IK4 IKERLAN
Research Alliance

(On the way to) Success Stories From Non-Space Domains

10th ESA Workshop on Avionics, Data, Control and Software Systems
ESA/ESTEC , Noordwijk - The Netherlands (19th October)

Jon Pérez
jmperez@ikerlan.es

DREAMS PROXIMA SAFEPOWER

Outline

1. Executive summary
2. Introduction
3. The wind turbine example
4. The railway example
5. The industrial example
6. The automotive example
7. Conclusions and lessons learnt

IKERLAN

01

Executive Summary

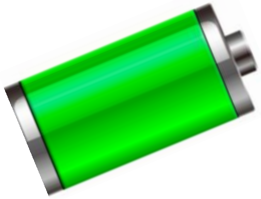
Presentation in a nutshell

Market Pull

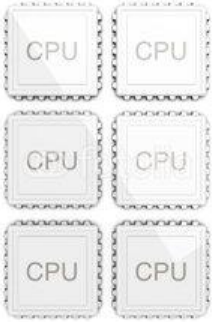
Safety

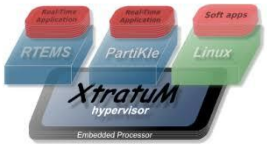
+ Functionalities

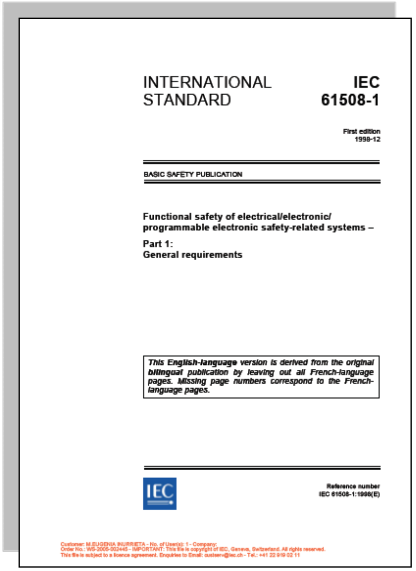
- Weight / Volume



Technology Push







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

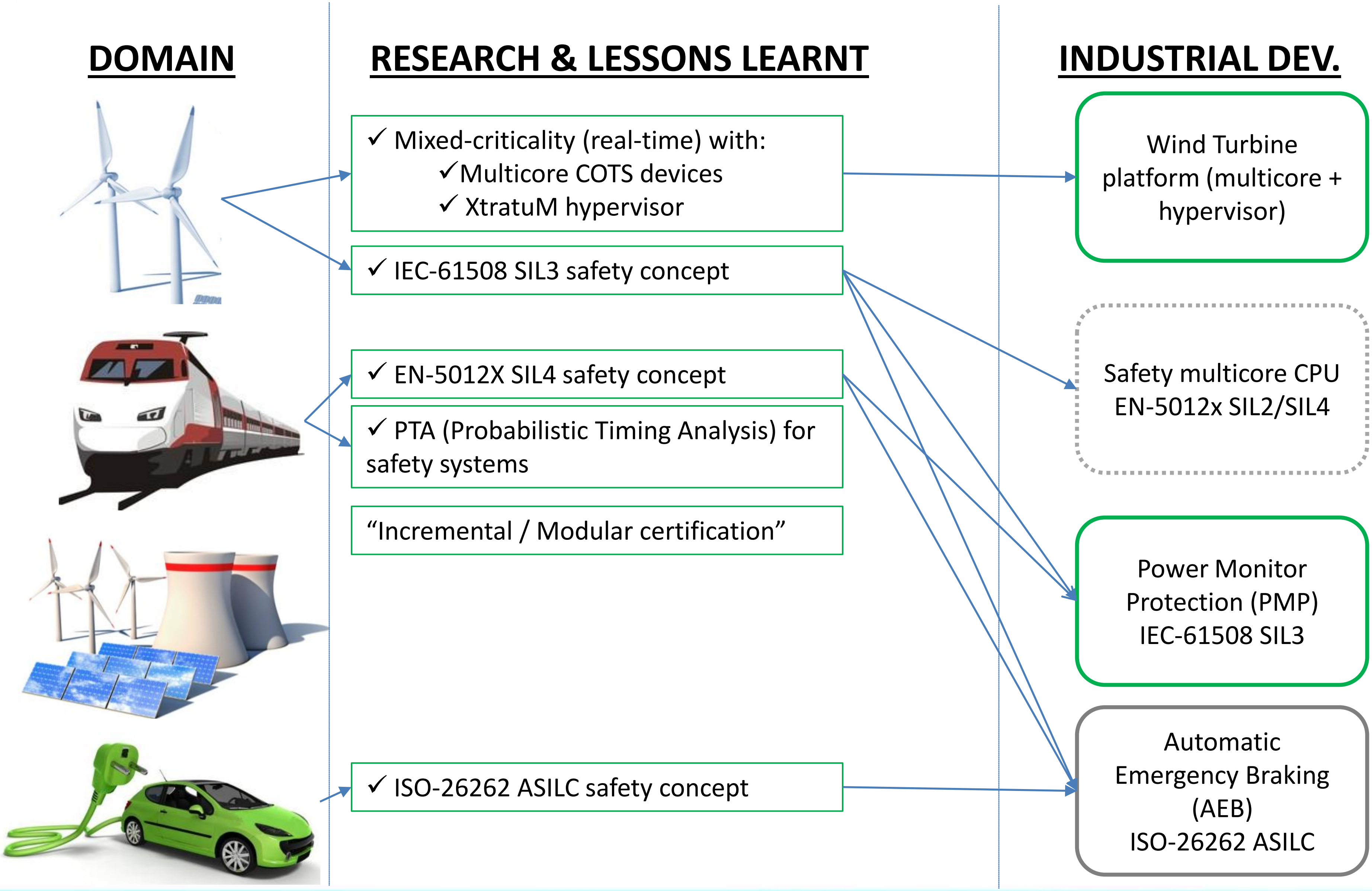
Reference number
IEC 61508-1:1998(E)

Customer: M.EUGENIA INURRIETA - No. of User(s): 1 - Company:
Order No.: WS-2005-002445 - IMPORTANT: This file is copyright of IEC, Geneva, Switzerland. All rights reserved.
This file is subject to a licence agreement. Enquiries to Email: custserv@iec.ch - Tel.: +41 22 919 02 11

Product H2020+

Presentation in a nutshell

IK4 IKERLAN
Research Alliance



DOMAIN

RESEARCH & LESSONS LEARNT

INDUSTRIAL DEV.

✓ Mixed-criticality (real-time) with:
- ✓Multicore COTS devices
- ✓ XtratuM hypervisor

✓ IEC-61508 SIL3 safety concept

✓ EN-5012X SIL4 safety concept

✓ PTA (Probabilistic Timing Analysis) for safety systems

"Incremental / Modular certification"

✓ ISO-26262 ASILC safety concept

Wind Turbine platform (multicore + hypervisor)

Safety multicore CPU
EN-5012x SIL2/SIL4

Power Monitor Protection (PMP)
IEC-61508 SIL3

Automatic Emergency Braking (AEB)
ISO-26262 ASILC

02

Introduction

Some Research Projects: Multicore & mixed-criticality

DREAMS

Contrex

PROXIMA

SAFEPOWER

MultiPARTES

CERTAINTY

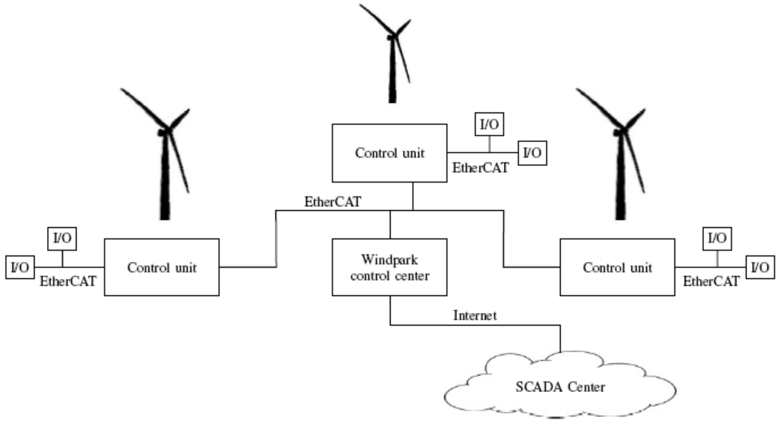
EMC^2

CRYSTAL

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] Pérez, 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.

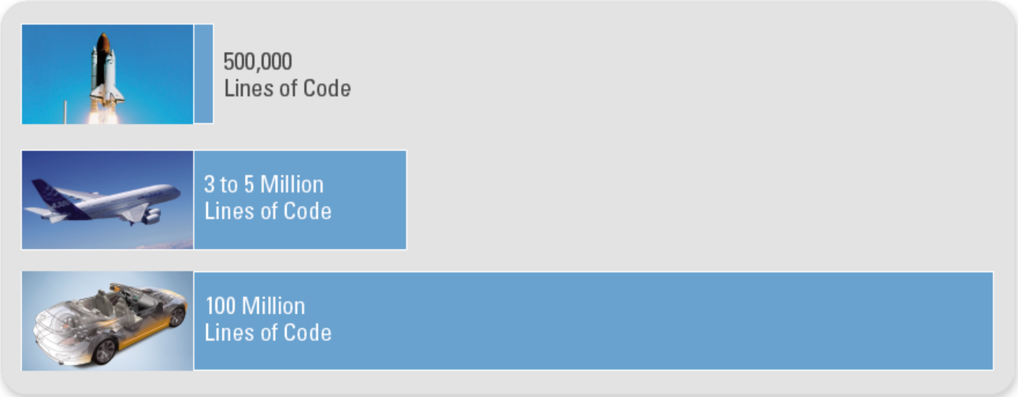
[2] Pérez, J., et al. (2014). "A safety certification strategy for IEC-61508 compliant industrial mixed-criticality systems based on multicore partitioning." Euromicro DSD/SEAA Verona, Italy.

Automotive

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.

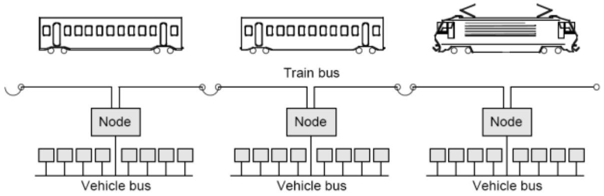
[3] Leohold, J. Communication Requirements for Automotive Systems. 5thIEEE Workshop on Factory Communication Systems (WCFS). Wien, 2004.

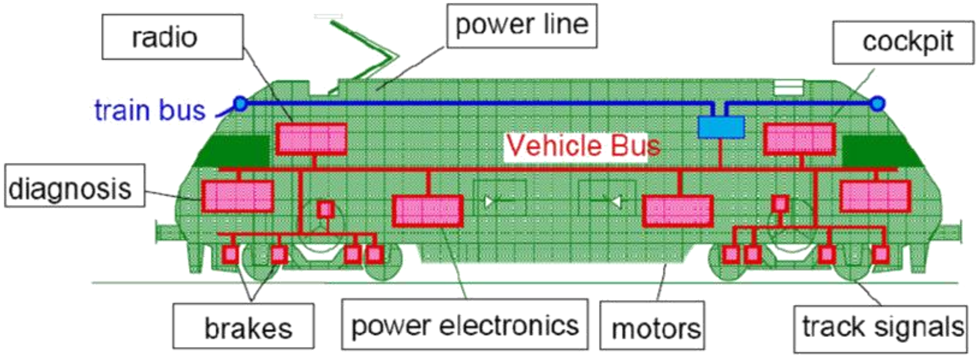
[4] National Instruments, How engineers are reinventing the automobile,, http://www.ni.com/newsletter/51684/en/ , 2013.

On-board) 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.





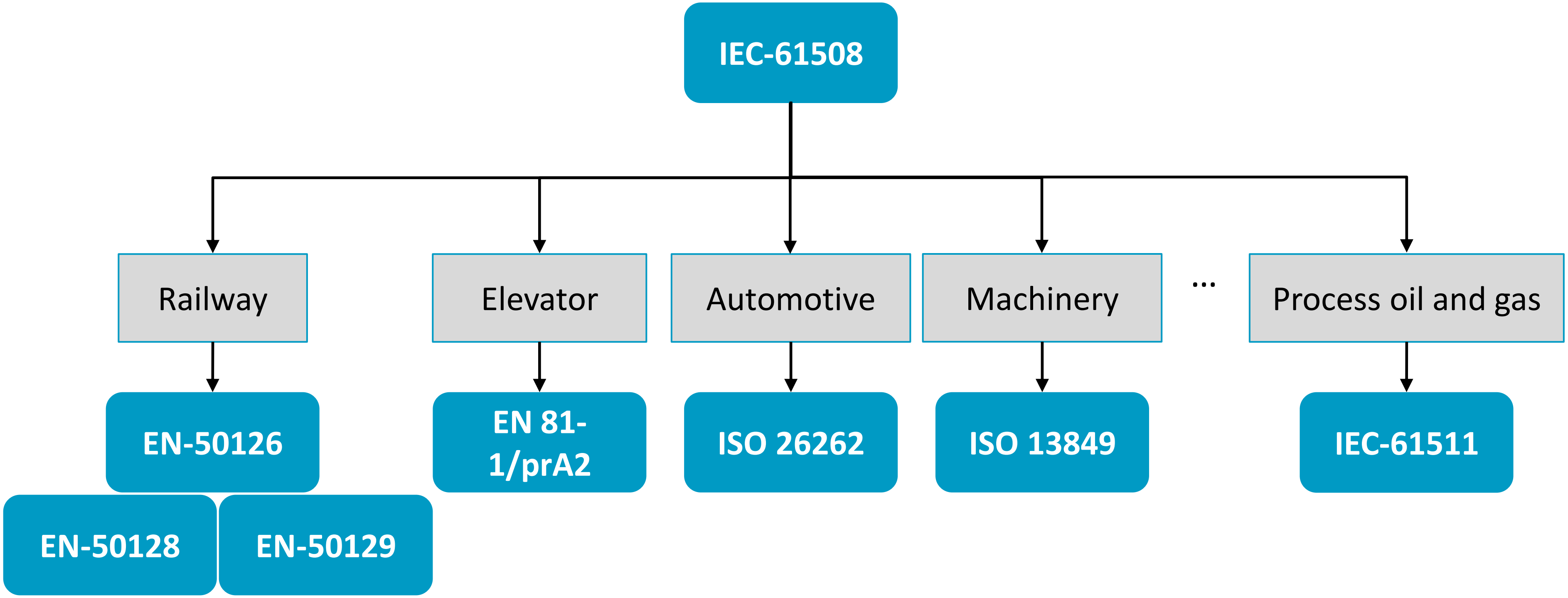
[1] The European Rail Research Advisory Council (ERRAC), Joint Strategy for European Rail Research 2020.

[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 certification (IEC-61508)

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



Mixed Criticality – Already in the market

There are already certified Mixed-Criticality safety systems already in the market:

- Some of them based on safety RTOS that provide partitioning (e.g., INTEGRITY)
- Some of them based on ‘ad-hoc’ solutions, e.g.,
  - A Linux based non-safety related application
  - A periodic Non-Maskable Interrupt (NMI) that implements the safety function
- But this presentation will focus on….

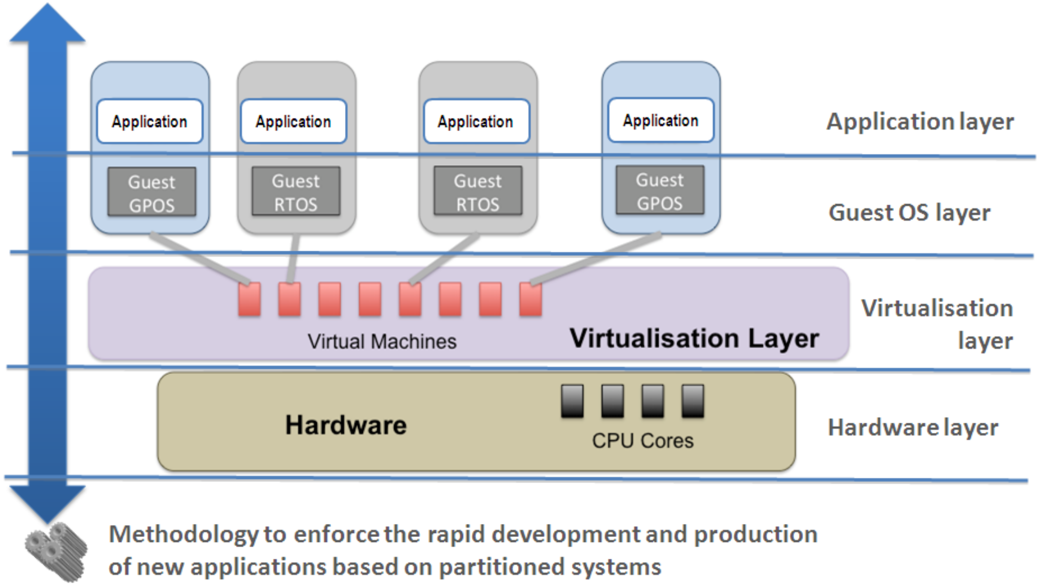
Mixed Criticality

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

The focus is:

- Systematic approach (and not ‘ad-hoc’ approach) that considers:
  - Composition of mixed-criticality functionalities provided by ‘third parties’ and ‘legacy SW’
  - Safety certification approach, methodology and restrictions according to applicable standards
- Using available COTS ‘multicore devices’ and ‘hypervisor’ technology

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

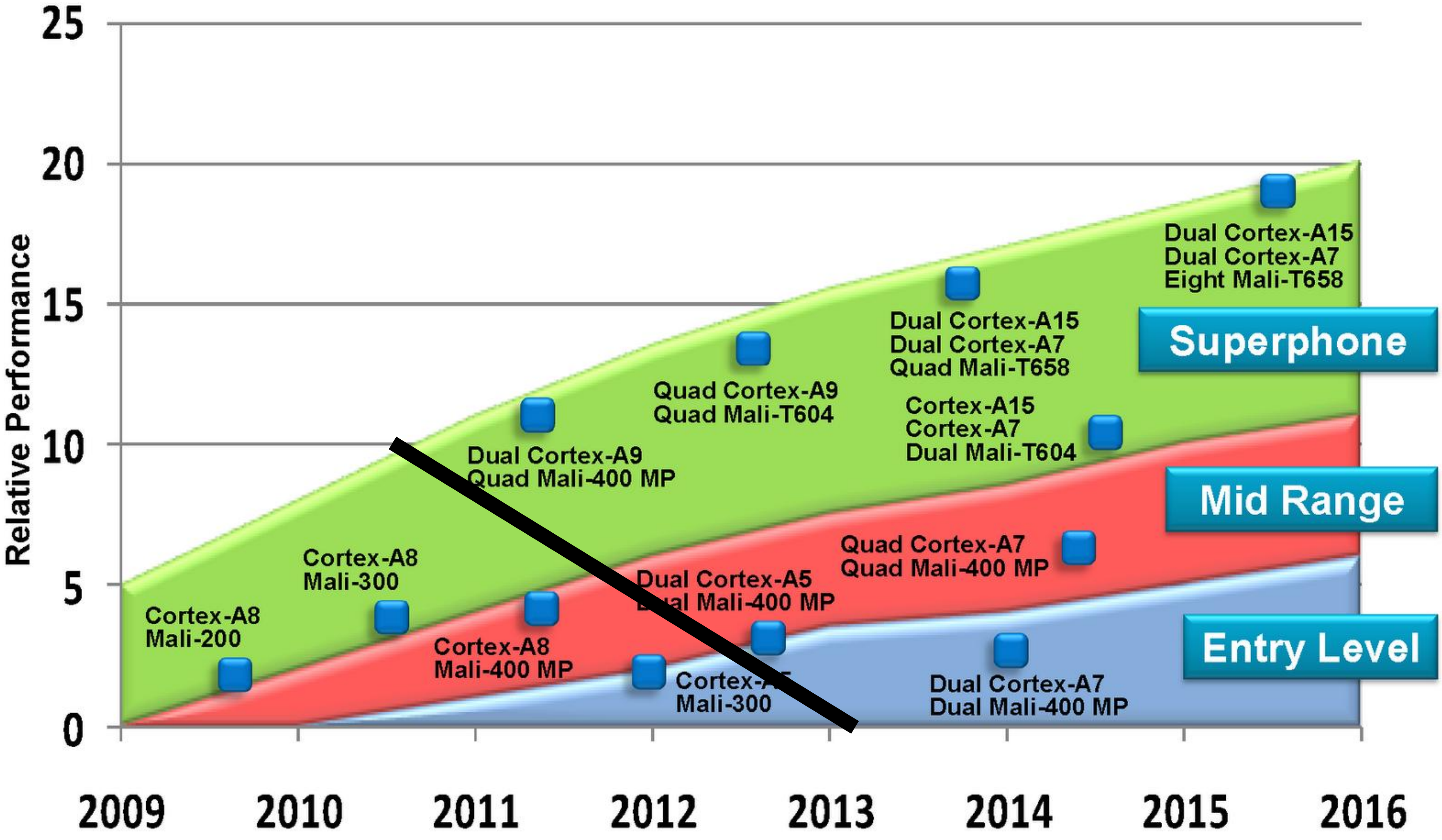


Methodology to enforce the rapid development and production of new applications based on partitioned systems

02.A

Introduction - Multicore

Multicore – Smartphones

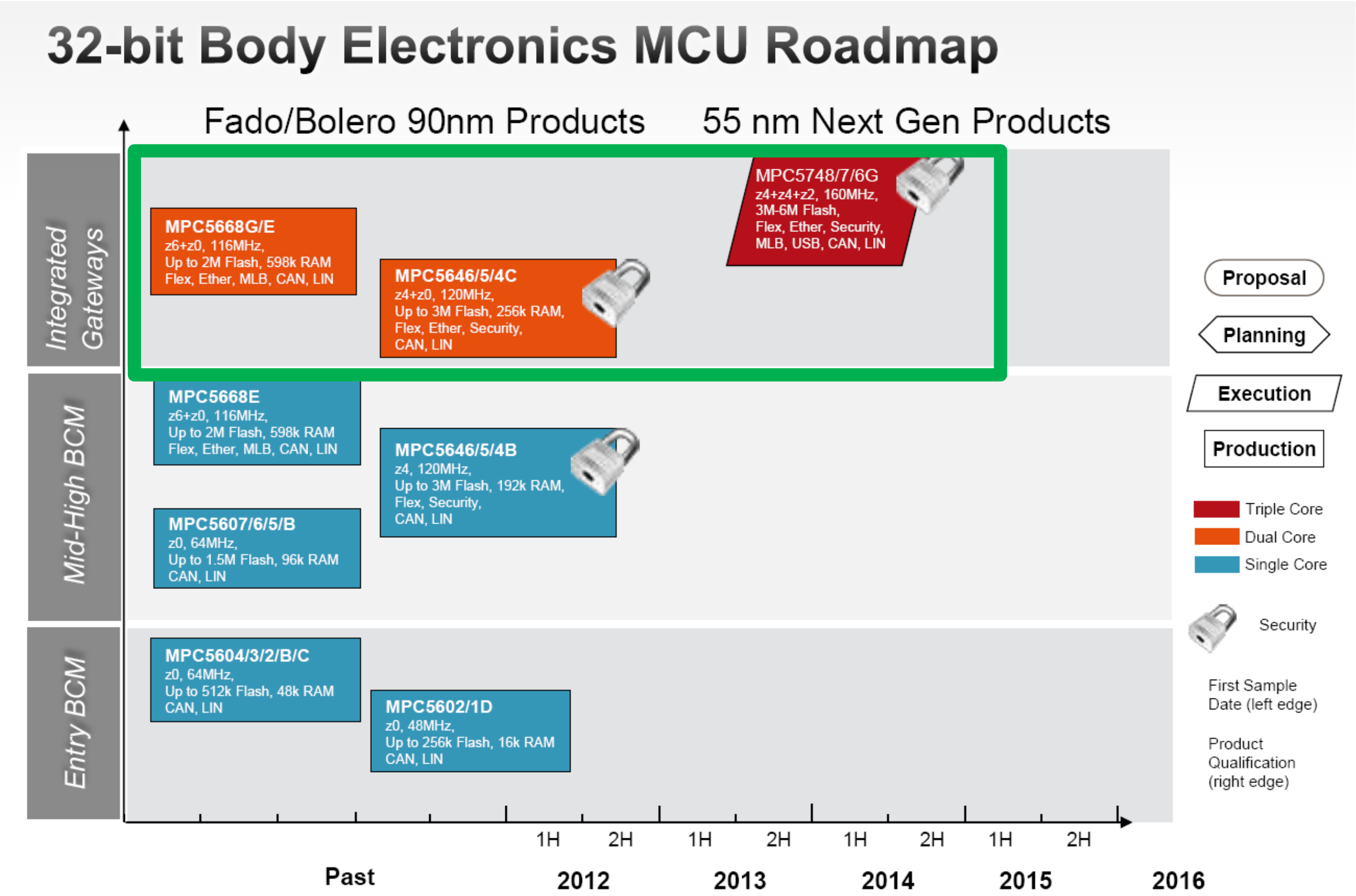


Source: www.arm.com

Multicore - Automotive

2nd International Conference Automotive Embedded Multi-Core Systems.

Roadmaps:



32-bit Body Electronics MCU Roadmap

Fado/Bolero 90nm Products 55 nm Next Gen Products

Integrated Gateways

MPC5668G/E
z6+z0, 116MHz,
Up to 2M Flash, 598k RAM
Flex, Ether, MLB, CAN, LIN

MPC5646/5/4C
z4+z0, 120MHz,
Up to 3M Flash, 256k RAM,
Flex, Ether, Security,
CAN, LIN

MPC5748/7/6G
z4+z4+z2, 160MHz,
3M-6M Flash,
Flex, Ether, Security,
MLB, USB, CAN, LIN

Mid-High BCM

MPC5668E
z6+z0, 116MHz,
Up to 2M Flash, 598k RAM
Flex, Ether, MLB, CAN, LIN

MPC5607/6/5/B
z0, 64MHz,
Up to 1.5M Flash, 96k RAM
CAN, LIN

MPC5646/5/4B
z4, 120MHz,
Up to 3M Flash, 192k RAM,
Flex, Security,
CAN, LIN

Entry BCM

MPC5604/3/2/B/C
z0, 64MHz,
Up to 512k Flash, 48k RAM
CAN, LIN

MPC5602/1D
z0, 48MHz,
Up to 256k Flash, 16k RAM
CAN, LIN

Proposal

Planning

Execution

Production

🟥 Triple Core
🟧 Dual Core
🟦 Single Core

🔒 Security

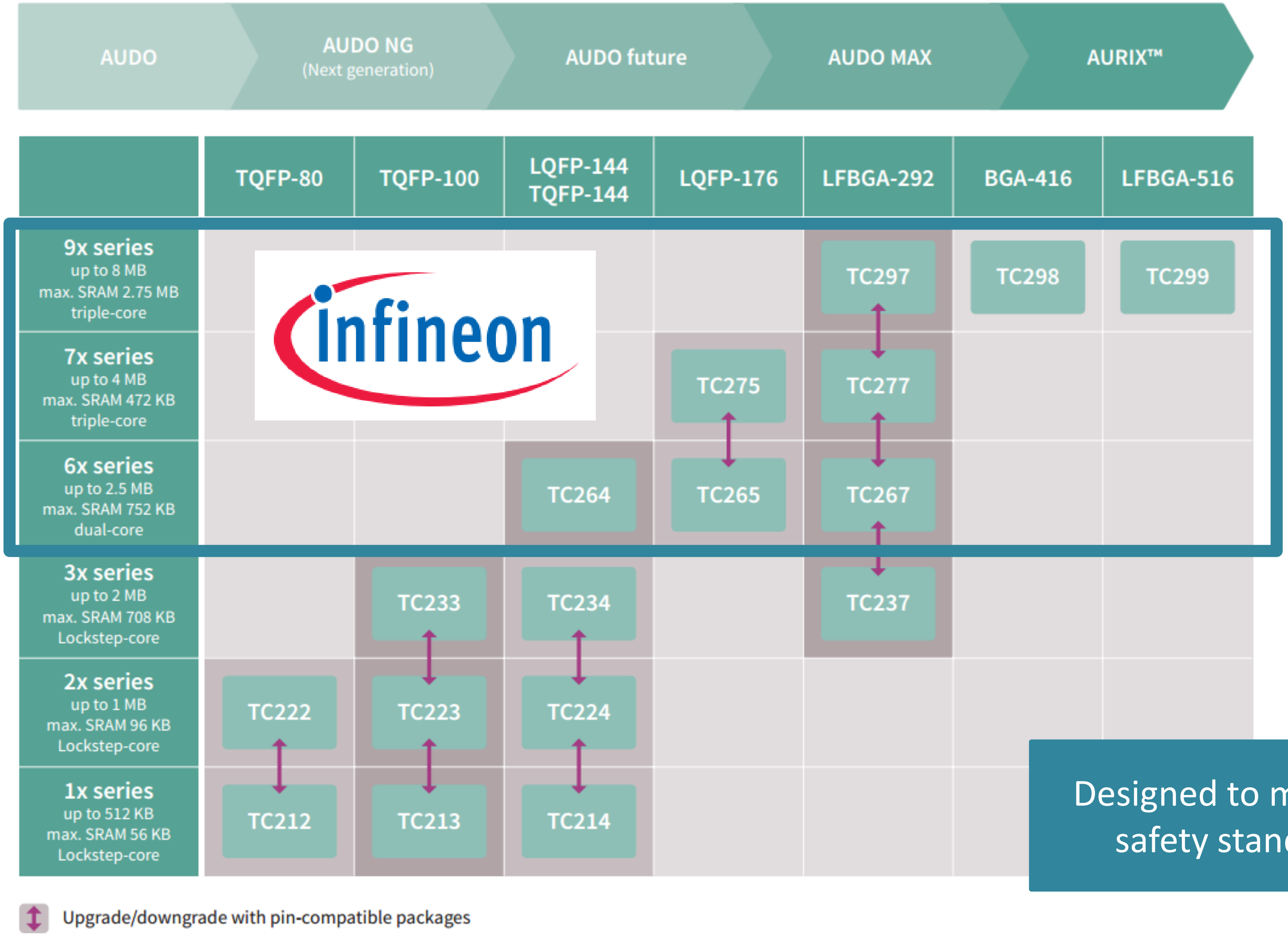
First Sample Date (left edge)

Product Qualification (right edge)

Source: www.freescale.com

Multicore - Automotive

5th Generation Infineon TriCore Processors: AURIX



AUDO → AUDO NG (Next generation) → AUDO future → AUDO MAX → AURIX™

	TQFP-80	TQFP-100	LQFP-144 TQFP-144	LQFP-176	LFBGA-292	BGA-416	LFBGA-516
9x series up to 8 MB max. SRAM 2.75 MB triple-core					TC297	TC298	TC299
7x series up to 4 MB max. SRAM 472 KB triple-core				TC275	TC277		
6x series up to 2.5 MB max. SRAM 752 KB dual-core			TC264	TC265	TC267		
3x series up to 2 MB max. SRAM 708 KB Lockstep-core		TC233	TC234		TC237		
2x series up to 1 MB max. SRAM 96 KB Lockstep-core	TC222	TC223	TC224				
1x series up to 512 KB max. SRAM 56 KB Lockstep-core	TC212	TC213	TC214				

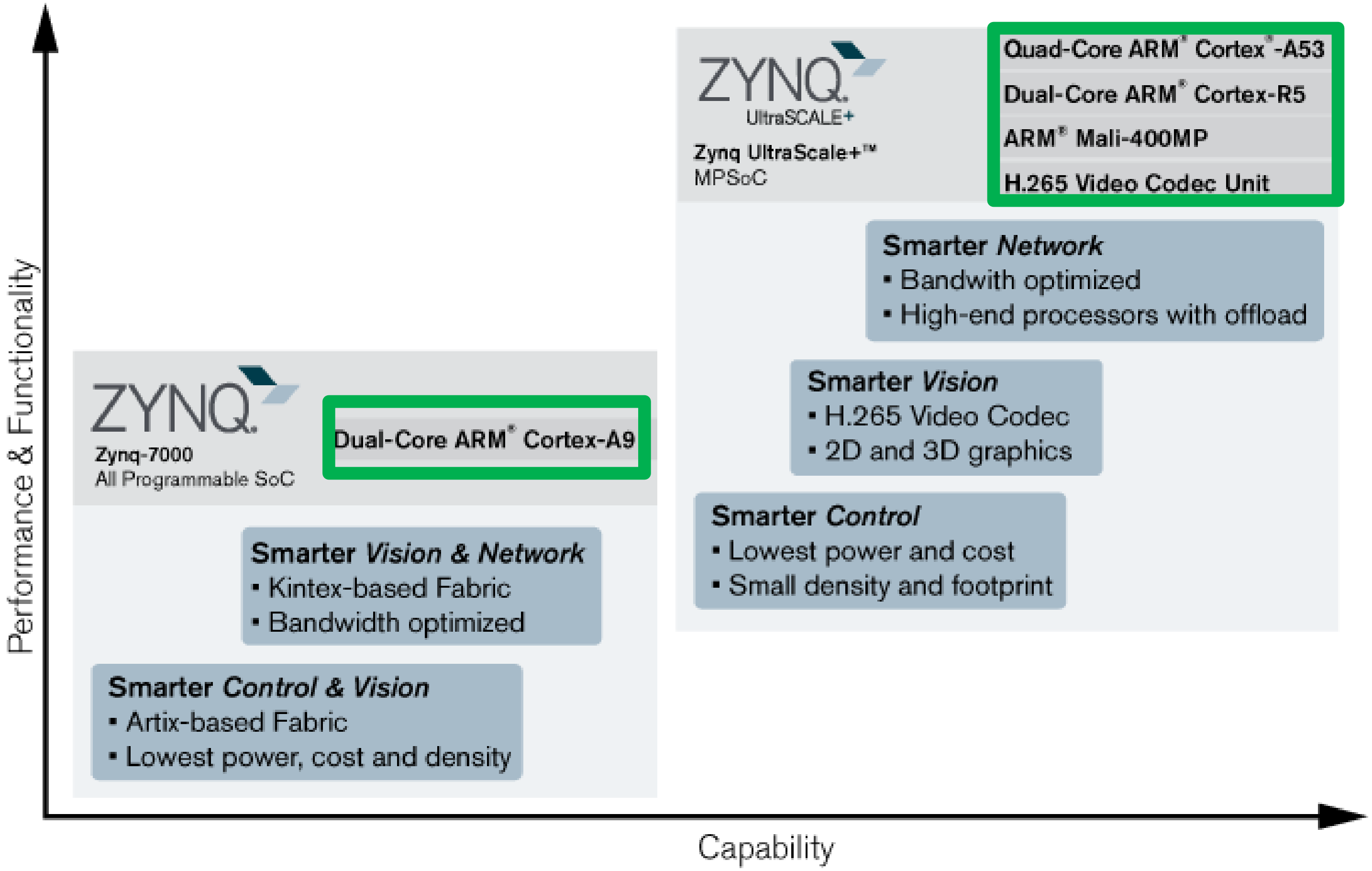
Infineon

↕ Upgrade/downgrade with pin-compatible packages

Designed to meet the safety standards

Source: http://www.infineon.com/aurix (Highly integrated and performance optimized 32-bit microcontrollers for automotive and industrial applications)

Multicore - Generic purpose



Smarter *Network*
- Bandwith optimized
- High-end processors with offload

Smarter *Vision*
- H.265 Video Codec
- 2D and 3D graphics

Smarter *Control*
- Lowest power and cost
- Small density and footprint

Smarter *Vision & Network*
- Kintex-based Fabric
- Bandwidth optimized

Smarter *Control & Vision*
- Artix-based Fabric
- Lowest power, cost and density

Source: www.xilinx.com

IEC-61508 and multicore

IEC-61508-3 Annex F (Informative) – “Techniques for achieving non-interference between software elements on a single computer”

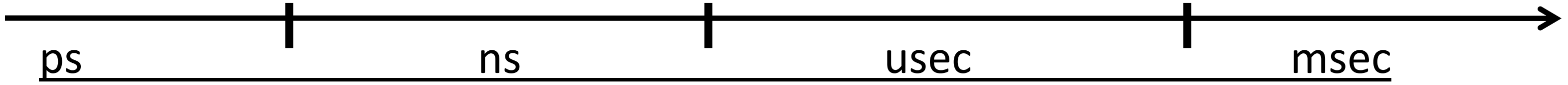
- “Independence of execution should be achieved and demonstrated both in the spatial and temporal domains.”
  - **“Spatial:** the data used by a one element shall not be changed by a another element. In particular, it shall not be changed by a non-safety related element.”
  - **“Temporal:** one element 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 behavior such that a dangerous failure would occur.”**

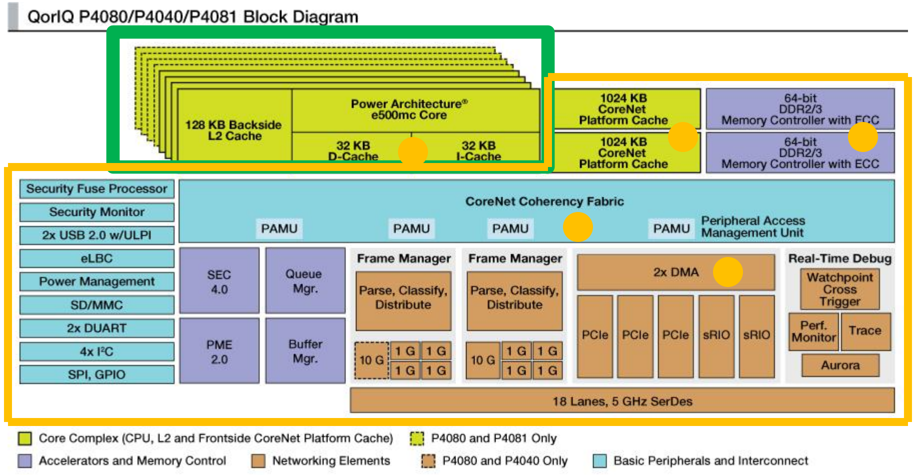
Threats to be considered and managed

Threats to be considered and managed

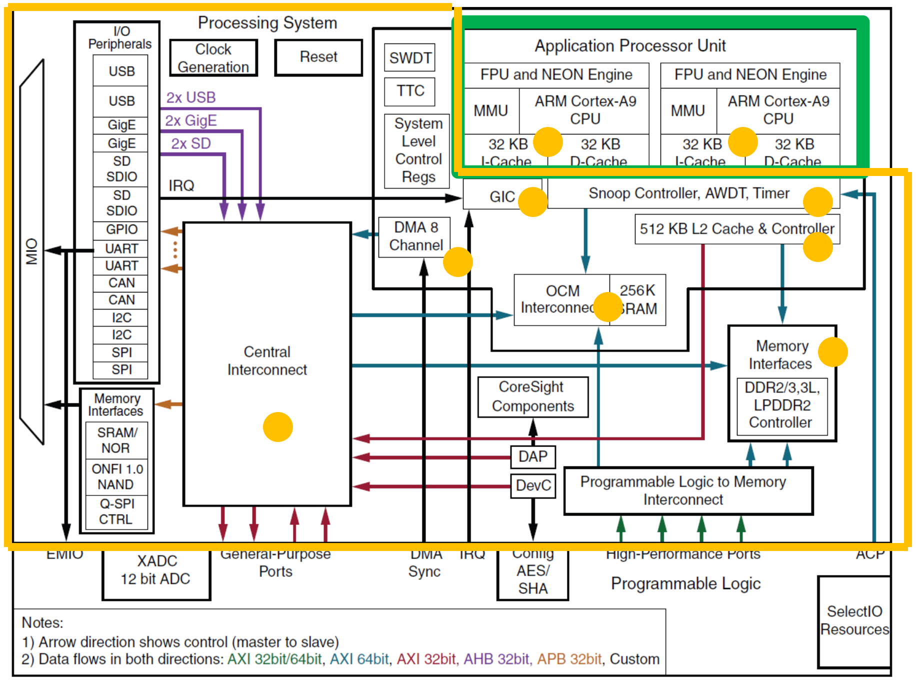
Temporal & Spatial independence, e.g., Shared resources (e.g., memory, cache, bus, interrupts) [1]

Which is the time-scale of the temporal interference?




QorIQ P4080/P4040/P4081 Block Diagram

🟨 Core Complex (CPU, L2 and Frontside CoreNet Platform Cache)		⬚ P4080 and P4081 Only	
🟪 Accelerators and Memory Control	🟧 Networking Elements	⬚ P4080 and P4040 Only	🟦 Basic Peripherals and Interconnect



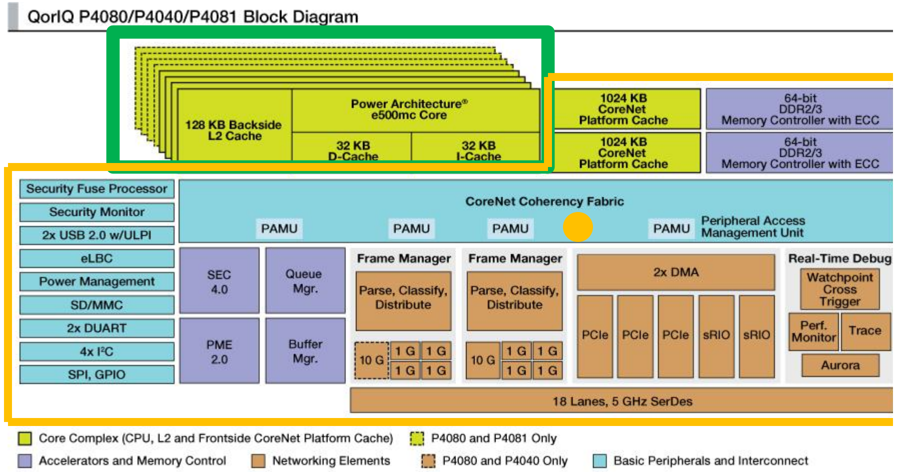
Notes:
1) Arrow direction shows control (master to slave)
2) Data flows in both directions: AXI 32bit/64bit, AXI 64bit, AXI 32bit, AHB 32bit, APB 32bit, Custom

[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

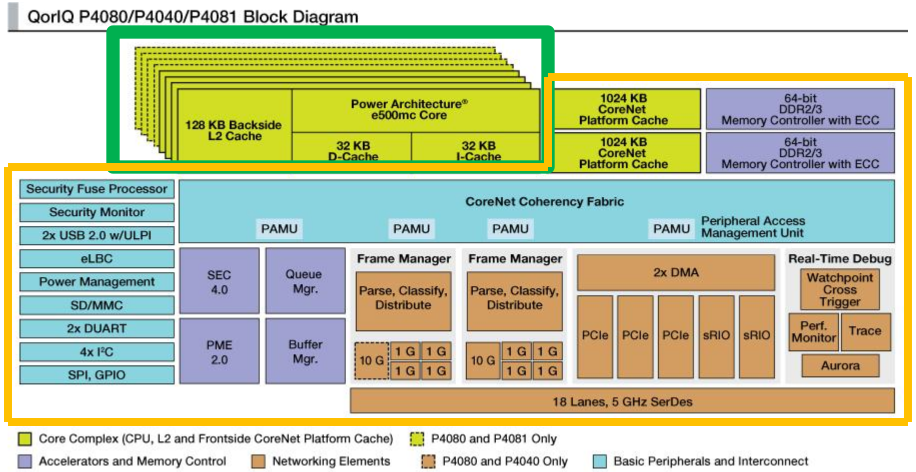


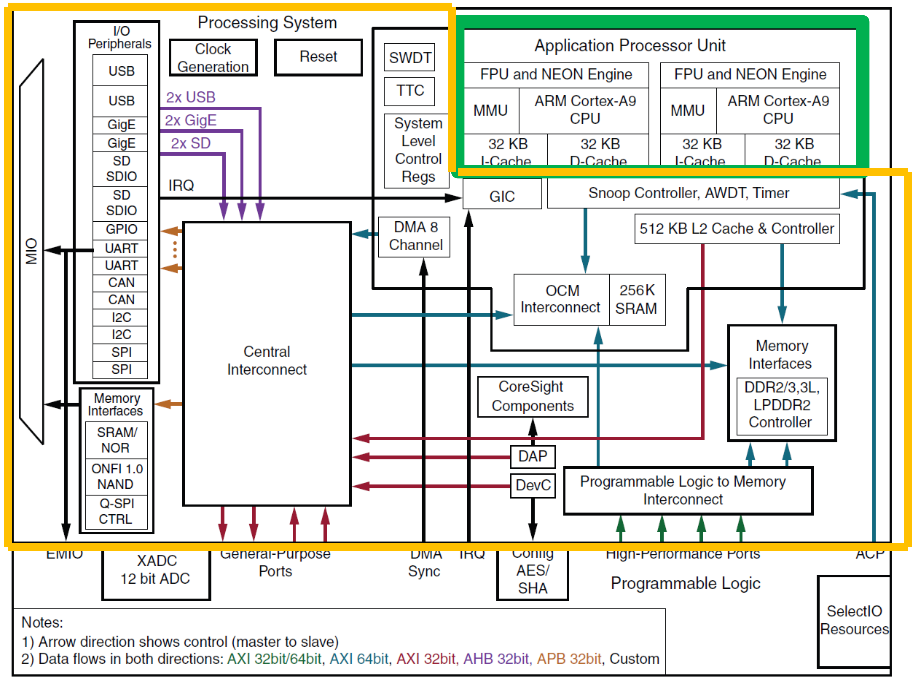
[1] http://www.advancedsubstratenews.com/2009/12/multicores-perfect-balance/

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

Threats to be considered and managed

Worst Case Execution Time (WCET)





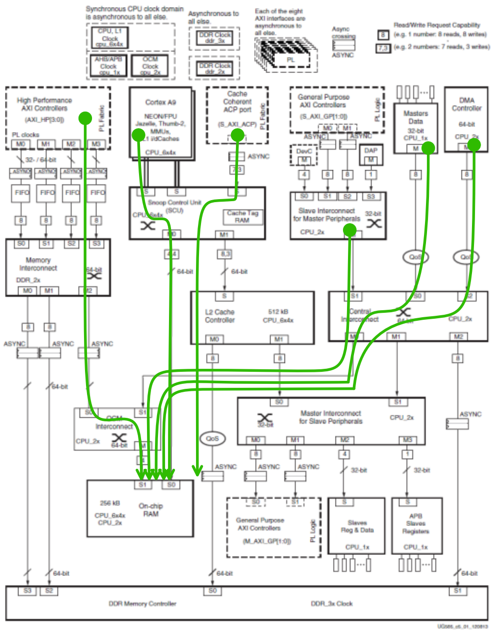
Source: www.freescale.com, www.xilinx.com

Threats to be considered and managed

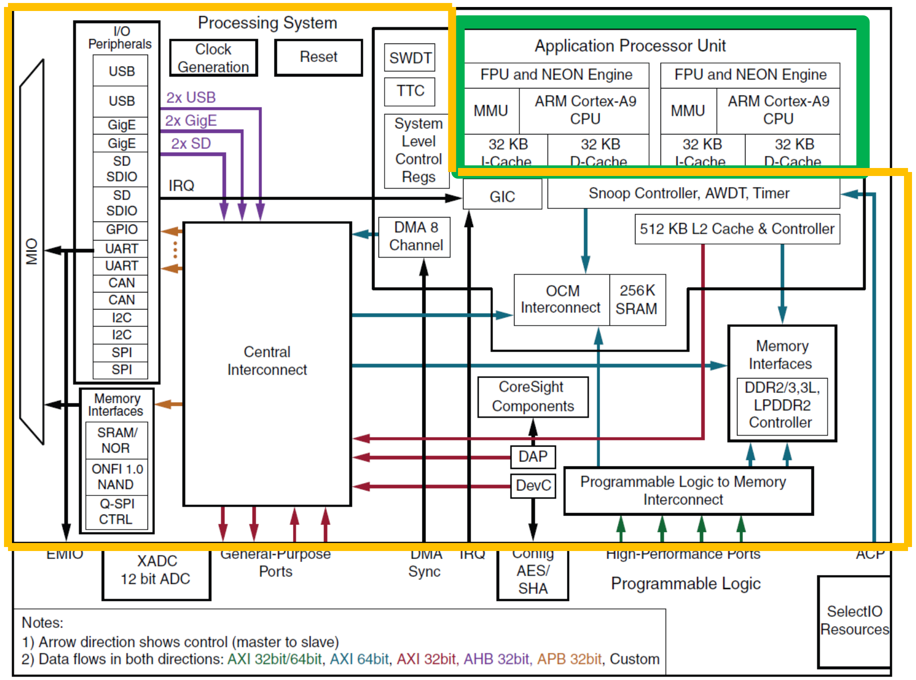
Interference among safety related and non safety related functions, e.g.,

- Safe startup and boot
- Safe shutdown
- Safe configuration
- Exclusive access to peripherals
- Resource virtualization

Diagnosis



Synchronous CPU clock domain is asynchronous to all else.
Asynchronous to all else.
Each of the eight AXI interfaces are asynchronous to all else.
Async crossing
ASYNC
Read/Write Request Capability
High Performance AXI Controllers
Cortex A9
Cache Coherent ACP port
General Purpose AXI Controllers
DMA Controller
Snoop Control Unit (SCU)
Slave Interconnect for Master Peripherals
Memory Interconnect
L2 Cache Controller
512 kB
Central Interconnect
OCM Interconnect
Master Interconnect for Slave Peripherals
256 kB On-chip RAM
General Purpose AXI Controllers
Slaves Reg & Data
APB Slaves Registers
DDR Memory Controller
DDR_3x Clock



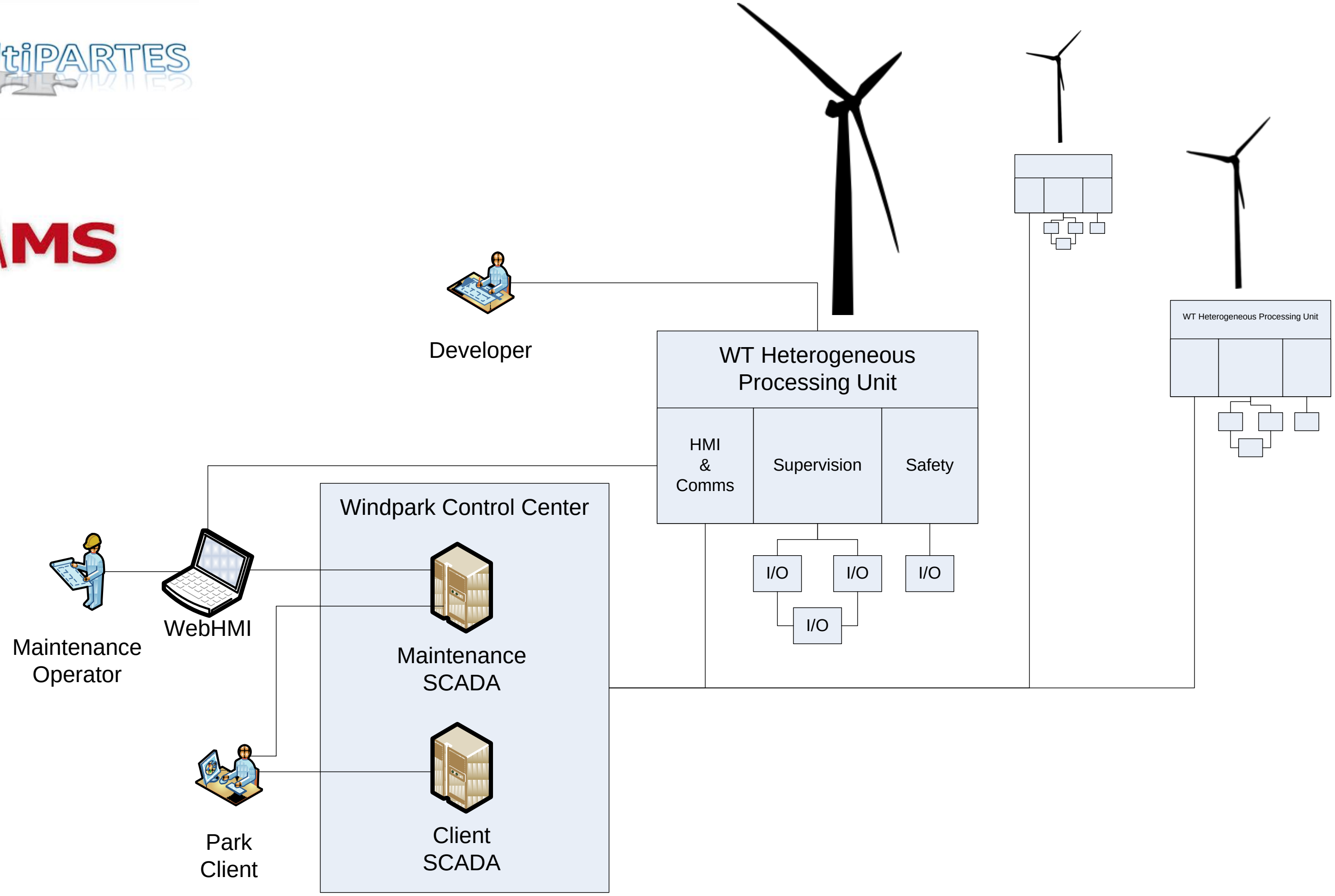
Notes:
1) Arrow direction shows control (master to slave)
2) Data flows in both directions: AXI 32bit/64bit, AXI 64bit, AXI 32bit, AHB 32bit, APB 32bit, Custom

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

03

The wind turbine example

Introduction – Context Diagram

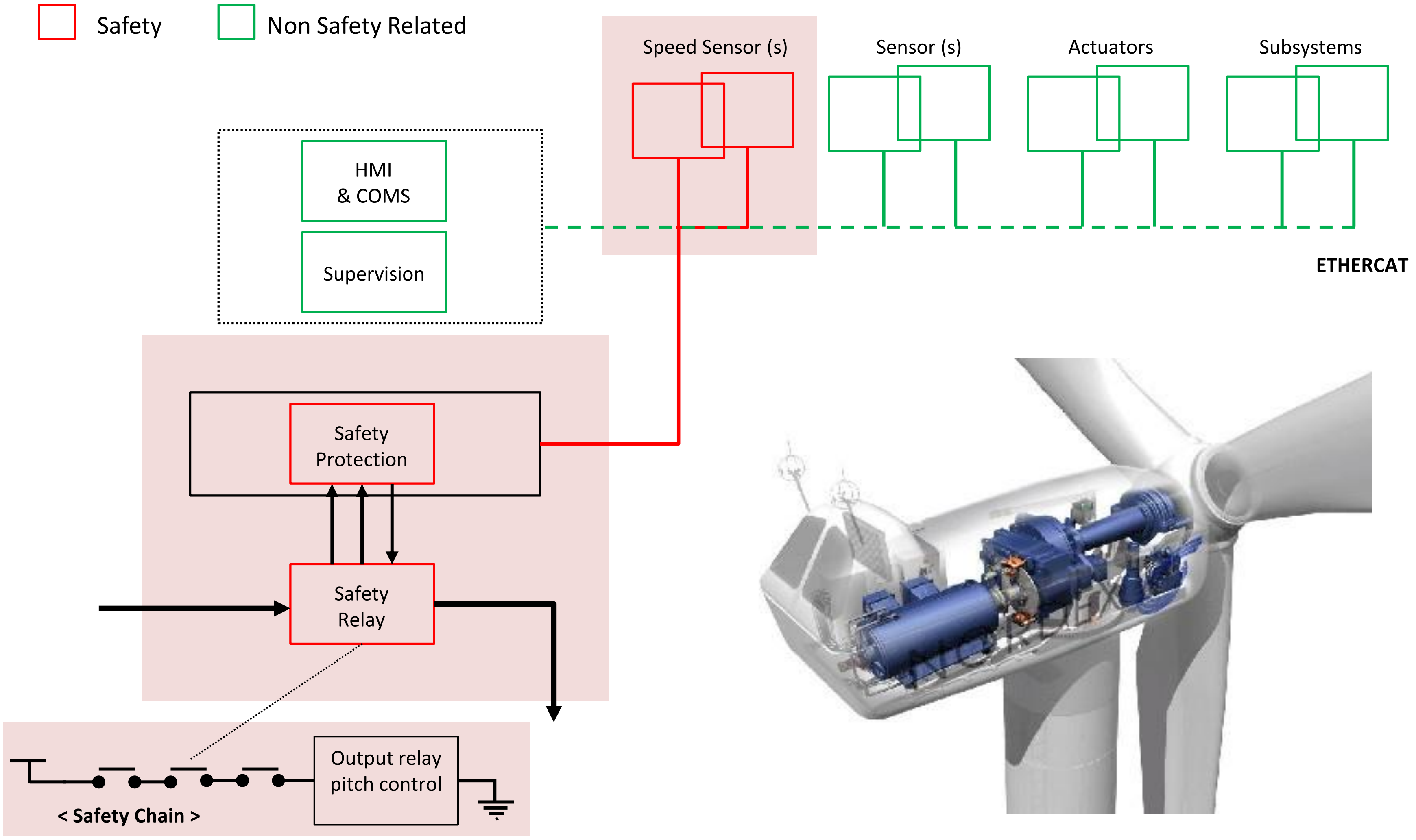


[1] Pérez, J., et al. (2014). A safety concept for a wind power mixed-criticality embedded system based on multicore partitioning. Functional Safety in Industry Application, 11th International TÜV Rheinland Symposium, Cologne, Germany.

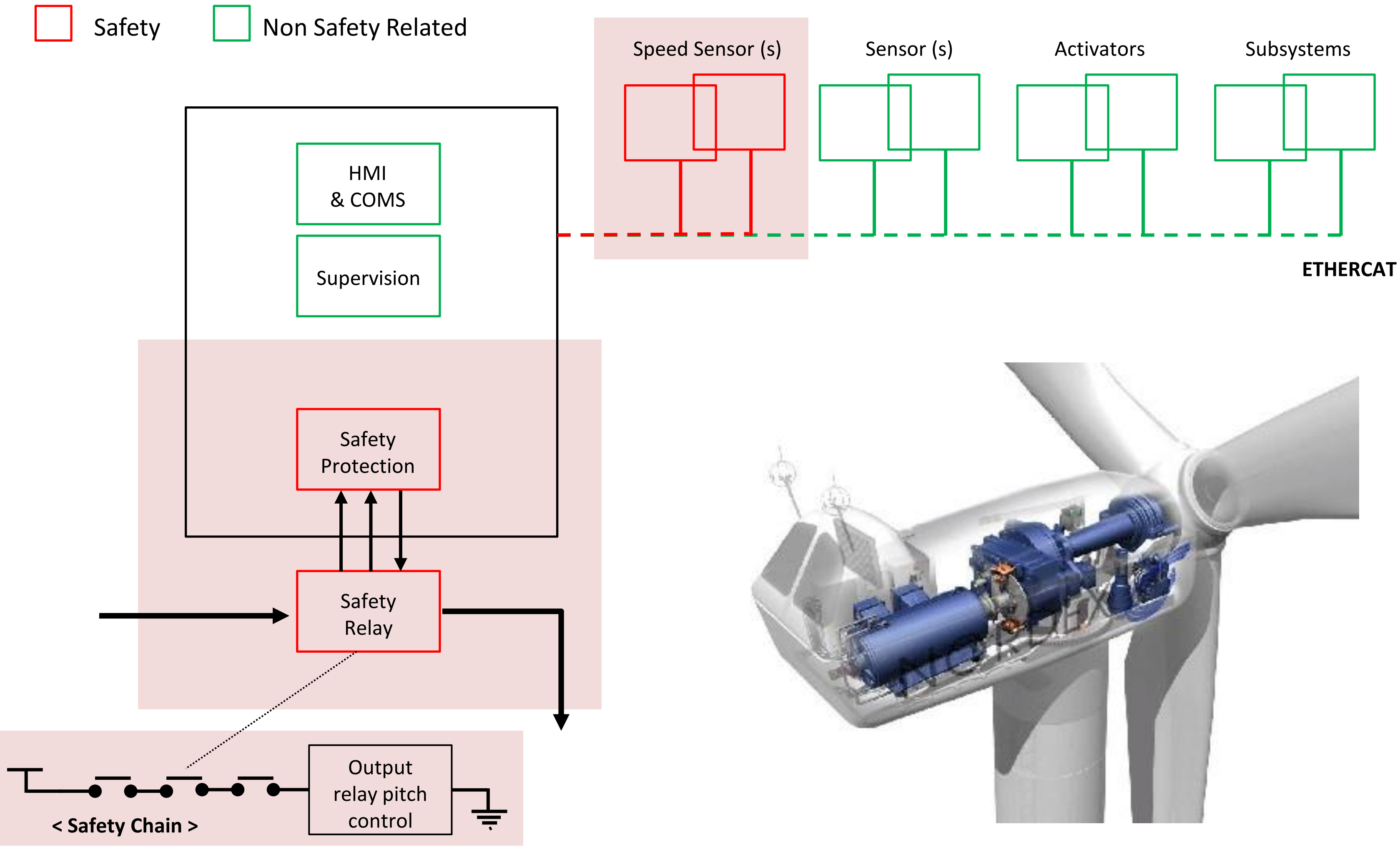
[2] Pérez, J., et al. (2014). "A safety certification strategy for IEC-61508 compliant industrial mixed-criticality systems based on multicore partitioning." Euromicro DSD/SEAA Verona, Italy.

[3] Pérez, J. and A. Trapman (2013). Deliverable D7.2 (Annex) - Wind power case-study safety concept, FP7 MultiPARTES.

Introduction – Context Diagram

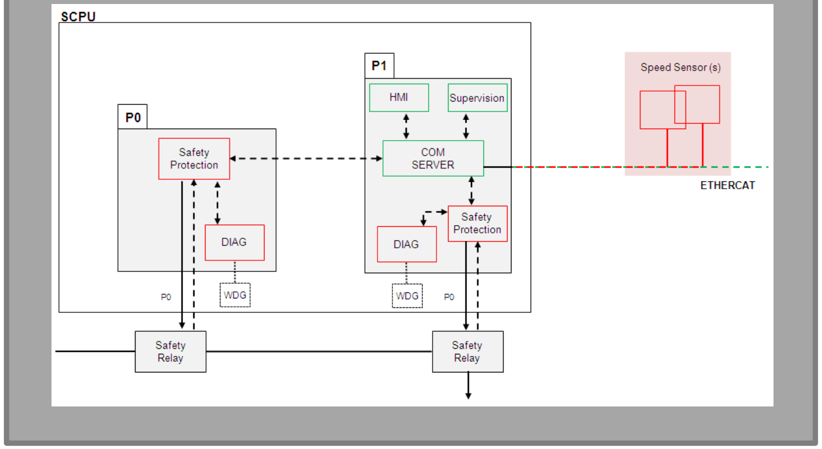


Introduction – Proposed solution

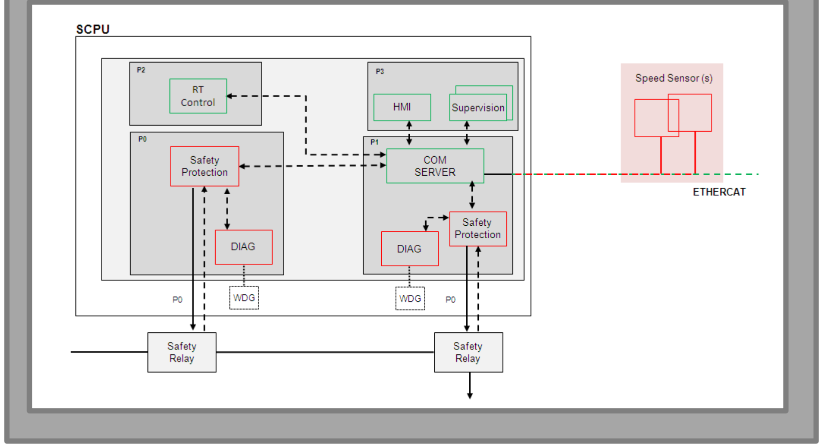


Safety concept – the approach

DUAL PROCESSOR – 1oo2



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

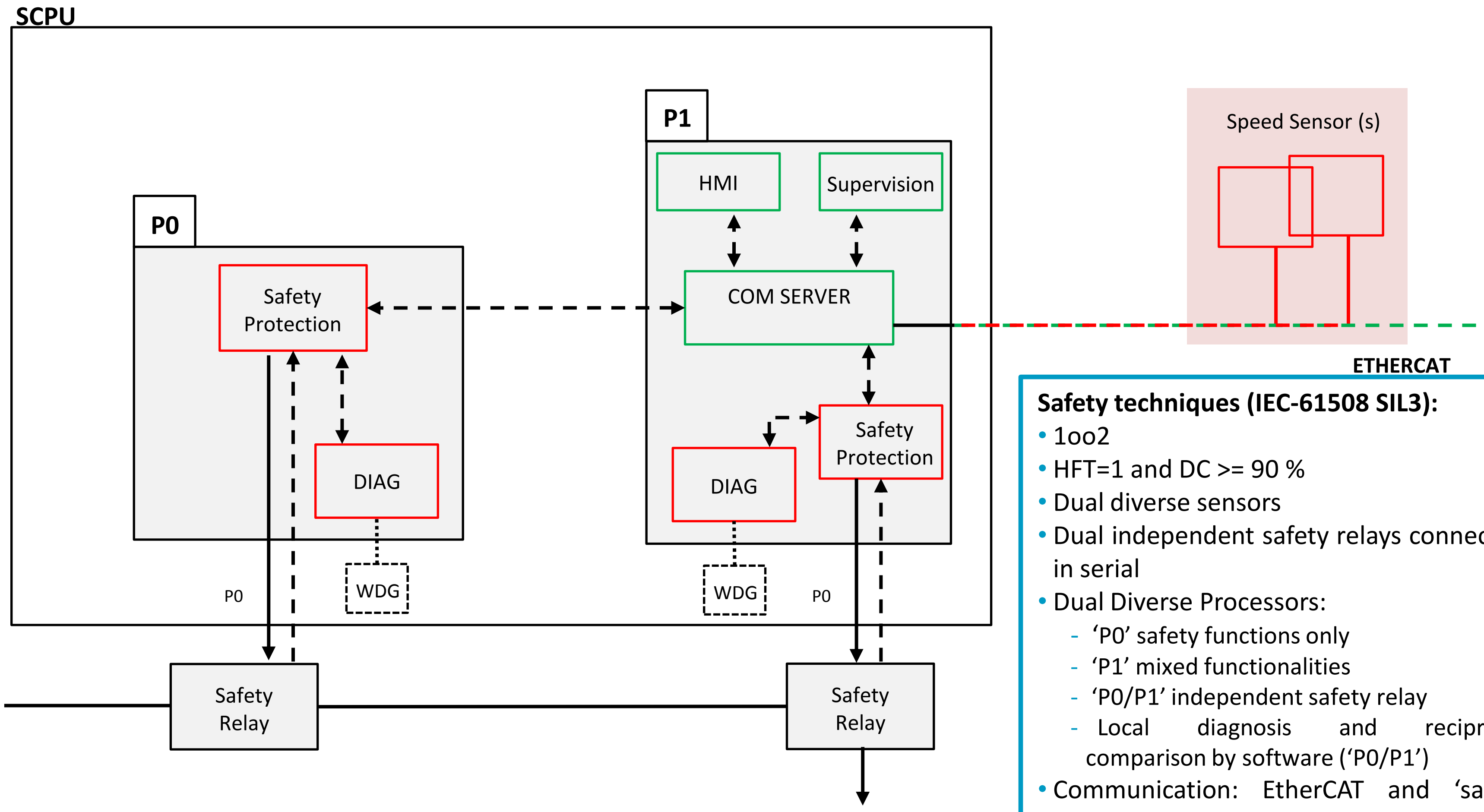


- Safety concept based on 'common practice in industry'
- Serves as a reference, not detailed

- Analogous safety concept using heterogeneous multicore and hypervisor
- The MultiPARTES contribution

Safety Concept – (A- ‘Traditional’)

DUAL-PROCESSOR – 1oo2

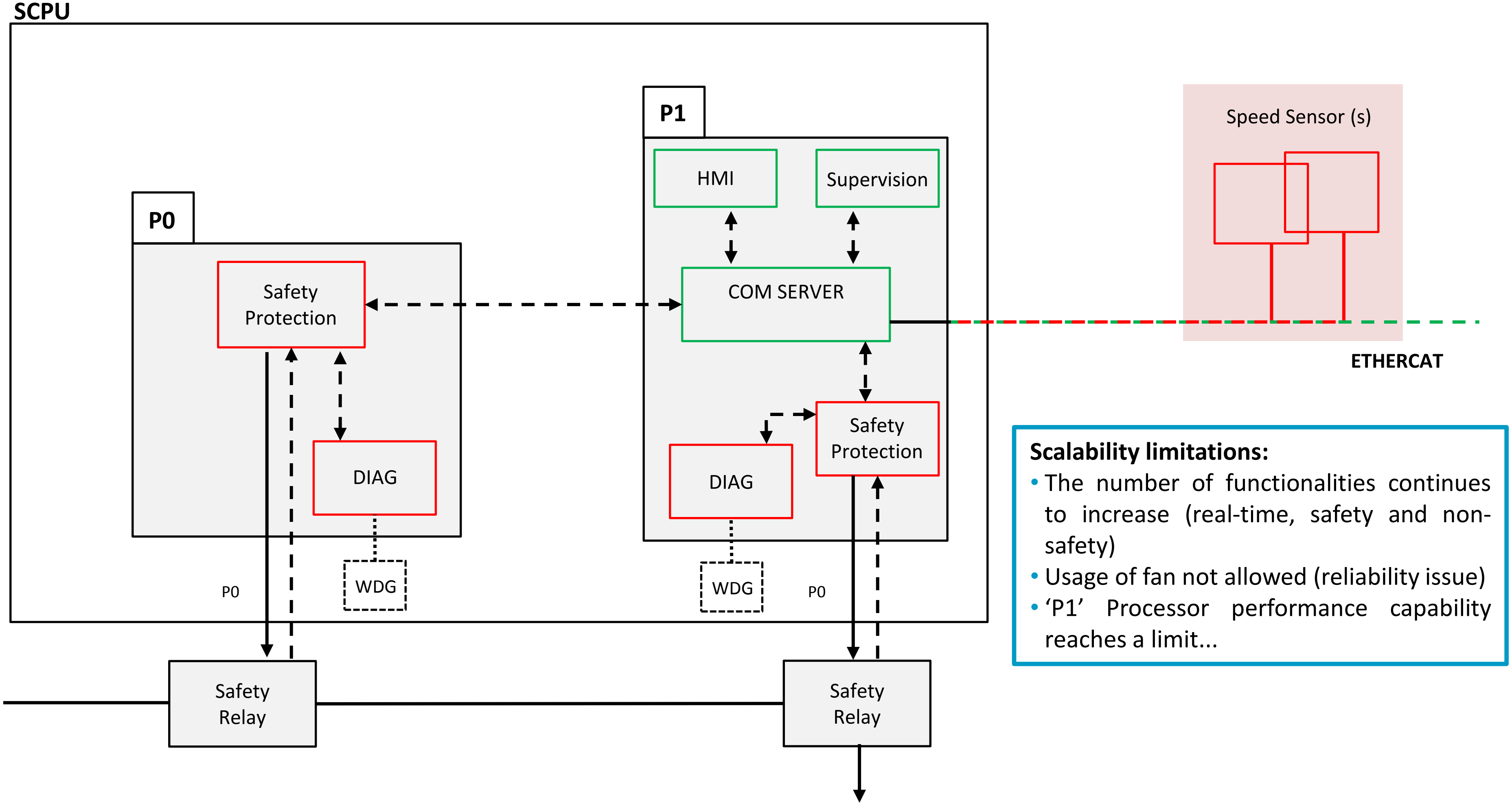


Safety techniques (IEC-61508 SIL3):

- 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

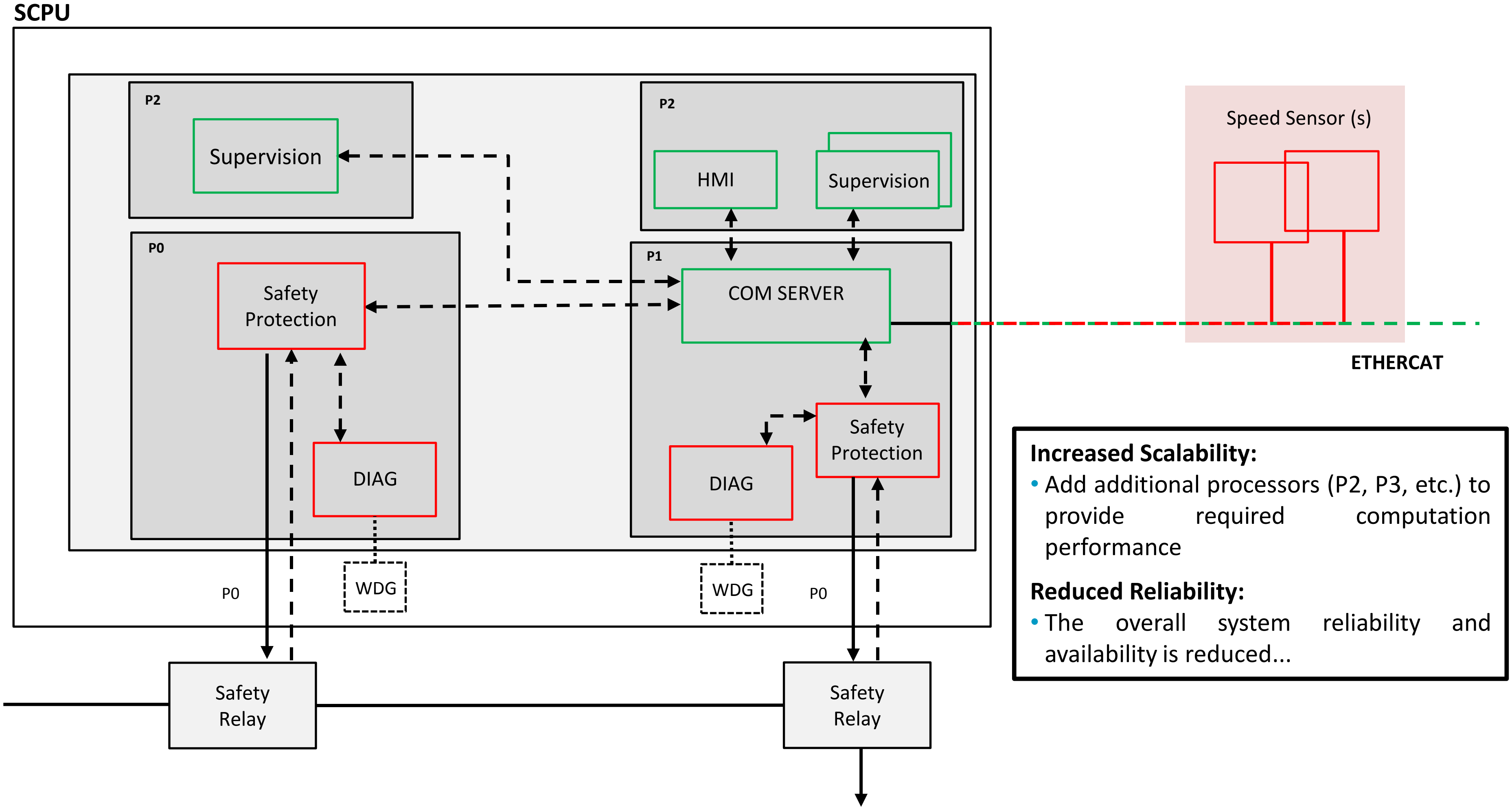


Scalability limitations:

- 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:

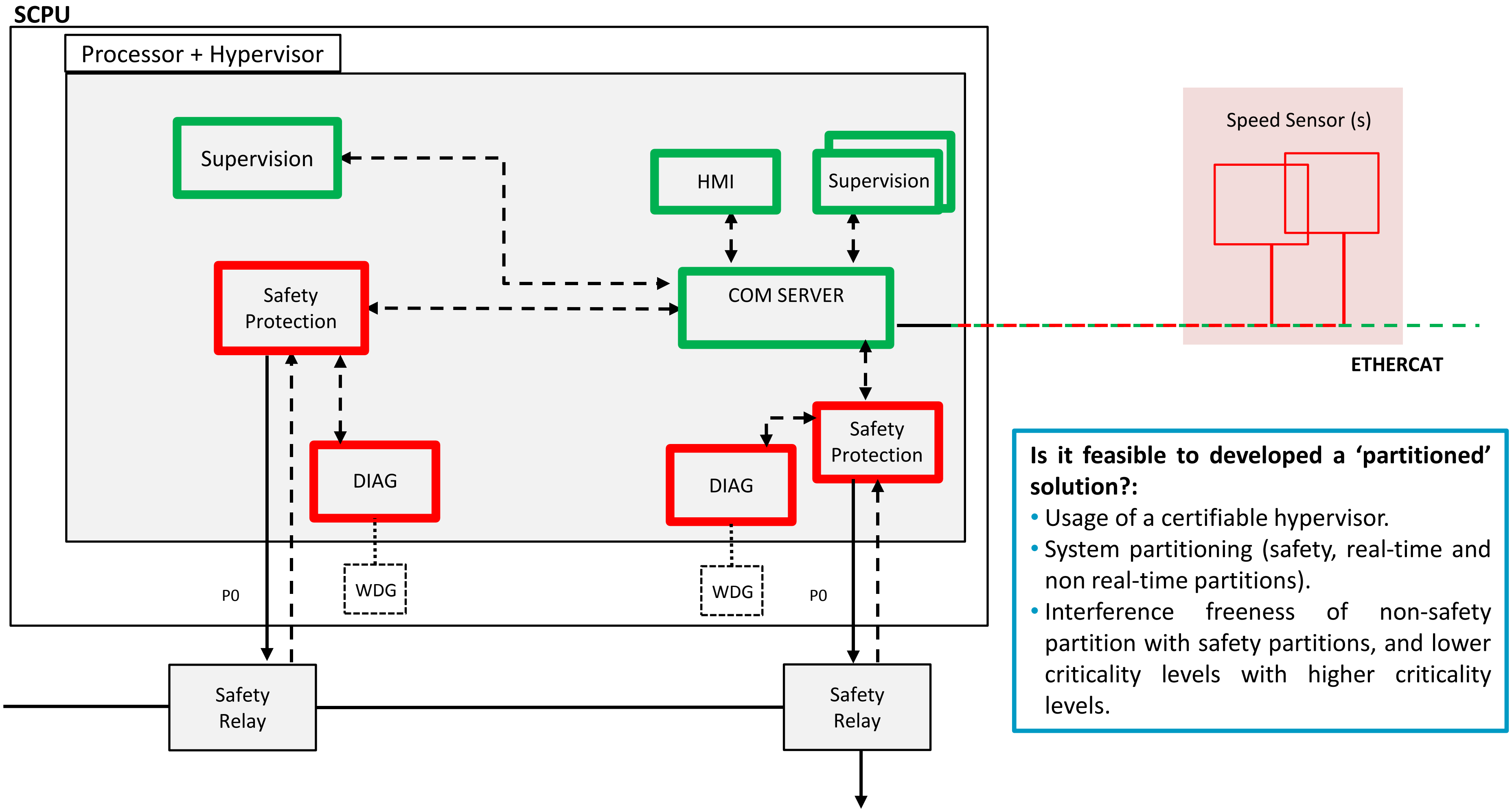
- Add additional processors (P2, P3, etc.) to provide required computation performance

Reduced Reliability:

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

Safety Concept – (B - ‘Multicore partitioning’)

PARTITIONED



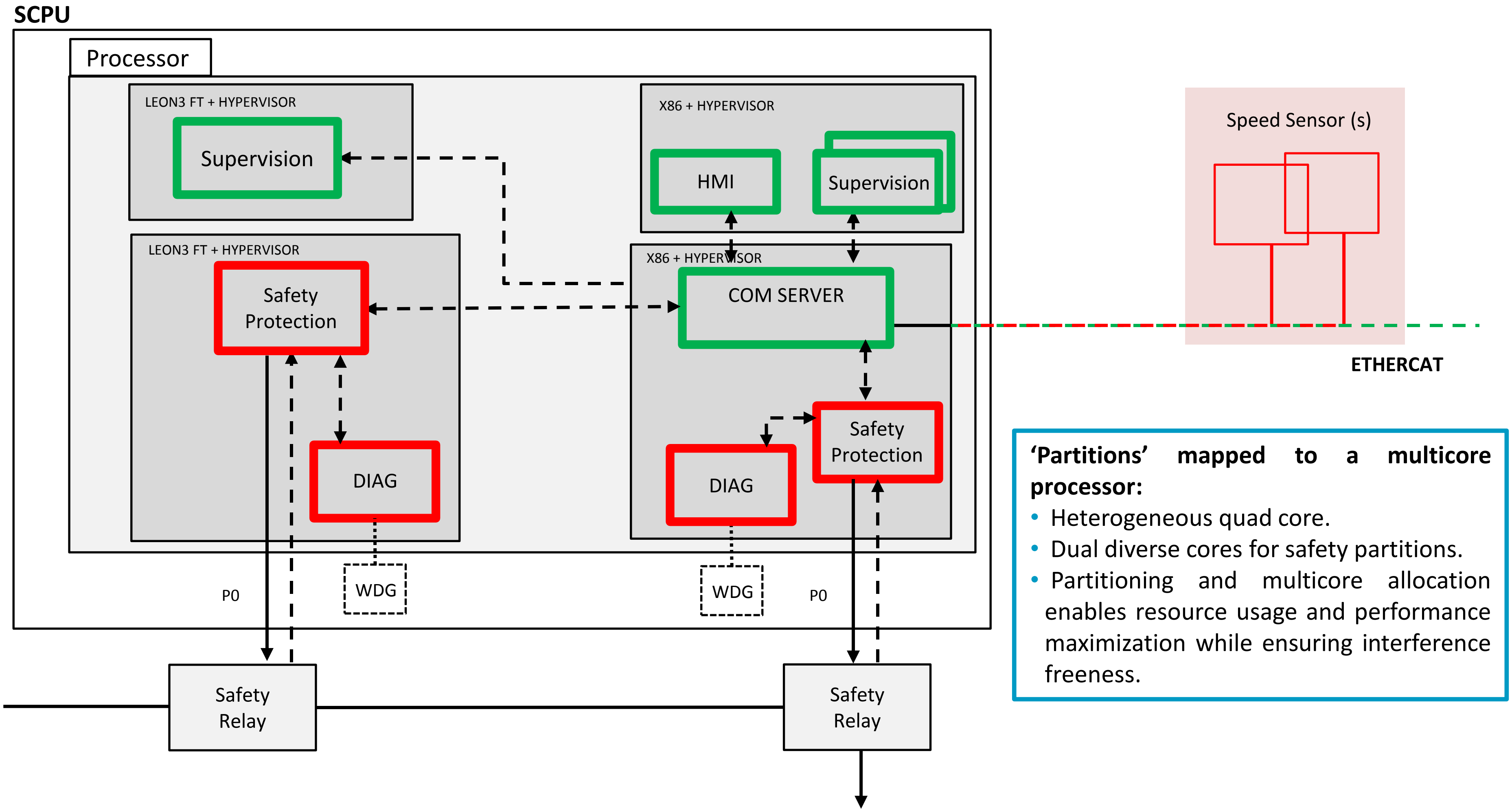
Is it feasible to developed a ‘partitioned’ solution?:

- 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')

IK4 IKERLAN Research Alliance

Safety CPU single processor quad core partitioned – 1oo2

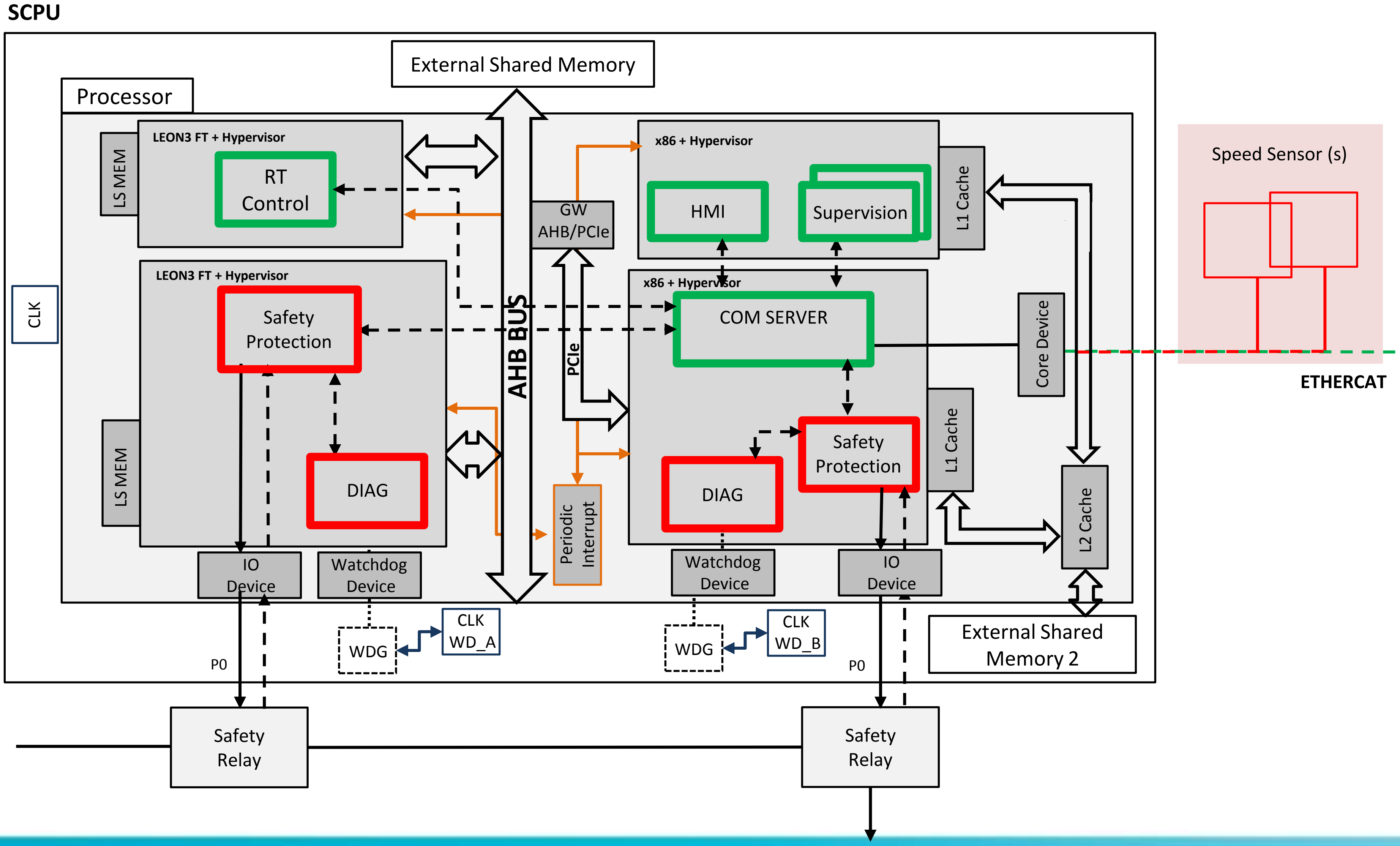


'Partitions' mapped to a multicore processor:

- 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’)

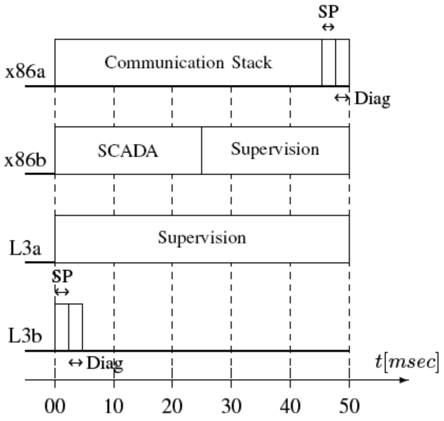
Safety CPU single processor quad core partitioned – 1002



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.

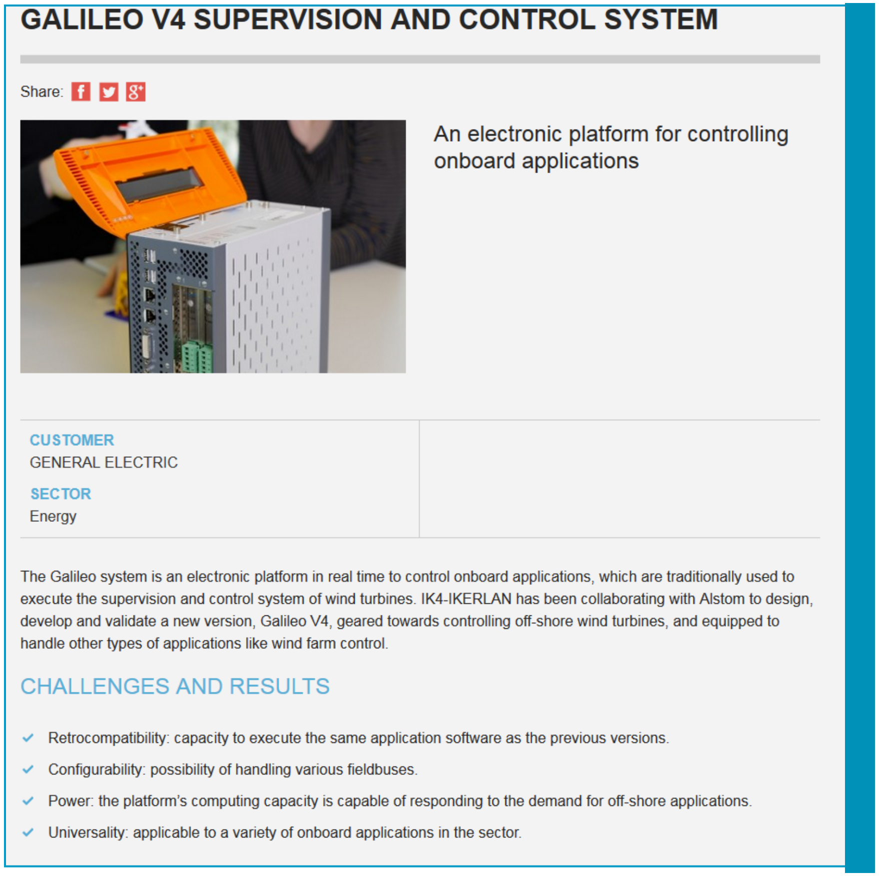


Diagnosis:

- 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.

Industrial Development – ALSTOM



GALILEO V4 SUPERVISION AND CONTROL SYSTEM

Share: f 🐦 g+

An electronic platform for controlling onboard applications

CUSTOMER
GENERAL ELECTRIC

SECTOR
Energy

The Galileo system is an electronic platform in real time to control onboard applications, which are traditionally used to execute the supervision and control system of wind turbines. IK4-IKERLAN has been collaborating with Alstom to design, develop and validate a new version, Galileo V4, geared towards controlling off-shore wind turbines, and equipped to handle other types of applications like wind farm control.

CHALLENGES AND RESULTS

- ✓ Retrocompatibility: capacity to execute the same application software as the previous versions.
- ✓ Configurability: possibility of handling various fieldbuses.
- ✓ Power: the platform's computing capacity is capable of responding to the demand for off-shore applications.
- ✓ Universality: applicable to a variety of onboard applications in the sector.

http://www.ikerlan.es/en/rd-companies/projects/galileo-v4-supervision-and-control-system

Alstom Renewables, Galileo platform for offshore wind turbines:

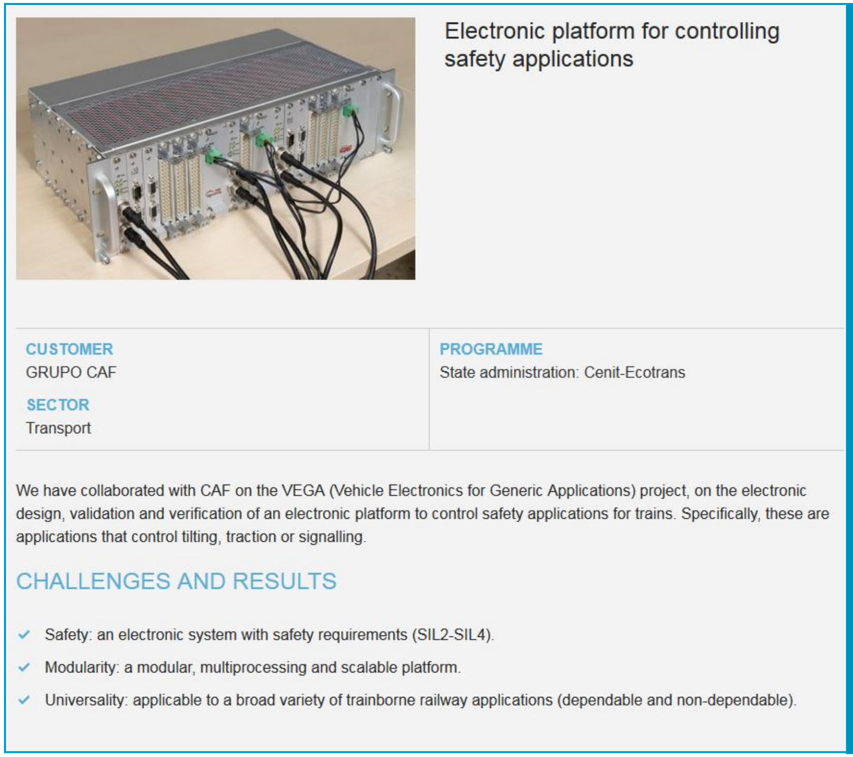
1. Multicore COTS platform (x86)
2. COTS Hypervisor
3. Combines:
   - Control partitions (real-time)
   - HMI & SCADA communication partition (QoS)
4. Multiple RTOS / GPOS
5. Comms: EtherCAT, OPC-DA, Web Services, etc.

IKERLAN

04

The railway example

Industrial projects – CAF railway



Electronic platform for controlling safety applications

CUSTOMER
GRUPO CAF

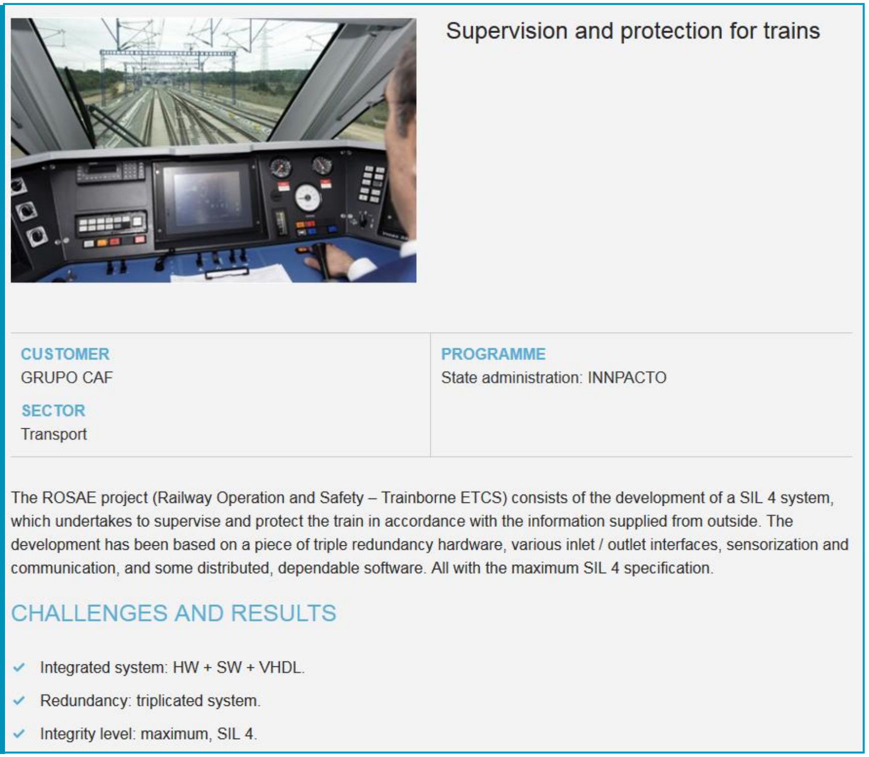
SECTOR
Transport

PROGRAMME
State administration: Cenit-Ecotrans

We have collaborated with CAF on the VEGA (Vehicle Electronics for Generic Applications) project, on the electronic design, validation and verification of an electronic platform to control safety applications for trains. Specifically, these are applications that control tilting, traction or signalling.

CHALLENGES AND RESULTS

- ✓ Safety: an electronic system with safety requirements (SIL2-SIL4).
- ✓ Modularity: a modular, multiprocessing and scalable platform.
- ✓ Universality: applicable to a broad variety of trainborne railway applications (dependable and non-dependable).



Supervision and protection for trains

CUSTOMER
GRUPO CAF

SECTOR
Transport

PROGRAMME
State administration: INNPACTO

The ROSAE project (Railway Operation and Safety – Trainborne ETCS) consists of the development of a SIL 4 system, which undertakes to supervise and protect the train in accordance with the information supplied from outside. The development has been based on a piece of triple redundancy hardware, various inlet / outlet interfaces, sensorization and communication, and some distributed, dependable software. All with the maximum SIL 4 specification.

CHALLENGES AND RESULTS

- ✓ Integrated system: HW + SW + VHDL.
- ✓ Redundancy: triplicated system.
- ✓ Integrity level: maximum, SIL 4.

http://www.ikerlan.es/en/rd-companies/projects/vega
http://www.ikerlan.es/en/rd-companies/projects/rosae

Introduction – Safety Concept

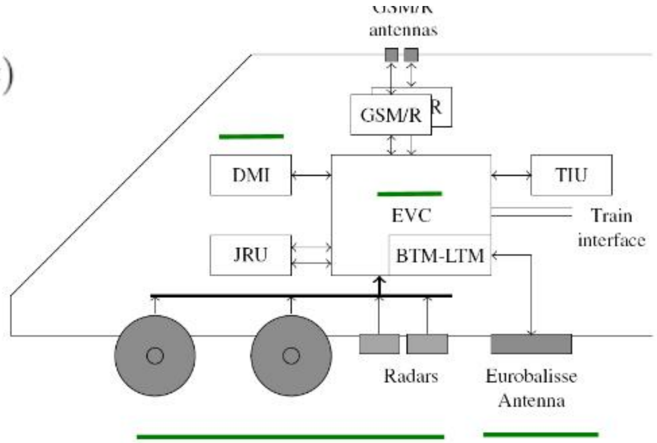
Railway Case Study composed of:

- SIL4: Simplified SIL4 ETCS railway signaling subsystem (sETCS)
- SIL0: Traction control subsystem

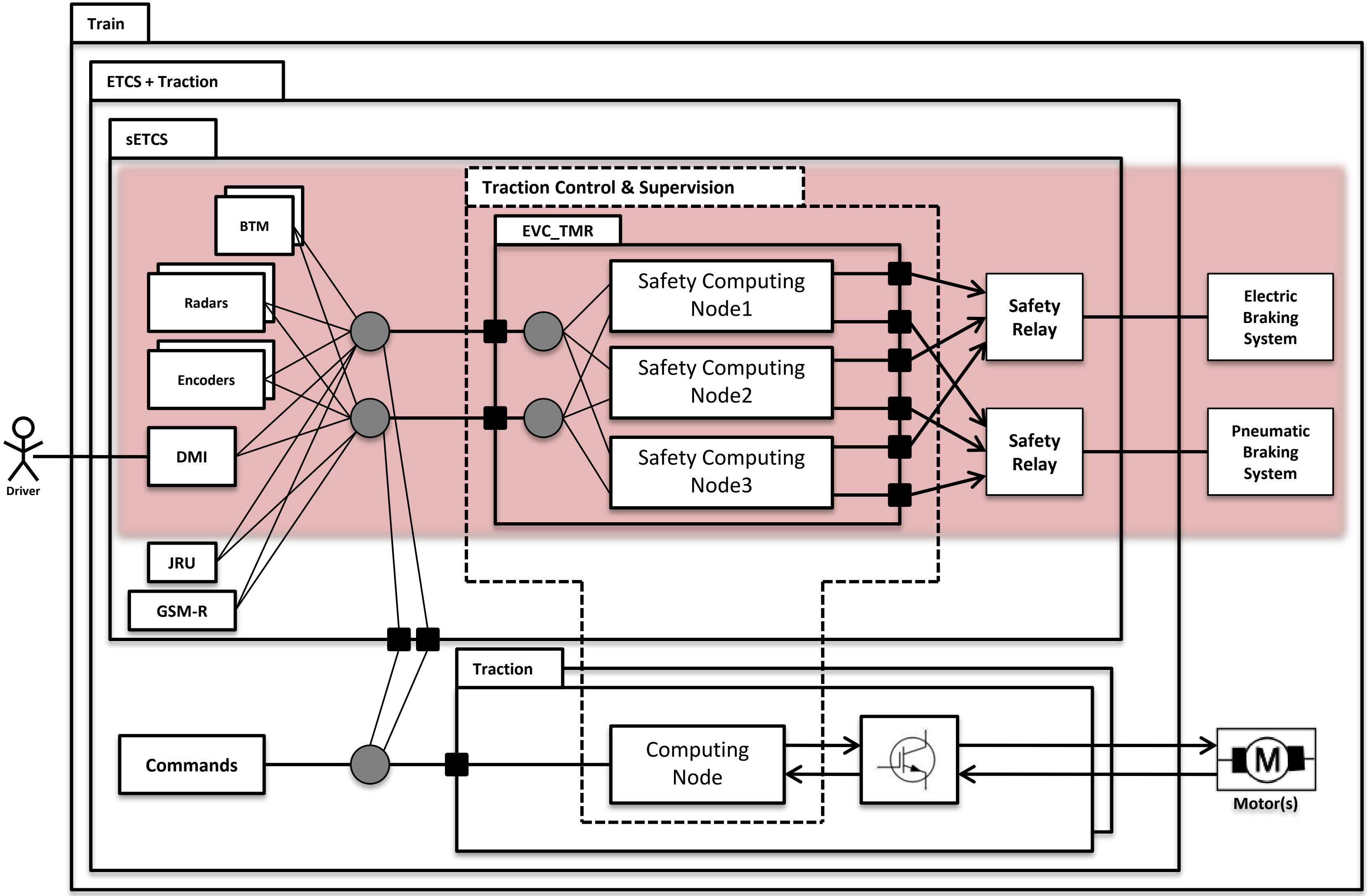
ERTMS / ETCS:

- ERTMS (European Railway Traffic Management System) is an European union backed initiative for the definition of a unique train signaling standard.
- ETCS (European Train Control System) is the on-board automatic train protection, safety-critical embedded system, that protects the train by supervising the traveled distance and speed, activating the emergency brake if authorized values are exceeded.

$$\forall t, |s_m(t) - s(t)| \leq 5m + (5/100) \cdot s(t)$$



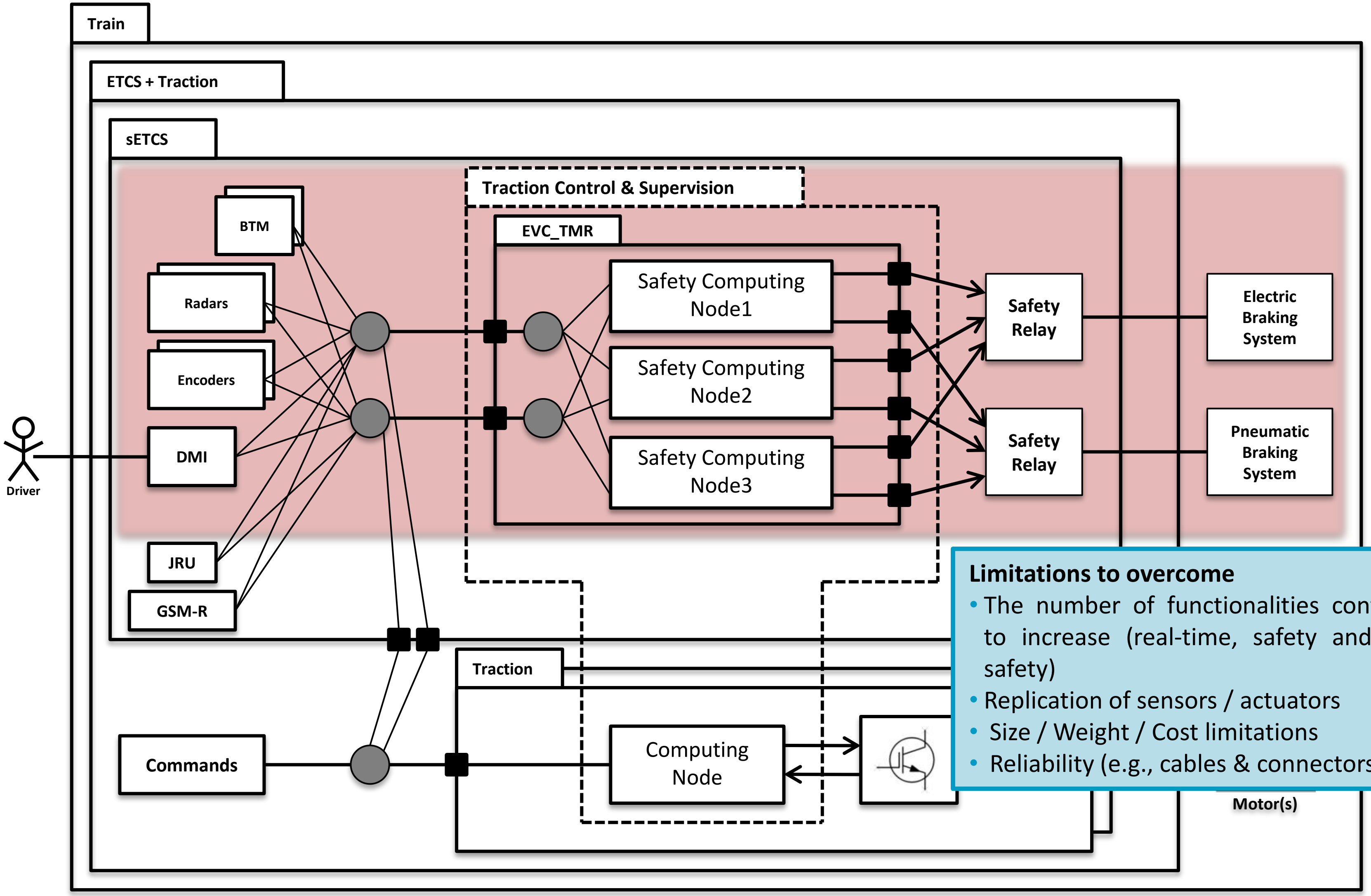
Safety Concept – System Level - Traditional



Safety Concept – System Level - Traditional

Architecture	European Vital Computer (EVC) is SIL4, Composite Fail Safety: 1. Triple Modular Redundancy: IEC-61508 → HFT=1 2. Platform compliant item: Each node IEC-61508 → SIL3 (composed of HW and associated platform SW) a) In TMR can achieve: EN-50128/EN-50129 → SIL4 b) The platform provides a RTOS or equivalent to ensure interference freeness (temporal and spatial) among SW tasks 3. Safe Communication Protocol: 4. External Interface: a) Safety related I/Os b) Other safety & black channels
Safe state	De-Energization of safety digital output connected to external safety-relays a) The default state during *no-power* and *startup* b) Reached whenever the system, HW or SW diagnosis detects an error
Diagnosis techniques	The EVC implements diagnosis techniques according to EN-5012x and IEC-61508 (Up to SIL4 level with HFT = 2 and DC > 99 % in addition to compliance with EN-50129) 1. Each node: SIL3 (IEC-61508) compliant item with HFT = 0 and DC > 99 % a) Diagnosis for memories, power supply, temporal constraints, I/Os, etc. 2. Safety Related Software techniques 3. Monitoring of external safety relays 4. Safe product development considering safety manuals of all COTS compliant items

Safety Concept – System Level - Traditional



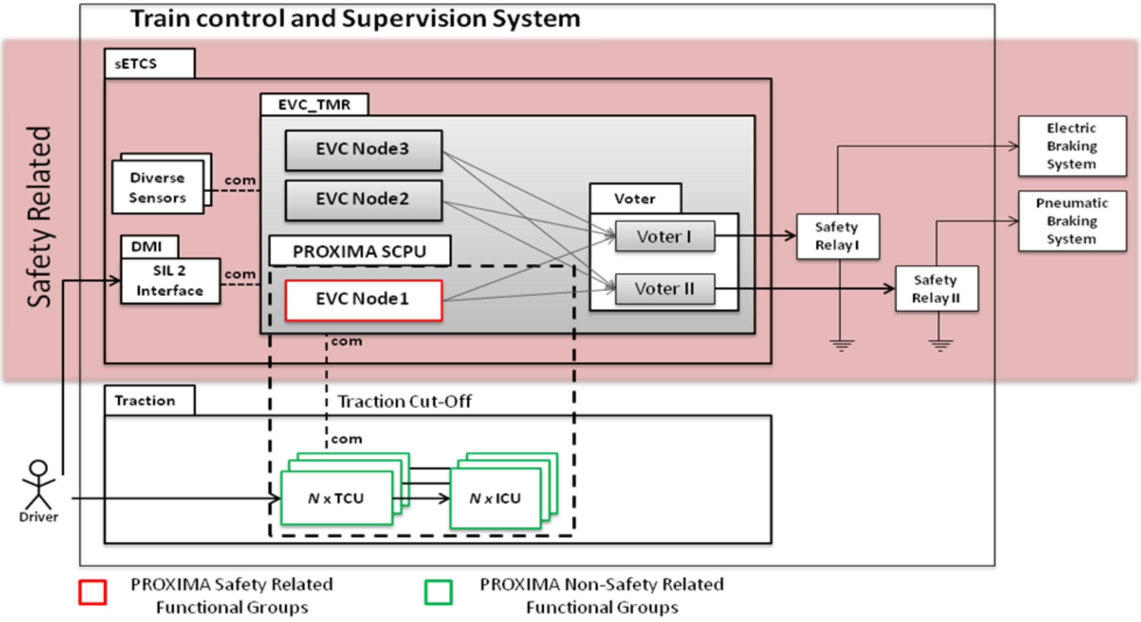
Limitations to overcome

- The number of functionalities continues to increase (real-time, safety and non-safety)
- Replication of sensors / actuators
- Size / Weight / Cost limitations
- Reliability (e.g., cables & connectors)

SC2-Integrated System Level Safety Concept

Mixed-Criticality Integrated Approach: Non-Safety related traction computing nodes integrated with one EVC node.

- **Multicore Approach** (with virtualization): each computing node becomes a software partition and off-chip communication becomes on-chip communication. Overcomes main limitations.



Mixed-Criticality Node Level Safety Concept

Fault Hypothesis

- SIL4 software (EN-50128) and methodology (EN-5012x)
- Safety CPU (SCPU) SIL3 IEC-61508 compliant item
  - The SCPU forms a single Fault-Containment Region
- The hypervisor:
  - Provides interference freeness (temporal and spatial isolation)
  - Is certifiable (compliant item)
  - Fails in arbitrary failure mode
- A partition can fail in arbitrary failure mode both in the temporal as well as in the spatial domain

Mixed-Criticality Node Level Safety Concept

Top-Down Approach:

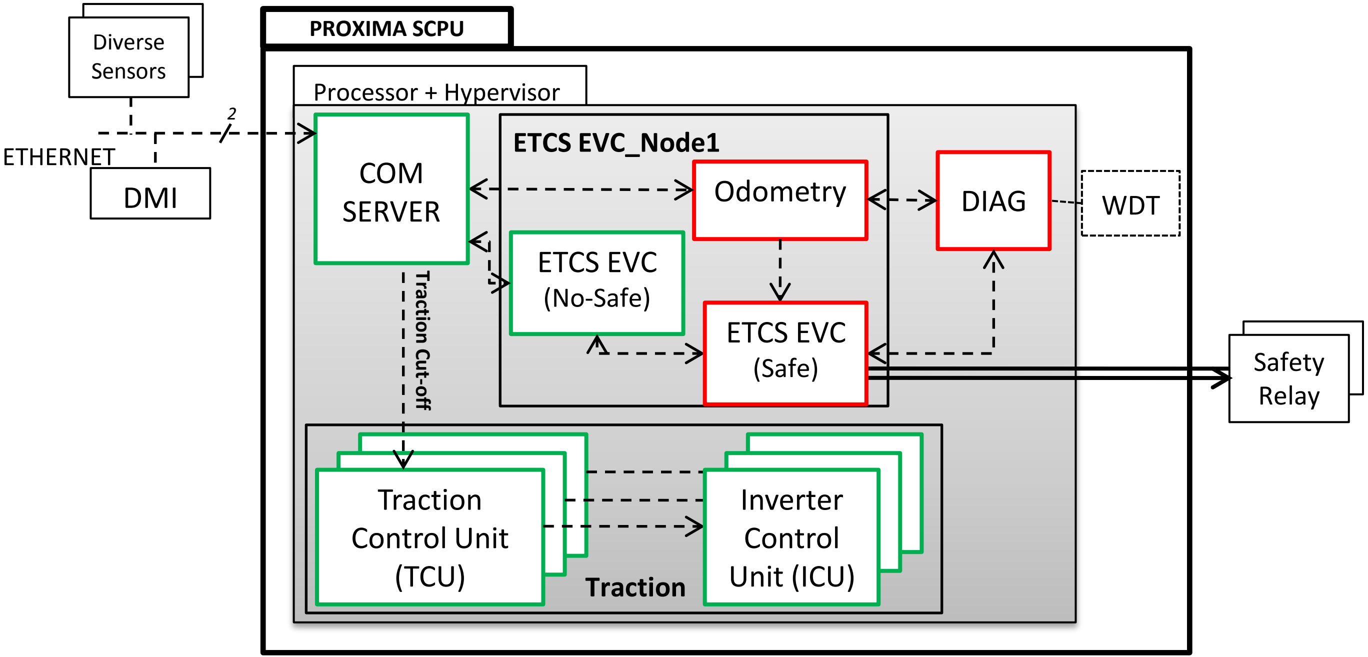
1. **Partitioned Solution on Top of a virtualized processor with Hypervisor.**

2. **Partitioned solution allocated to a multicore processor.**

3. **Partitioned solution allocated to a multicore processor with all Hardware resources of interest.**

Mixed-Criticality Node (SC2.1/SC2.2 (1/3))

Partitioned Solution on Top of a virtualized processor with Hypervisor



🟥 PROXIMA Safety Related Partitions

🟩 PROXIMA Non Safety Related Partitions

Is it Feasible to develop a Partitioned Solution?

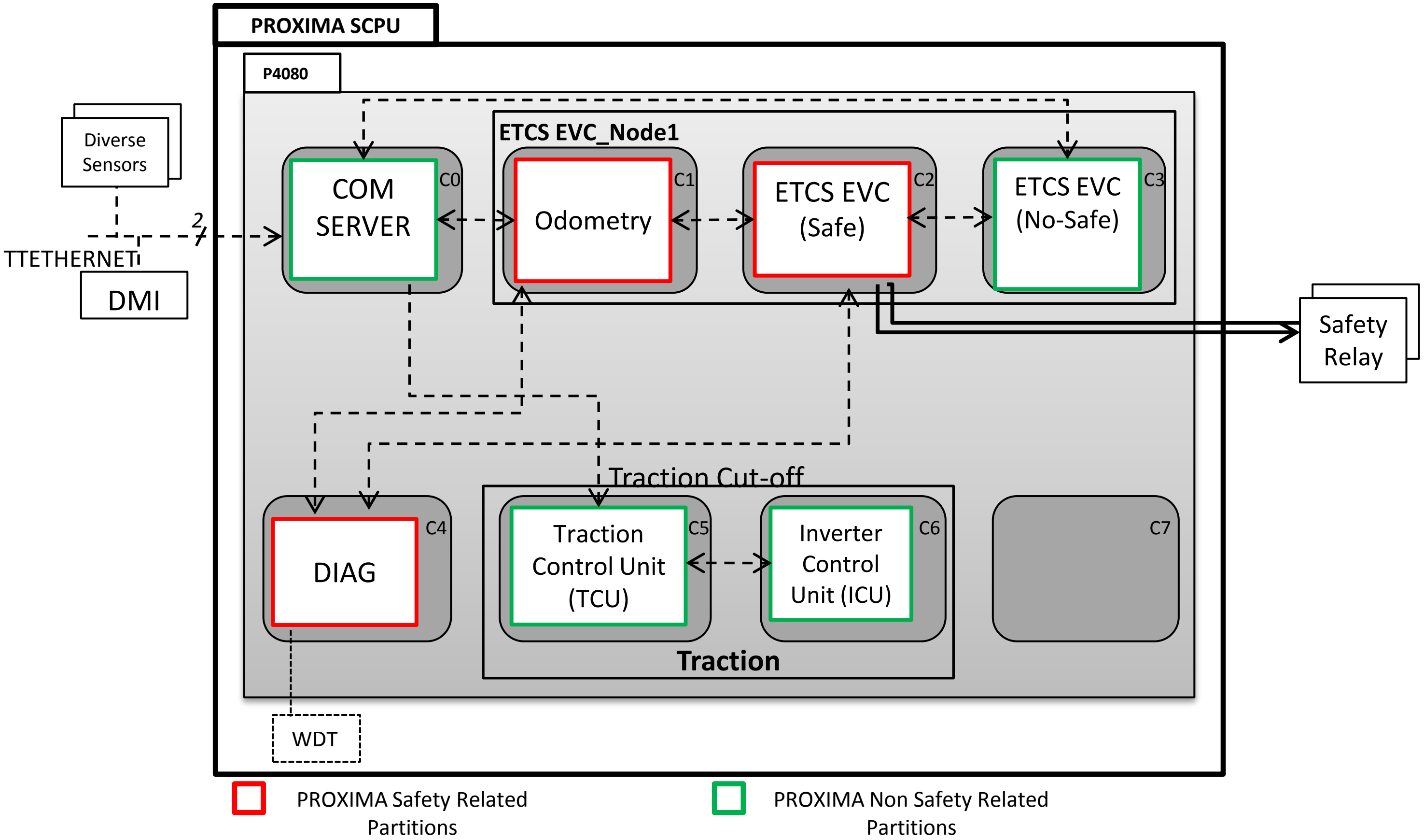
Certifiable Hypervisor

System partitioning (safety / real-time / non-real time partitions)

Interference freeness between safety and non-safety partitions

SC2.2-Mixed-Criticality Node: COTS (2/3)

Partitioned solution allocated to P4080 multicore processor



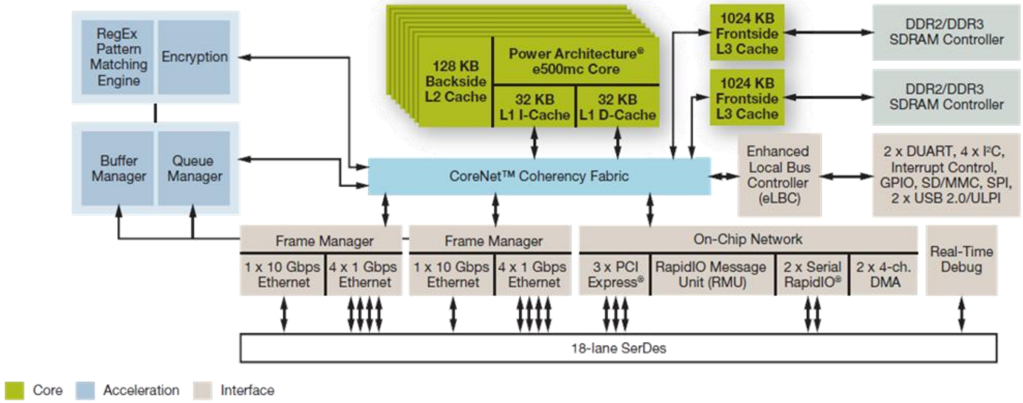
'Partitions' mapped to a multicore processor:

Partitioning and multicore allocation enables resource usage and performance maximization while ensuring interference freeness.

SC2.2-Mixed-Criticality Node: COTS (3/3)

Partitioned solution allocated to P4080 multicore processor with all hardware resources of relevance

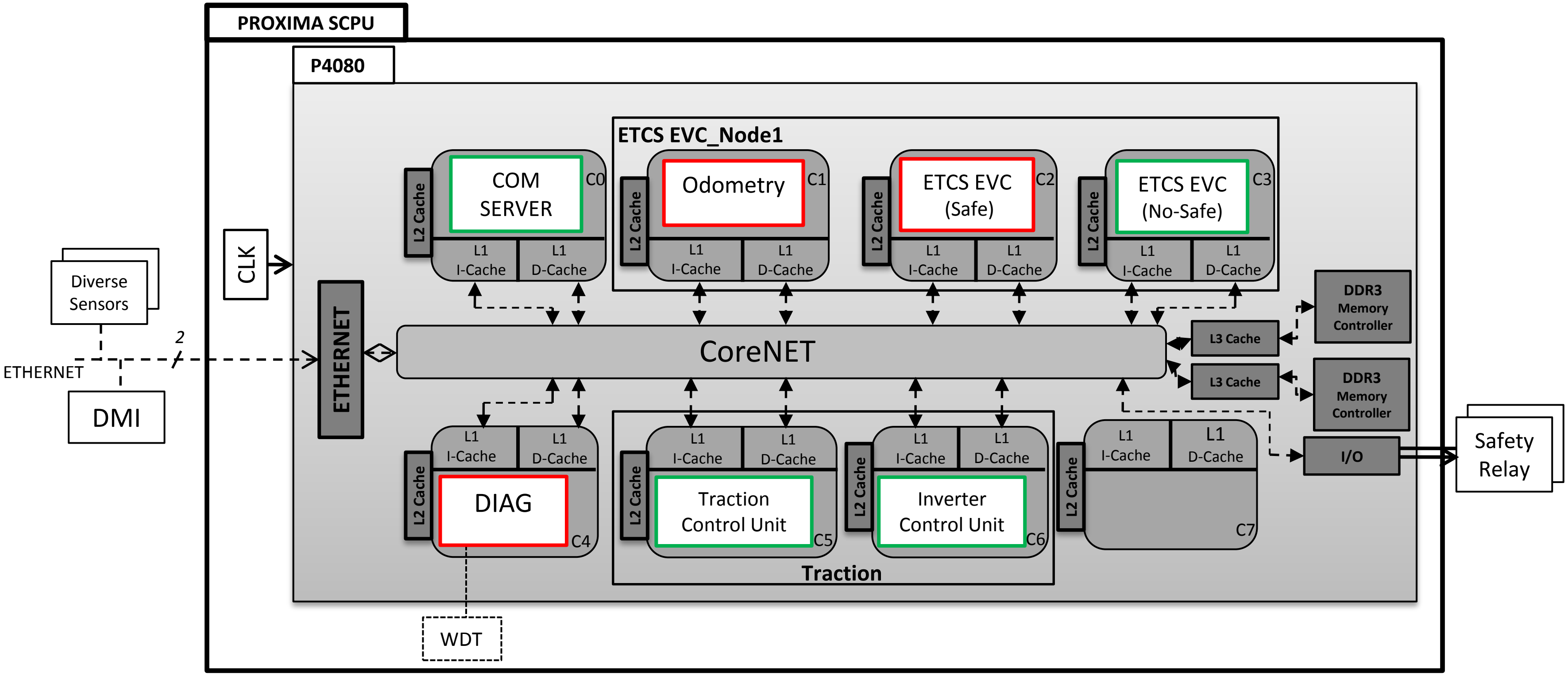
- SCPU:
  - Independent watchdog controller
  - Additional safety techniques (IEC-61508 SIL3, HFT = 0, DC>=99%)
- Processor:
  - P4080 platform: 8 Power architecture em500c cores
- Hypervisor:
  - Compliant item
- System Configuration:
  - Static
  - Designed with qualified tools



RegEx Pattern Matching Engine
Encryption
Buffer Manager
Queue Manager
128 KB Backside L2 Cache
Power Architecture® e500mc Core
32 KB L1 I-Cache
32 KB L1 D-Cache
1024 KB Frontside L3 Cache
1024 KB Frontside L3 Cache
DDR2/DDR3 SDRAM Controller
DDR2/DDR3 SDRAM Controller
CoreNet™ Coherency Fabric
Enhanced Local Bus Controller (eLBC)
2 x DUART, 4 x I²C, Interrupt Control, GPIO, SD/MMC, SPI, 2 x USB 2.0/ULPI
Frame Manager
1 x 10 Gbps Ethernet
4 x 1 Gbps Ethernet
Frame Manager
1 x 10 Gbps Ethernet
4 x 1 Gbps Ethernet
On-Chip Network
3 x PCI Express®
RapidIO Message Unit (RMU)
2 x Serial RapidIO®
2 x 4-ch. DMA
Real-Time Debug
18-lane SerDes
🟩 Core
🟦 Acceleration
▨ Interface

SC2.2-Mixed-Criticality Node: COTS (3/3)

Partitioned solution allocated to P4080 multicore processor with all hardware resources of relevance



🟥 PROXIMA Safety Related Partitions

🟩 PROXIMA Non Safety Related Partitions

SC2.2-Mixed-Criticality Node: COTS - PTA

Commercial off-the-shelf processor

- Access to the information of hardware temporal response
- PTA compliancy through software (e.g., Software Randomization)
- PTA as a sound method to determine WCET with improved guaranteed performance
  - Integration tests, measurements, fault injection etc. to check coherency of results.

IKERLAN

05

The industrial protection example

Industrial Development - Xilinx

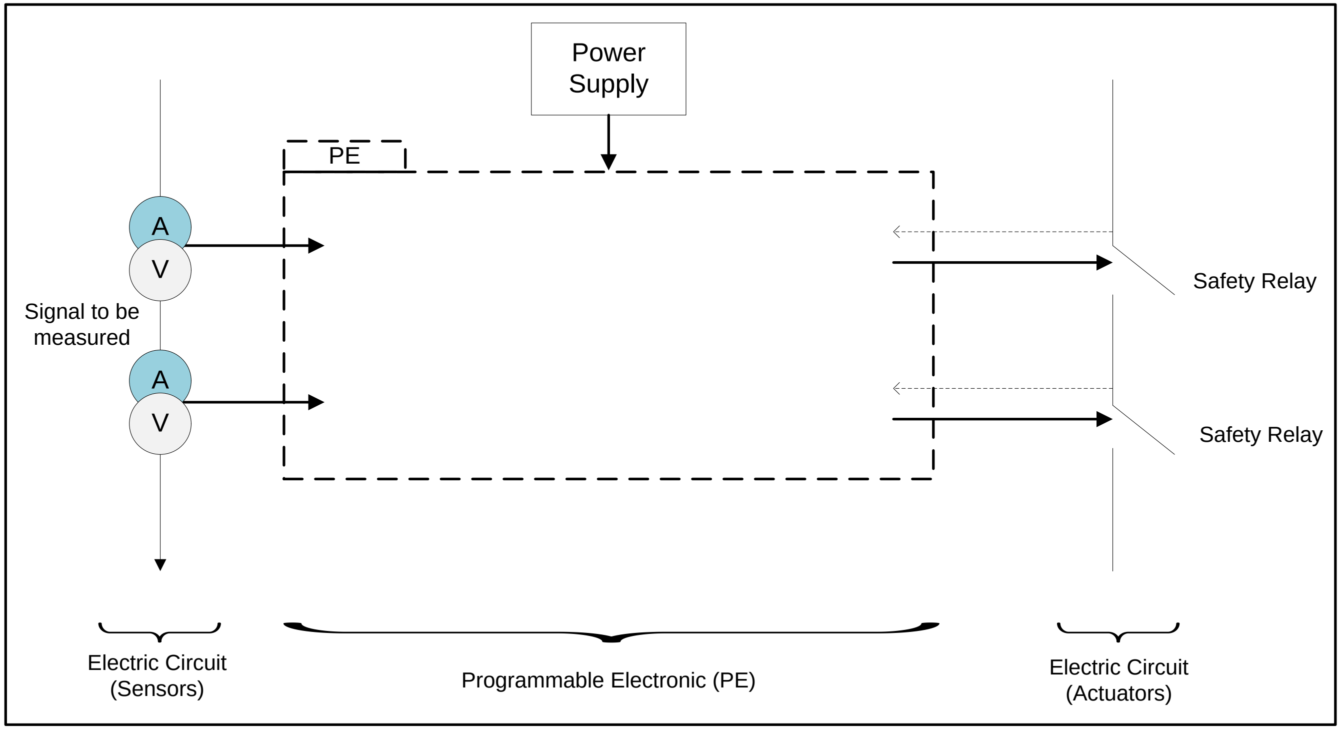
IK4 IKERLAN
Research Alliance

Safety Reference Design (SRD)

1. Power Monitor Protection (PMP) safety function IEC-61508 SIL3
2. Zynq-7000 multicore device
3. Multiple architectural variants

Safety Concept assessment by certification authority (in progress)

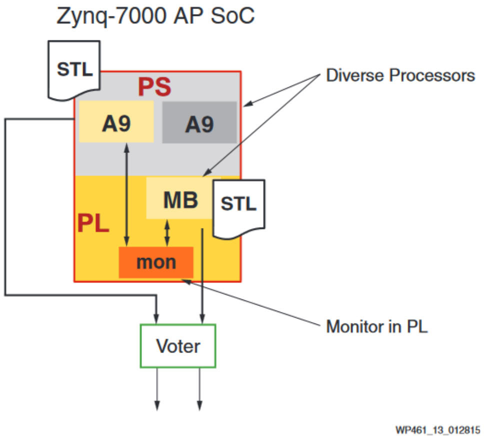
More details in SPS IPC Drives (Germany, November)

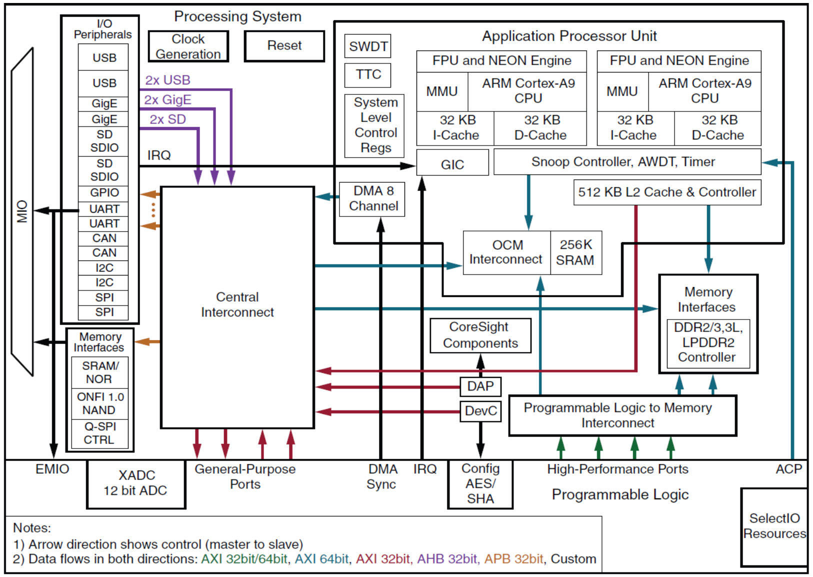

Power Supply
PE
A
V
Signal to be measured
A
V
Safety Relay
Safety Relay
Electric Circuit (Sensors)
Programmable Electronic (PE)
Electric Circuit (Actuators)

Xilinx – Safety Reference Design (SRD)

IK4 IKERLAN Research Alliance

- STL = Software Test Library
- MB = MicroBlaze processor
- A9 = ARM Cortex A9
- MON = Diagnostic Monitor





Diversity:

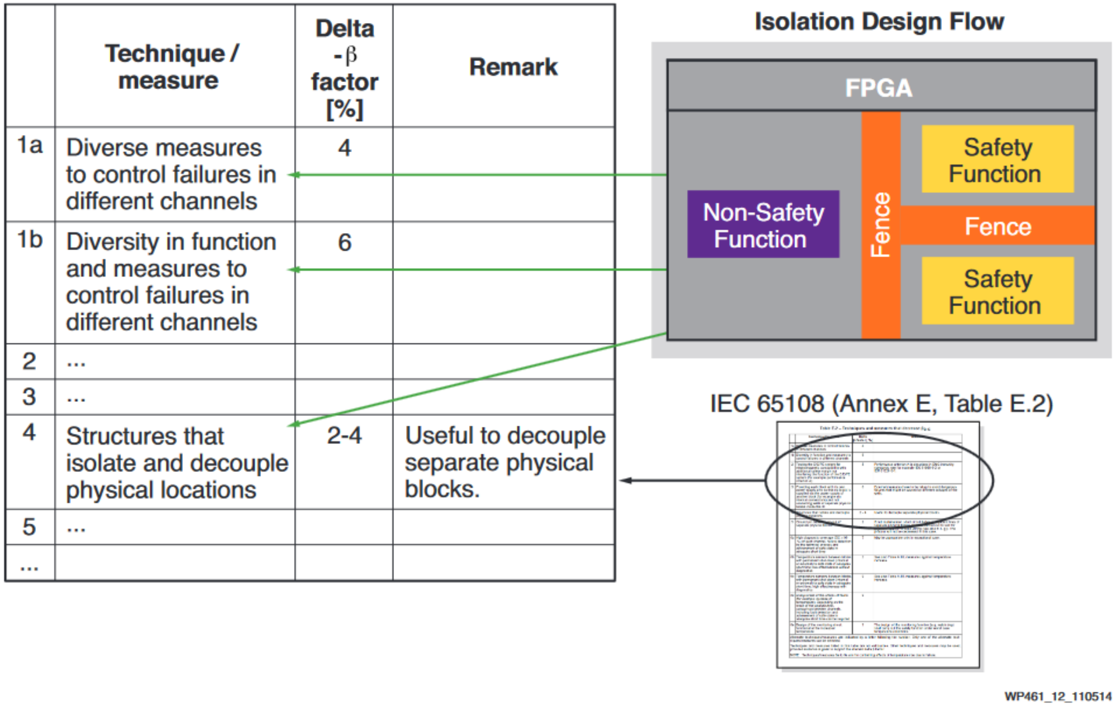
1. HW: PS vs PL, ARM9 vs MicroBlaze
2. Compilers & Tools

Qualified safety development flow and tools

TrustZone to ensure time & space independence between safety and non-safety applications running ARM9 cores

http://www.xilinx.com/support/documentation/white_papers/wp461-functional-safety.pdf
https://www.xilinx.com/publications/prod_mktg/safety-guidelines.pdf
http://www.xilinx.com/support/documentation/user_guides/ug1019-zynq-trustzone.pdf

On-chip redundancy with Isolation Design Flow (IDF)



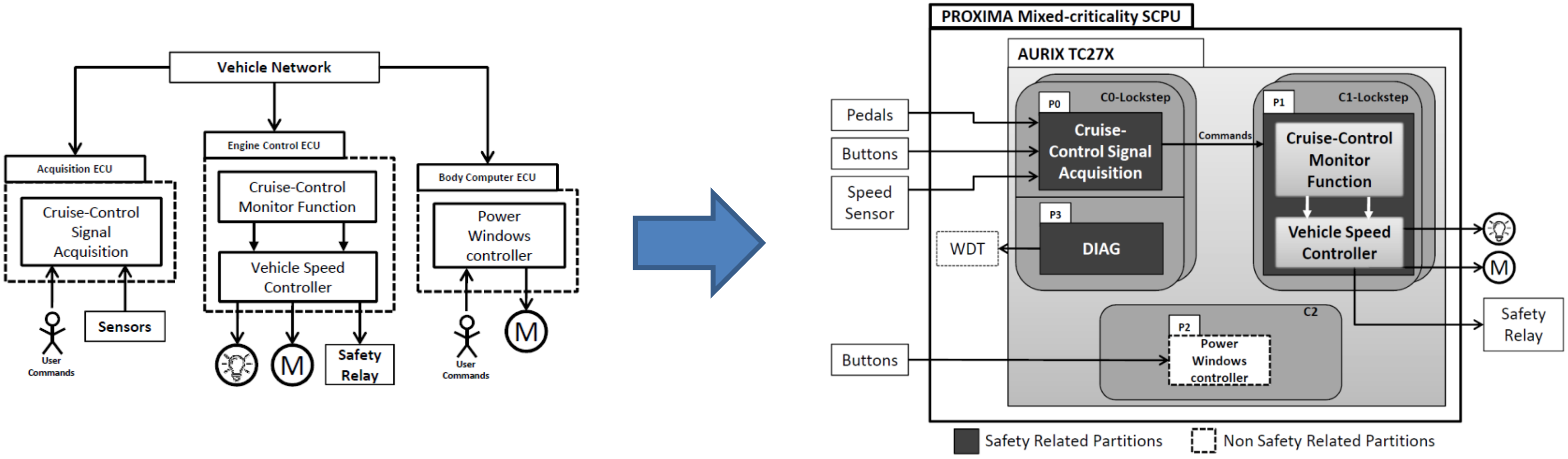
	Technique / measure	Delta -β factor [%]	Remark
1a	Diverse measures to control failures in different channels	4	
1b	Diversity in function and measures to control failures in different channels	6	
2	...		
3	...		
4	Structures that isolate and decouple physical locations	2-4	Useful to decouple separate physical blocks.
5	...		
...			

IKERLAN

06

The automotive example

Safety Concept – Cruise Control



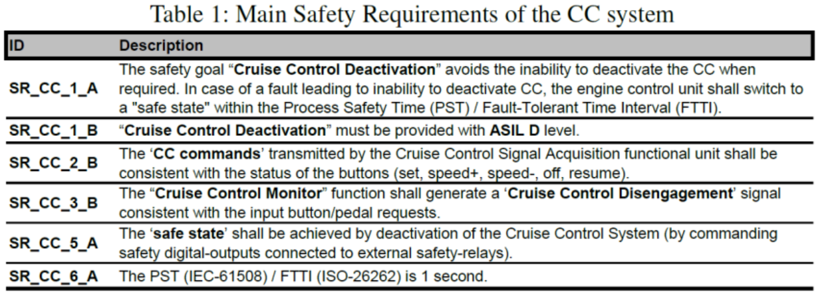
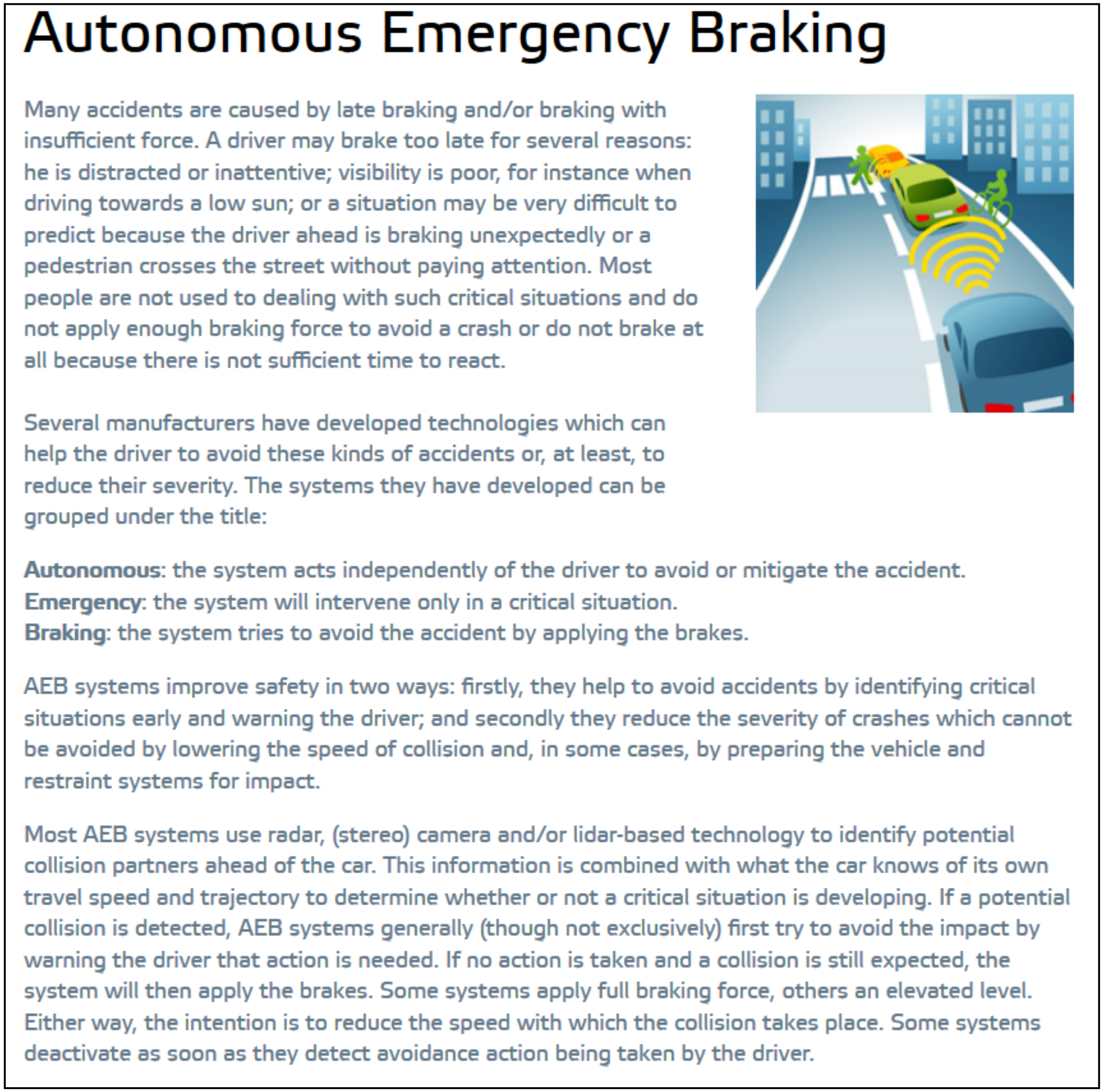


Table 1: Main Safety Requirements of the CC system

ID	Description
SR_CC_1_A	The safety goal "**Cruise Control Deactivation**" avoids the inability to deactivate the CC when required. In case of a fault leading to inability to deactivate CC, the engine control unit shall switch to a "safe state" within the Process Safety Time (PST) / Fault-Tolerant Time Interval (FTTI).
SR_CC_1_B	"**Cruise Control Deactivation**" must be provided with **ASIL D** level.
SR_CC_2_B	The '**CC commands**' transmitted by the Cruise Control Signal Acquisition functional unit shall be consistent with the status of the buttons (set, speed+, speed-, off, resume).
SR_CC_3_B	The "**Cruise Control Monitor**" function shall generate a '**Cruise Control Disengagement**' signal consistent with the input button/pedal requests.
SR_CC_5_A	The '**safe state**' shall be achieved by deactivation of the Cruise Control System (by commanding safety digital-outputs connected to external safety-relays).
SR_CC_6_A	The PST (IEC-61508) / FTTI (ISO-26262) is 1 second.

[1] Agirre, I., et al. (2016). "Automotive Safety Concept Definition for Mixed-Criticality Integration on a COTS Multicore", Computer Safety, Reliability, and Security, Volume 9923, Series Lecture Notes in Computer Science, pp 273-285.

Industrial project – Autonomous Emergency Braking (AEB)



Autonomous Emergency Braking

Many accidents are caused by late braking and/or braking with insufficient force. A driver may brake too late for several reasons: he is distracted or inattentive; visibility is poor, for instance when driving towards a low sun; or a situation may be very difficult to predict because the driver ahead is braking unexpectedly or a pedestrian crosses the street without paying attention. Most people are not used to dealing with such critical situations and do not apply enough braking force to avoid a crash or do not brake at all because there is not sufficient time to react.

Several manufacturers have developed technologies which can help the driver to avoid these kinds of accidents or, at least, to reduce their severity. The systems they have developed can be grouped under the title:

Autonomous: the system acts independently of the driver to avoid or mitigate the accident.
Emergency: the system will intervene only in a critical situation.
Braking: the system tries to avoid the accident by applying the brakes.

AEB systems improve safety in two ways: firstly, they help to avoid accidents by identifying critical situations early and warning the driver; and secondly they reduce the severity of crashes which cannot be avoided by lowering the speed of collision and, in some cases, by preparing the vehicle and restraint systems for impact.

Most AEB systems use radar, (stereo) camera and/or lidar-based technology to identify potential collision partners ahead of the car. This information is combined with what the car knows of its own travel speed and trajectory to determine whether or not a critical situation is developing. If a potential collision is detected, AEB systems generally (though not exclusively) first try to avoid the impact by warning the driver that action is needed. If no action is taken and a collision is still expected, the system will then apply the brakes. Some systems apply full braking force, others an elevated level. Either way, the intention is to reduce the speed with which the collision takes place. Some systems deactivate as soon as they detect avoidance action being taken by the driver.

http://www.euroncap.com/en/vehicle-safety/the-rewards-explained/autonomous-emergency-braking/

IKERLAN

07

Conclusions and lessons learnt

Conclusions and lessons learnt

It is feasible to achieve SIL3 IEC-61508 / Pld ISO-13849 / SIL4 EN-5012x / ASILC ISO-26262 with COTS multicore, hypervisor partitioning and current safety standard versions. (Not easy, but feasible)

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)
- Industrial protection, IEC-61508 SIL3
- Automotive, ASILC ISO-26262