Road to certification in multicore partitioned mixed criticality systems

(Experience from MultiPARTES, DREAMS and PROXIMA FP7)

Dr. Jon Perez
Dr. Alfons Crespo

Agenda

- Introduction
  - IKERLAN
  - FENTISS
  - Road to certification
  - Basic concepts

- Industrial domain (IEC-61508)
  - Dissemination
  - Safety concept
  - What we have learnt

- Space domain
  - Dissemination
  - Qualification
  - What we have learnt

- Achievements are the foundation for…
  - FP7 PROXIMA
  - FP7 DREAMS

- Questions
“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]
Introduction
Basic concepts – Different terms

Academia

Temporal isolation, safety, safety-critical, ....

Industry

IEC-61508

Fail-safe / operational
Temporal Independence
Compliant Item
High Demand
Diagnostic Coverage

....

....
INDUSTRIAL DOMAIN

(IEC-61508)
Dissemination

- **Academic / Scientific:**

- **Industry:**
The safety concept was **positively assessed** by TÜV Rheinland, a relevant certification body in the industrial domain. Goals:

- The review of a safety-concept for a wind power case-study, which serves as a representative proof of concept example to discuss the MultiPARTES contribution and limitations / comments that should be taken into account in a future certification process.
- The dissemination of MultiPARTES contribution to TÜV Rheinland
- The gathering of detailed feedback from TÜV Rheinland
- The definition of an action plan based on the feedback (if needed)
Introduction – Context Diagram

Windpark Control Center
WebHMI
Maintenance
SCADA
Client
WT Heterogeneous Processing Unit
Safety Supervision HMI & Comms
Developer
Maintenance Operator
Park Client
I/O
I/O
I/O
WT Heterogeneous Processing Unit
Industrial Domain (IEC-61508)
A modern off-shore wind turbine dependable control system manages [1]:
- **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

Introduction – Proposed Solution

- Safety
- Non Safety Related

- Safety Protection
- Safety Relay

< Safety Chain >

Output relay pitch control

HMI & COMS
Supervision

Speed Sensor (s)
Sensor (s)
Activators
Subsystems

ETHERCAT

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

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

Reduced Reliability:
• The overall system reliability and availability is reduced...
The fault-hypothesis [1] of this strategy consists of the following assumptions:

- **FSM**: All safety relevant systems are developed with an IEC-61508 Functional Safety Management (FSM)
- **Node**: The node computer forms a single Fault-Containment Region (FCR) that can fail in an arbitrary failure mode. The permanent failure rate is assumed to be in the order of 10-100 FIT and the transient failure rate is assumed to be in the order of 100,000 FIT
- **Processor**: The multicore processor might not provide temporal isolation (or not sufficient evidence for certification), but bounded temporal interference can be estimated and validated with measurements
- **Hypervisor**: The hypervisor provides interference freeness among partitions (bounded time and spatial isolation), it is a compliant item and fails in an arbitrary failure mode when it is affected by a fault. Qualified tools.
- **Partition**: A partition can fail in an arbitrary failure mode, both in the temporal as well as the spatial domain

Is it feasible to develop 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
‘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 CPU SINGLE PROCESSOR QUAD CORE PARTITIONED – 1oo2
Safety Concept (B – ‘Multicore partitioning’) 3/3

SAFETY CPU SINGLE PROCESSOR QUAD CORE PARTITIONED – 1oo2
Safety Concept (B – ‘Multicore partitioning’)

- **Scheduling:**
  - 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

Safety Concept (B – ‘Multicore partitioning’)

- Safety techniques:
  - Measures to reduce the probability of systematic faults
    - The overall system is developed and certified using a SIL3 FSM compliant with IEC-61508.
    - The hypervisor is a compliant item
    - Qualified tools according to IEC-61508-3 (see chapter 7.4.4)
  - Detailed FMEAs, measures to control errors and system reaction to errors
Industrial Domain (IEC_61508) - Safety Concept
Lessons learnt

- Mixed-criticality paradigm based on COTS multicore and partitioning provides multiple potential benefits but certification is a challenge.
- It is possible... to achieve SIL3 IEC-61508 / Pld ISO-13849 with multicore and partitioning.
- Temporal independence (IEC-61508):
  - Temporal isolation simplifies the safety argumentation but .... Temporal independence does not necessarily require temporal isolation.
  - Temporal independence must be met according to IEC-61508. The lack of temporal isolation could reduce the availability of the system but should not jeopardize safety (fault avoidance and control).
- The safety-concept highly depends on the details of the underlying processor.
- 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.
SPACE DOMAIN
(ECSS)
Space application assessment

- Space applications are qualified using ECSS-E-ST-40 and ECSS-Q-ST-80 standards.
- E-40 defines software engineering requirements for space software systems. The standard has a similar view as ISO/IEC 12207, using an approach to software development based on a defined set of processes.
- Q-80 defines product assurance requirements for developing software for space systems.
- ECSS standards partially implemented:
  - Requirements, design, implementation, V&V processes used in virtualization layer, guest-OS & most of application development.
  - Quality requirements being considered in some parts of the system.
Space application assessment

- Current achievements
  - A technological assessment of XtratuM has been carried out by ‘Softwcare’ (ESA contract)
    - Roadmap for XtratuM qualification as defined
  - The ORK OS has been qualified to level B for space applications
  - Model-based techniques used for application design are consistent with ESA practice (e.g. Matlab/Simulink)
  - Schedulability analysis as per E-40 requirements for level-B software
- ‘Softwcare’ working on extended assessment of the case study:
  - advice on roadmap to qualification
  - assessment on the use of safety mechanisms and conformity to E-40/Q-80
Results used in other projects:

- **FP7 DREAMS**
  - Modular safety cases (hypervisor, COTS processor, partition, system)
  - Certification of product lines (variability)
  - Updated wind turbine safety concept

- **FP7 PROXIMA**
  - Safety concept, SIL4 railway signalling EN-5012X
Questions