[2] ALSTOM

[1] IK4 IKERLAN
Research Alliance

A safety concept for a wind power mixed-criticality embedded system based on multicore partitioning

Jon Perez[1], David Gonzalez[1] (dgonzalez@ikerlan.es), Salvador Trujillo[1], Jose Miguel Gárate[2], Ton Trapman[2]

1st International Workshop on Mixed Criticality Systems

Vancouver, Dec. 3th, 2013

Contribution of the paper

- This paper presents a **safety certification strategy for IEC-61508** compliant industrial mixed-criticality systems based on **multicore and virtualization**.

- The **safety concept** of a wind power case-study is currently **under review by a certification body**.

Definitions and problem statement

- **Criticality level of an application** is a classification of how severe a deviation of the intended behavior is.
- **Criticality level of a system** is defined as the highest criticality of the jobs executed within it.
- Today's **embedded systems** typically integrate functionalities with different criticality levels.
- Without appropriate preconditions, the **integration of mixed-criticality subsystems** can lead to a significant and potentially unacceptable increase of certification efforts.

Towards mixed-criticality systems

- **Federated architectures** have limitations:
  - **Complexity.**
  - **Scalability.**
  - Number of subsystems, connectors and wires impacts on overall **reliability**.
  - **Cost-size-weight**.

- **Mixed-criticality systems** overcome these limitations.

- **Safety certification** according to industrial standards **becomes a challenge.**

IEC-61508 and derived standards

- IEC-61508 is an international standard for **electrical, electronic and programmable electronic safety related systems**.
- IEC-61508 is a **generic safety standard** from which different domain specific standards have been **derived for industrial and transportation** domains.
- It defines **Safety Integrity Level** (SIL) 1 .. 4
- It is intended for **fail-safe** systems.
  - **Fail-safe: there is a safe-state**
  - Fail-operational: there is no safe-sate

Multicore and virtualization

- **Multicore and virtualization** technology can support the development of mixed-criticality systems.
- **Partitions** provide functional separation of the applications and fault containment.
- The **challenge** is to provide **sufficient evidence of isolation**, separation and independence among safety and non-safety related functions.
- **IEC-61508** safety standard does not directly support nor restrict the certification of mixed-criticality systems, but:
  - Sufficient independence must be shown.
  - Otherwise, all integrated functions will need to meet the highest integrity level.

Temporal and spatial isolation

- Sufficient independence implies **temporal and spatial isolation**:
  - **The temporal isolation** is achieved if the duration of every single action performed by applications in one partition is independent from actions performed by all other partitions.
  - **Spatial isolation** (inter partition) must prevent all partitions from accessing memory or interfaces that are not in their a-priori known scope.
- If temporal and spatial isolation is achieved, **subsystems with different levels of criticality can be placed in different partitions** and can be verified and validated in isolation.

Safety certification strategy

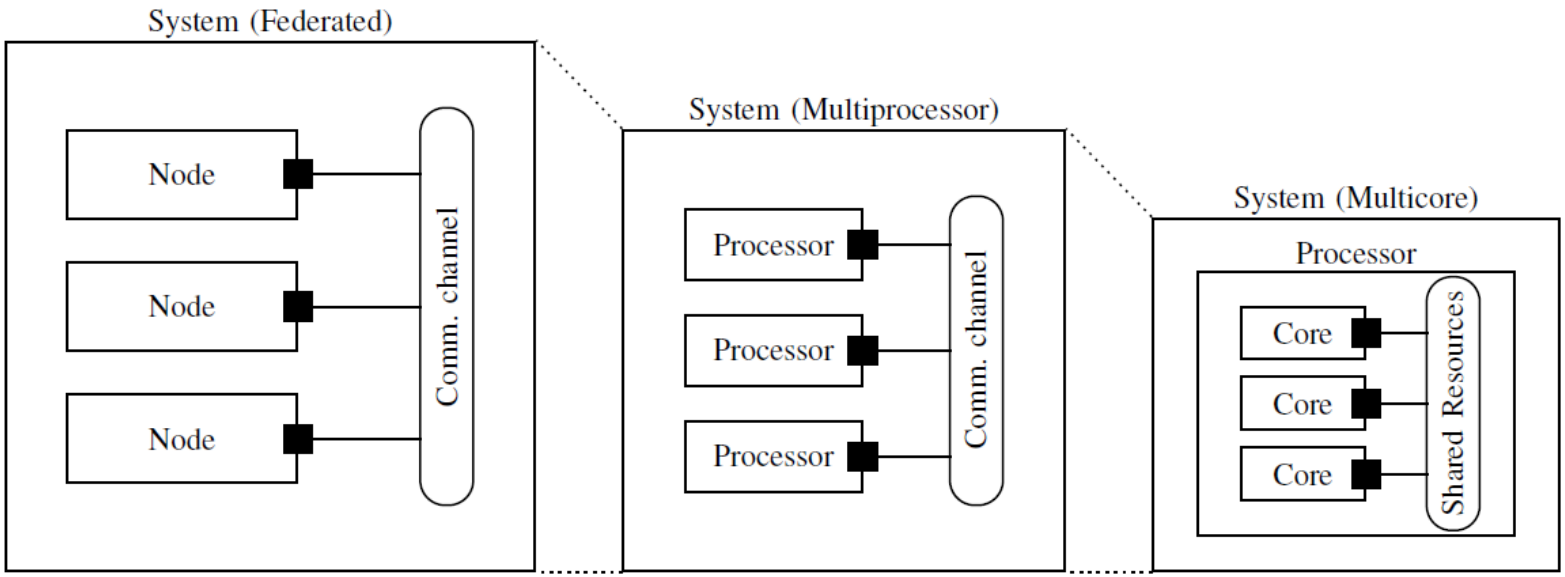
- IEC-61508 and **fail-safe** systems:
  - **Diagnosis techniques** must be used to detect temporal isolation violations.
  - Thus, the **lack of complete temporal isolation** does not compromise safety, but availability.
- **Hypervisor and platform** as a compliant item:
  - Startup, configuration and initialization
  - Virtualization of resources
  - Isolation, diagnosis and integrity
  - Communication and synchronization
- **Static cyclic scheduling** of partitions with guaranteed timeslots defined at design time.
- **Diagnosis strategy**

Wind power case study

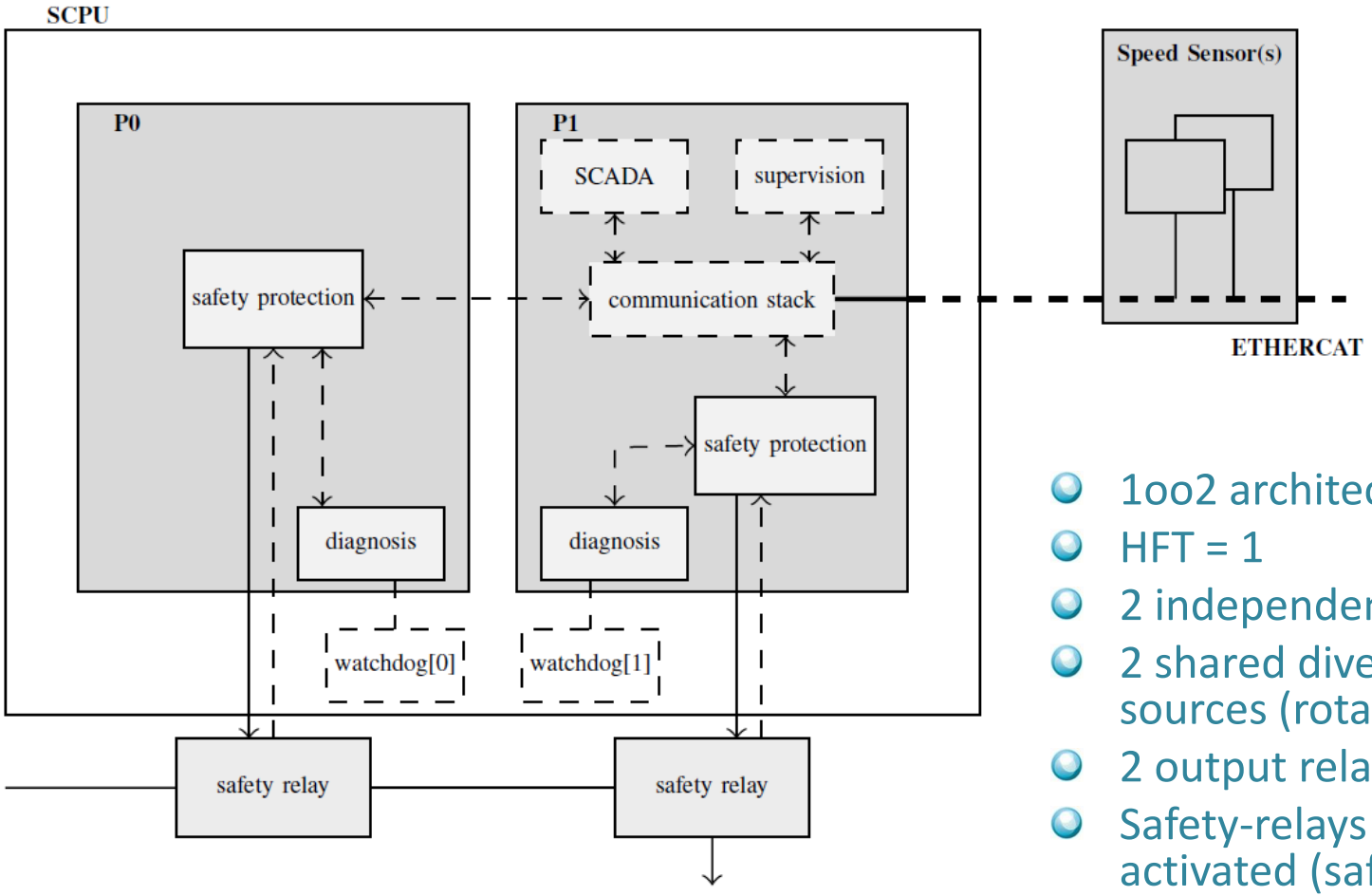
- Wind turbine supervision and control system provides **three major functionalities**:
  - **Supervision**: wind turbine real-time control and supervision.
  - **Communications and HMI**: non real-time Human Machine Interface (HMI) and communication with SCADA system.
  - **Protection**: safety functions to ensure that the design limits of the wind turbine are not exceeded (e.g. overspeed, ISO-13849 PLd).
- These functionalities are currently deployed in **different platforms.**

Safety Concept in two steps

- **Two transformations**
  - From a **federated** architecture to **multiprocessor**
  - From **multiprocessor** to **multicore**



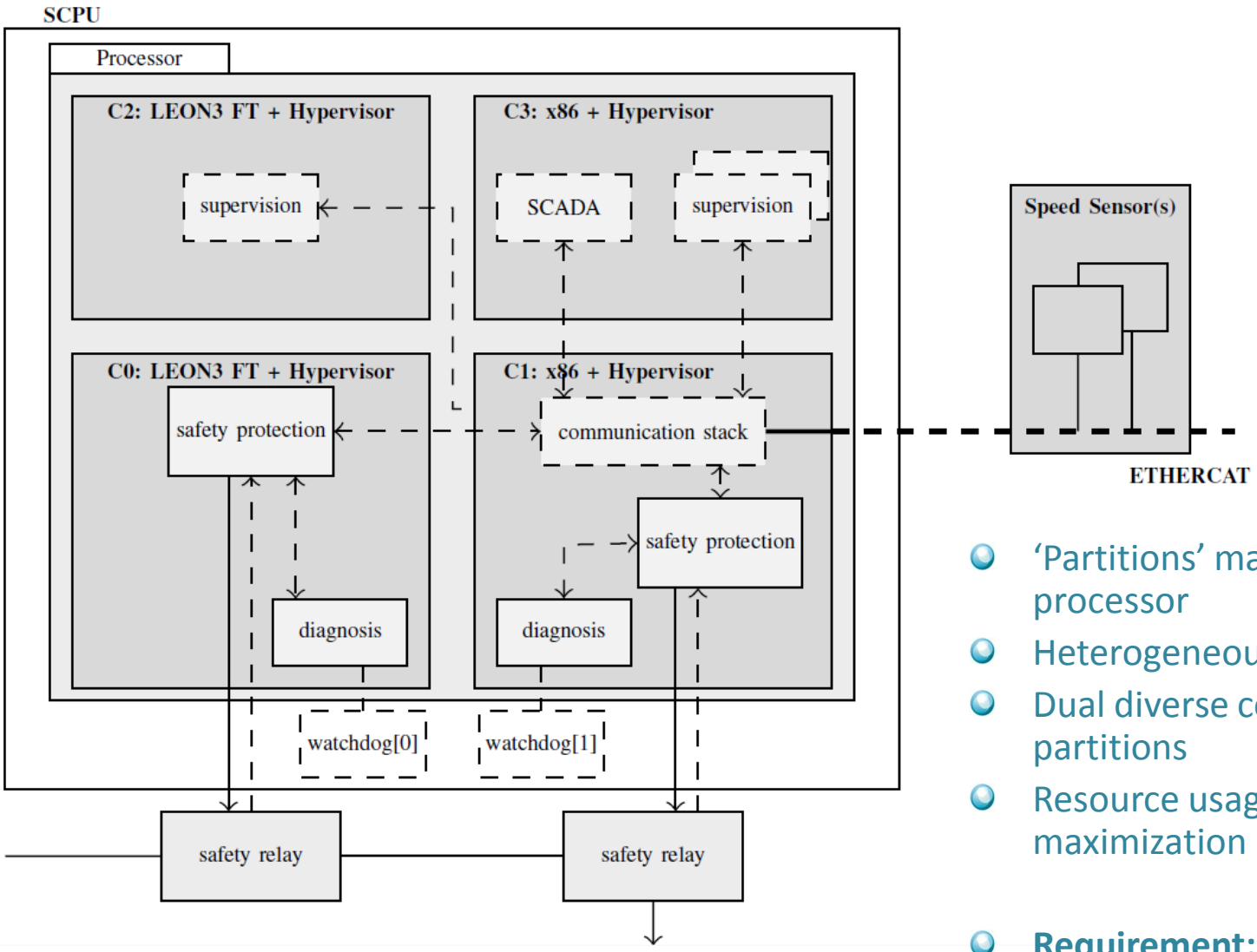
Safety Concept: Multiprocessor



- 1oo2 architecture
- HFT = 1
- 2 independent processors
- 2 shared diverse input sources (rotation speed)
- 2 output relays
- Safety-relays can be de-activated (safe-state) either directly by 'safety protection' or indirectly by 'diagnosis'.

- **Limitation: scalability**

Safety Concept: Multicore with virtualization



- 'Partitions' mapped to a multicore processor
- Heterogeneous quad core
- Dual diverse cores for safety partitions
- Resource usage and performance maximization

- **Requirement: IEC-61508-2 Annex E for on-chip redundancy**

Conclusions and future work

- **Safety certification** of mixed-criticality systems based on COTS multicore processors is challenging, but **feasible**.
- This paper presents a **safety-certification strategy for IEC-61508** compliant safety systems based on COTS multicore processors.
- The **safety concept** of a wind power case-study is currently **under detailed review** by a certification body.
- The **assumptions and analysis** considered at this stage **will be reviewed in the following design stages** and validated at the final stage of the case-study within FP7 MultiPARTES project.

IKERLAN

Eskerrik asko

Muchas gracias

Thank you

Merci beaucoup

P.º J.M. Arizmendiarrieta, 2

20500 Arrasate-Mondragón (Gipuzkoa)

Tel.: 943 71 24 00

Fax: 943 79 69 44

www.ikerlan.es