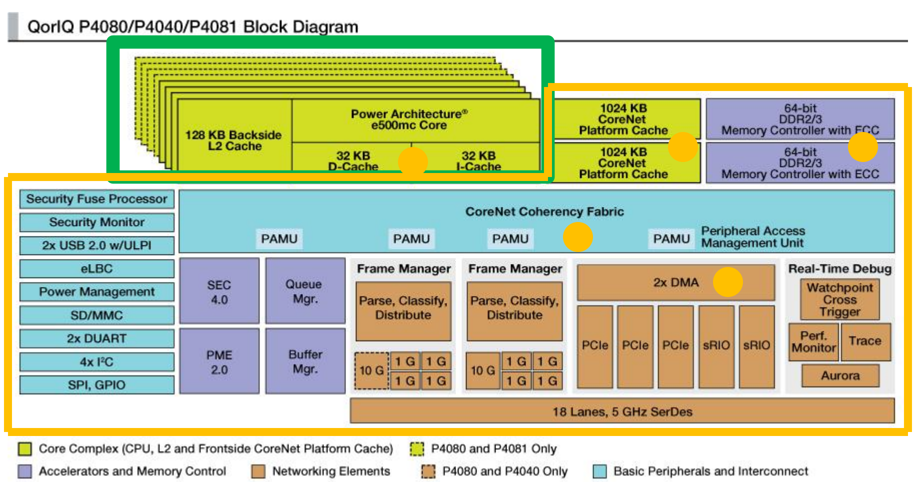

INTERNATIONAL STANDARD
IEC 61508-1
First edition 1998-12
BASIC SAFETY PUBLICATION
Functional safety of electrical/electronic/programmable electronic safety-related systems –
Part 1:
General requirements
This English-language version is derived from the original bilingual publication by leaving out all French-language pages. Missing page numbers correspond to the French-language pages.
Reference number
IEC 61508-1:1998(E)

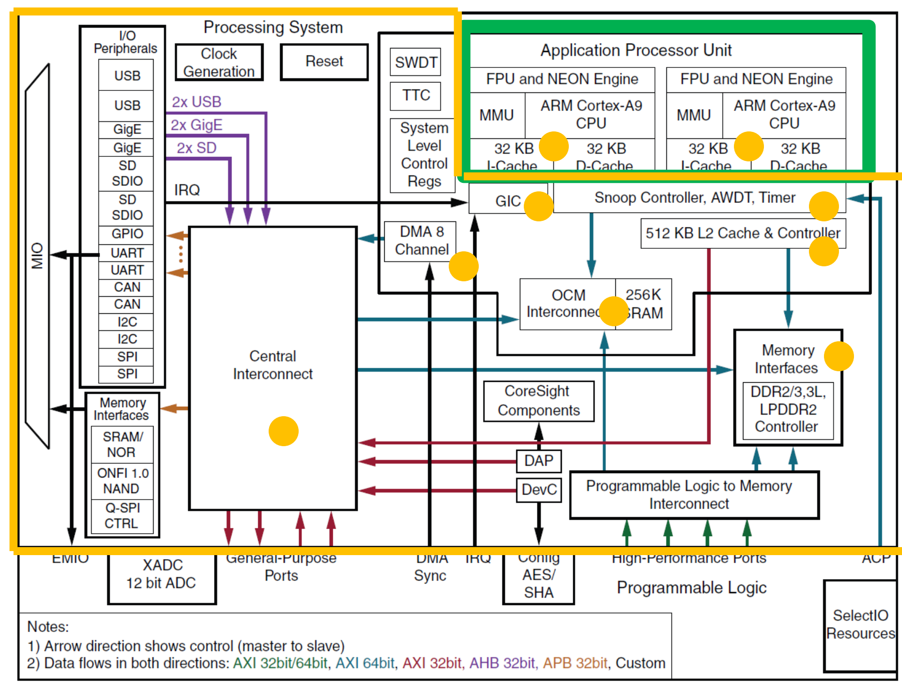
Threats to be considered and managed

◊ Temporal & Spatial independence, e.g., Shared resources (e.g., memory, cache, bus, interrupts) [1]

Which is the time-scale of the temporal interference?







[1] Kotaba, O., et al. (2013). Multicore In Real-Time Systems – Temporal Isolation Challenges Due To Shared Resources. Workshop on Industry-Driven Approaches for Cost-effective Certification of Safety-Critical, Mixed-Criticality Systems (WICERT). Dresden (Germany).

Source: www.freescale.com, www.xilinx.com

IKERLAN

03-B

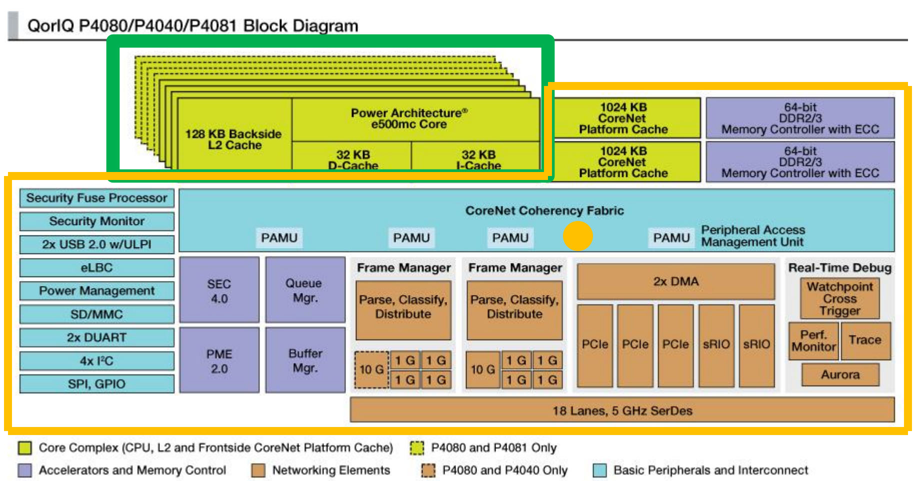
Complexity Management

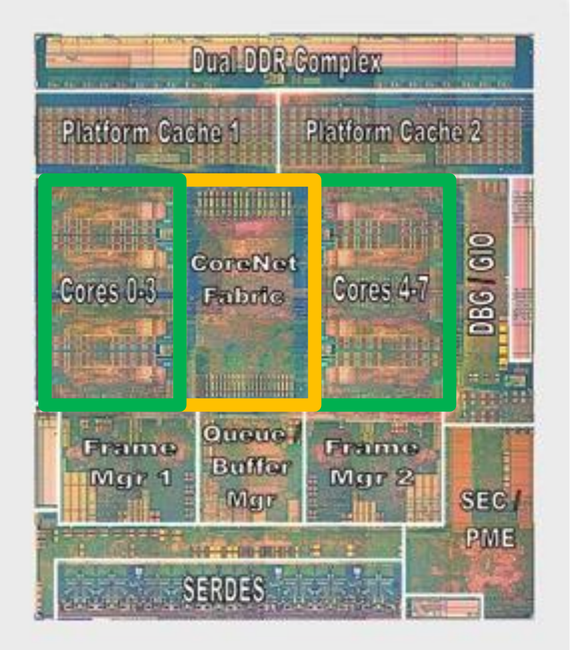
"Simplicity does not precede complexity, but follows it." (Alan Perlis)

"Fools ignore complexity. Pragmatists suffer it. Some can avoid it. Geniuses remove it." (Alan Perlis)

Threats to be considered and managed

- Complex (new) hardware components, e.g., Core interconnect fabric
- Lack of detailed documentation



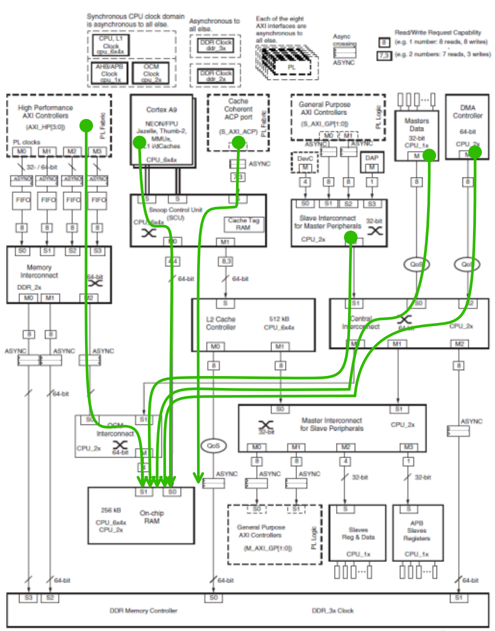


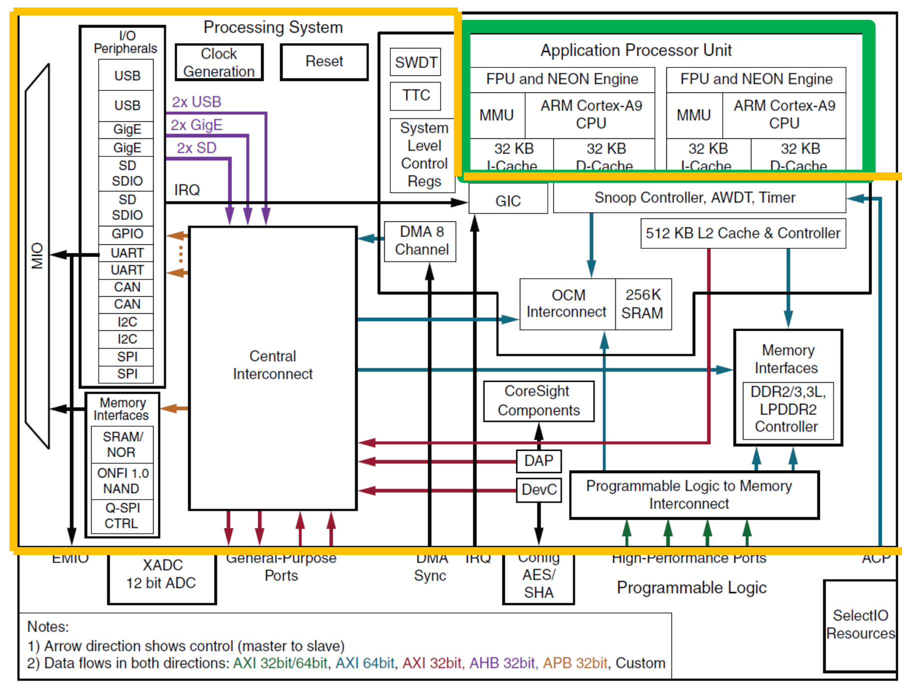
[1] http://www.advancedsubstratenews.com/2009/12/multicores-perfect-balance/

Source: www.freescale.com, www.xilinx.com

Threats to be considered and managed

- Interference among safety related and non safety related functions, e.g.
  - Safe configuration.
  - Safe startup and boot.
  - Safe shutdown.
  - Exclusive access to peripherals.
  - Resource virtualization.
- Diagnosis





Source: www.freescale.com, www.xilinx.com

Complexity management

Complexity management

- Complexity: "the degree to which a system or component has a design or implementation that is difficult to understand and verify"
- Cognitive complexity and number four:
  - Human cognitive capabilities and four simultaneous relationships [1, 2]
  - Working memory capacity for up to four simultaneous chunks of information [3]
  - Quaternary relations are the most complex we can handle [1, 2]
  - Human working memory capacity limited also to about four chunks of information [3]
- Complexity Management [4]: abstraction, partition and segmentation

Simplicity does not precede complexity, but follows it. (Alan Perlis)

Fools ignore complexity. Pragmatists suffer it. Some can avoid it. Geniuses remove it. (Alan Perlis)

[1] Bernhard Rumpler et al. Considerations on the complexity of embedded real-time system design tasks. In IEEE International Conference on Computational Cybernetics (ICCC), Tallinn, Estonia, 2006..

[2] Graeme S. Halford et al. How many variables can humans process? Psychological Science, 16(1):70–76, 2005.

[3] Nelson Cowan. The magical number 4 in short-term memory: a reconsideration of mental storage capacity. Behavioral and Brain Sciences, 24(1):87–114, 2001.

[4] H. Kopetz. The complexity challenge in embedded system design. In 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC), pages 3–12, 2008.

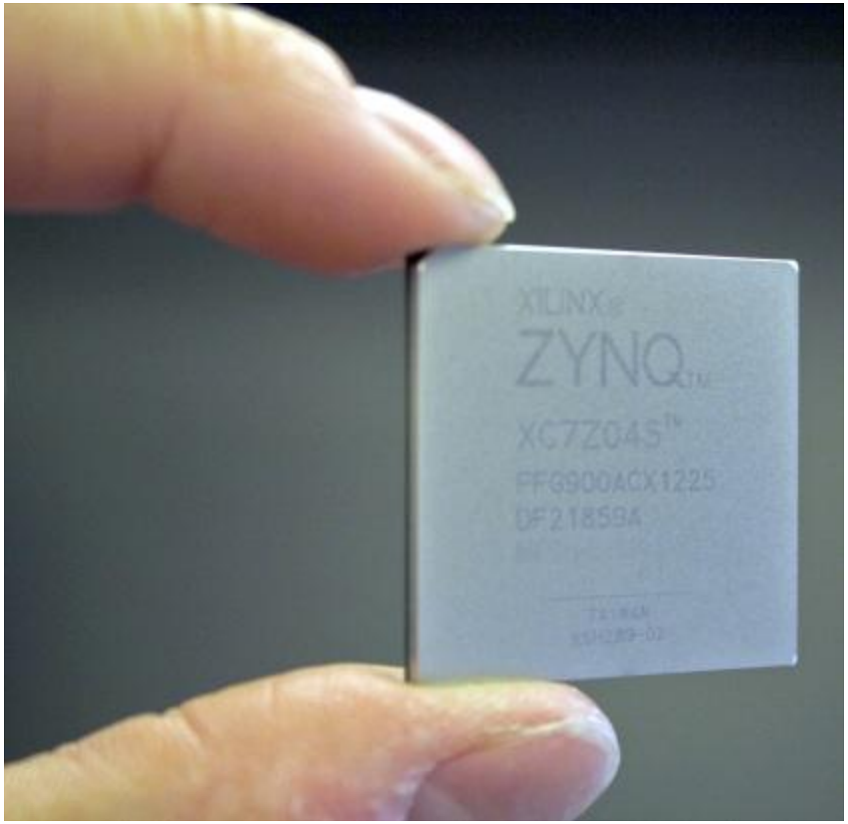
IKERLAN

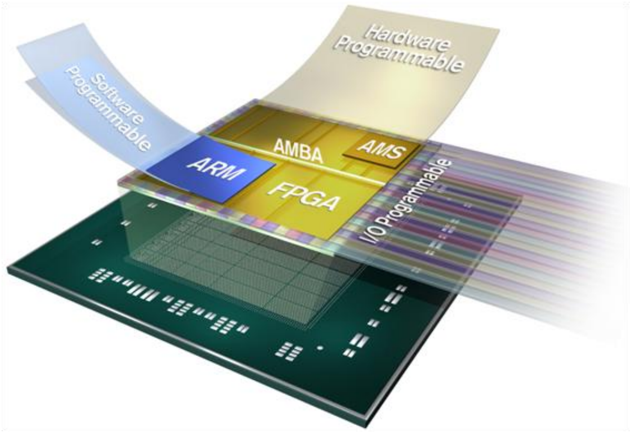
03-C

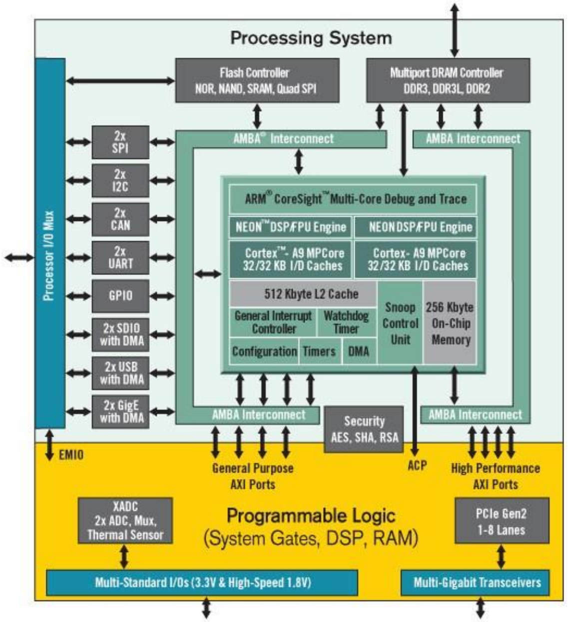
Product Context

"However beautiful the strategy, you should occasionally look at the results." (Sir Winston Churchill)

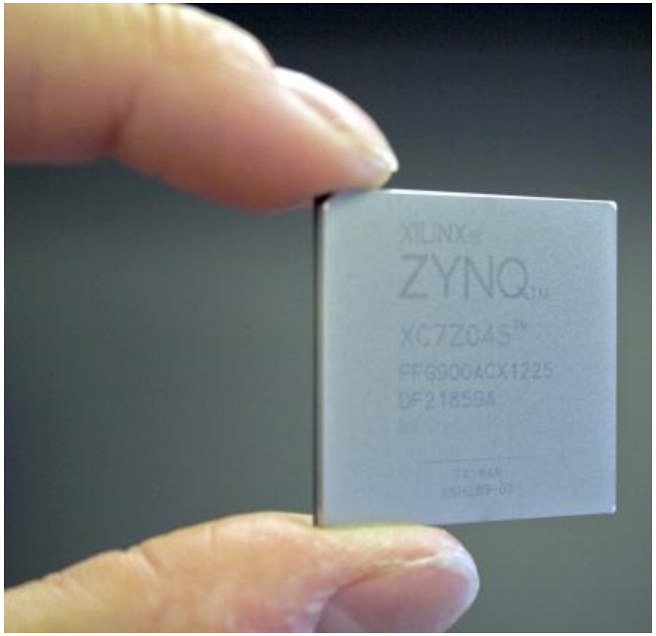
Understand the context..... Product





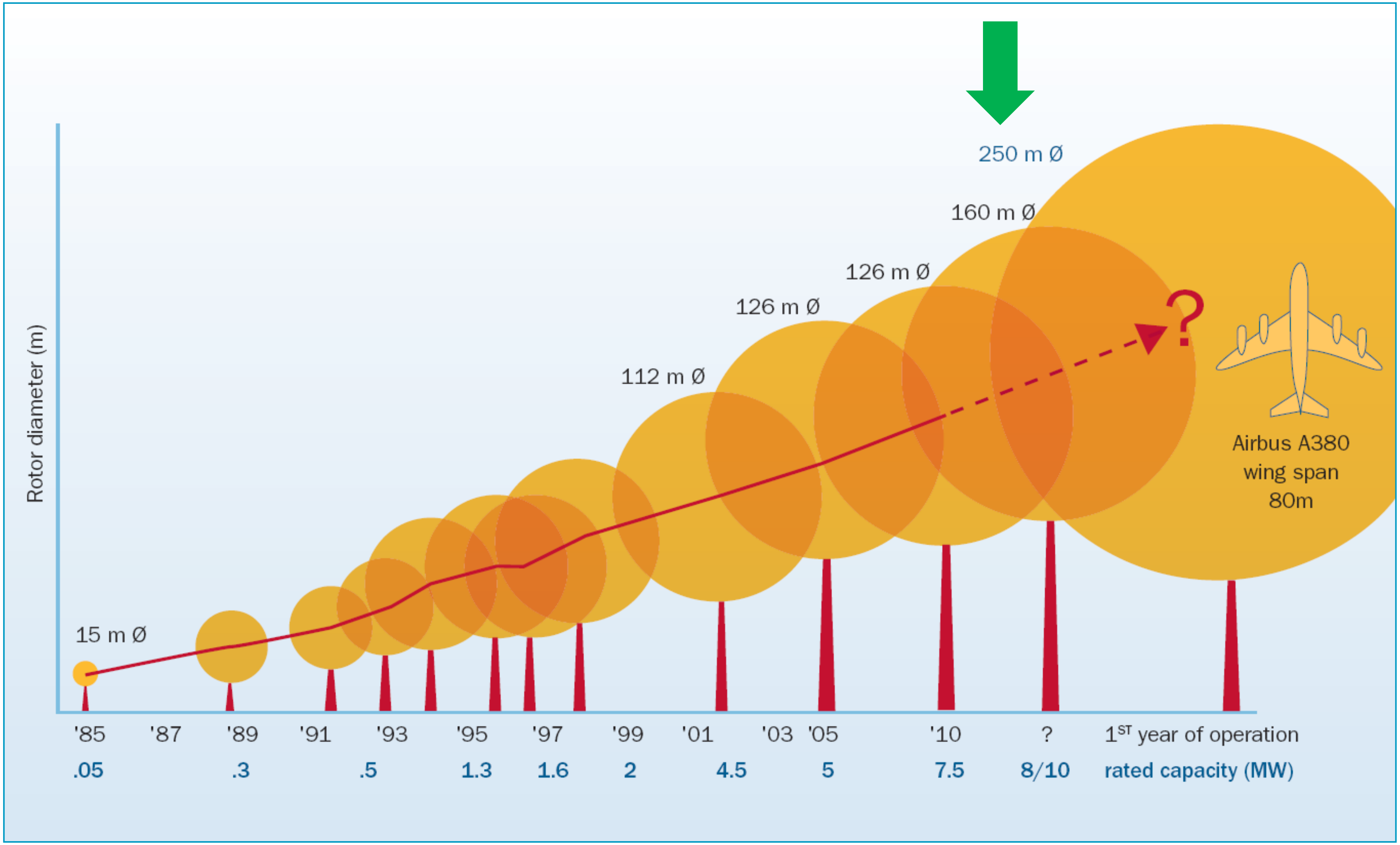


Understand the context..... Product



Source: www.xilinx.com, www.alstom.com

Understand the context..... Product



[1] Upwind – Design limits and solutions for very large wind turbines, March 2011

Understand the context..... Product

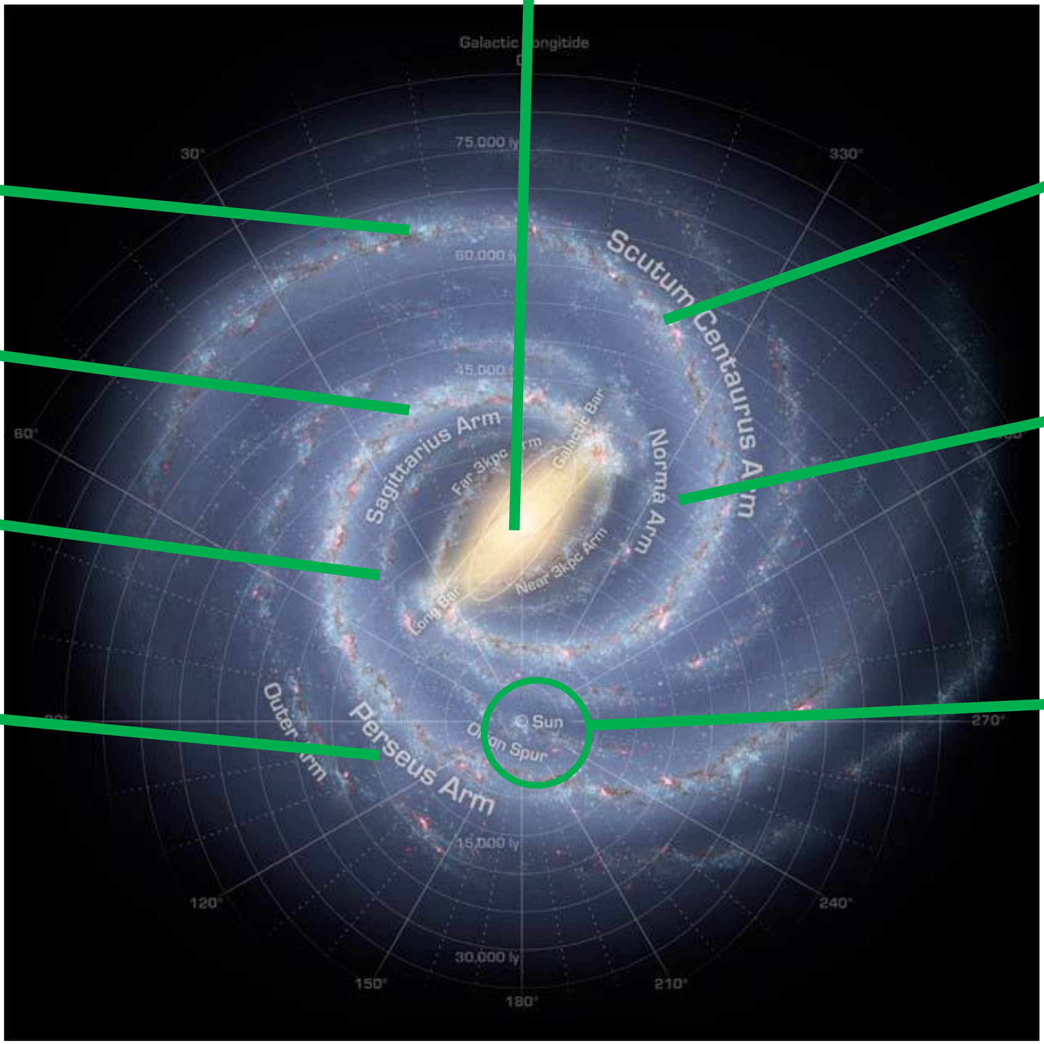
€ & time

Production

Installation, commission, etc.

Maintenance

Control Engineering



Mechanical Engineering

Electrical & Power Electronics Engineering

Embedded Systems

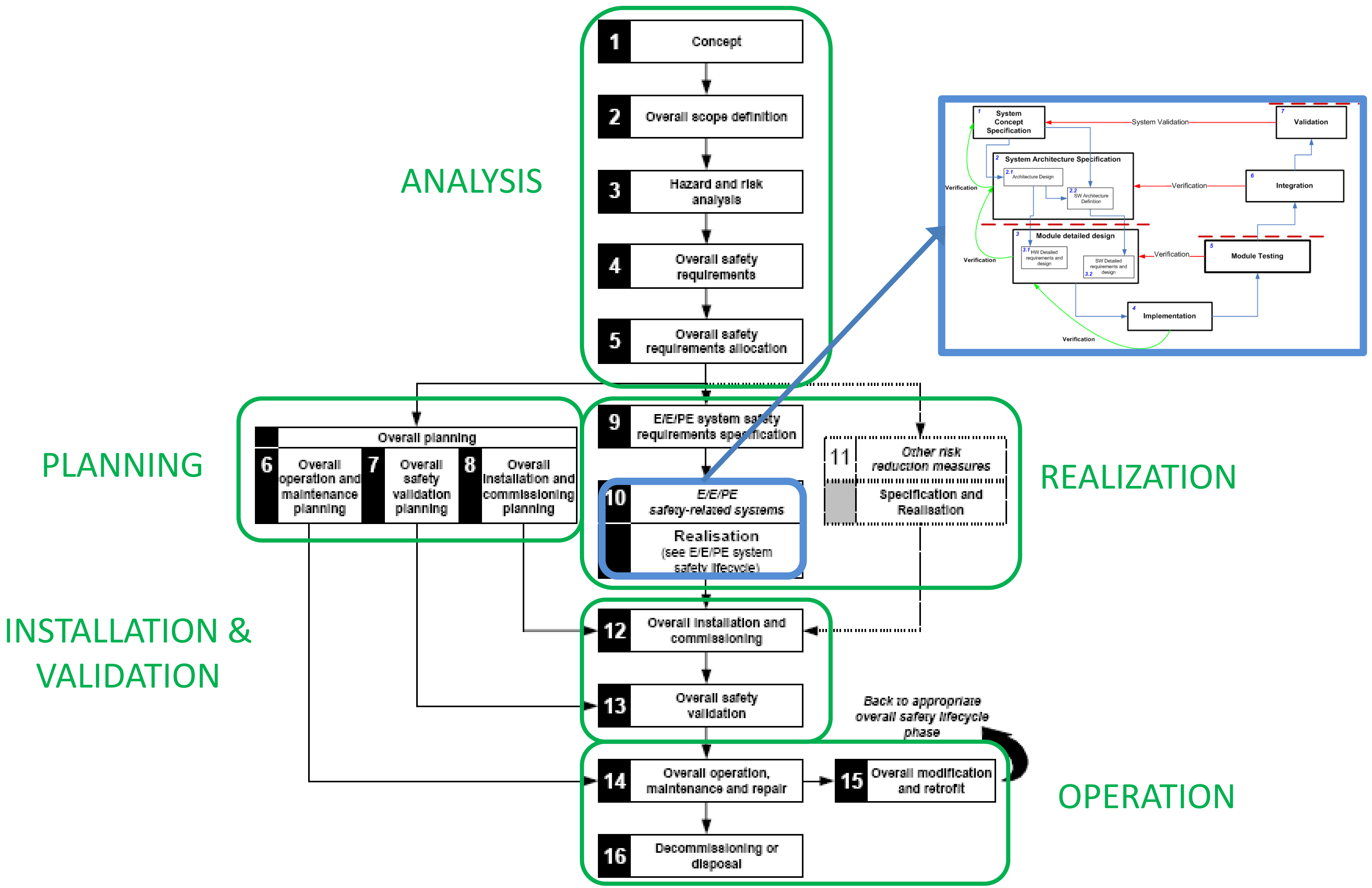
Source: http://www.space.com/5448-images-milky-loses-arms.html

03-D

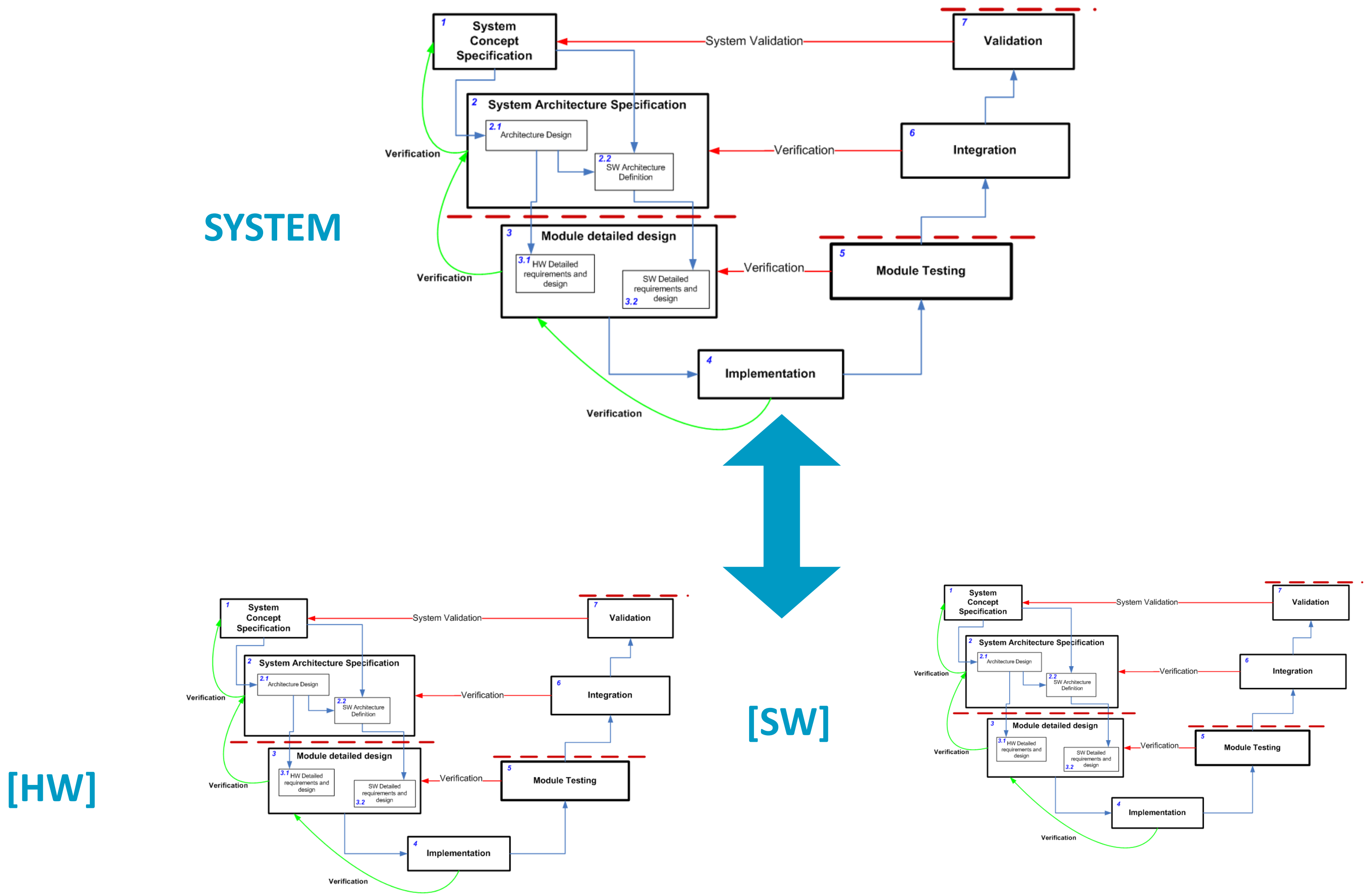
Safety certification context

"For me context is the key - from that comes the understanding of everything." (Kenneth Noland)

Understand the context... Safety Standard



Understand the context... Safety Standard



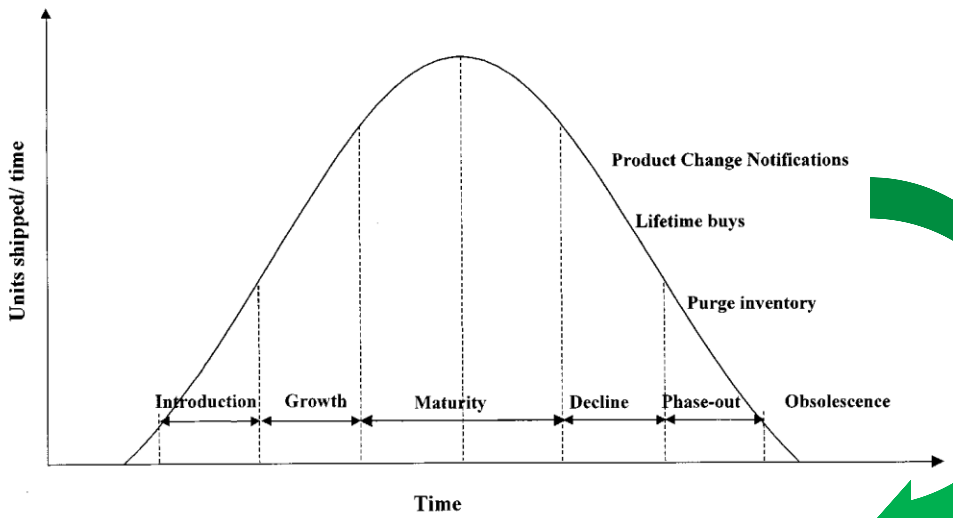
IKERLAN

03-E

Product Life Cycle & Variability

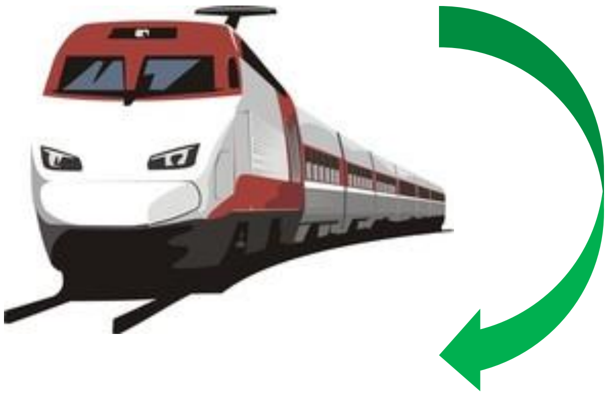
"The ability to ask the right question is more than half the battle of finding the answer." (Thomas J. Watson)

Product vs. Part life cycle curves



Part life cycle curves [1]

5 years



40 years

[|] Pecht, M. G. and D. Das (2000). "Electronic part life cycle." Components and Packaging Technologies, IEEE Transactions on 23(1): 190-192.

Variability of embedded processor features

- **Manufacturer**
- **Core Family**
  - ARM
  - X86
  - PowerPC
- **Number of cores**
- **Timers**
- **Memory, e.g.,**
  - Cache (hierarchy, size, type)
  - RAM Memory (hierarchy, size, type)
  - ROM Memory (e.g., Flash)
  - External memory support (e.g. DDR3)
- **Buses, e.g.,**
  - Internal bus (hierarchy, type, width)
  - External bus interfaces (e.g. PCIe)
  - Communication buses (e.g. CAN, Ethernet, I2C, I2S, SPI, USB)
  - DMA
- **I/Os, e.g.,**
  - GPIOs
  - ADCs (type, resolution, number of channels)
  - PWM
- **Safety compliance**
- **Target Application**
- **Temperature Range (e.g. Industrial)**
- **Clock Frequency**
- **Supply voltage**
- **Package Type**

IKERLAN

04

Wind turbine and railway case studies

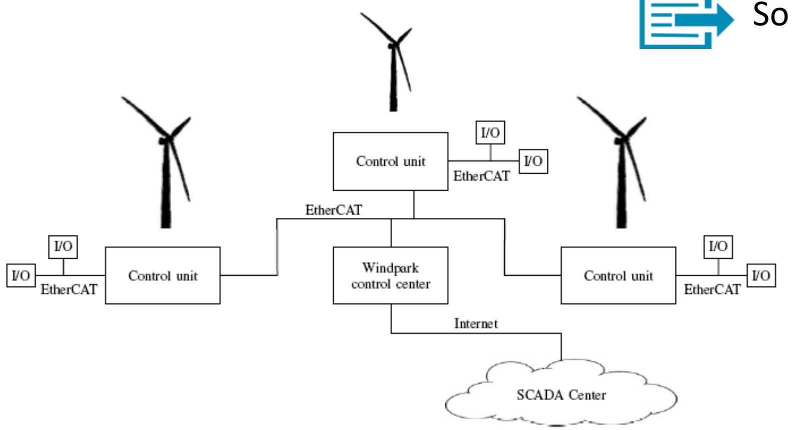
"Nihil est enim simul et inventum et perfectum." (Nothing is ever invented and perfected at the same time)

(Cicero, Brutus 71)

Off-shore Wind Turbine

◊ A modern off-shore wind turbine dependable control system manages [1,2]:

- **I/Os**: up to three thousand inputs / outputs.
- **Function & Nodes**: several hundreds of functions distributed over several hundred of nodes.
- **Distributed**: grouped into eight subsystems interconnected with a fieldbus.
- **Software**: several hundred thousand lines of code.



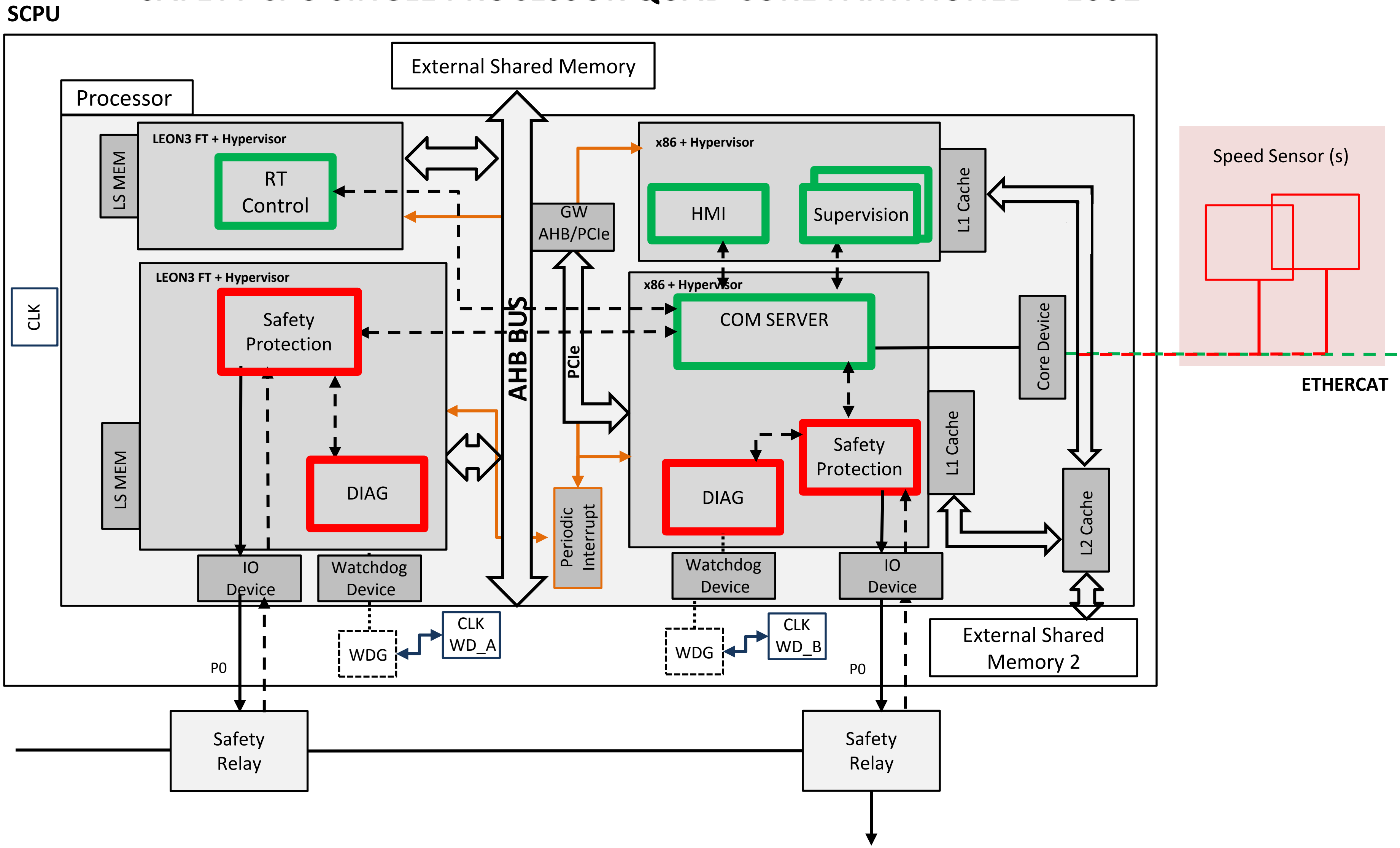
Source: www.alstom.com

[1] Perez, J., et al. (2014). A safety concept for a wind power mixed-criticality embedded system based on multicore partitioning. Functional Safety in Industry Application, 11th International TÜV Rheinland Symposium, Cologne, Germany.

[2] Perez, J., et al. (2014). "A safety certification strategy for IEC-61508 compliant industrial mixed-criticality systems based on multicore partitioning." Euromicro DSD/SEAA Verona, Italy.

Safety Concept – (B - 'Multicore partitioning')

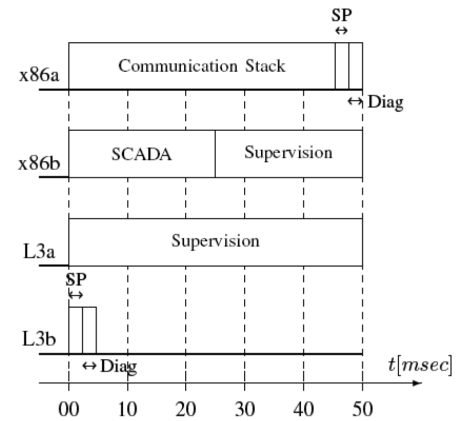
SAFETY CPU SINGLE PROCESSOR QUAD CORE PARTITIONED – 1oo2



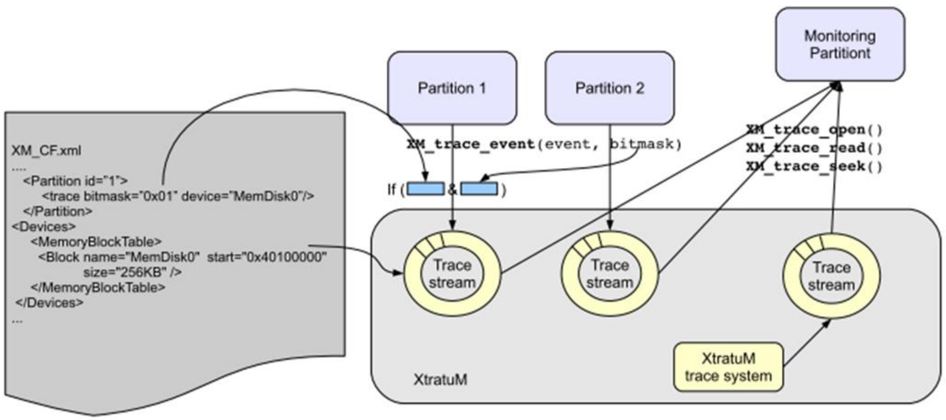
IK4 IKERLAN Research Alliance

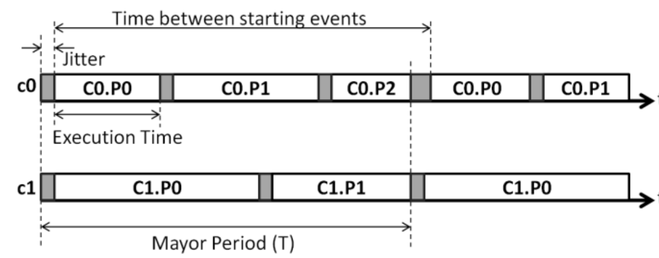
Safety Concept – (B - ‘Multicore partitioning’)

- Scheduling (IEC-61508-3 Annex E):
  - Static cyclic scheduling algorithm.
  - Pre-assigned guaranteed time slots defined at design
  - Synchronized based on the global notion of time



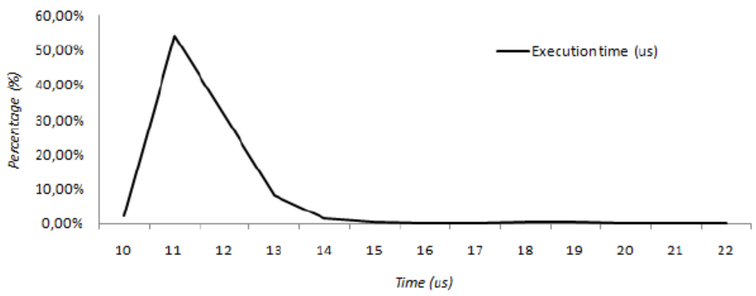
- Measurement Based Timing Analysis (MBTA):
  - Acquisition of run-time events using tracing support provided by hypervisor
  - Definition and execution of worst case scenarios and error injection



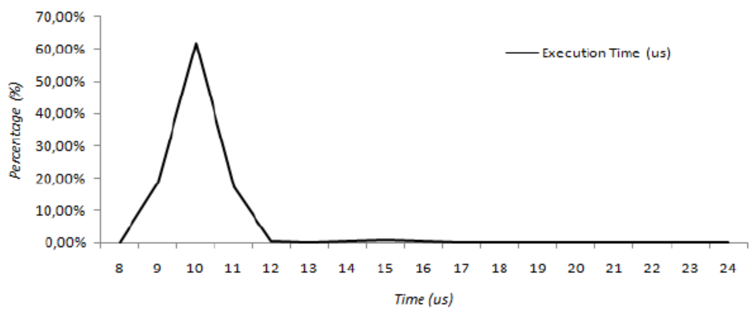


[1] Larrucea A. et al, “Temporal Independence Validation for IEC-61508 compliant Mixed-Criticality Systems based on Multicore Partitioning”, Forum on specification & Design Languages (FDL), 2015

Measurements

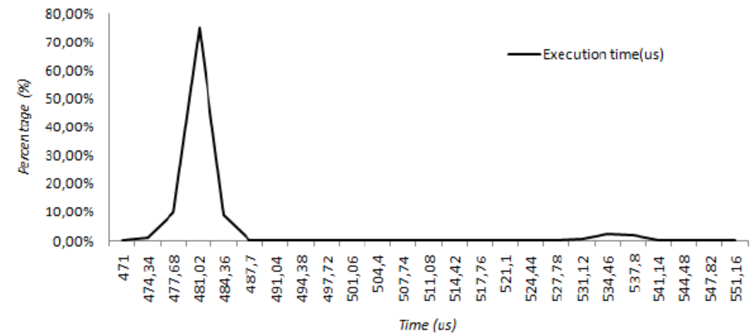


(a) Safety Protection partition on x86 processor.

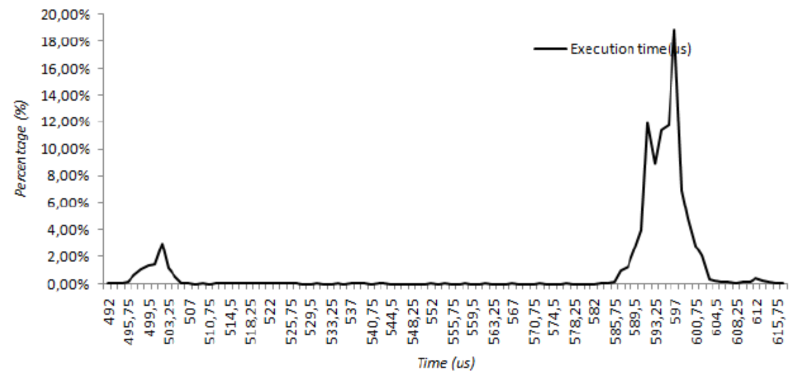


(b) Supervision partition on x86 processor.

Fig. 7. Execution Time measurements on x86 processor.



(a) Safety Protection partition on LEON3 processor.



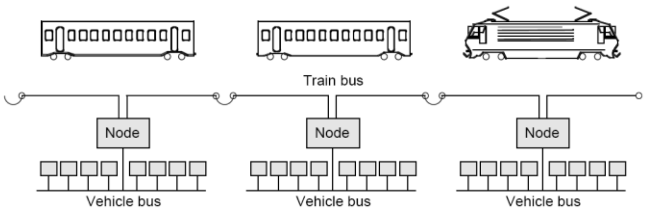
(b) Supervision partition on LEON3 processor.

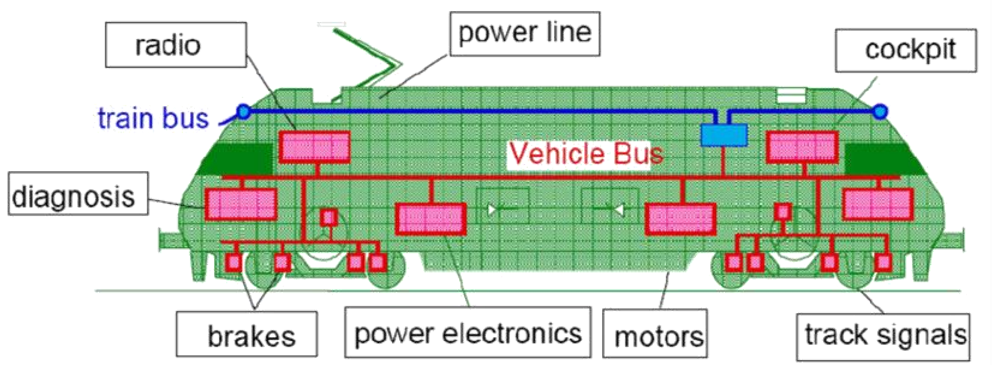
[1] Larrucea A. et al, "Temporal Independence Validation for IEC-61508 compliant Mixed-Criticality Systems based on Multicore Partitioning", Forum on specification & Design Languages (FDL), 2015

Railway

◊ (On-board) railway domain:

- The ever increasing request for safety, better performance, energy efficient, environmentally friendly and cost reduction in modern railway trains have forced the introduction of sophisticated dependable embedded systems [1].
- The number of ECUs (Electric Control Units) within a train system is of the order of a few hundred [2,3].
- Groups of distributed embedded systems:
  - Train Control Unit.
  - Railway Signalling (e.g. ETCS).
  - Traction Control.
  - Brake Control.
  - Etc.



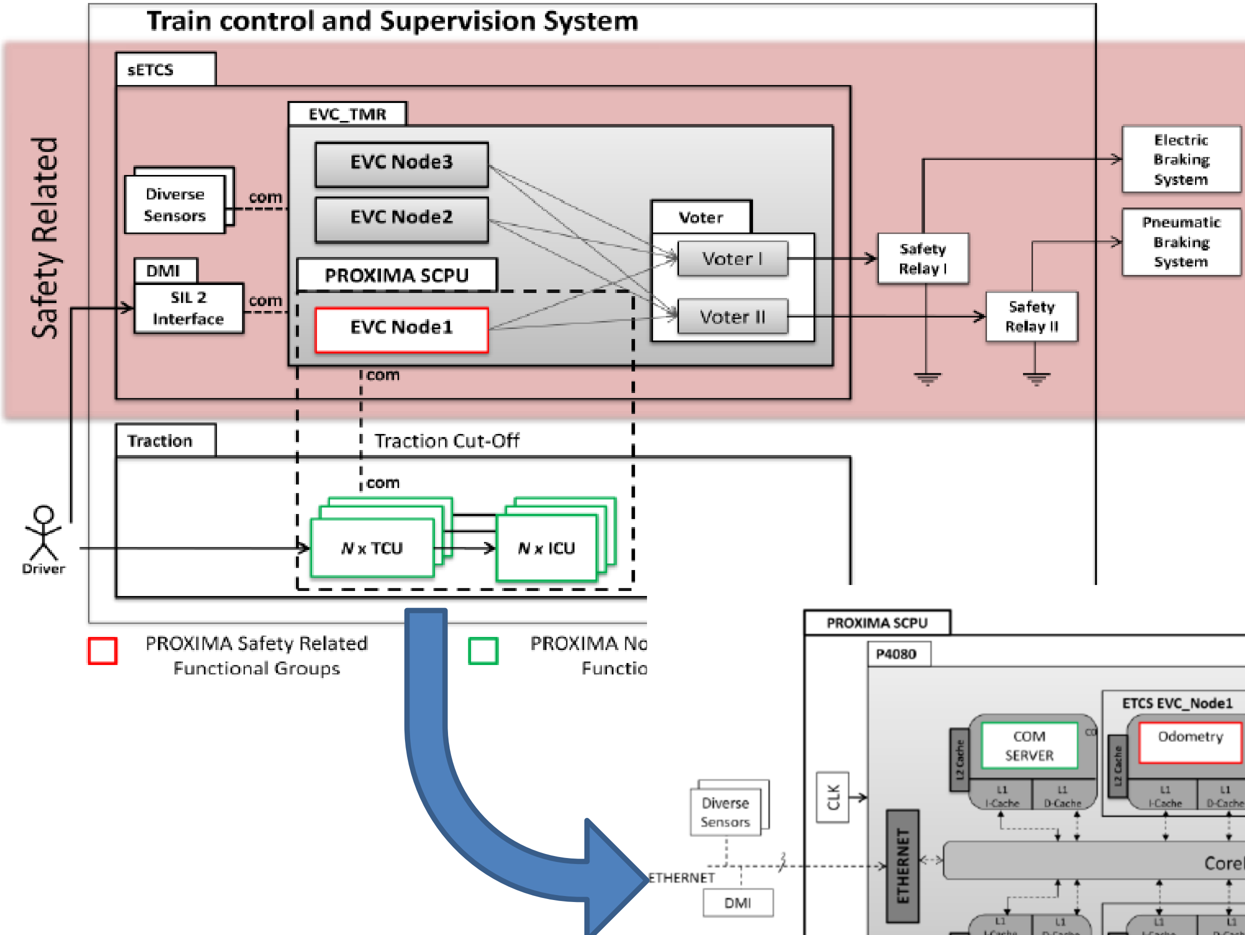


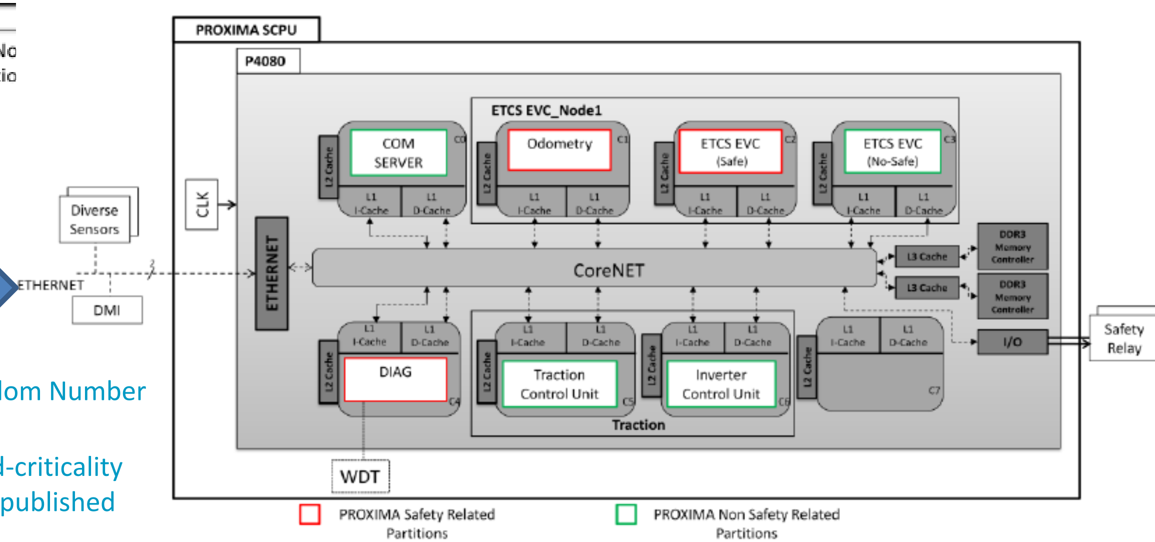
[1] The European Rail Research Advisory Council (ERRAC), Joint Strategy for European Rail Research 2020.

[2] Kirrmann, H. and P. A. Zuber (2001). "The IEC/IEEE Train Communication Network." IEEE Micro vol. 21, no. 2: 81-92.

[3] F. Corbier, et al, *How Train Transportation Design Challenges can be addressed with Simulation-based Virtual Prototyping for Distributed Systems,* 3rdEuropean congress Embedded Real Time Software (ERTS), France, 2006.

Safety Concept





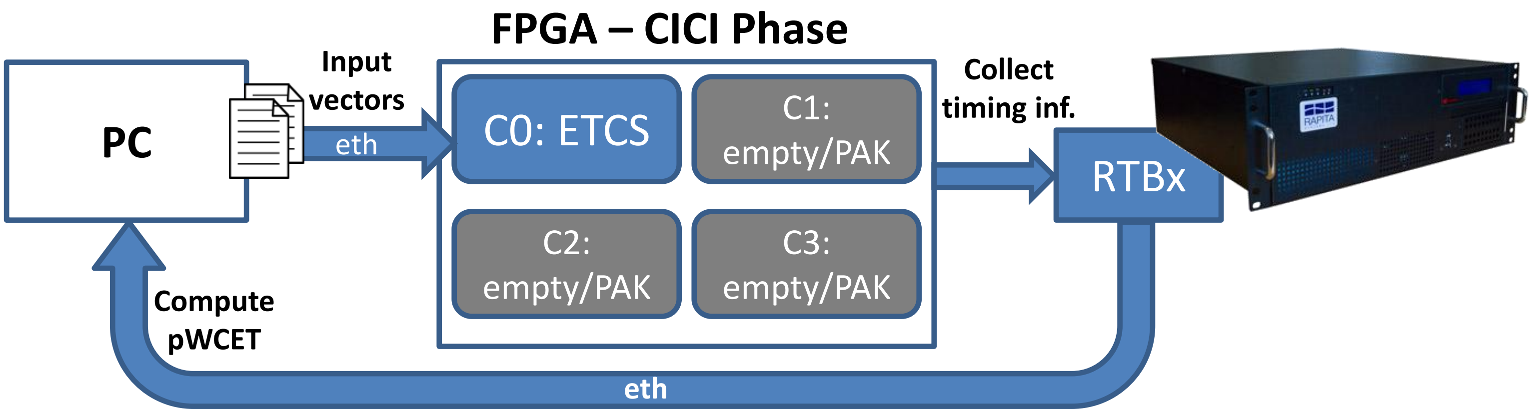
[1] Agirre, Irune et al, “61508 SIL 3-compliant Pseudo-Random Number Generators for Probabilistic Timing Analysis”, DSD 2015

[2] Agirre, Irune et al. “A safety concept for a railway mixed-criticality embedded system based on multicore partitioning”, To be published

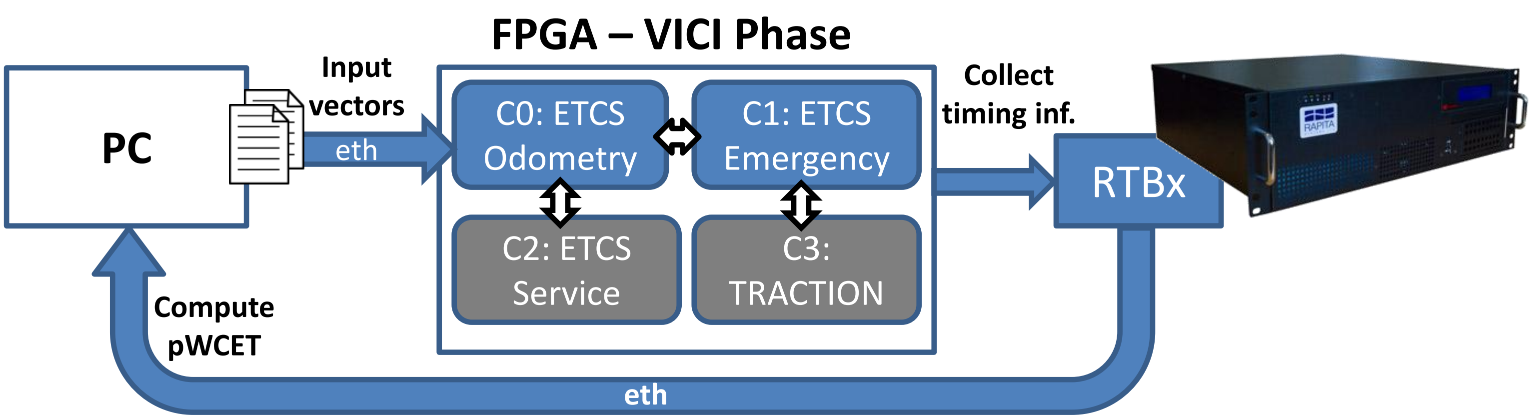
PTA (Probabilistic Timing Analysis)

- Railway Case study Experiments:

CICI phase:



VICI phase:



IKERLAN

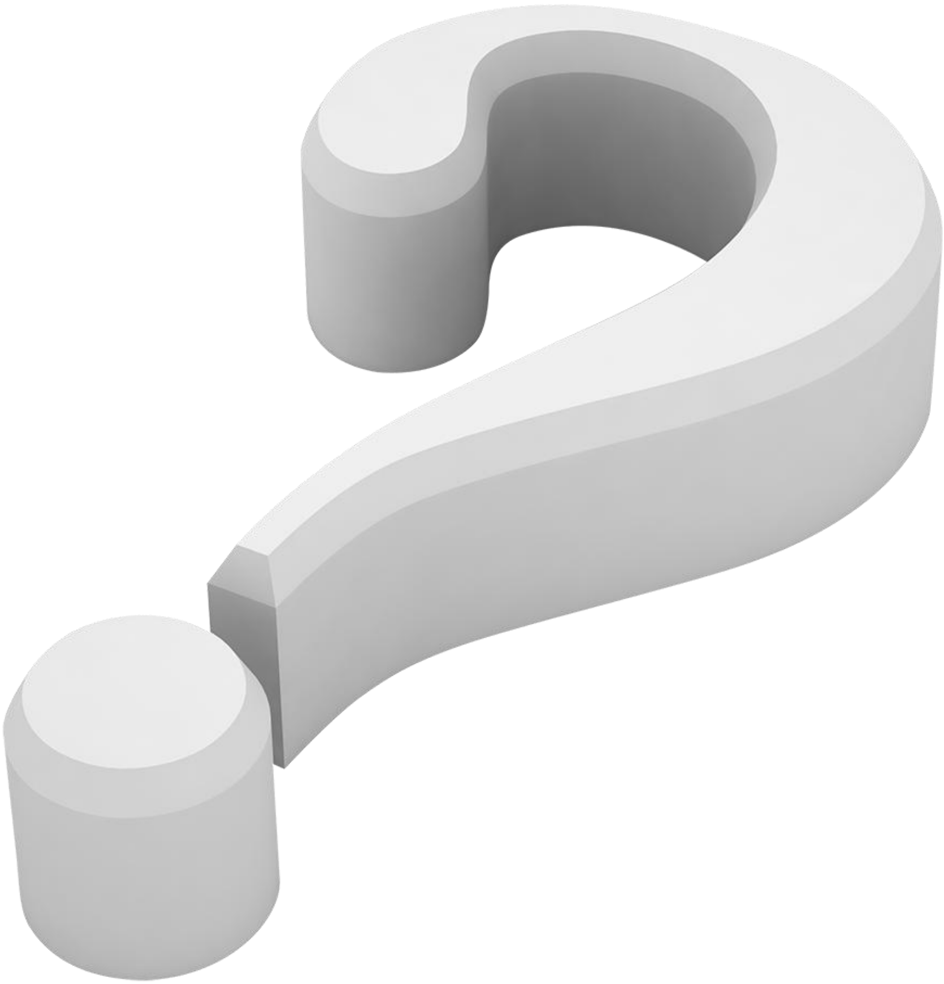
05

Conclusions and lessons learnt

IK4 IKERLAN Research Alliance

Conclusions and lessons learnt

- It is feasible to achieve SIL3 IEC-61508 / Pld ISO-13849 / SILX EN-50128 in research 'case studies' with current safety standard versions using:
  - COTS multicore
  - Partitioning with hypervisor
  - WCET estimation based on MBTA and PTA
- There is a need and opportunity for WCET, but consider industry & research worlds:
  - Common understanding (e.g., fail safe, temporal isolation vs. Temporal independence)
  - Complexity management
  - Product and safety certification context
  - Product life-cycle and variability
- The same strategy can be extended to different domains with safety standards that use IEC-61508 as reference standard.
  - √ Wind Turbine, IEC-61508 SIL3 and ISO-13849 Pld.
  - √ Railway signaling, SIL4 EN-5012X
  - Working with automotive domain case study ASILC ISO-26262.



IK4 IKERLAN
Research Alliance

IKERLAN - GARAIA
Polo de Innovación Garaia
C/ Goiru , 9
20500 Arrasate-Mondragón

IKERLAN - MIÑANO
Parque tecnológico de Álava,
C/ Juan de la Cierva, 1
01510 Miñano

IKERLAN - GALARRETA
Pol. Industrial Galarreta,
Parcela 10.5, Edificio A3
20120 Hernani

IKERLAN - OLANDIXO
Pº. J. Mª. Arizmendiarrieta, 2
20500 Arrasate-Mondragón

Tel.: 943 71 24 00
Fax: 943 79 69 44

www.ikerlan.es