ACES (Autonomous and Critical Embedded Systems)

Réunion du Groupe de Travail en Ingénierie des Exigences, 28/05/2021

Dominique Blouin

Telecom Paris, Institut Polytechnique de Paris

dominique.blouin@telecom-paris.fr

ACES: Autonomous and Critical Embedded Systems (https://aces.wp.imt.fr/)

Loosely Coupled Systems

- Complex autonomic systems
- Fault-tolerant and asynchronous distributed computing
- Model Based Testing
- Security in Internet of Things
- Distributed Services

Strongly Coupled Systems

- Real-Time Systems
- Deterministic Platform
- Critical Systems Design Process
- Security and Safety
- Energy Consumption of Computation

Team

Leader : Laurent Pautet, Full Professor

Team Members :

Dominique Blouin, Research Engineer
Etienne Borde, Assistant Professor
Florian Brandner, Assistant Professor
Ada Diaconescu, Assistant Professor
Petr Kuznetsov, Full Professor
Jean Leneutre, Assistant Professor
Gérard Memmi, Full Professor
Mounira Msahli, Assistant Professor
Elie Najm, Full Professor (Emeritus)
Matthieu Rambaud, Assistant Professor
Thomas Robert, Assistant Professor
Samuel Tardieu, Assistant Professor
Sylvie Vignes, Assistant Professor (Emeritus)

SAE AADL
(Architecture Analysis & Design Language)

- **Modeling Language for Safety-Critical Systems**
- **Analysis of properties such as:**
  - Timing, safety, schedulability, fault tolerance, security, functional simulation...
- **Textual and graphical notations**
- **AS2C committee members:**
  - Etienne Borde, Dominique Blouin, Laurent Pautet

- **AADL tools developed at Telecom**
  - Behavior Annex
  - RAMSES (Refinement of AADL Models for the Synthesis of Embedded Systems)
  - RDAL (Requirements Definition and Analysis Language)
  - ALISA (Architecture-Led Incremental System Assurance)

ALISA in a Nutshell (Architecture-Led Incremental System Assurance)

- **Initiated from RDAL**
  - **Fragment language** that can be coupled with an architecture language
  - Inspired from FAA Requirements Engineering Management Handbook and other RE approaches (SysML, KAOS, i*)
- **Re-implemented and extended as the ALISA set of textual notations**
  - **ReqSpec**: Stakeholder goals and system requirements.
  - **Verify**: verification methods, activities and verification plans with claims that requirements are satisfied by the results of verification activities
  - **Alisa**: Assurance cases (consist of one or more assurance plan)
  - **Assure**: Assurance case result instance, i.e., the evidence as the result of executing verification plans on one or more system instance models.
  - **Organization**: Defines the stakeholders of a project
- **Future work**
  - Review and standardize as **Assurance Annex (Telecom Paris lead)**

Engineering Railway Systems with an Architecture-Centric Process Supported by AADL and ALISA: an Experience Report

Paolo Crisafulli[1], Dominique Blouin[2], Françoise Caron[3], and Cristian Maxim[1]

[1] IRT SystemX, Paris, France firstname.lastname@irt-systemx.fr
[2] LTCI, Telecom Paris, Institut Polytechnique de Paris, France dominique.blouin@telecom-paris.fr
[3] Eiris Conseil, France francoise.caron@eiris.fr

```
system requirements ETCS_OnBoard_Performance_Requirements for Functions_2oo3::Integrated.basic [
    description "These are some ERA performance requirements for the ETCS on board system"

    requirement ERA_5_2_1_1 :
            "Emergency break delay" [
        val MaxEVCResponseTime = 300 ms
        val MaxUpstreamResponseTime = 350 ms
        val MaxDownhillResponseTime = 350 ms
        val MaxEmergencyBreakDelay = MaxUpstreamResponseTime + MaxEVCResponseTime + MaxDownhillResponseTime
        value predicate MaxEmergencyBreakDelay <= 1 sec
        description "Delay between receiving of a balise message and applying the emergency brake."
                "Sta
                "Sto
                MaxE
        category Qua
    ]

    requirement ERA_
        decomposes E
        compute Syst
        compute MinL
        compute MaxL
        description
                MaxEVCRespons
        value predicate MaxL
        category Quality.Late

    ]
```

```
verification plan ETCS_OnBoard_Performance_Verification for ETCS_OnBoard_Performance_Requirements [

    claim ERA_5_2_1_1 [
        // Just check the predicate defined in the requirement itself
    ]

    clai

    ]
]
```

rmation | Assurance View | Progress | Search | Error Log | Assurance Case | Console | History

Evidence	Pass	Fail	Err	Todo	Description
Case ETCS_OnBoard_Case	5	1	1		
Plan ETCS_OnBoard_Middleware_Plan(Integrated.basic)	5	1	1		
Claim engineering_design_rules_full_connect		1			As a design good practice, all components in a model shall have all
Claim engineering_design_rules_perdiodic_threads	1				All threads shall be periodic
Claim ERA_5_2_1_1	1				Delay between receiving of a balise message and applying the emer
Predicate	1				(MaxEmergencyBreakDelay <= 1 sec)
Claim ERA_5_2_1_1_evc(message_processing_flow)	1				Delay between reception of an input data message and output com
Evidence responsetime	1				Analysis of all end-to-end flows in a system instance or for a specific
Success: message_processing_flow					Latency results for message_processing_flow
Value:					
Value: 23.338					
Value: 146.18					

A Requirements Engineering Approach for Usability-Driven DSL Development

Ankica Barišić
NOVA-LINCS, FCT/UNL
Caparica, Portugal
a.barisic@campus.fct.unl.pt

Dominique Blouin
LTCI Lab, Telecom ParisTech
Paris, France
dominique.blouin@
telecom-paristech.fr

Vasco Amaral
Miguel Goulão
NOVA-LINCS, FCT/UNL
Caparica, Portugal
(vma,mgoul)@fct.unl.pt