IK4 IKERLAN
Research Alliance

IEC-61508 certification of mixed-criticality systems based on multicore and partitioning

Ada Europe 2015
Madrid (23rd June)

Jon Perez
jmperez@ikerlan.es

Outline

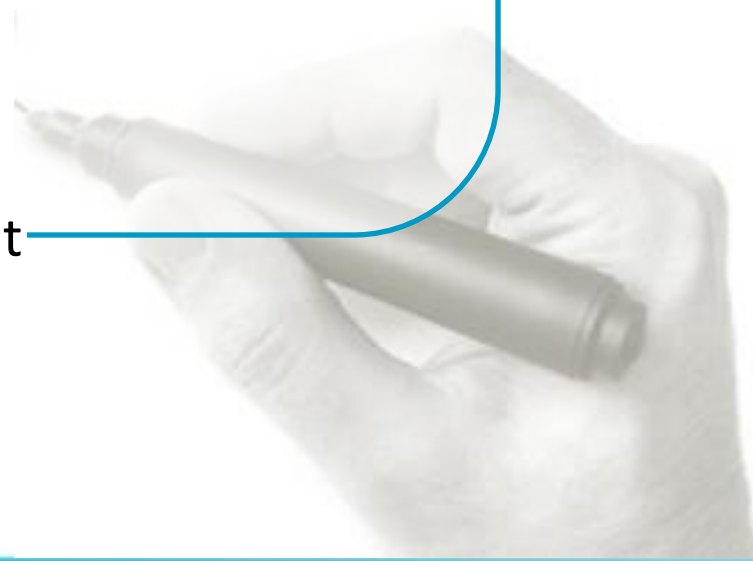
01 Context

02 Multicore is what you need / what you will have

03 The business need and opportunity

04 The wind turbine example

05 Conclusions and lessons learnt



IKERLAN

01

Context

Some Research Projects: Multicore & mixed-criticality

DREAMS

MultiPARTES

Contrex

CERTAINTY

PROXIMA

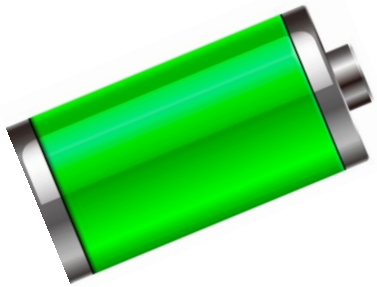
recomp

EMC²

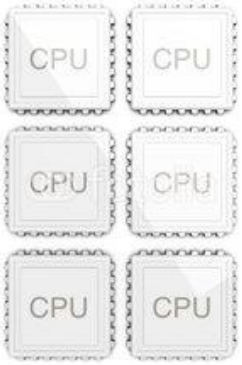
CRYSTAL

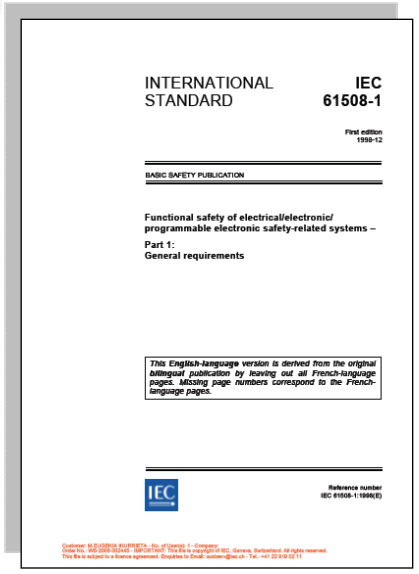
Keynote in a nutshell

Market Pull



Technology Push





Product H2020

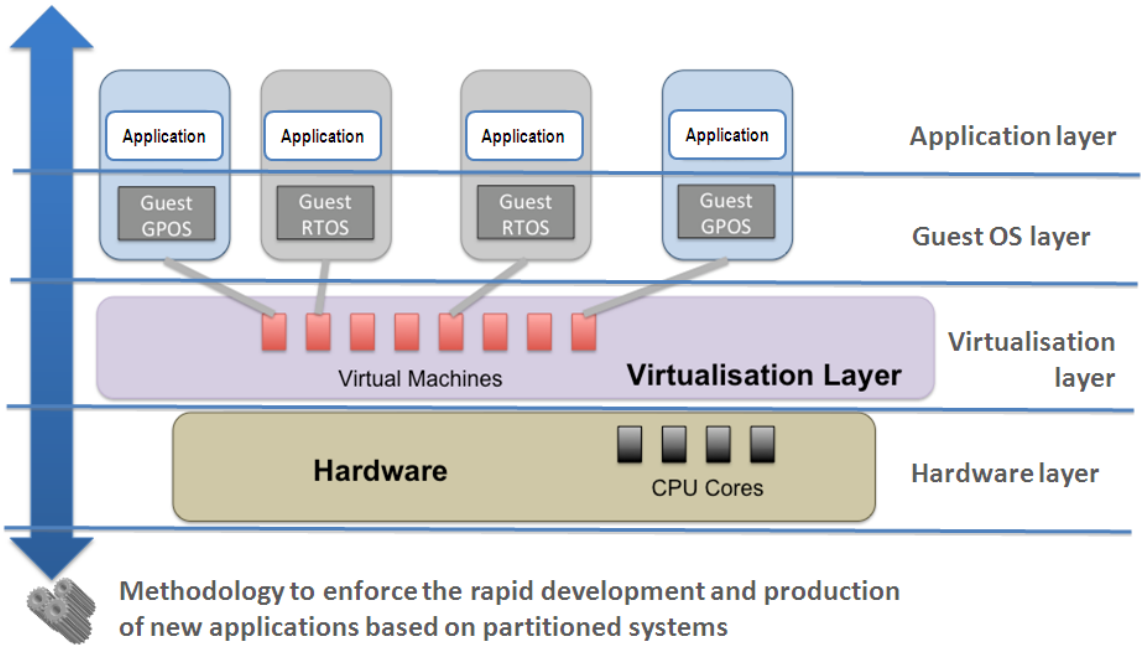
Introduction – Mixed Criticality

- "Modern electronic systems used in industry (avionics, automotive, etc.) combine applications with different security, safety, and real-time requirements. Systems with such mixed requirements are often referred to as mixed-criticality systems".

  [Baumann, 2011]

- "The integration of applications of different criticality (safety, security, real-time and non-real time) in a single embedded system is referred as mixed-criticality system".

  [Perez, 2014]



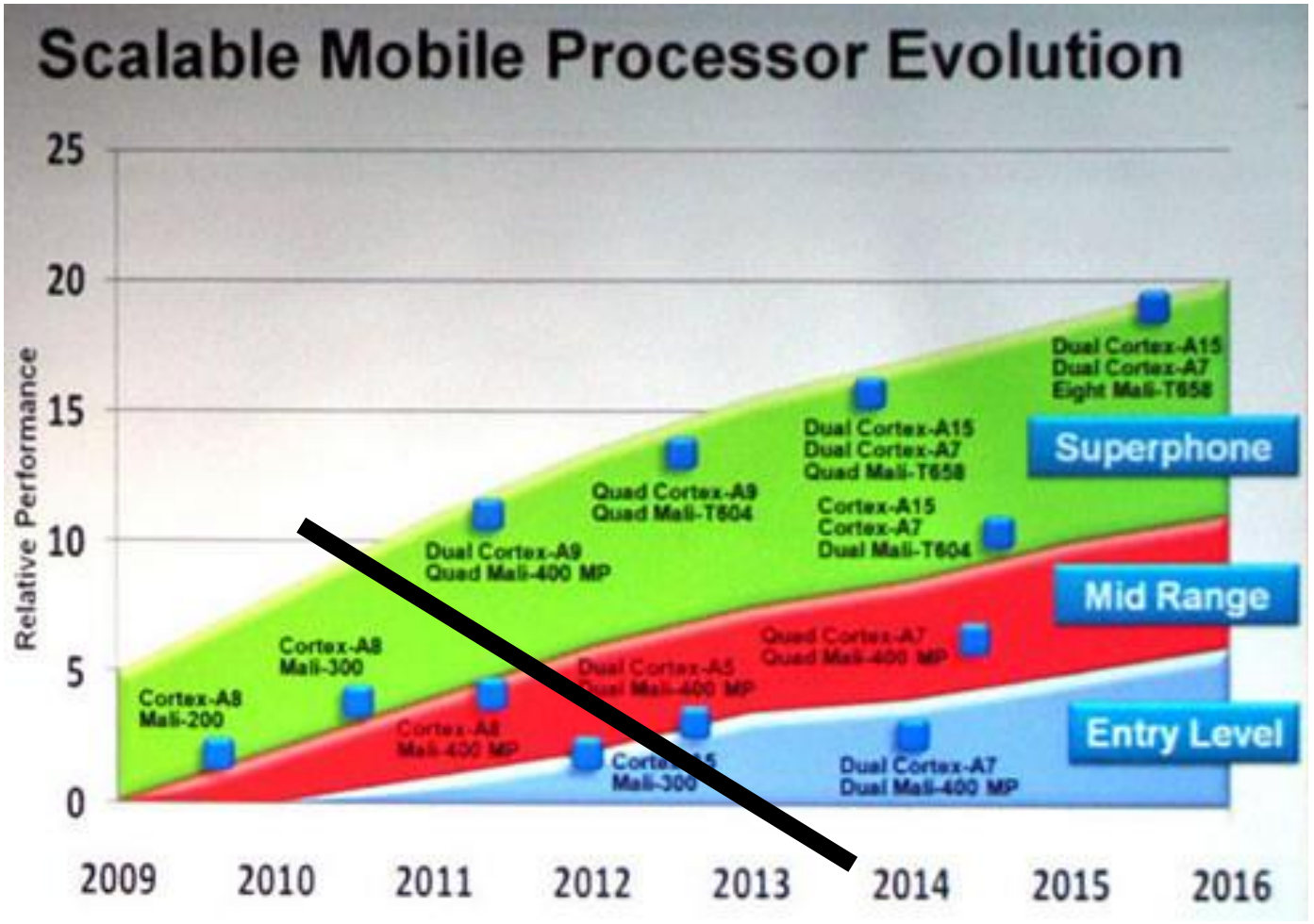
Source: www.multipartes.eu, www.xtratum.org

IKERLAN

02

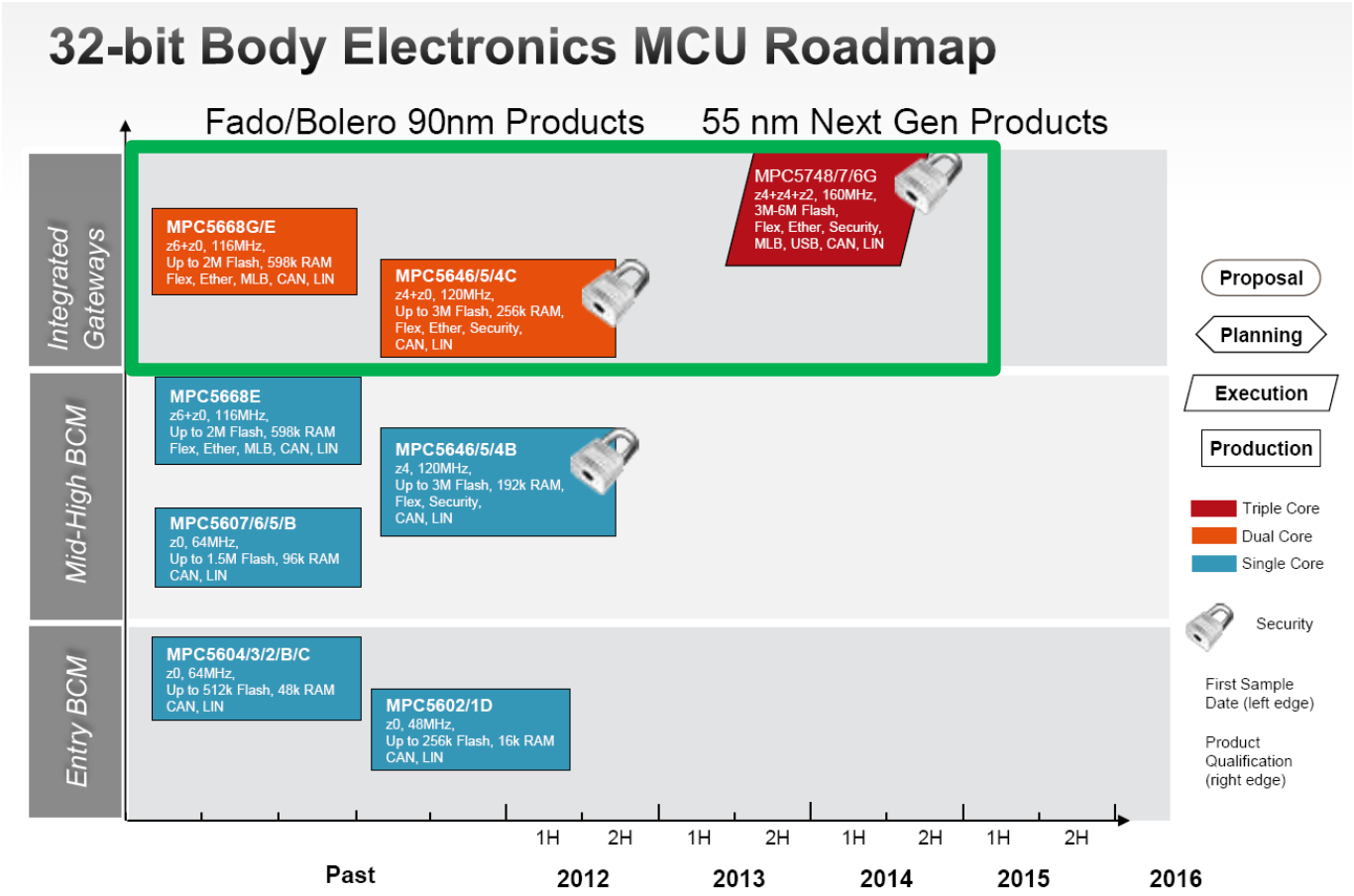
Multicore is what you need...
Multicore is what you will have...

Multicore & Mobile



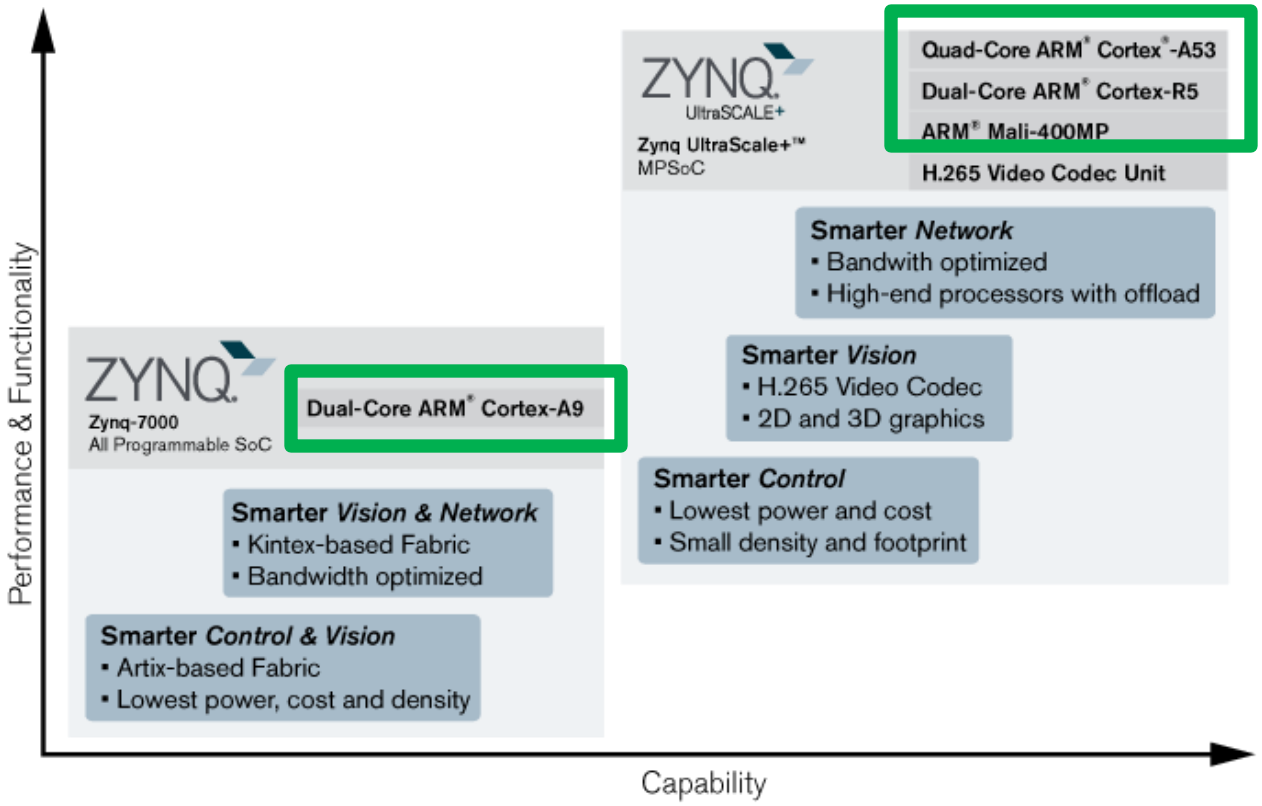
Source: www.arm.com

- 2nd International Conference Automotive Embedded Multi-Core Systems.
- Roadmaps:



Source: www.freescale.com

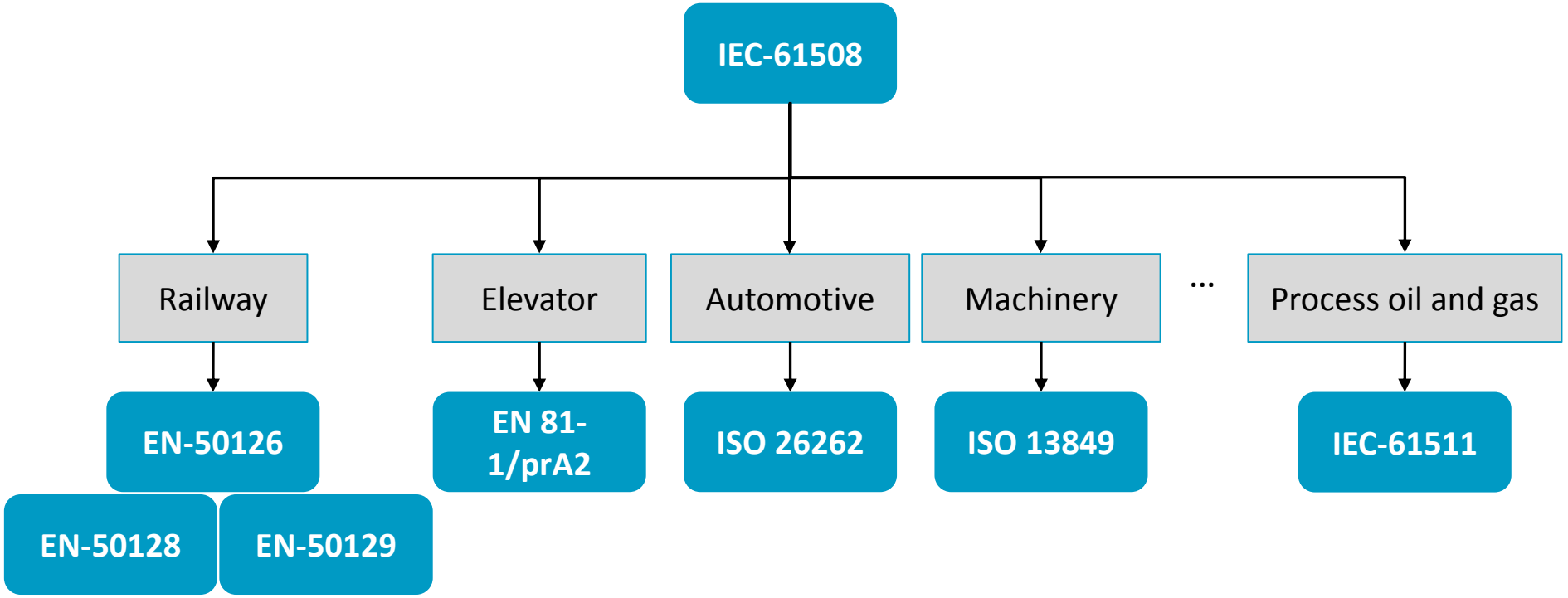
Generic purpose multicore



Source: www.xilinx.com

Safety certification (IEC-61508)

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



IEC-61508 and multicore

- IEC-61508-3 Annex F (Informative) – "Techniques for achieving non-interference between software elements on a single computer"
  - "Independence of execution should be achieved and demonstrated both in the spatial and temporal domains."
    - "**Spatial**: the data used by a one element shall not be changed by a another element. In particular, it shall not be changed by a non-safety related element."
    - "**Temporal**: one element shall not cause another element to function incorrectly by taking too high a share of the available processor execution time, or by blocking execution of the other element by locking a shared resource of some kind"
  - "**The term "independence of execution" means that elements will not adversely interfere with each other's execution behaviour such that a dangerous failure would occur**."

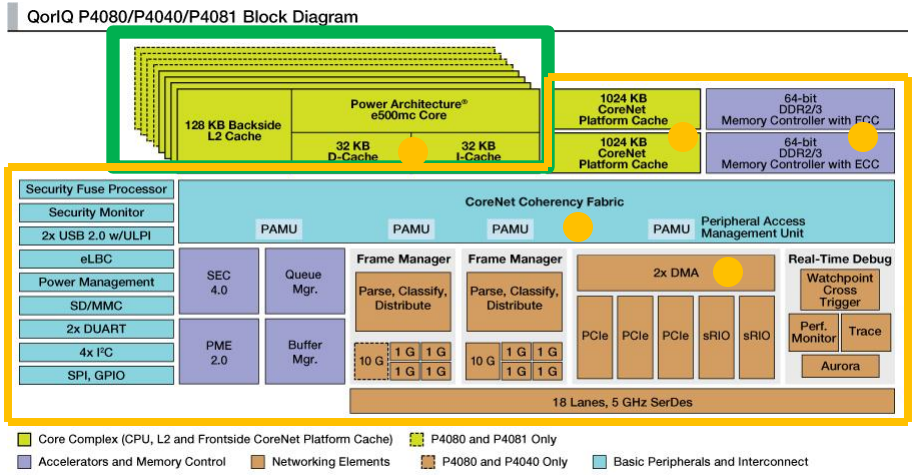
Threats to be considered and managed

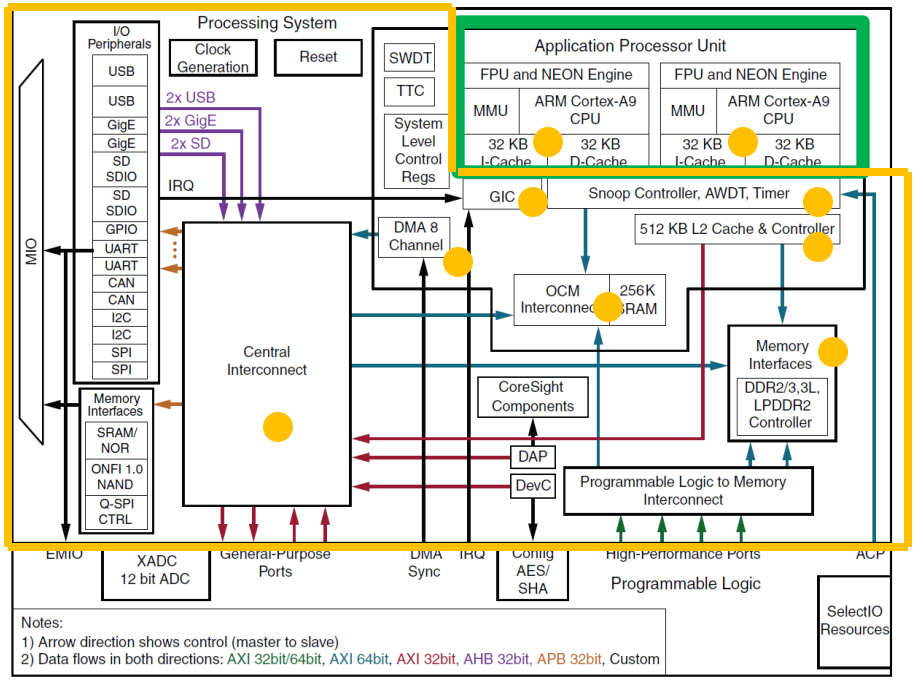
Threats to be considered and managed

- Temporal & Spatial <u>independence</u>, e.g., Shared resources (e.g., memory, cache, bus, interrupts) [1]

<u>Which is the time-scale of the temporal interference?</u>

ps — ns — msec — second



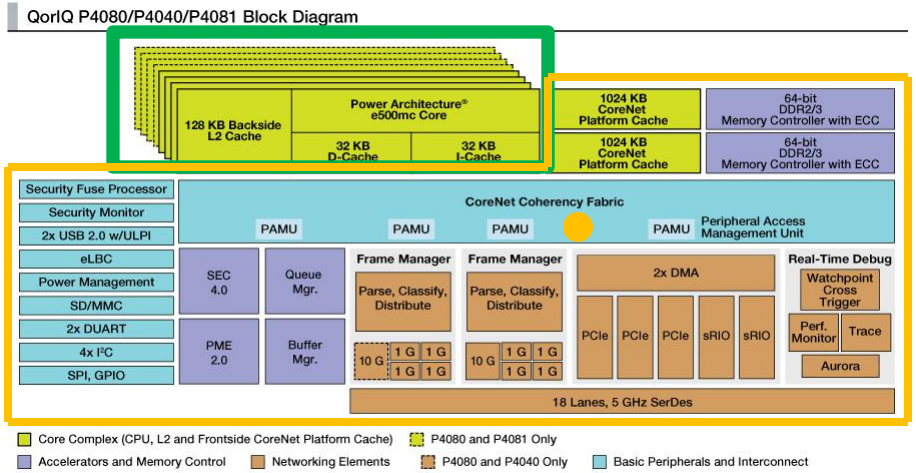


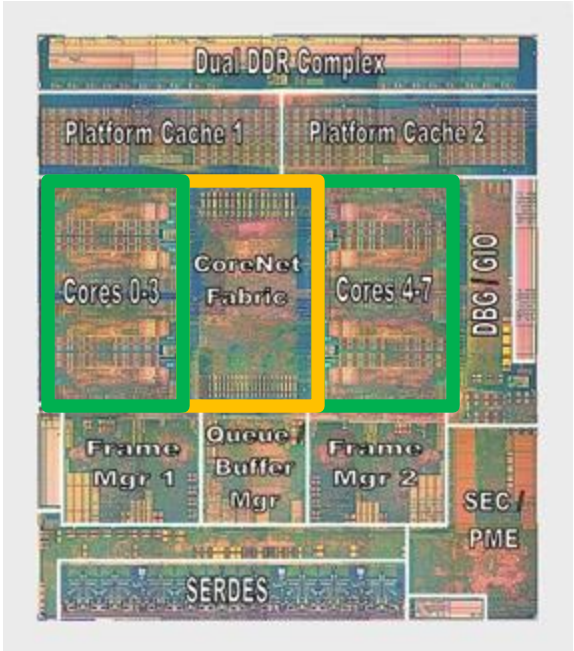
[1] Kotaba, O., et al. (2013). Multicore In Real-Time Systems – Temporal Isolation Challenges Due To Shared Resources. Workshop on Industry-Driven Approaches for Cost-effective Certification of Safety-Critical, Mixed-Criticality Systems (WICERT). Dresden (Germany).

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

Threats to be considered and managed

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



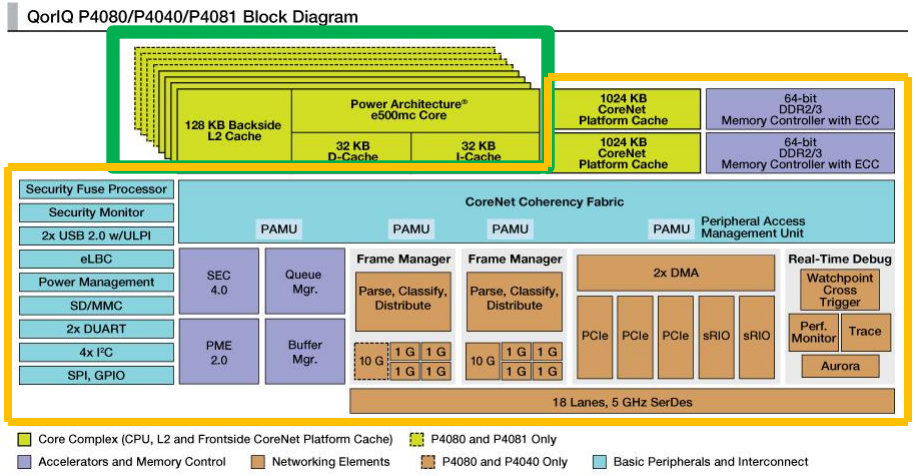


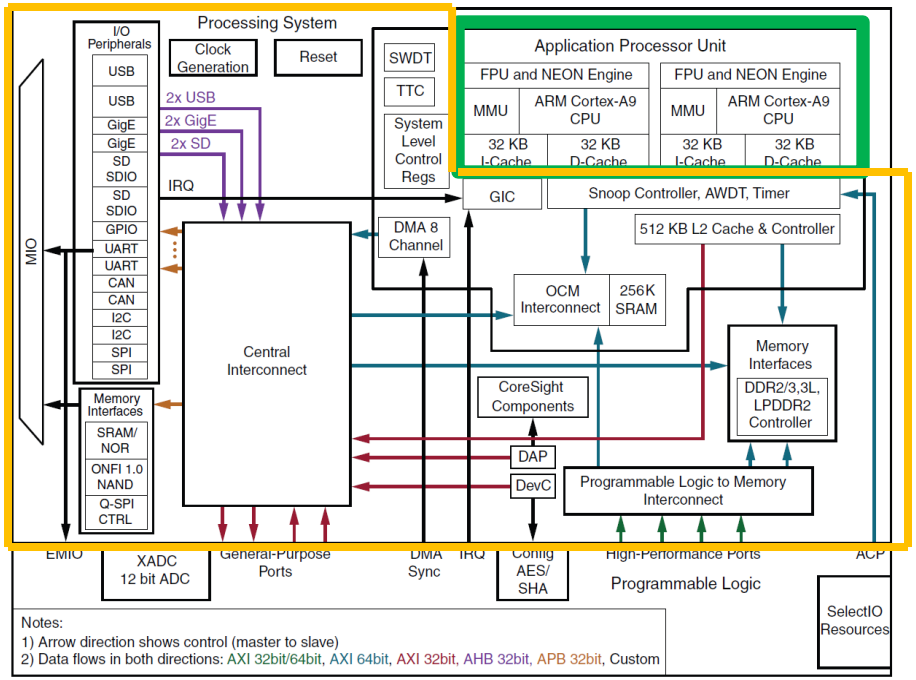
[1] http://www.advancedsubstratenews.com/2009/12/multicores-perfect-balance/

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

Threats to be considered and managed

- Worst Case Execution Time (WCET)

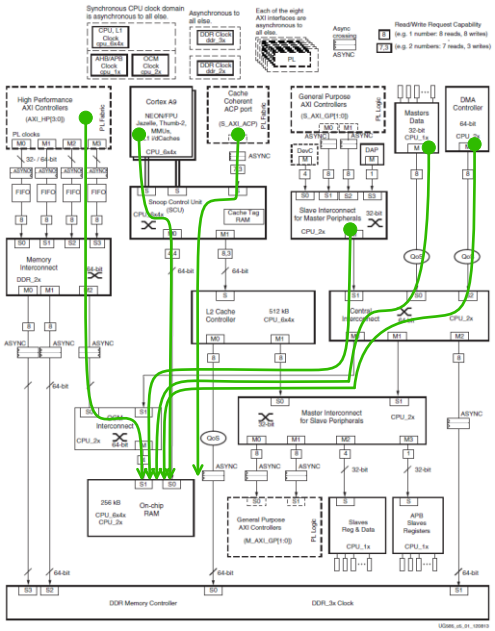


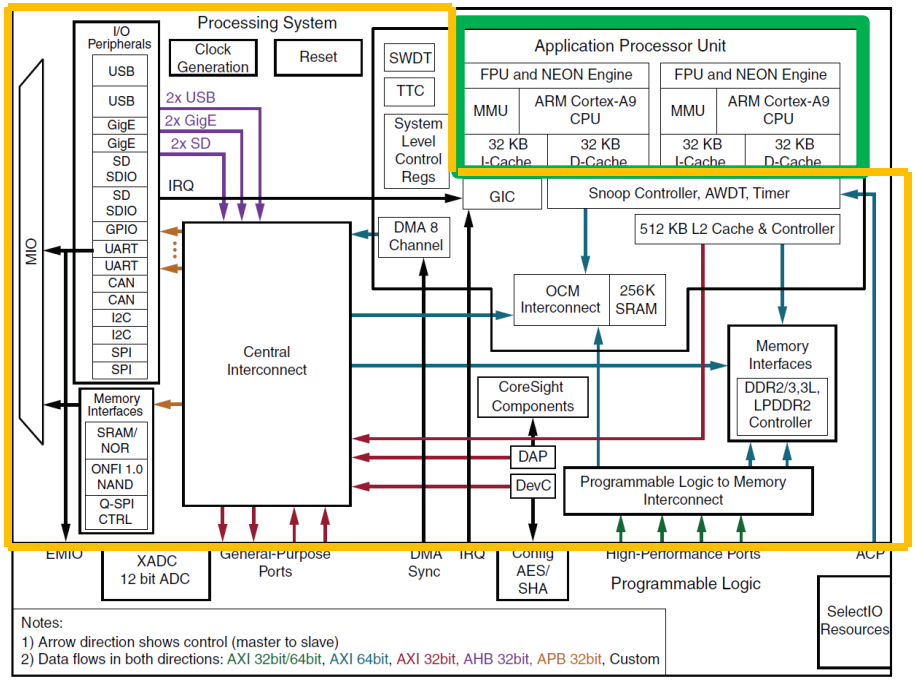


Source: www.freescale.com, www.xilinx.com

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





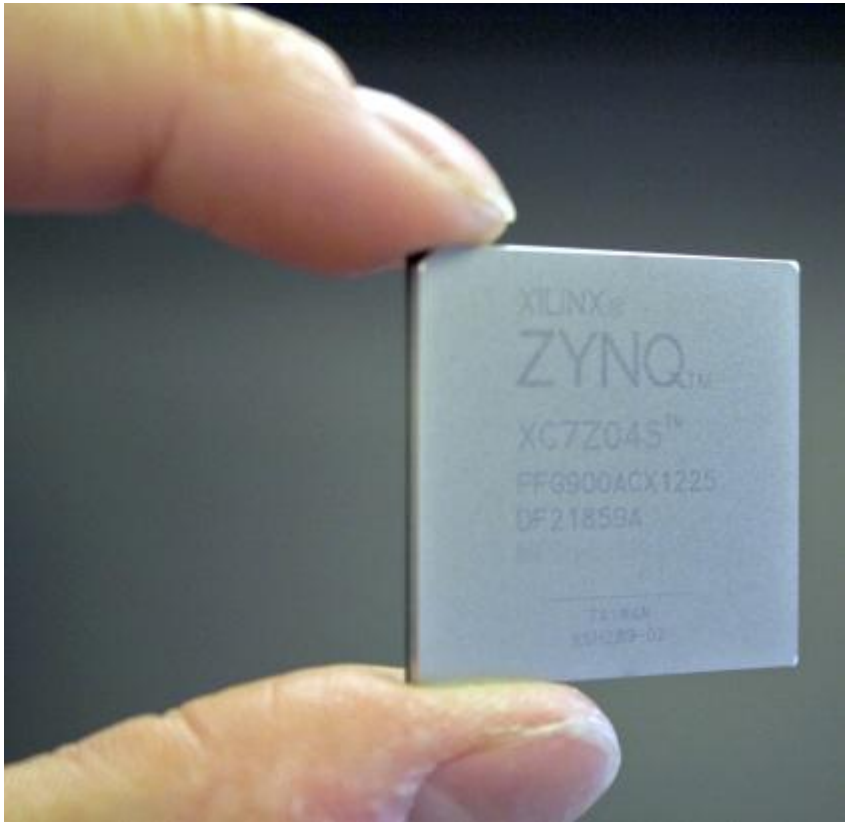
Source: www.freescale.com, www.xilinx.com

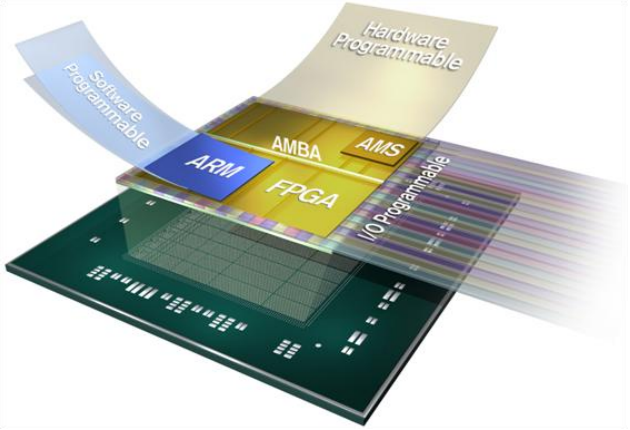
IKERLAN

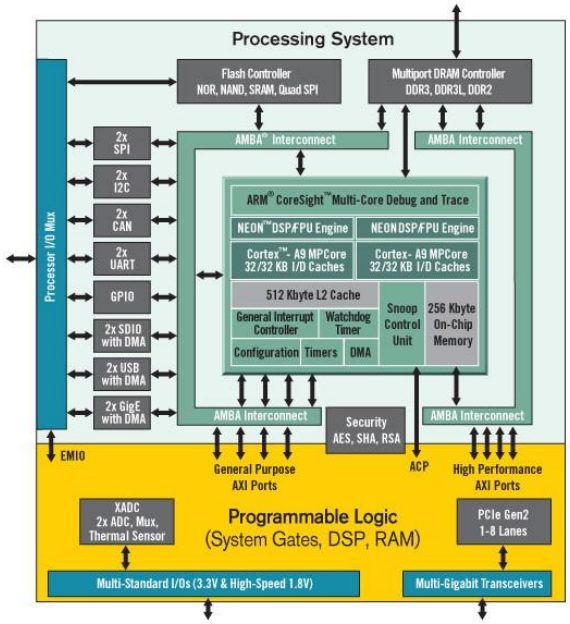
03

The need and opportunity

Impact

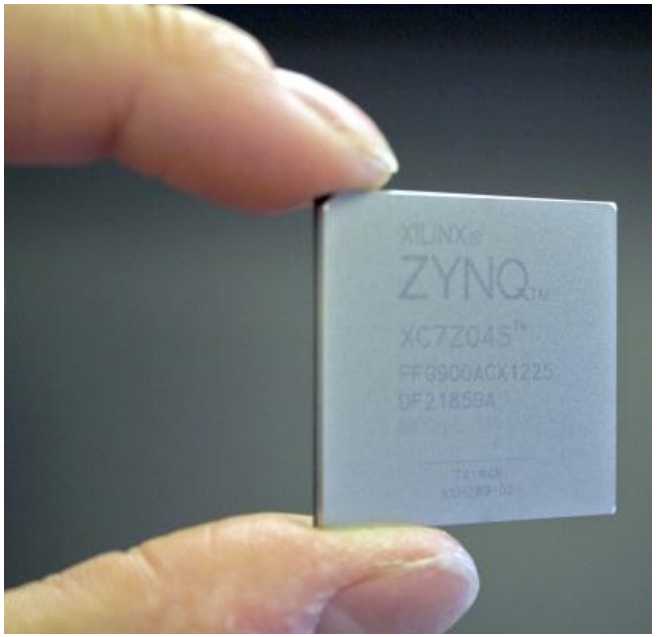






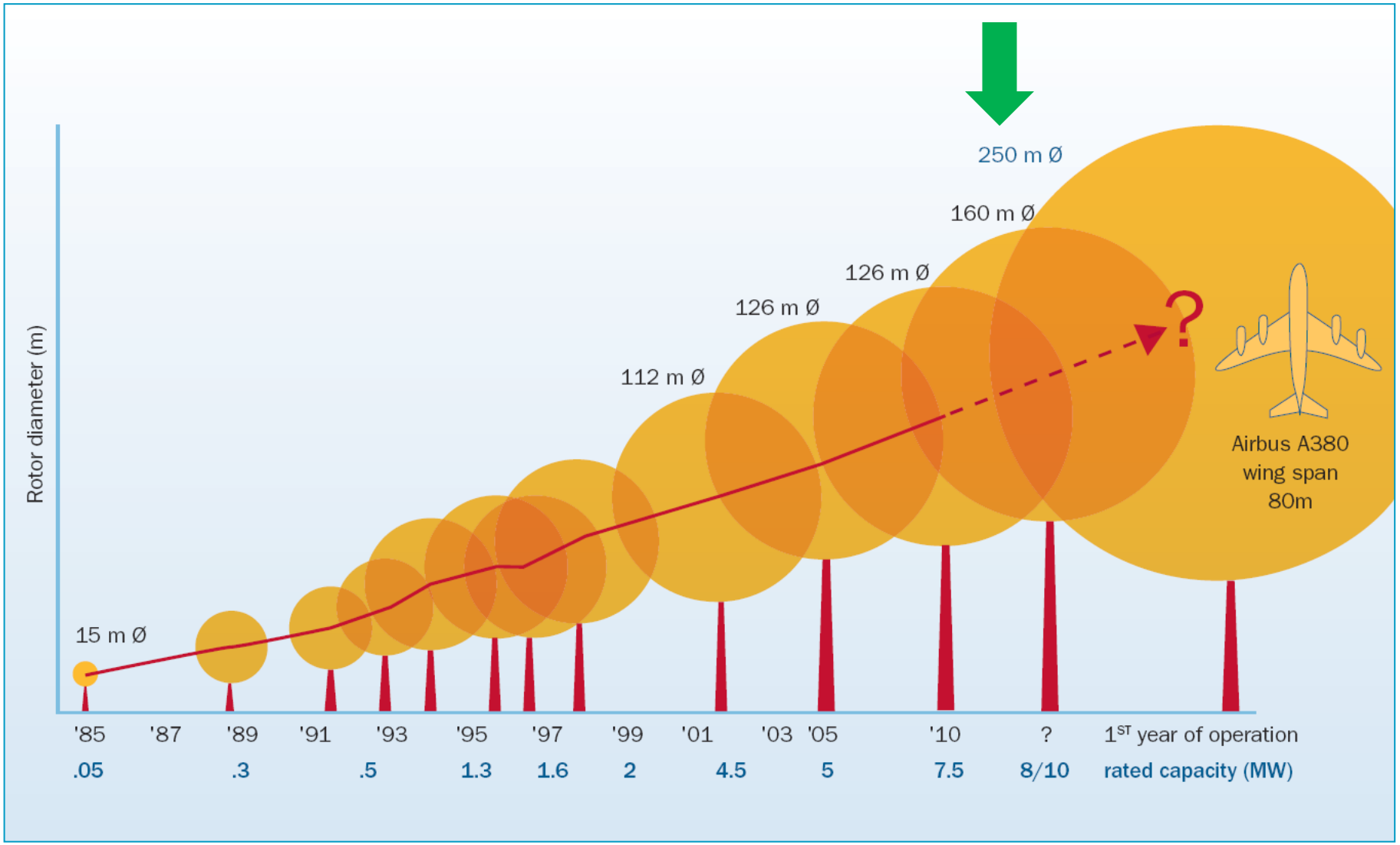
Source: www.xilinx.com

Impact perspective



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

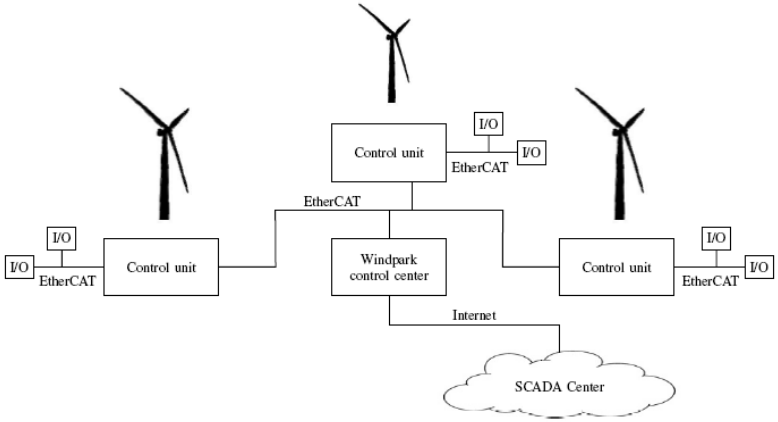
Impact Perspective – The right scale



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

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.



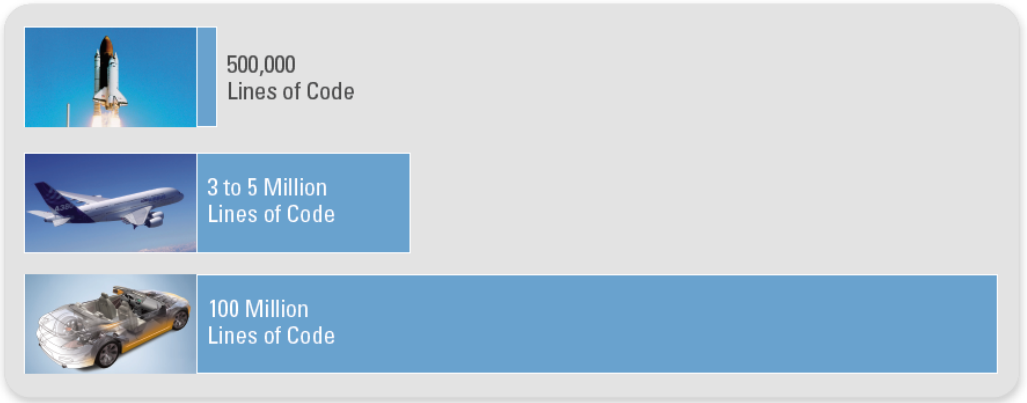
[1] Perez, J., et al. (2014). A safety concept for a wind power mixed-criticality embedded system based on multicore partitioning. Functional Safety in Industry Application, 11th International TÜV Rheinland Symposium, Cologne, Germany.
[2] Perez, J., et al. (2014). "A safety certification strategy for IEC-61508 compliant industrial mixed-criticality systems based on multicore partitioning." Euromicro DSD/SEAA Verona, Italy.

Source: www.alstom.com

Automotive

- 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]

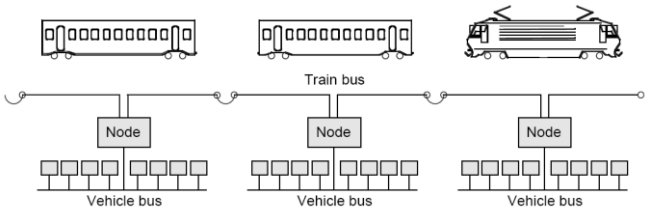


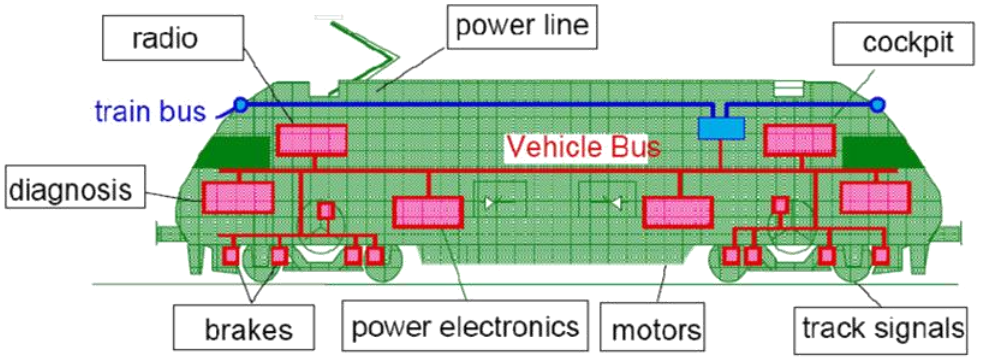
[4]

[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.

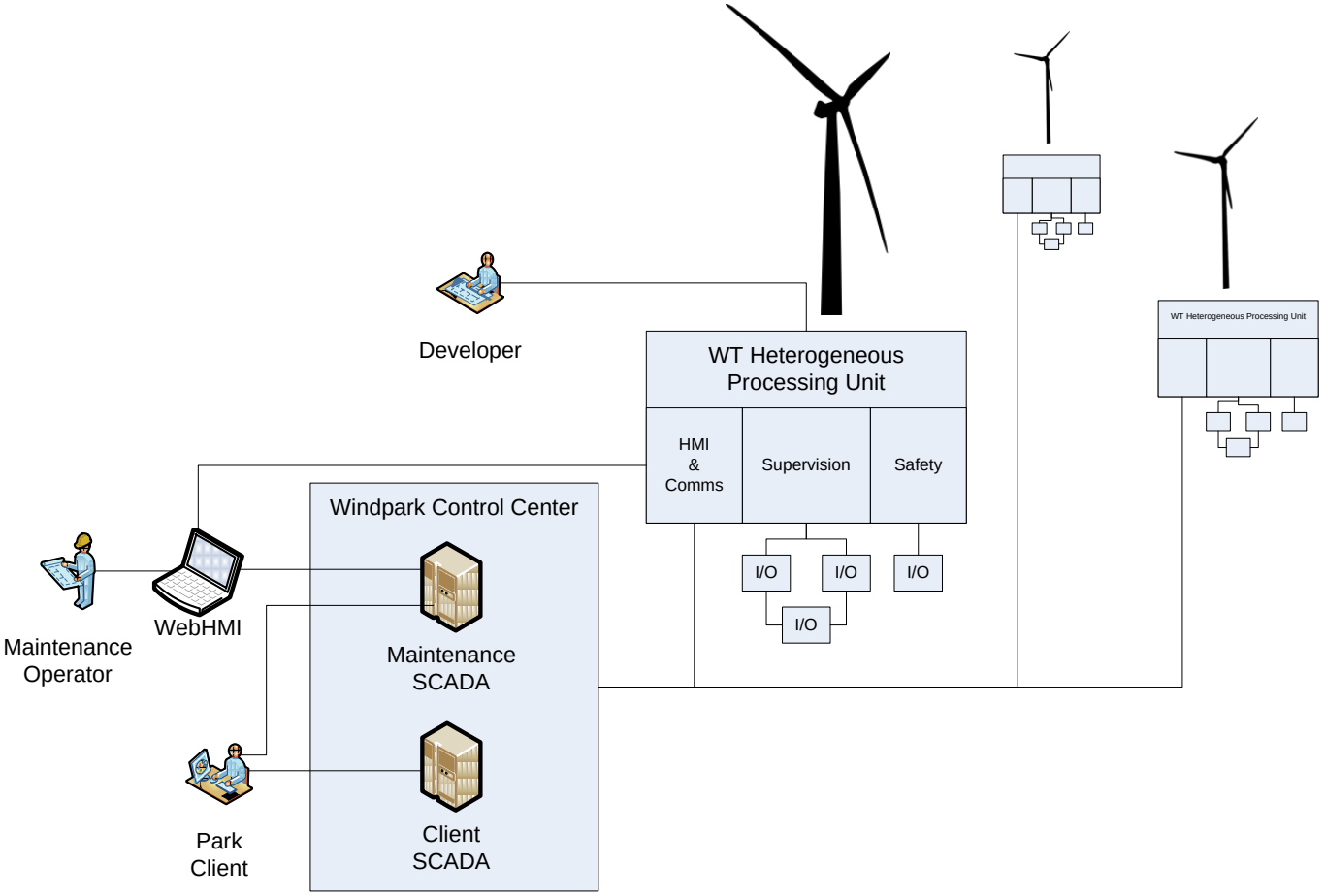
[3] F. Corbier, et al, *How Train Transportation Design Challenges can be addressed with Simulation-based Virtual Prototyping for Distributed Systems,* 3rdEuropean congress Embedded Real Time Software (ERTS), France, 2006.

IKERLAN

04

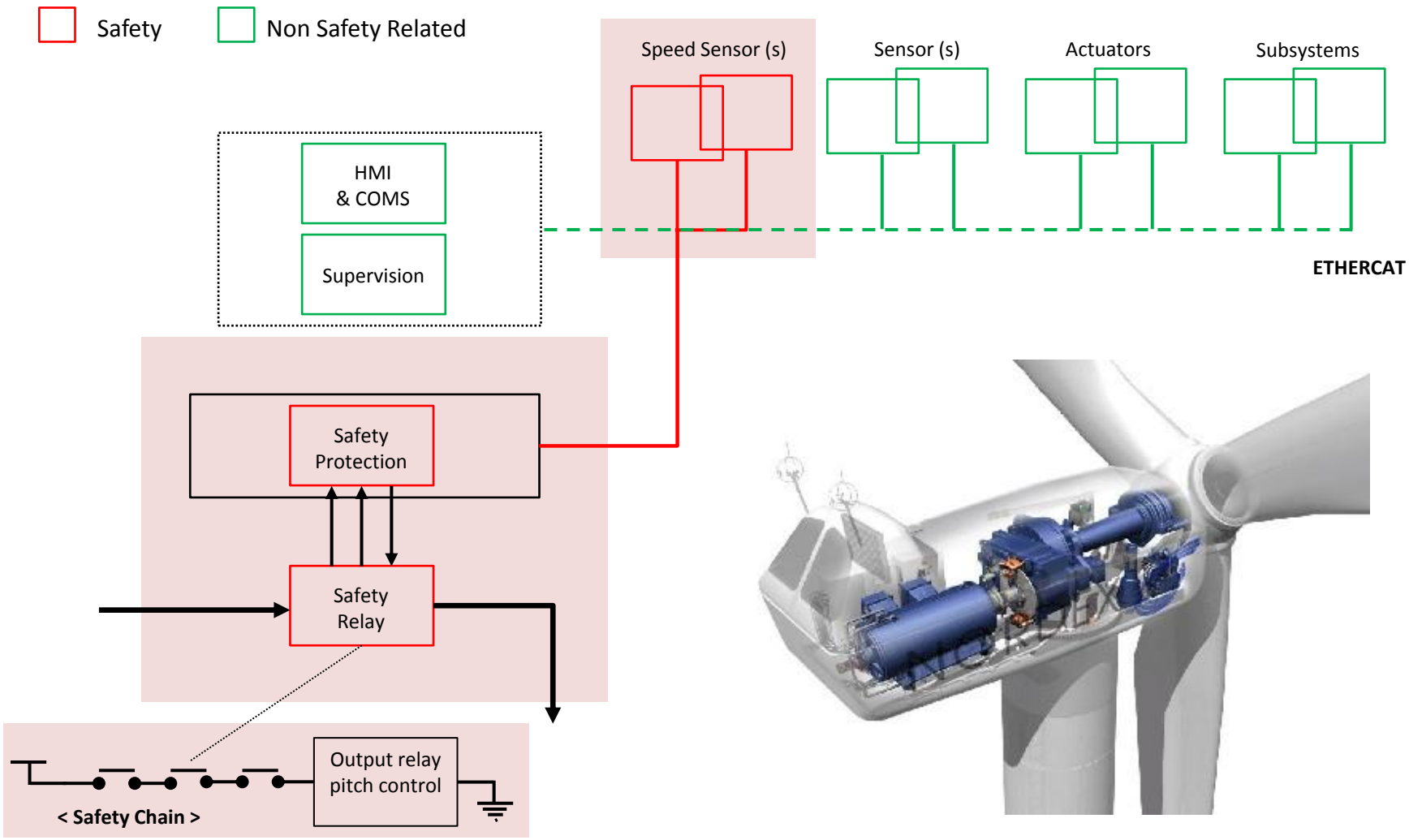
The wind turbine example

Introduction – Context Diagram

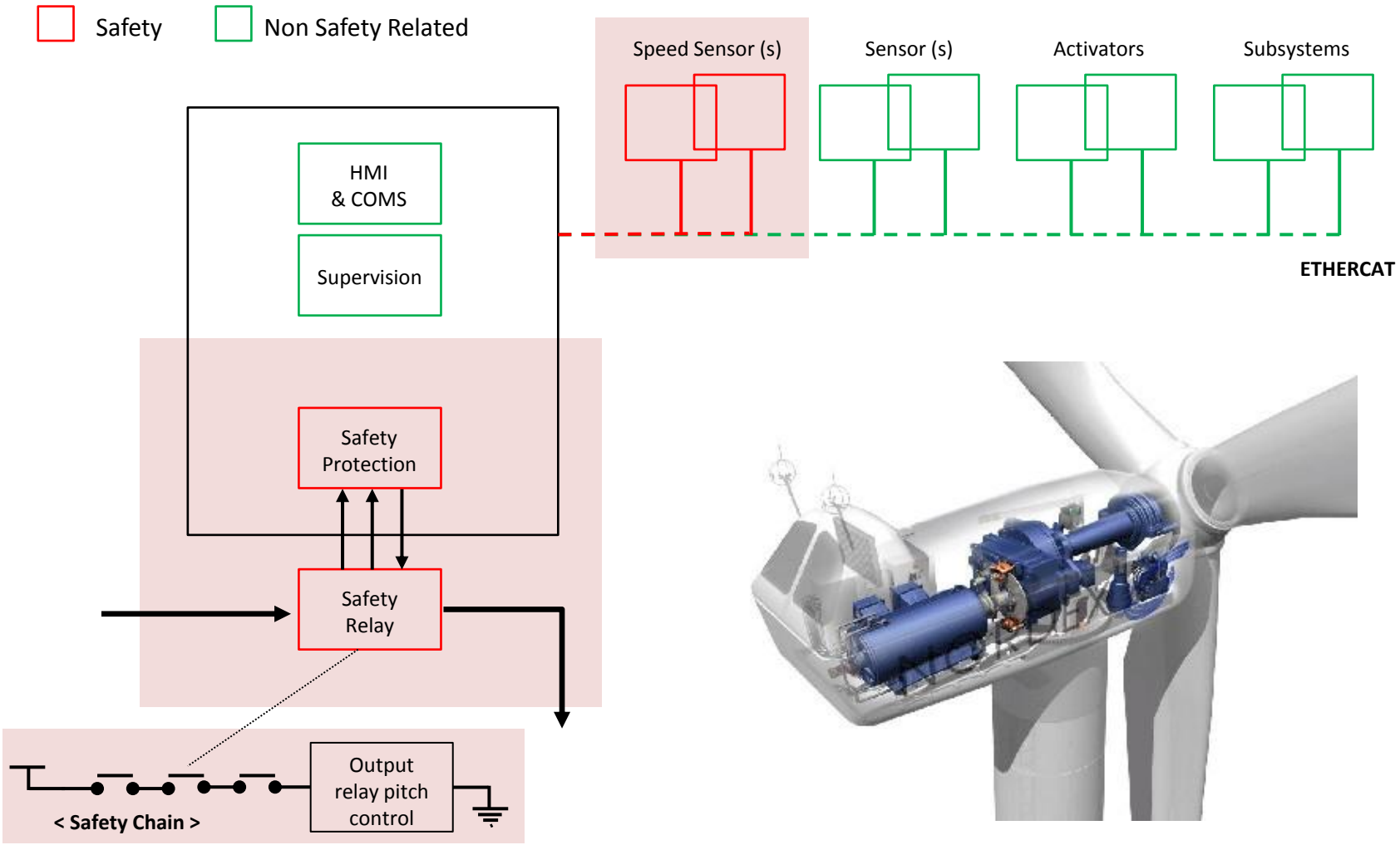


[1] Perez, J., et al. (2014). A safety concept for a wind power mixed-criticality embedded system based on multicore partitioning. Functional Safety in Industry Application, 11th International TÜV Rheinland Symposium, Cologne, Germany.
[2] Perez, J., et al. (2014). "A safety certification strategy for IEC-61508 compliant industrial mixed-criticality systems based on multicore partitioning." Euromicro DSD/SEAA Verona, Italy.
[3] Perez, J. and A. Trapman (2013). Deliverable D7.2 (Annex) - Wind power case-study safety concept, FP7 MultiPARTES.

Introduction – Context Diagram



Introduction – Proposed solution

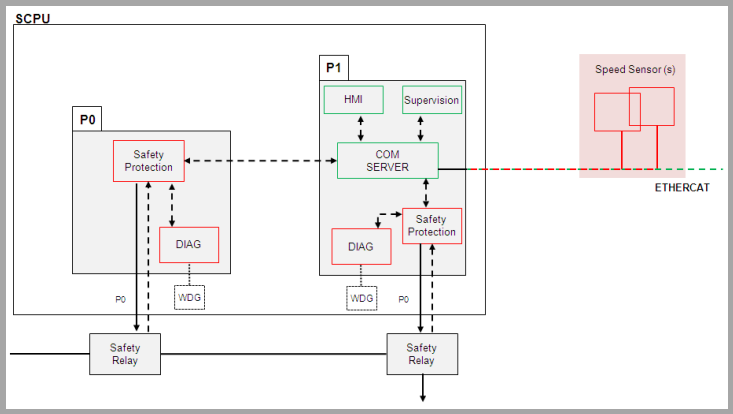


Safety Concept - Requirements

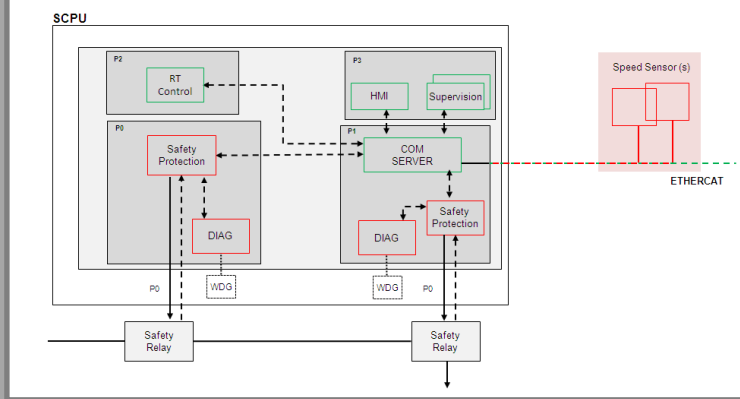
ID	Requirement
SR_WT_4	The <Protection System> safety function must activate the “safe state” if the “rotation speed” exceeds the “maximum rotation speed”
SR_WT_5	The <Protection System> safety function must ensure “safe state” during system initialization (prior to the running state where rotation speeds are compared)
SR_WT_6	<Protection System> safety function must be provided with a SIL3 integrity level (IEC-61508).
SR_WT_7	The safe state is the de-energization of output “safety relay(s)”
SR_WT_8	Output “safety relay(s)” is(/are) connected in serial within the safety chain.
SR_WT_9	A single fault does not lead to the loss of the safety function: HFT=1 and Diagnostic Coverage (DC) of the system >= 90% (according to IEC-61508).
SR_WT_10	The reaction time must not exceed PST (SW_WT_14)
SR_WT_11	Detected ‘severe errors’ lead to a “safe state” in less than PST (SW_WT_14)
SR_WT_12	The “rotation speed” absolute measurement error must be equal or below 1 rpm to be used by <Protection System>. If measurement error ≥ 1 rpm it must be neglected
SR_WT_13	The “Maximum Rotation Speed” must be configurable only during start-up (not running)
SR_WT_14	The Process Safety Time (PST) is 2 seconds

Safety Concept – The approach

DUAL PROCESSOR – 1oo2



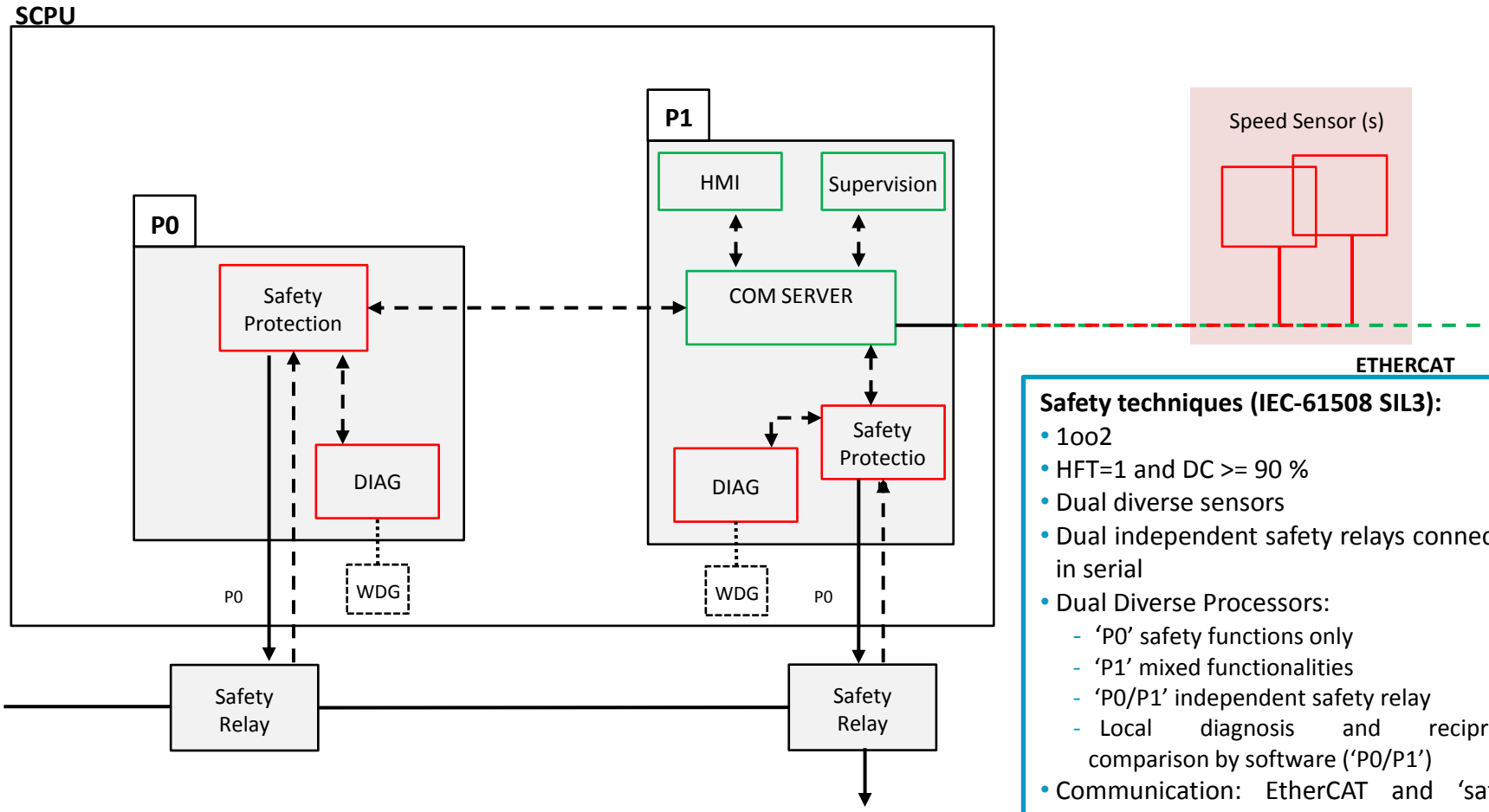
SINGLE PROCESSOR – 1oo2, partitioned, heterogeneous quad-core



- Safety concept based on ‘common practice in industry’
- Serves as a reference, not detailed
- Analogous safety concept using heterogeneous multicore and hypervisor
- The MultiPARTES contribution

Safety Concept – (A- 'Traditional')

DUAL-PROCESSOR – 1oo2

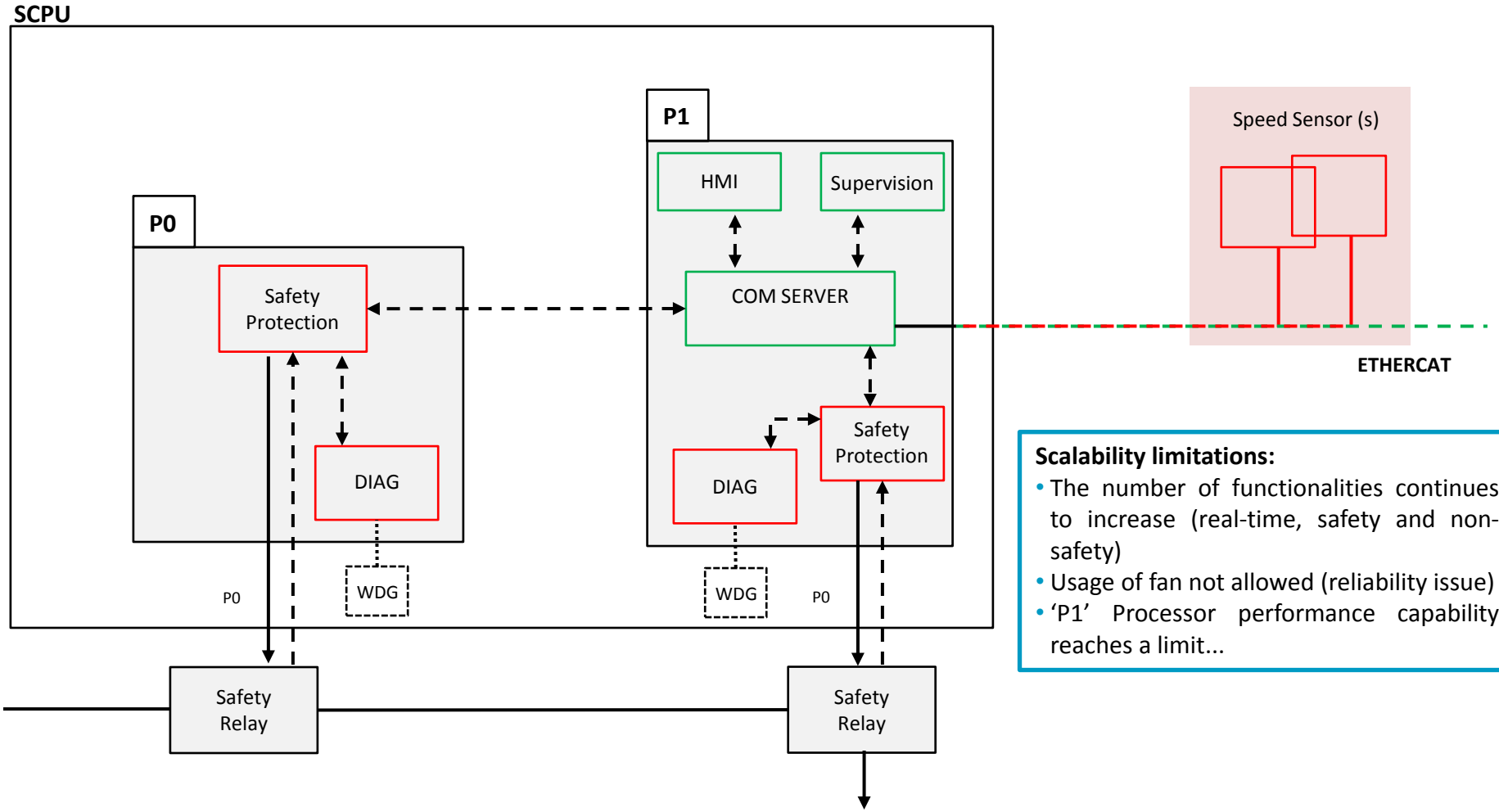


Safety techniques (IEC-61508 SIL3):

- 1oo2
- HFT=1 and DC >= 90 %
- Dual diverse sensors
- Dual independent safety relays connected in serial
- Dual Diverse Processors:
  - 'P0' safety functions only
  - 'P1' mixed functionalities
  - 'P0/P1' independent safety relay
  - Local diagnosis and reciprocal comparison by software ('P0/P1')
- Communication: EtherCAT and 'safety over EtherCAT'

Safety Concept – (A- 'Traditional')

DUAL-PROCESSOR – 1oo2

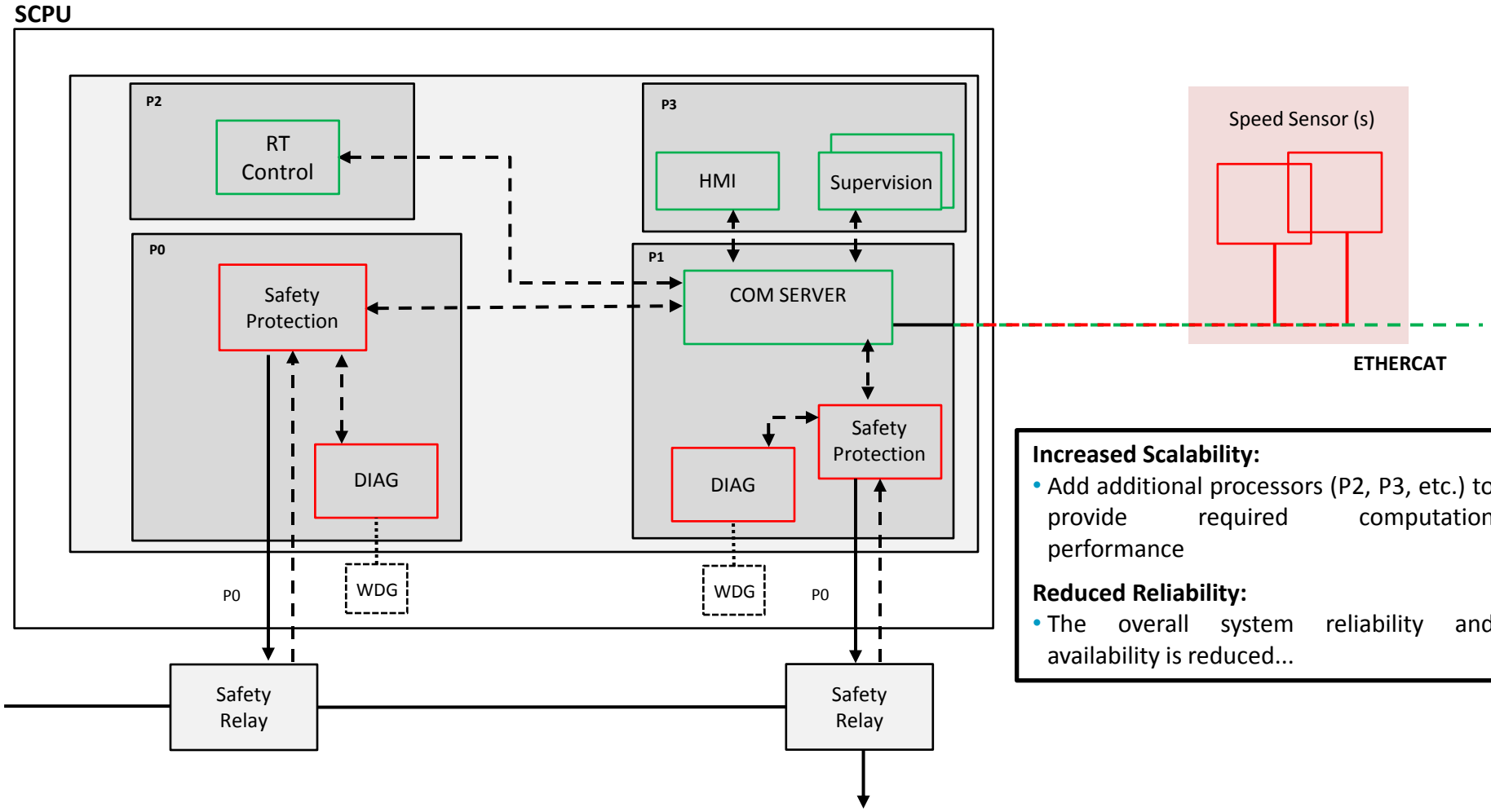


Scalability limitations:

- The number of functionalities continues to increase (real-time, safety and non-safety)
- Usage of fan not allowed (reliability issue)
- 'P1' Processor performance capability reaches a limit...

Safety Concept – (A- 'Traditional')

N PROCESSOR – 1oo2



Increased Scalability:

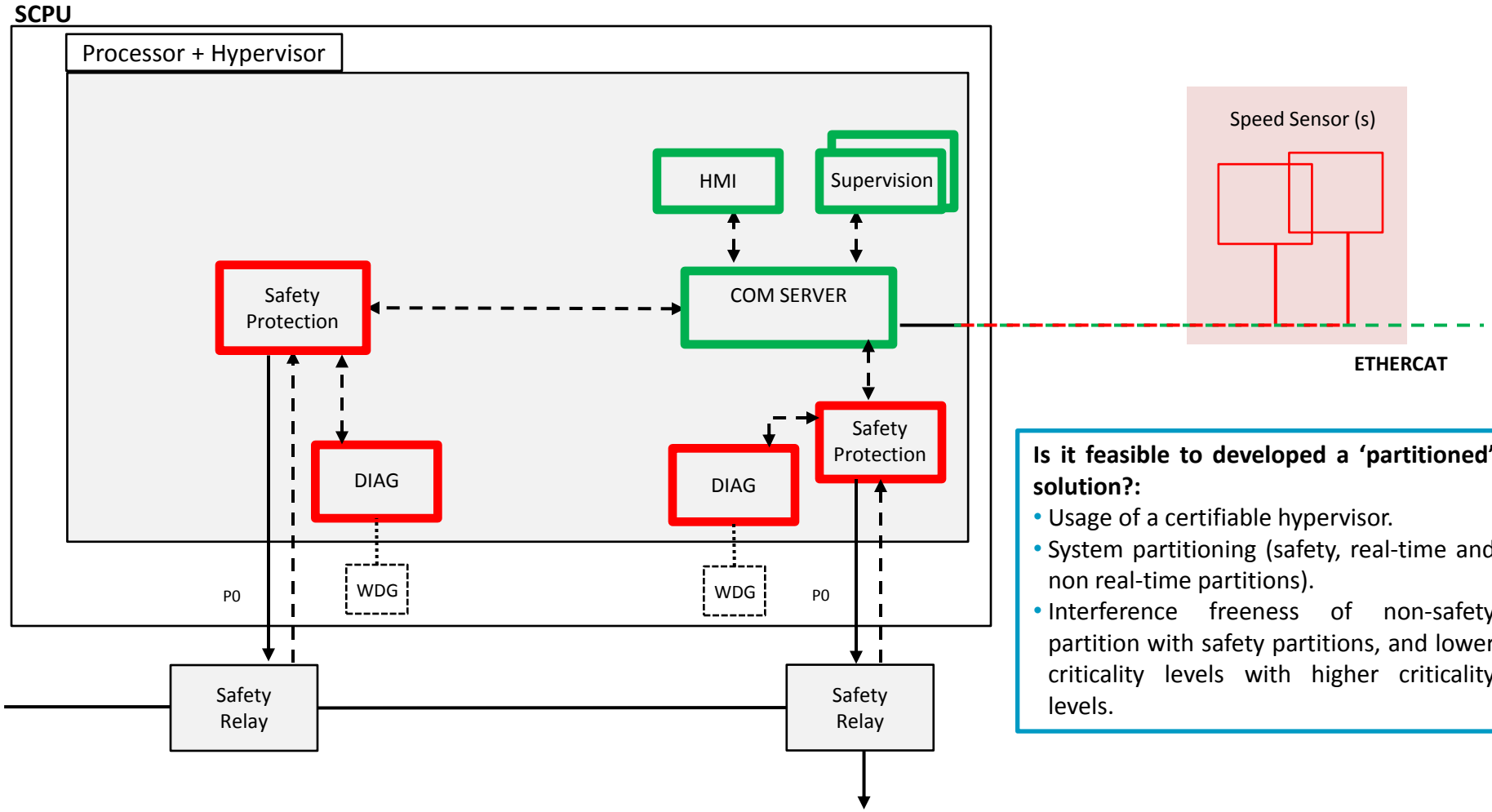
- Add additional processors (P2, P3, etc.) to provide required computation performance

Reduced Reliability:

- The overall system reliability and availability is reduced...

Safety Concept – (B - 'Multicore partitioning')

PARTITIONED

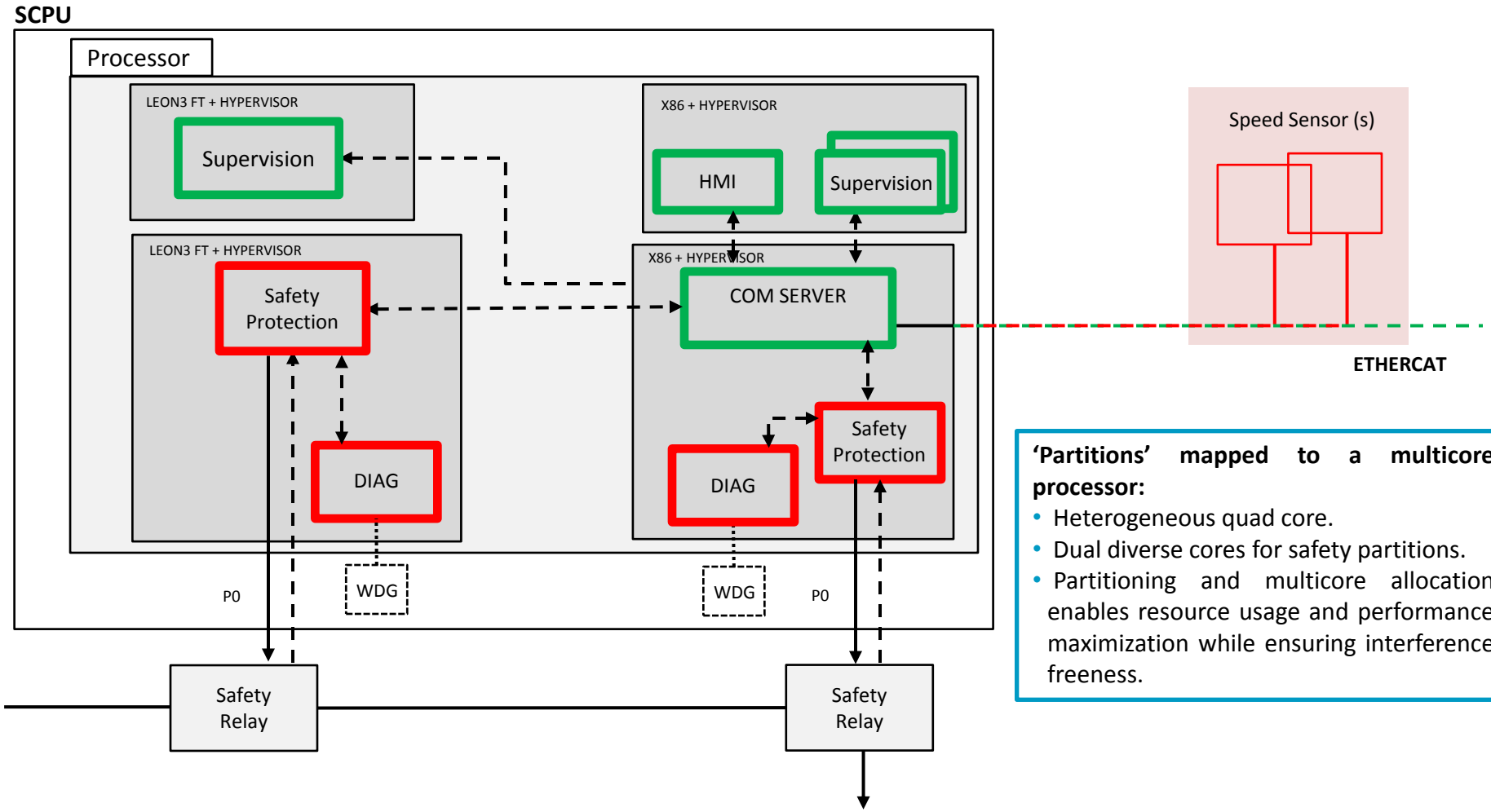


Is it feasible to developed a 'partitioned' solution?:

- Usage of a certifiable hypervisor.
- System partitioning (safety, real-time and non real-time partitions).
- Interference freeness of non-safety partition with safety partitions, and lower criticality levels with higher criticality levels.

Safety Concept – (B - 'Multicore partitioning')

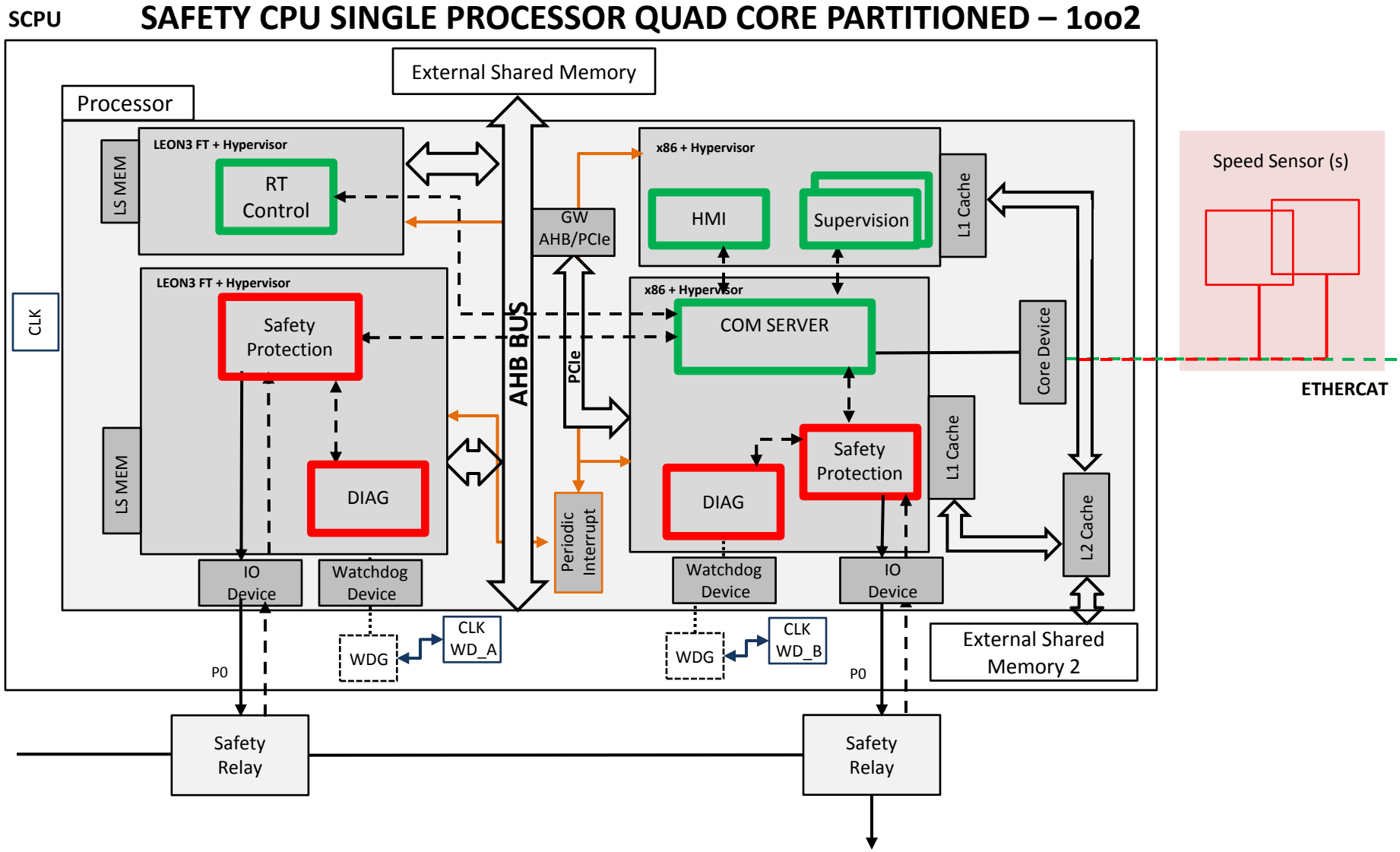
SAFETY CPU SINGLE PROCESSOR QUAD CORE PARTITIONED – 1oo2



'Partitions' mapped to a multicore processor:

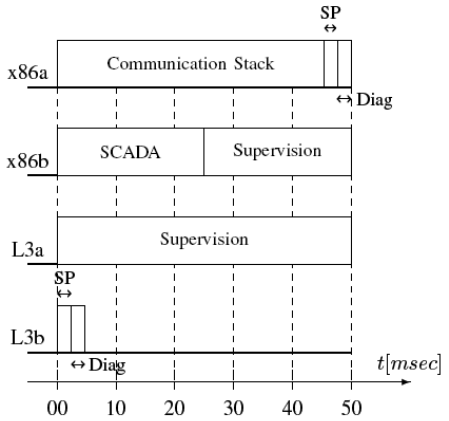
- Heterogeneous quad core.
- Dual diverse cores for safety partitions.
- Partitioning and multicore allocation enables resource usage and performance maximization while ensuring interference freeness.

Safety Concept – (B - 'Multicore partitioning')



Safety Concept – (B - 'Multicore partitioning')

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



- Diagnosis:
  - The partition should be self contained and should provide safety life-cycle related techniques and platform independent diagnosis abstracted from the details of the underlying platform.
  - The hardware provides autonomous diagnosis and diagnosis components to be commanded by software.
  - The hypervisor and associated diagnosis partitions should support platform related diagnosis.
  - The system architect specifies and integrates additional diagnosis partitions required to develop a safe product taking into consideration all safety manuals.

[1] H. Kopetz, On the Fault Hypothesis for a Safety-Critical Real-Time System, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2006, vol. 4147, ch. 3, pp. 31–42.

IKERLAN

05

Conclusions and lessons learnt

Conclusions and lessons learnt

- ◊ It is feasible to achieve SIL3 IEC-61508 / Pld ISO-13849 with COTS multicore, partitioning and current safety standard versions.
- ◊ Temporal independence and isolation:
  - Temporal isolation simplifies the safety argumentation but… Temporal independence does not necessarily require temporal isolation.
  - The lack of complete temporal isolation and rare (undocumented) temporal events could reduce the availability of the system but should not jeopardize safety (fault avoidance and control).
- ◊ 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 using PTA (Probabilistic Time Analysis)
  - ◊ 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