Leiden 12 April 2018

FORMAL METHODS AND TOOLS IN INDUSTRIAL APPLICATIONS: THE ASTRAIL APPROACH

SAFETY OF FUTURE SYSTEMS: SCIENCE MEETS INDUSTRY

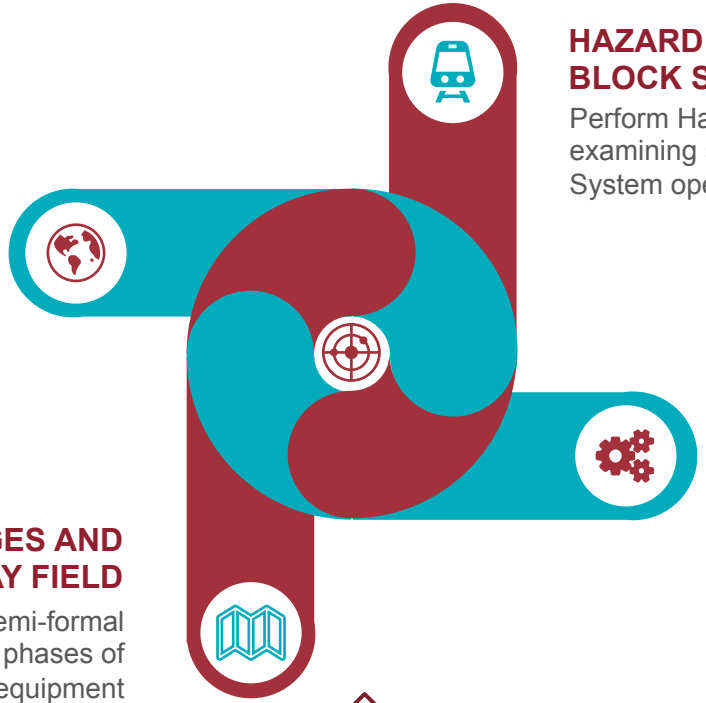
Stefania Gnesi
ISTI-CNR
PISA, ITALY

ASTRAIL CALL OVERVIEW

- Call: S2R JU Call for Proposals 2017
- Topic: S2R-OC-IP2-01-2017
- Research and Innovation Action
- S**A**tellite-based Signalling and Automation **S**ys**T**ems on **Rail**ways along with formal Method ad Moving Block Validation (ASTRail)
- A specific call was issued asking to analyse the suitability of formal methods in supporting the transition to the **next generation** of **ERTMS/ETCS** signalling systems, which will include **satellite-based train positioning, moving block distancing and automatic driving.**

ASTRAIL SCOPE

Enhance signalling and automation system leveraging cutting-edge technologies from different sectors and taking in particular care **safety and performance issues**



HAZARD ANALYSIS OF MOVING BLOCK SIGNALLING SYSTEM

Perform Hazard Analysis of the railway system examining safety level of Moving Block Signalling System operating without trackside detection

GNSS TECHNOLOGY INTO THE ERTMS SIGNALLING SYSTEM

Transfer the knowledge from the avionic sector to the application of fail-safe moving block localisation

AUTOMATIC DRIVING TECHNOLOGIES INSIGHT FROM AUTOMOTIVE SECTOR

Identify the most suitable technologies to be implemented in the railway field for performing automated driving

FORMAL LANGUAGES AND METHODS FOR THE RAILWAY FIELD

Identify the most promising formal and semi-formal methods for the different development phases of railway equipment

OBJECTIVES

- To examine **the safety level of a Moving Block system** in view of complete removal of trackside detection

1. To prepare a model of the moving block signalling system suitable for Hazard Analysis
2. To define system use cases to be analysed
3. To identify hazards derived from possible system errors and faulty states in main operative conditions
4. To assess the resulting risk level derived from identified hazards (risk qualifying)
5. To evaluate resulting safety level of a Moving Block signalling system operating without trackside train detection
6. To define Safety Related Application Conditions (operational procedures to be applied in normal or degraded conditions, according to GoAx, operational maintenance activities)

H2020/ SHIFT2RAIL – ASTRAIL

The H2020/ Shift2Rail initiative considers **formal methods** to be fundamental to the provision of **safe and reliable** technological advances to increase the competitiveness of the **railway industry**.

..... and

CENELEC EN 50128 for railway control and protection systems mentions **FMs** as **Higly Recommended** practices for SIL3-4 systems

But which FM method or which tools???

- Several FM methods exist (more than 100), with available support tools
- Several research experience on using FM in railways, and some success stories

Formal Methods and Railways Systems

- In the last decades, Formal and Semi-Formal Model Based Design has been largely adopted in the railway signalling industry, achieving lower costs and better quality software.
- The **B method** has been successfully applied to railway signaling systems, especially by MATRA Transport and ALSTOM, mainly in France
- **Simulink/Stateflow or SCADE** have been used for modelling, exploiting the offered possibilities of automatic code generation for the production of high quality code.
- **Model checking** have been employed for verifying portions of an interlocking system (symbolic model checker **NuSMV**, explicit model checker **SPIN**, **SAT/SMT-based Bounded MC**)
- **Model Based Testing** has been adopted for verification, either together with more traditional testing techniques, or with model checking or abstract interpretation

OUR OBJECTIVES IN ASTRAIL

- Identify the most suitable semi-formal and/or formal language and formal method to be applied in the railway field

1. review of the main formal modelling and verification languages and tools used in industrial railway applications
2. refine and rank identified languages and tools according to their use in the different phases of the development process of a railway application
3. evaluate usability and applicability of selected languages and tools in the railway domain by modelling the Moving Block signalling system
4. validate the identified languages and tools by modelling the integration of the Moving Block system with Automated Driving Technologies

OUR APPROACH

- Retrieve structured information about the state-of-the art and the state-of-the practice of FM in railways

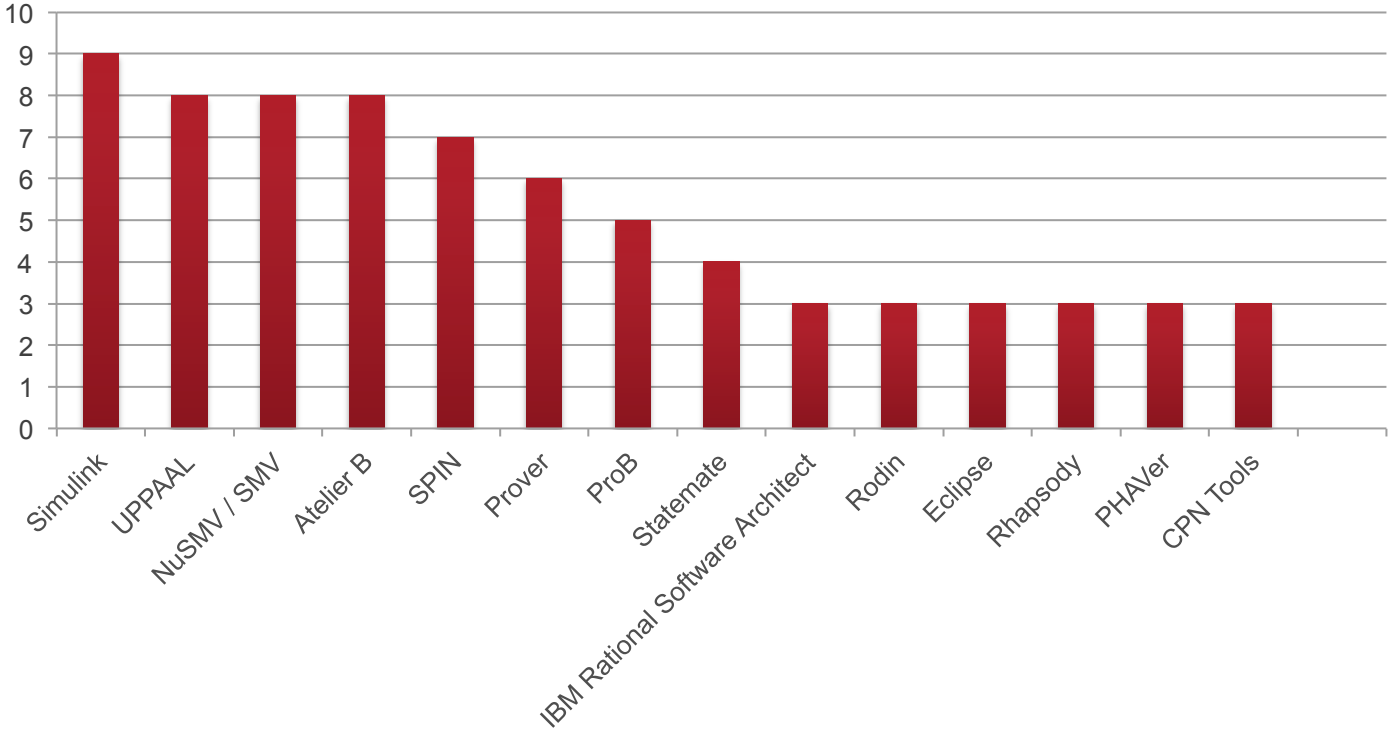
CURRENT RESULTS - SLR

SLR GOALS

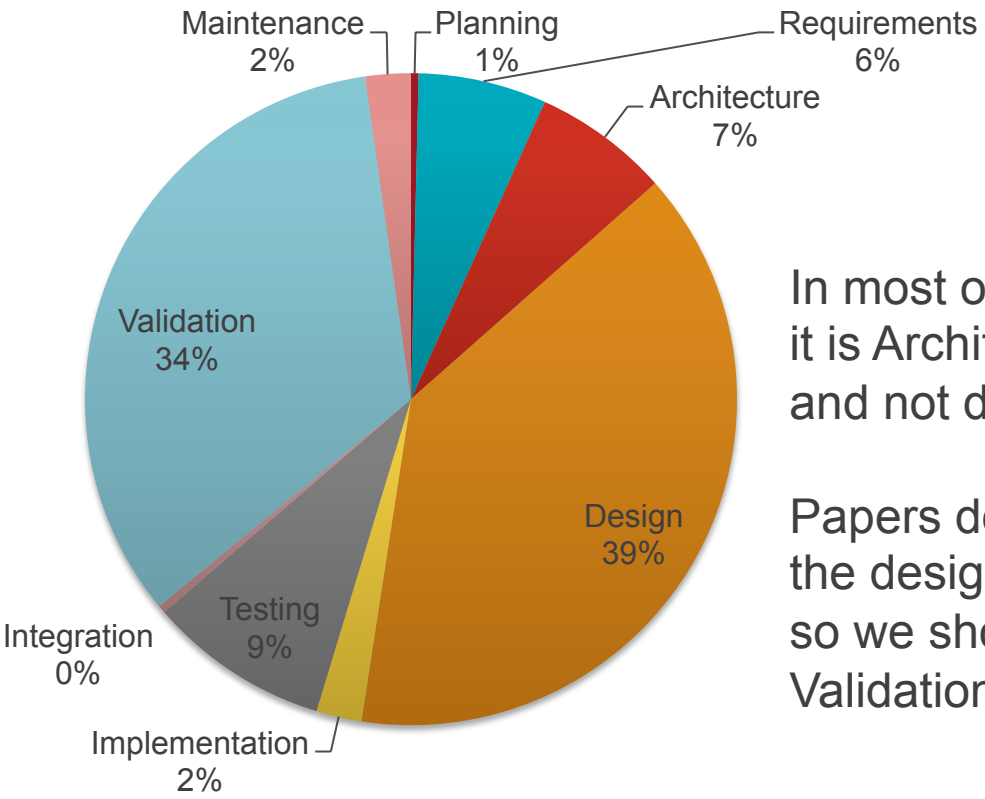
- Identify most used formal and semi-formal techniques used in railways
- Identify languages and tools
- Identify tasks performed
- Identify phase addressed
- Identify industry readiness

- A typical paper reviewed:
  - takes a railway system (e.g., entire ERTMS/ETCS)
  - models a sub-system with a semi-formal language (e.g., UML)
  - transforms the model into a formal model (e.g. UPPAAL, SPIN, NuSMV)
  - verifies properties on the model

SLR – TECHNIQUES AND TOOLS



SLR – PHASE OF THE SW PROCESS



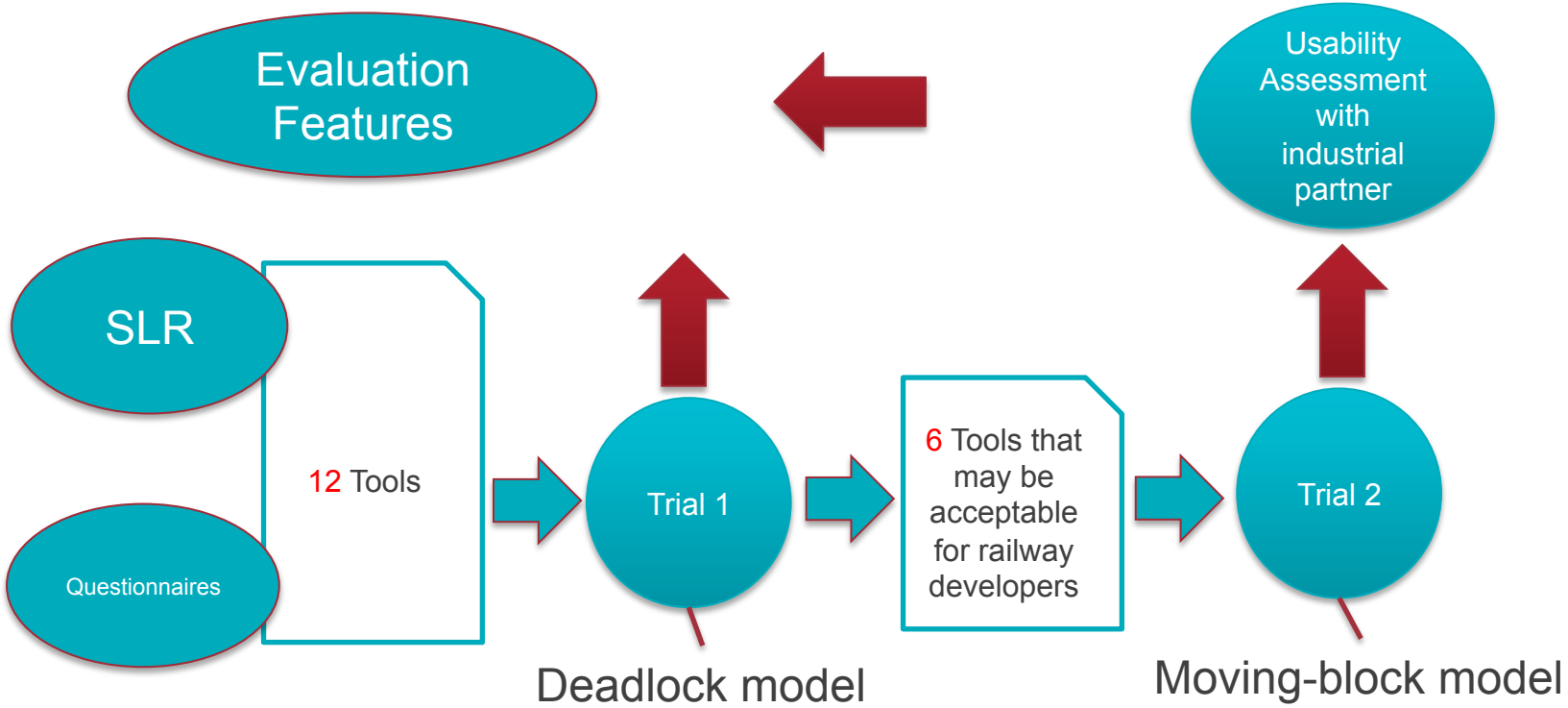
In most of the cases it is Architecture, and not design

Papers do verification in the design phase, so we should not select Validation

CURRENT RESULTS – TOOLS

TOOL REVIEW

SUBTITLE



TOOLS

- Tools are selected from SLR and from Questionnaires

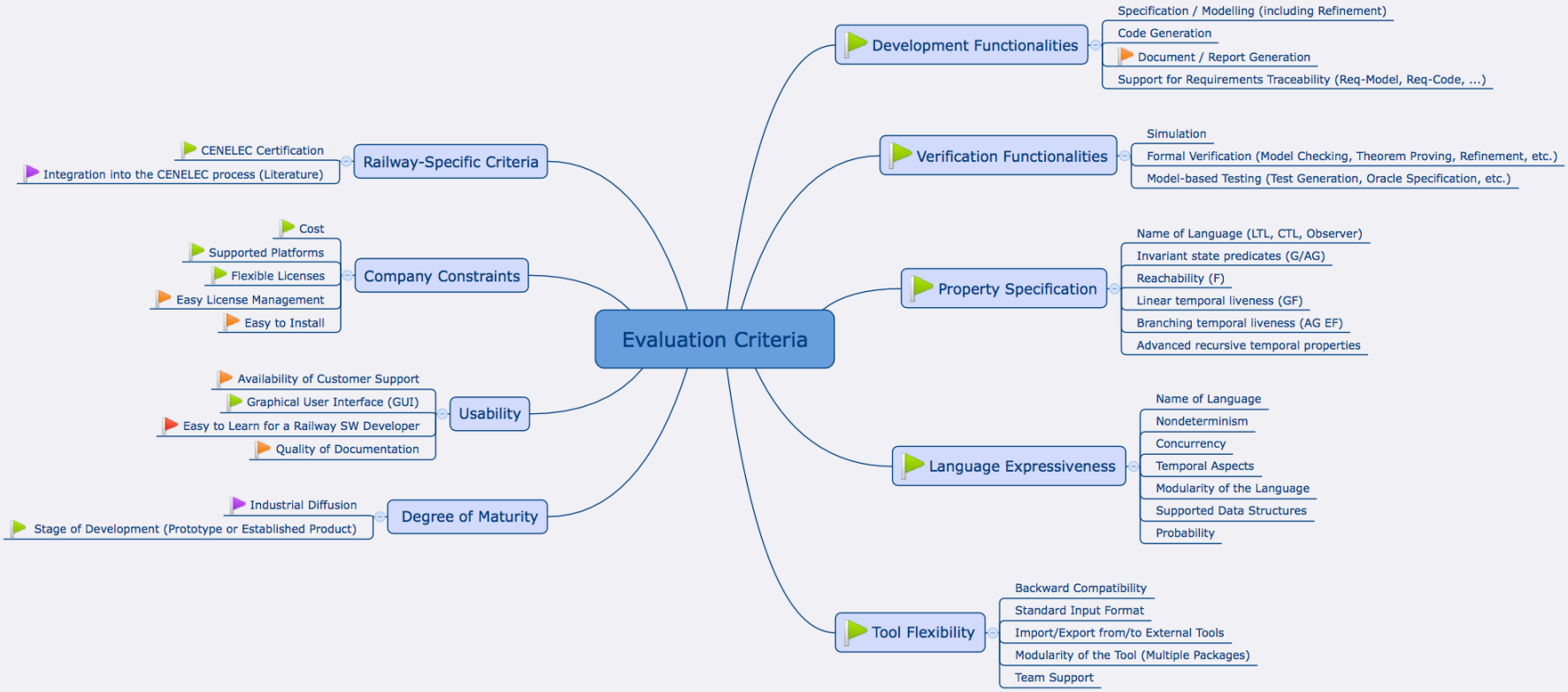
- Selected tools for **Trial 1** (**deadlock avoidance model**):
  - **Done (10):** CPN Tools, Atelier B/ProB, UPPAAL, NuSMV, SPIN, UMC, FDR4, mCRL2, CADP, TLA+
  - **TODO (2):** Simulink/Stateflow, SCADE

- Selected tools for **Trial 2** (**moving-block model**):
  - **Done (2):** UPPAAL, Atelier B/ProB
  - **TODO (4): NuSMV, SPIN, Simulink/Stateflow, SCADE**

Framework	Supported Verification Techniques
UMC	model checking CTL-like, state-event based logics
SPIN	model checking LTL, fairness requirements
NuSMV/nuXMV	LTL, CTL, PSL [1], SMT model checking, fairness requirements
CADP	MCL [22], Parametric Mu-Calculus model checking, equivalence checking
UPPAAL	MITL [3], time-related, and probability related properties
TLA+	LTL, Theorem Proving, Proof Validations
ProB	LTL, CTL model checking, constraints based checking
mCRL2	Parametric Mu Calculus model checking, equivalence checking
FDR4	Refinement Checking, fairness requirements
CPN	CTL, custom ML properties

Framework	Range of evalution times
UMC	38 - 86 seconds
SPIN	13 - 47 seconds
NuSMV/nuXMV	2.9 - 43 seconds
CADP	29 seconds
UPPAAL	16 seconds
TLA+	3 minutes
ProB	32 minutes
mCRL2	2 minutes -19 minutes
FDR4	15 seconds - 20 minutes
CPN	unable to deal with the state-space size

NEXT STEPS


Evaluation Criteria
Development Functionalities
Specification / Modelling (including Refinement)
Code Generation
Document / Report Generation
Support for Requirements Traceability (Req-Model, Req-Code, ...)
Verification Functionalities
Simulation
Formal Verification (Model Checking, Theorem Proving, Refinement, etc.)
Model-based Testing (Test Generation, Oracle Specification, etc.)
Property Specification
Name of Language (LTL, CTL, Observer)
Invariant state predicates (G/AG)
Reachability (F)
Linear temporal liveness (GF)
Branching temporal liveness (AG EF)
Advanced recursive temporal properties
Language Expressiveness
Name of Language
Nondeterminism
Concurrency
Temporal Aspects
Modularity of the Language
Supported Data Structures
Probability
Tool Flexibility
Backward Compatibility
Standard Input Format
Import/Export from/to External Tools
Modularity of the Tool (Multiple Packages)
Team Support
Railway-Specific Criteria
CENELEC Certification
Integration into the CENELEC process (Literature)
Company Constraints
Cost
Supported Platforms
Flexible Licenses
Easy License Management
Easy to Install
Usability
Availability of Customer Support
Graphical User Interface (GUI)
Easy to Learn for a Railway SW Developer
Quality of Documentation
Degree of Maturity
Industrial Diffusion
Stage of Development (Prototype or Established Product)

SOME CONCLUSIONS

Formal methods are often suggested to be used for system validation but verification tools are far from being themselves validated at the same safety level of the software they should verify.
Using “diversity” in formal modelling, i.e. more than one model and tool, might mitigate this problem.

A lot of variability comes out when trying to use the existing tools.
Depending on the tool specific choices made, the result can be orders of magnitude more efficient (or inefficent).
You really need to be an “expert” on a tool for reasonably use it.

When it comes to the analysis of likely incorrect system designs, the “feedback” provided by the tools, is often very inadeguate.

ASTRail

SAtellite-based Signalling and Automation SysTems on Railways along with Formal Method and Moving Block validation

THANK YOU!

Address CNR-ISTI, Via G. Moruzzi 1, 56124

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 777561
Call identifier: H2020-S2RJU-2017
Topic: S2R-OC-IP2-01-2017