UML/MARTE modelling for Mixed-Criticality Systems

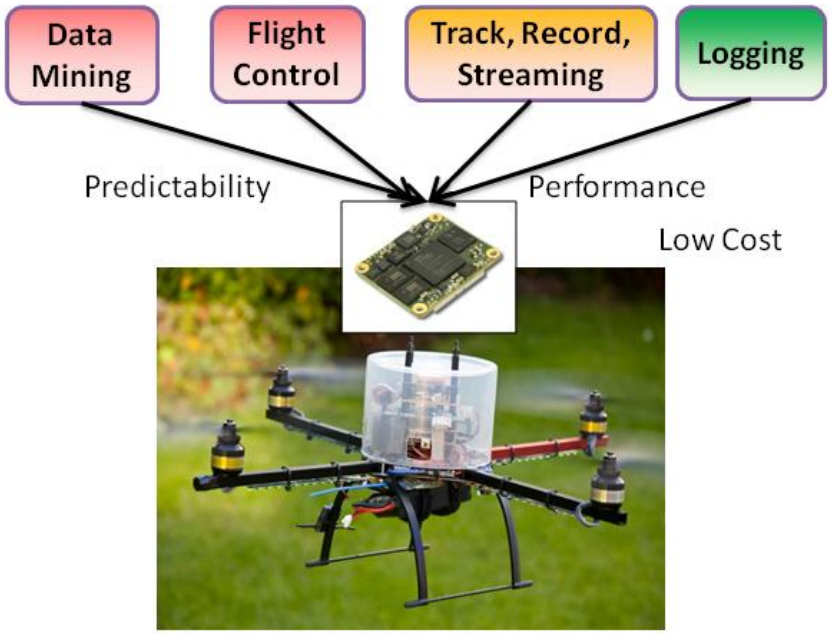
Fernando Herrera

University of Cantabria

Funded by the EC under

Grant Agreement 611146

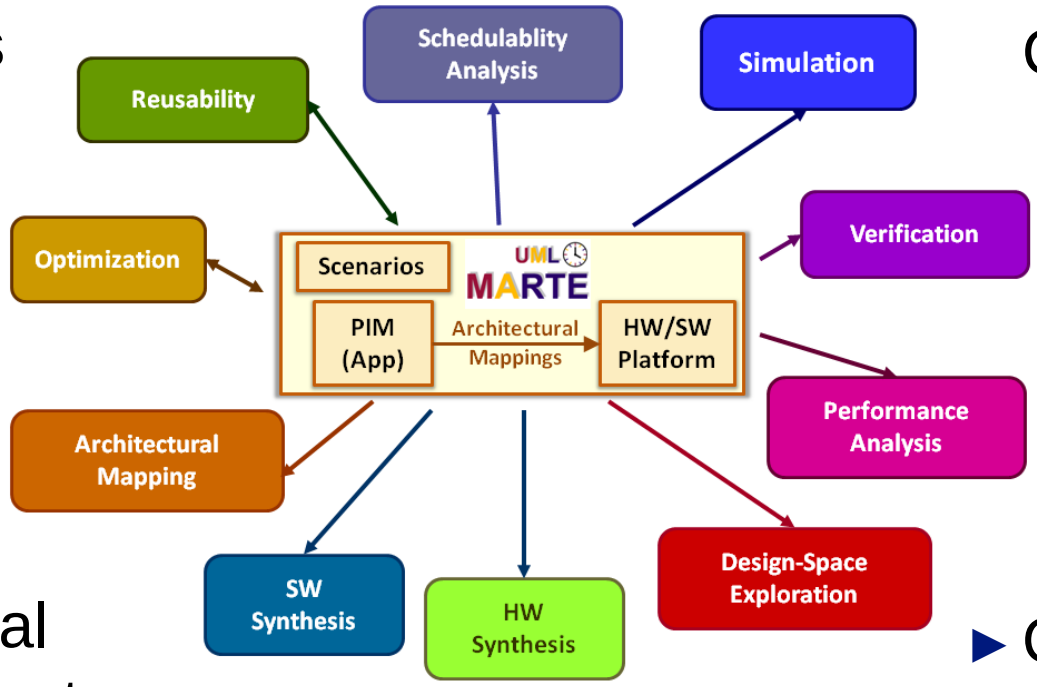
- System components and their associated requirements have different “importance”.



- **Modelling** and **Design** has to be **Mixed-Criticality aware**!

3 Modelling Methodology: Relevant Characteristics

- Single Source
- Relying on Standards
- Separation-of-Concerns



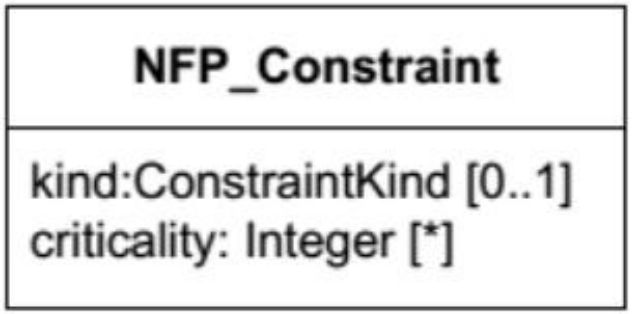
- Incremental development
- Component-based
- Support of system-level design activities: DSE, SLS

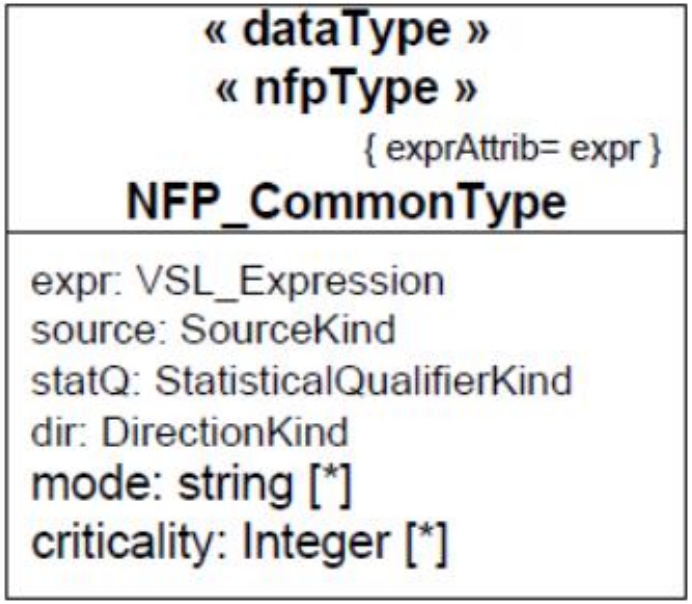
- Criticality: annotation that can be associated to
  - Application (PIM) Components
  - Platform Resources
  - Extra-Functional Requirements
  - Value annotations
- Generic concept and flexible interpretation that enables adapting the methodology to different domains

(CONTREX) Criticality	IEC 61508 SIL	EASA DAL
4	SIL4	A
3	SIL3	B
2	SIL2	C
1	SIL1	D
0	SIL0	E

(CONTREX) Criticality	ISO2626 ASIL
0xD	D
0xC	C
0xB	B
0xA	A

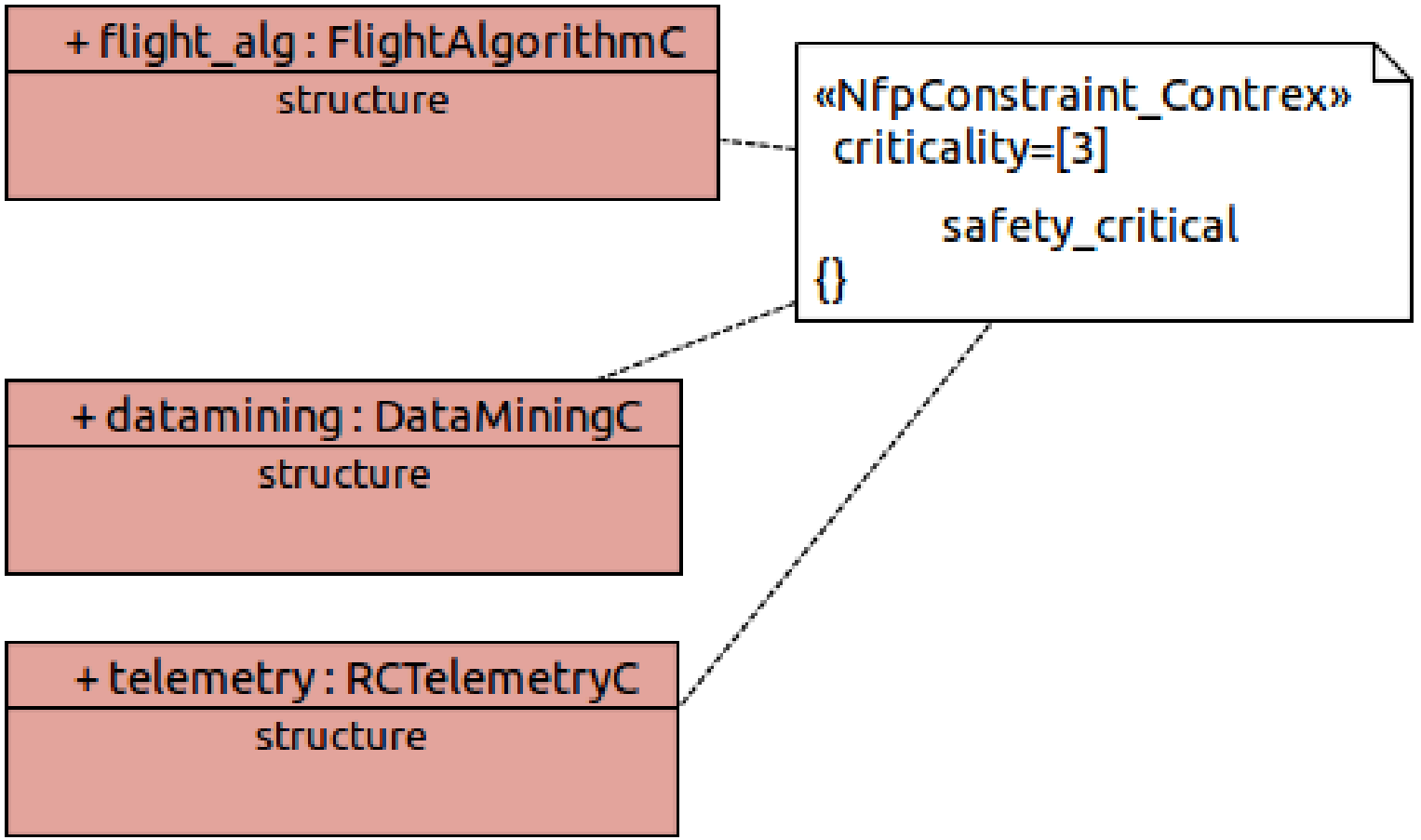
- Proposed minor MARTE extension



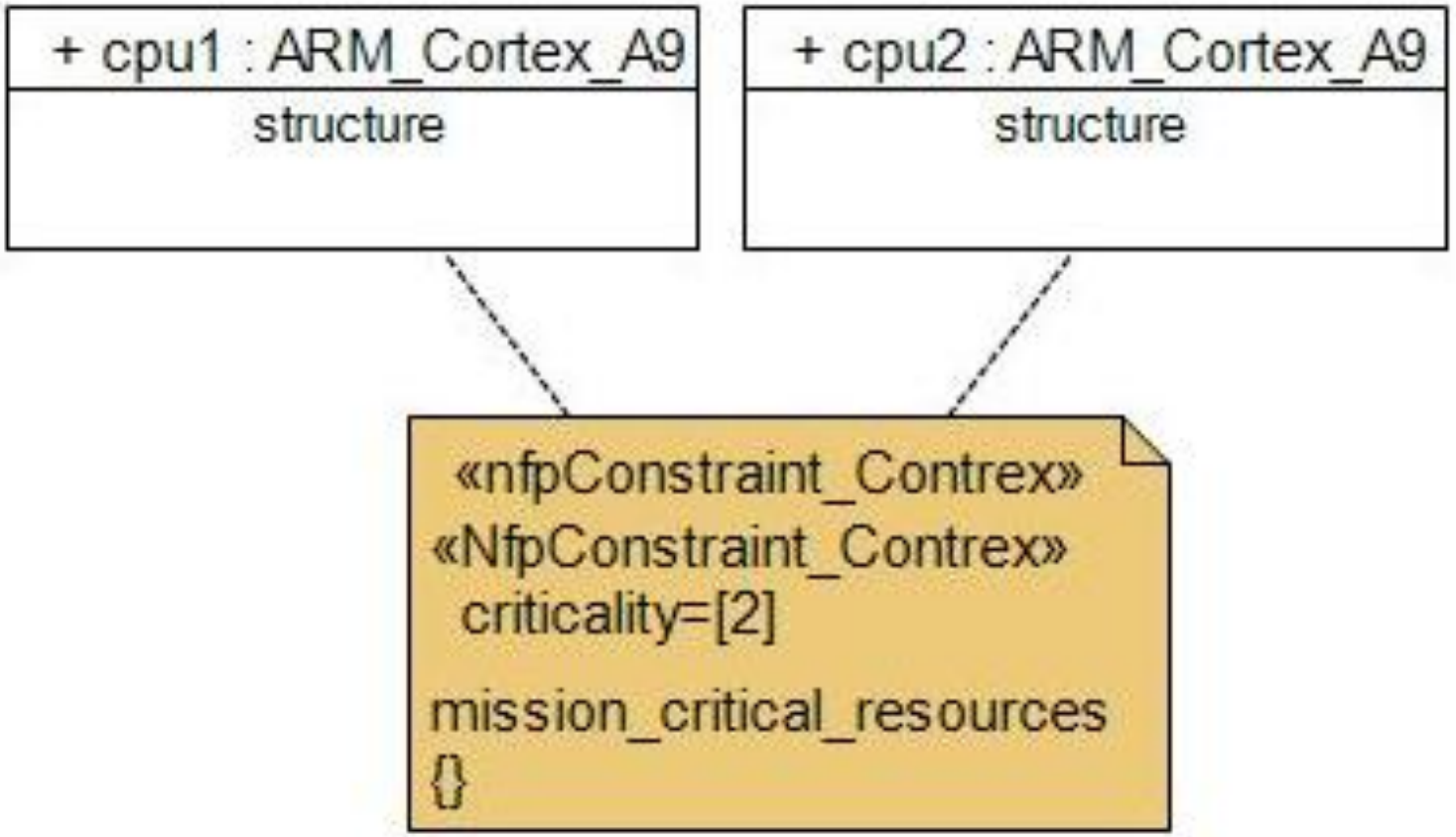


- Enables two basic modelling tecniques:
  - Criticality constraint associated to modelling element
  - Criticality associated to value

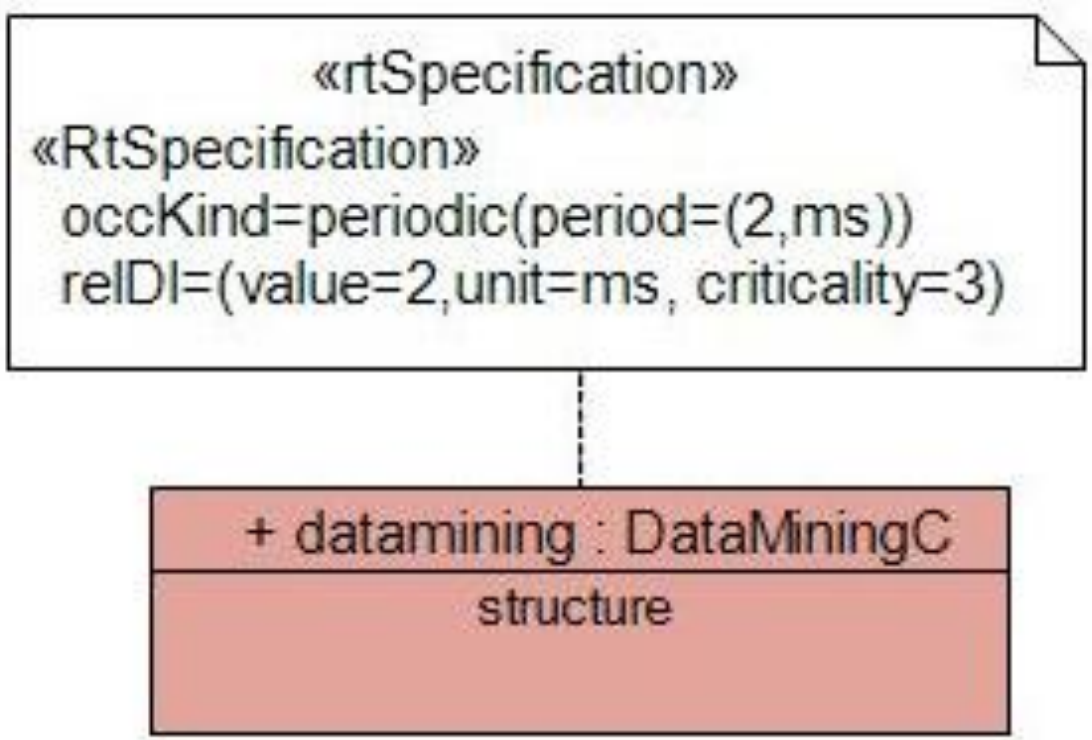
6 Associating criticalities to Modelling Elements (in PIM)



7 Associating criticalities to Modelling Elements (in HW resources)



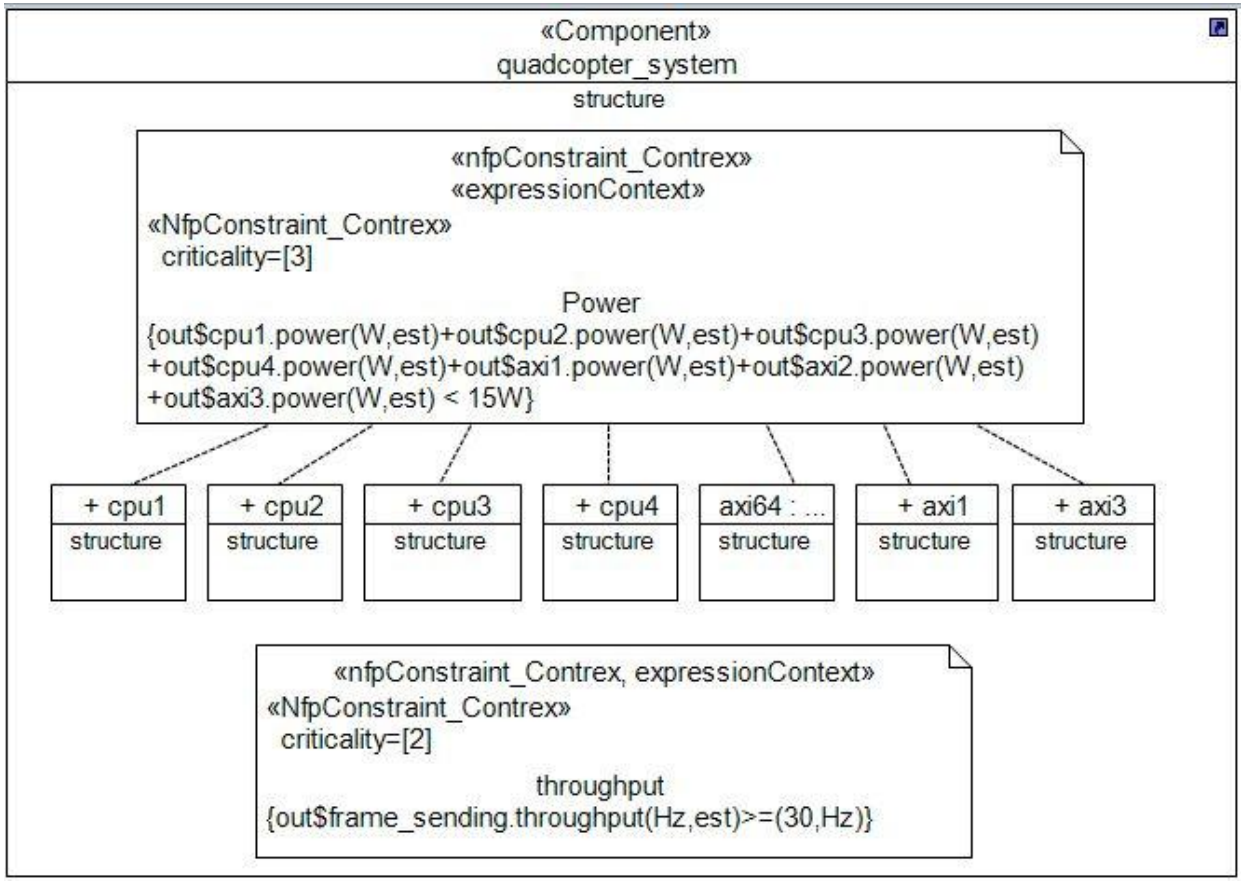
8 Associating criticalities to Performance Requirements



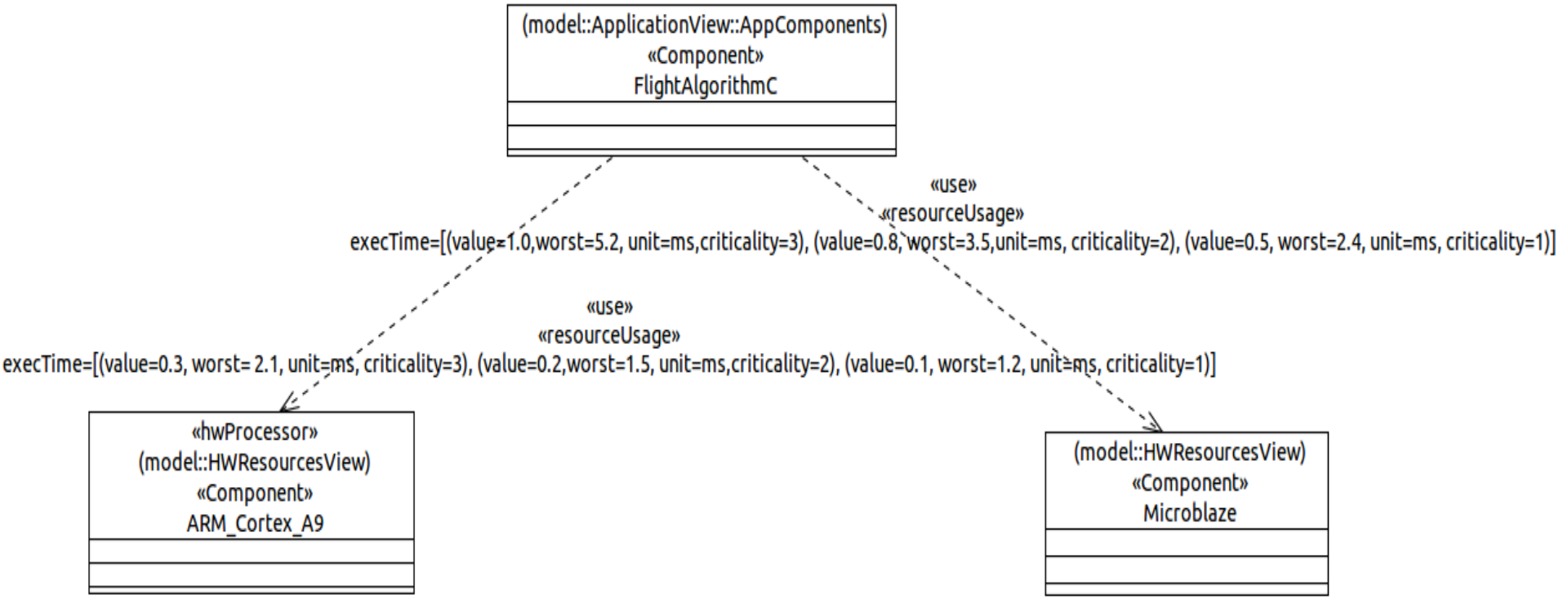
- VSL expression with criticality value:
- relDl={2,ms,**criticality=3**}

9 Associating criticalities to Performance Requirements

- NFP constraint with
  - **criticality annotation**
  - <<Expression Context>>: performance requirement



10 Associating criticalities to EFP annotations



Criticality Information in the Design Flow

- Mixed-Criticality Information can be used along the design flow at different phases, e.g.

- At **modelling**
- At verification
- At analysis (e.g., schedulability, performance)
- At the design space exploration phase
- At the implementaton

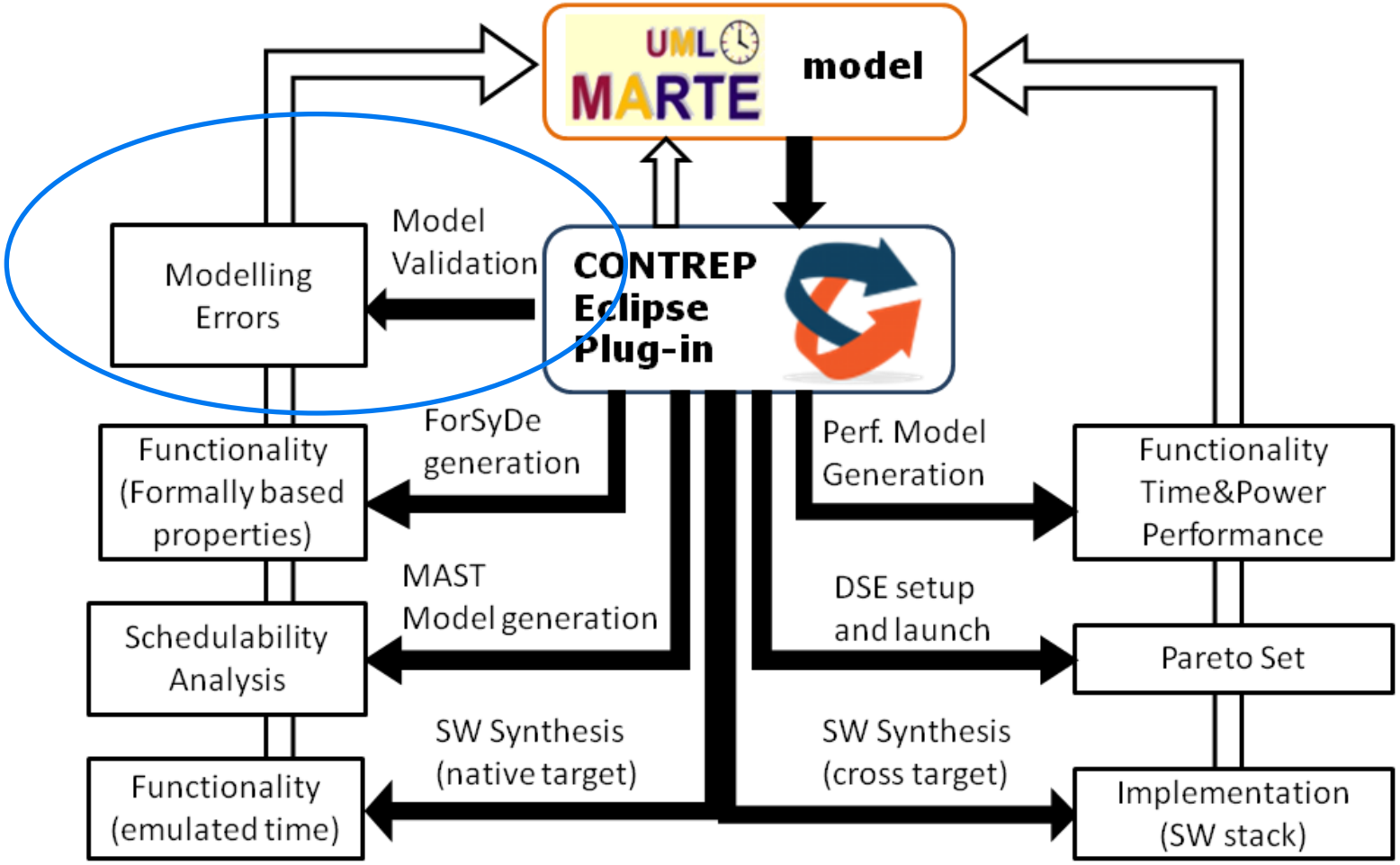
Mixed-Criticality aware modelling rules

Rule	Description
Criticality Assignation	
R1	A criticality shall be assigned to all RtUnit Instances
R2	A criticality shall be assigned to all PpUnit Instances
R3	A criticality shall be assigned to all HwProcessors
Allocation (Segregation of components with different criticalities)	
R4	There cannot be several application component instances with different criticalities allocated to the same memory space
R5	A memory space with the highest criticality level (or a given criticality level threshold) and a less critical memory spaced shall not be allocated to the same RTOS.
R6	Two or more component instances with different associated criticalities cannot be allocated to the same resource

Mixed-Criticality aware modelling rules

Rule	Description
Coherent Mapping	
R7	A PIM component instance of a given criticality shall not be mapped, either directly or indirectly, to a processing resource of a lower criticality
R8	A component instance of a given criticality cannot be mapped, either direct or indirectly, to a resource of a lower criticality

Single-Source Design Framework



Validation: Implementation Example

- Model Validation tool

- Mixed-Criticality aware Model Validation

- Identifying and Fixing a criticality-related modelling error

- Identifying more tricky criticality-related modelling errors

- Fixing the criticality-related modelling errors and warnings

Validator Implementation

- OML Model-To-Tex (MTL)
  - Queries (OCL): Model navigation and quering
  - Templates: Text generation
- OMG MTL Model-to-Text
  - Standard Description
  - Portable
  - Easy to Mantain and extend
- MTL for Validation:
  - Queries (OCL): Same as the ones for code generation
  - Templates: Report to the Eclipse “Error log” and dump a Model Validation Log File

- Mixed-Criticality: A novel and mandatory aspect to consider in complex embedded system design
- Mixed-Criticality Modelling tecniques
- Extension of a Single-Source Modelling Methodology
- Mixed-Criticality: Information used along the design process (**modelling**, verification, DSE, implementation)

- www.essyn.com
- CONTREX website. http://contrex.offis.de
- D2.1.1: CONTREX System meta-model
- D2.2.2: CONTREX System modelling methodology (final)
- D2.3.2: System Modelling, Analysis and Validation tools (final)
- Fernando Herrera, Pablo Peñil, Eugenio Villar
  "A model-based, single-source approach to design-space exploration and synthesis of mixed-criticality systems"
  18th International Workshop on Software and Compilers for Embedded Systems, SCoPES 2015, ACM. 2015
- Fernando Herrera, Pablo Peñil, Eugenio Villar
  "UML/MARTE Modelling for Design Space Exploration of Mixed-Criticality Systems on top of Time-Predictable HW/SW Platforms"
  Jornadas de Computación Empotrada (JCE15). 2015-09