4SECURail

Designing a Demonstrator of Formal Methods for Railways Infrastructure Managers

ISoLA 2021
25 - 29 Oct 2021
Rhodes, Greece

Davide Basile
Maurice H. ter Beek
Alessandro Fantechi
Alessio Ferrari
Stefania Gnesi
Franco Mazzanti

Laura Masullo
Andrea Piattino
Daniele Trentini

The problem

The railway infrastructure is a complex **System of Systems**

Spreading across many national borders

Managed by many administrative bodies

Developed by many producers

Expensive to develop, maintain and exercise safely

The solution

High Quality Standard Interfaces between components

* to reduce costs and vendors lock-in
* to increase competitivity, dependability and efficiency

The current efforts to advance the state of art
(e.g. EULYNX / ERTMS / SHIFT2RAIL initiatives)

recognize the importance of formal analysis

4SECURail: goals

https://www.4securail.eu/ is a Shift2Rail project

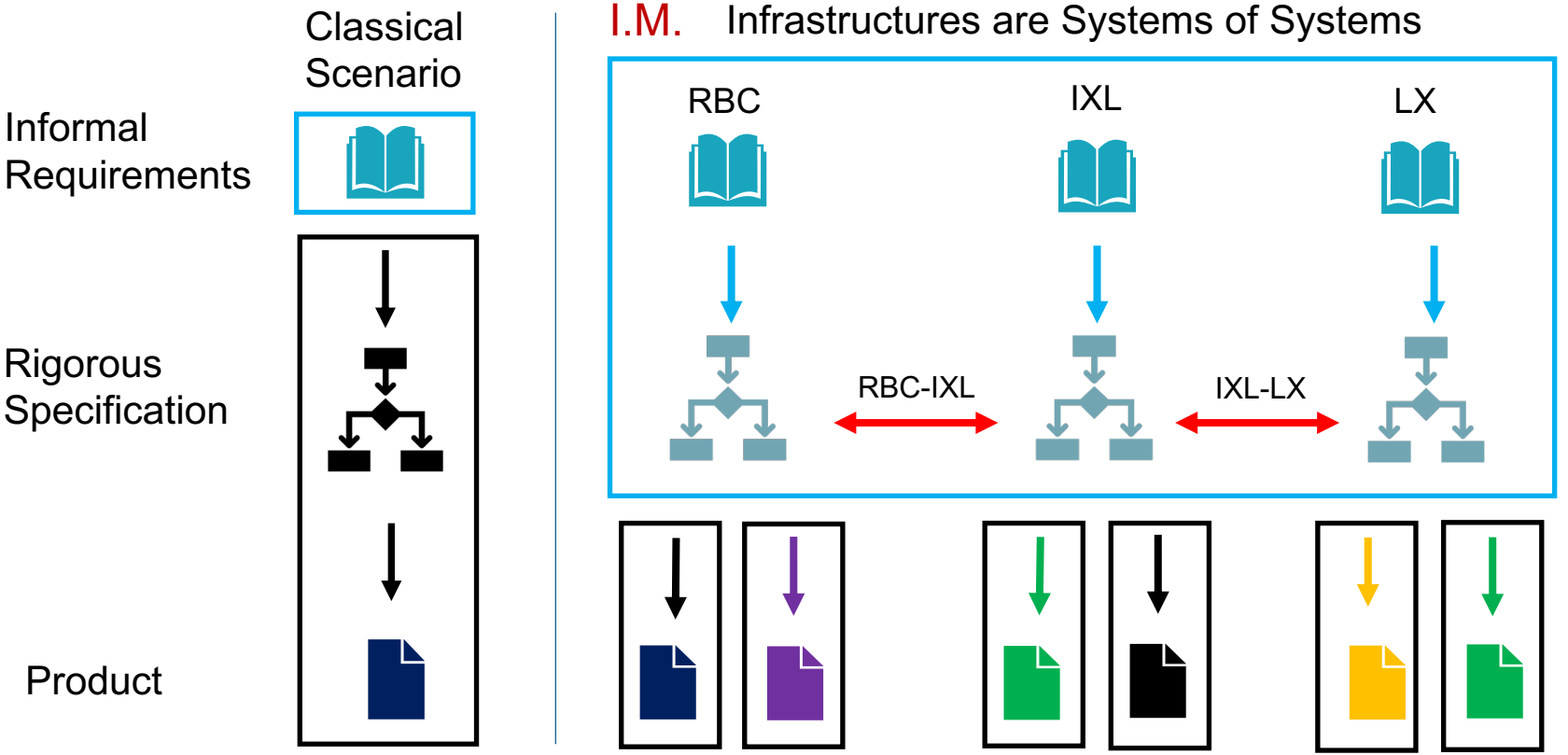
One of its goals is the definition and experimentation of a
Formal Methods Demonstrator:

A controlled experiment in exploiting
formal methods in the requirements definition phase
of a railway signalling system

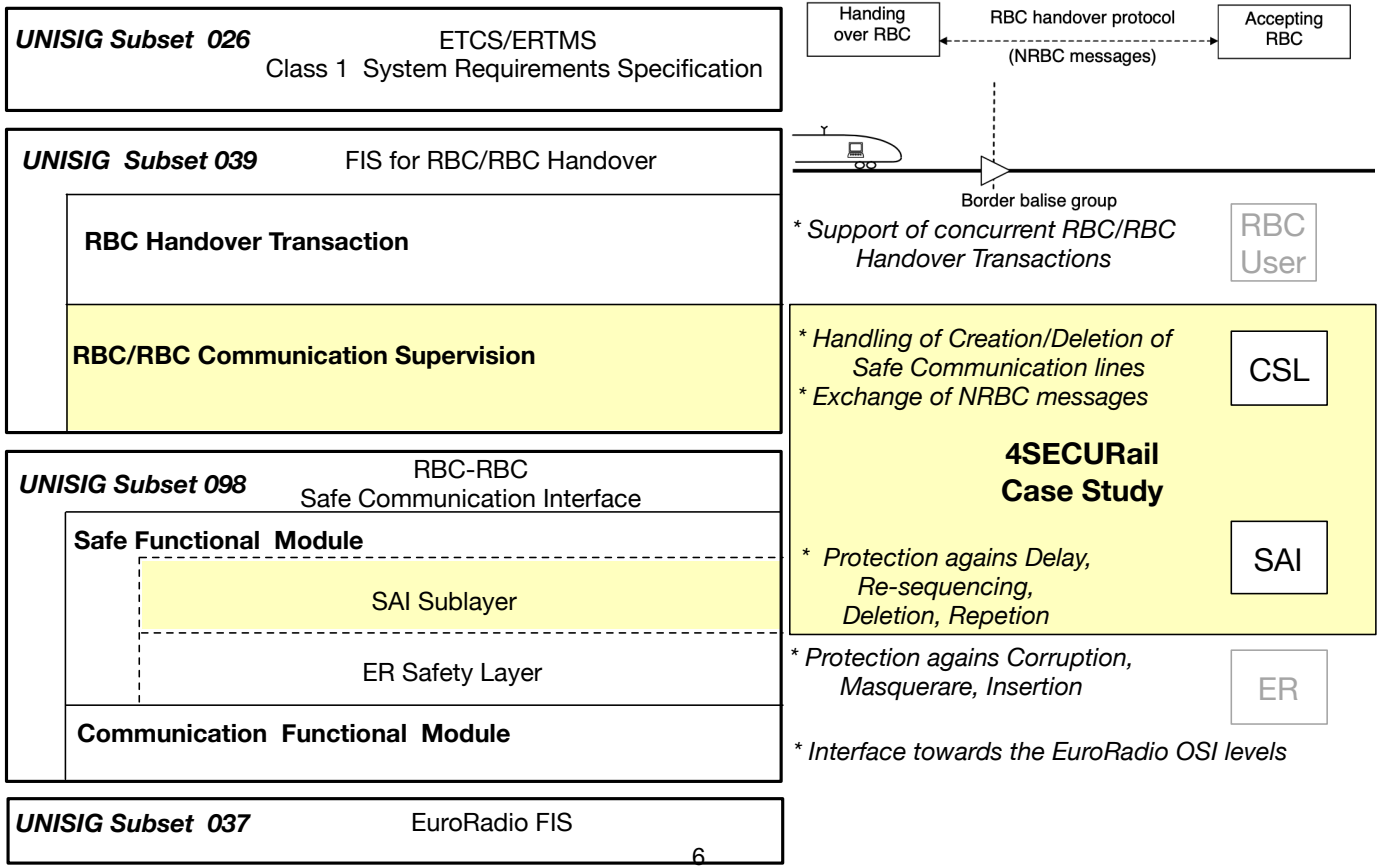
- Can formal methods help improving the quality of requirement specifications (standards)? How?

- Can their adoption be cost effective? How much?

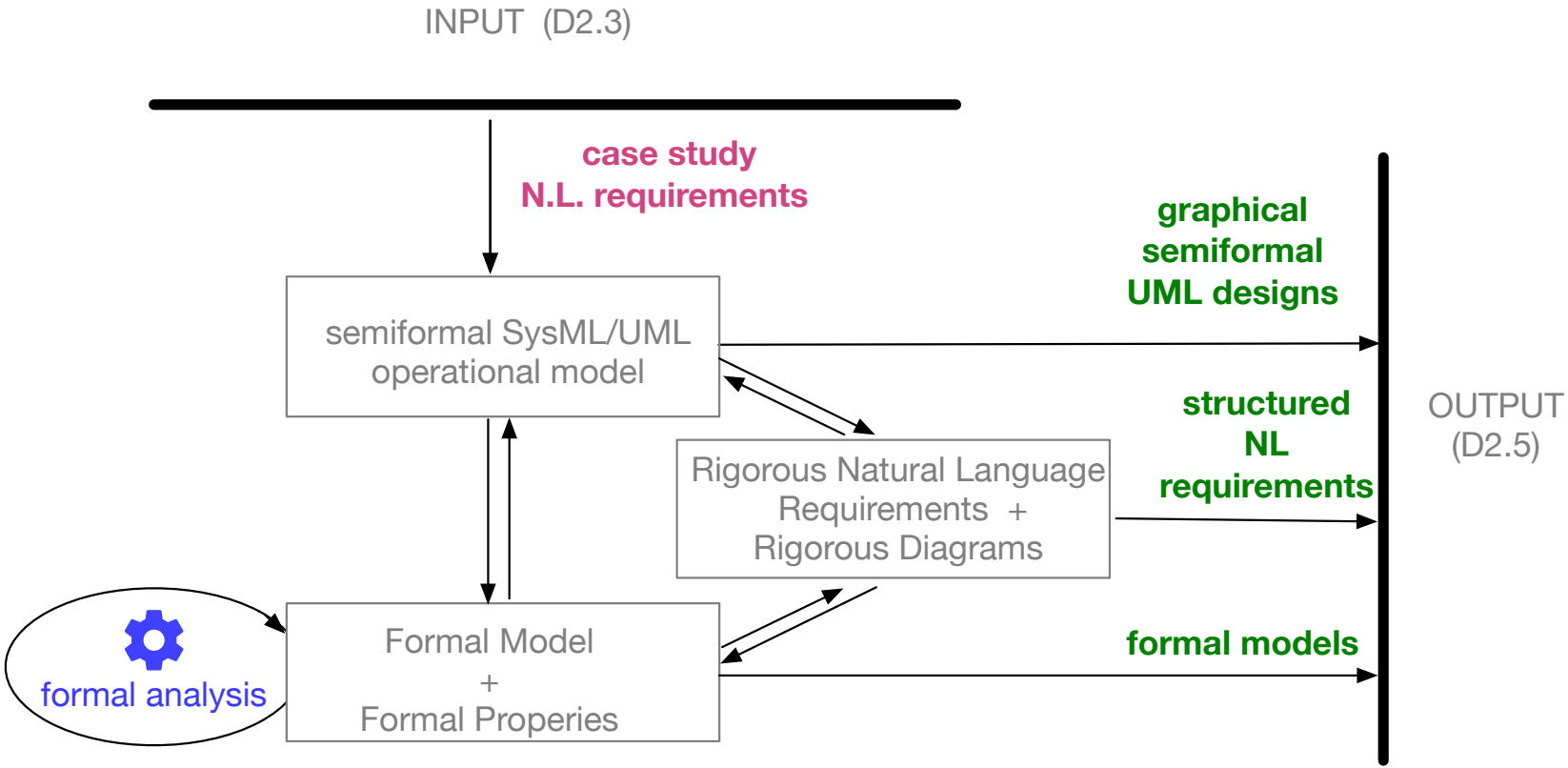
4SECURail: the point of view of Infrastructure Managers



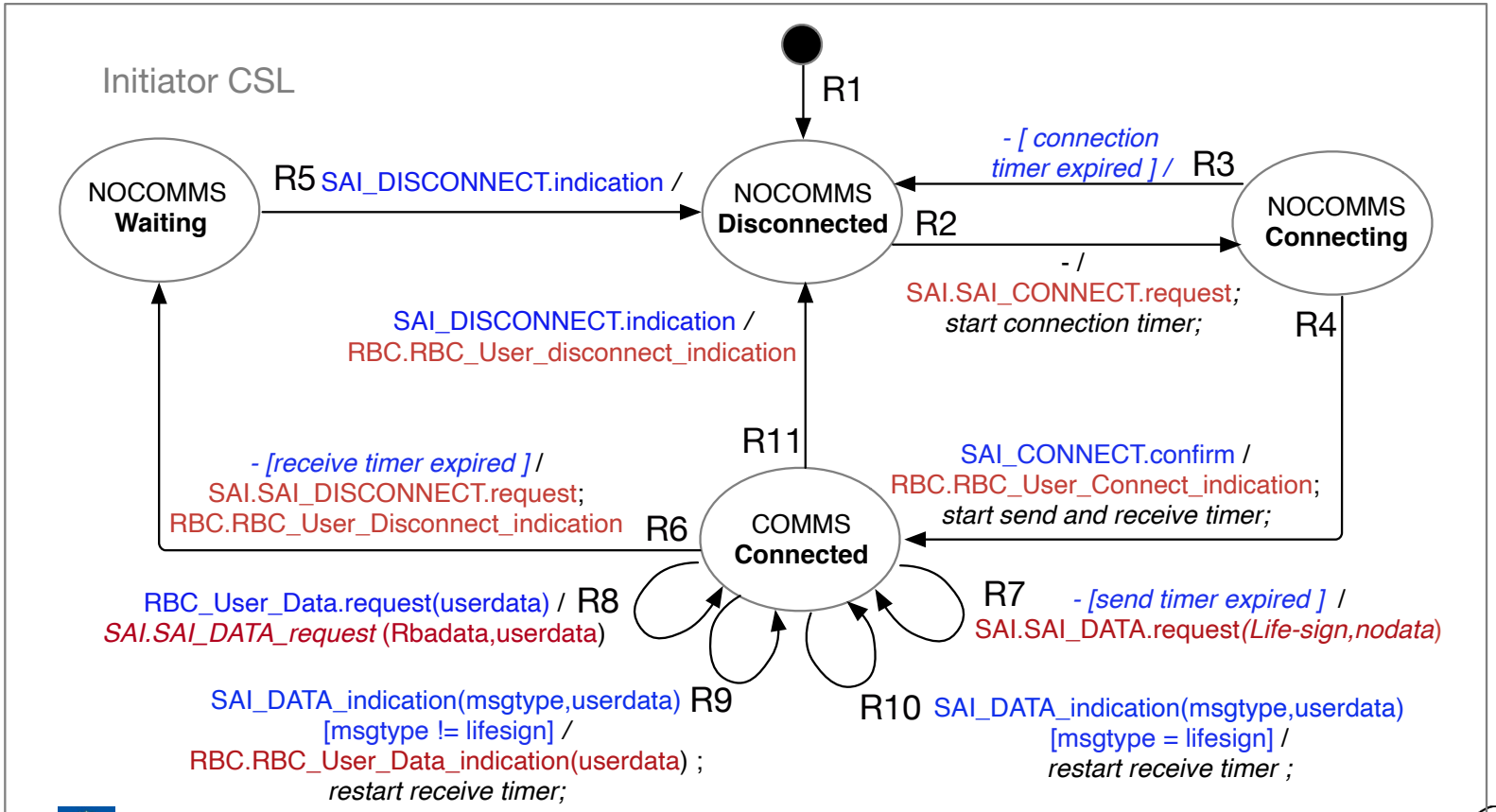
4SECURail: the case study (communications for RBC-RBC handover)



4SECURail: the approach of the demonstrator



4SECURail: semiformal modelling (freestyle UML)

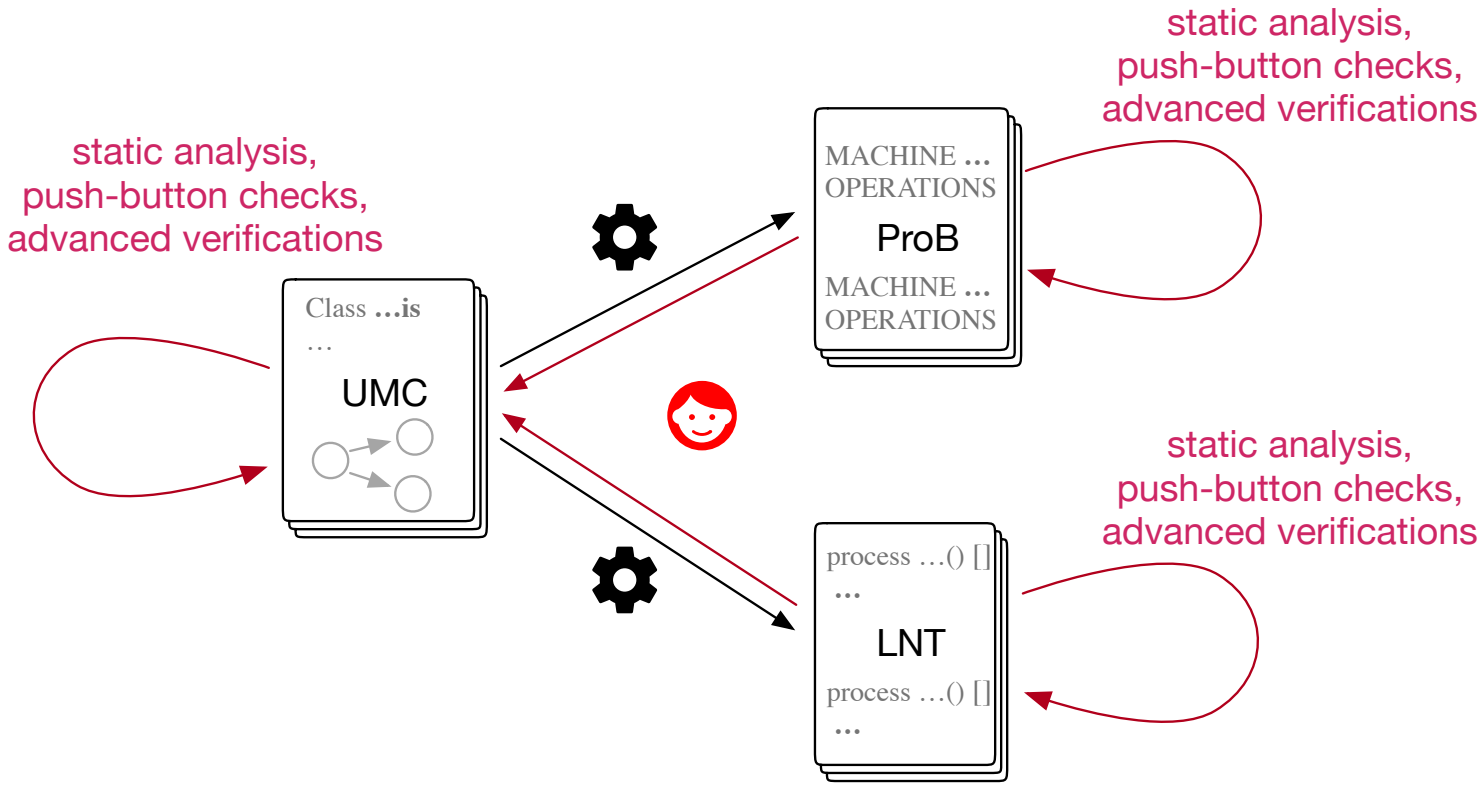


4SECURail: formal modelling and analysis

- Actually implementing freestyle fragments of the semiformal design

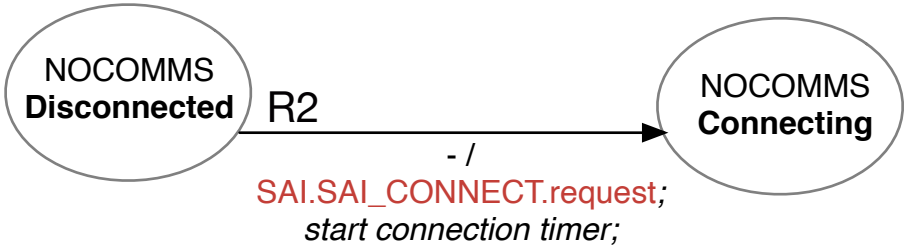
- Model checking of the resulting executable UML models, to detect:
    - introduced implementation errors
    - inconsistencies / missing points of the requirements
    - proofs of properties to be guaranteed

4SECURail: formal modelling and analysis



4SECURail: structured Natural Language requirements

- Based on the semiformal models for the control flow
- Abstracting the dataflow from the executable models

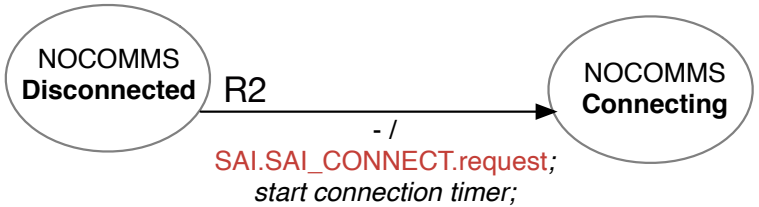


R2: When in *Disconnected* state, the inititor *CSL*
immediately sends a *SAI_CONNECT.request* to the *SAI* component,
starts a connTimer with the specified timeout,
and moves to the *Connecting* state.

4SECURail: more on formal modellling (1/4)

UMC used for the initial formal executable / verifiable system design

UMC is simple, direct textual notation for SysML / UML specification

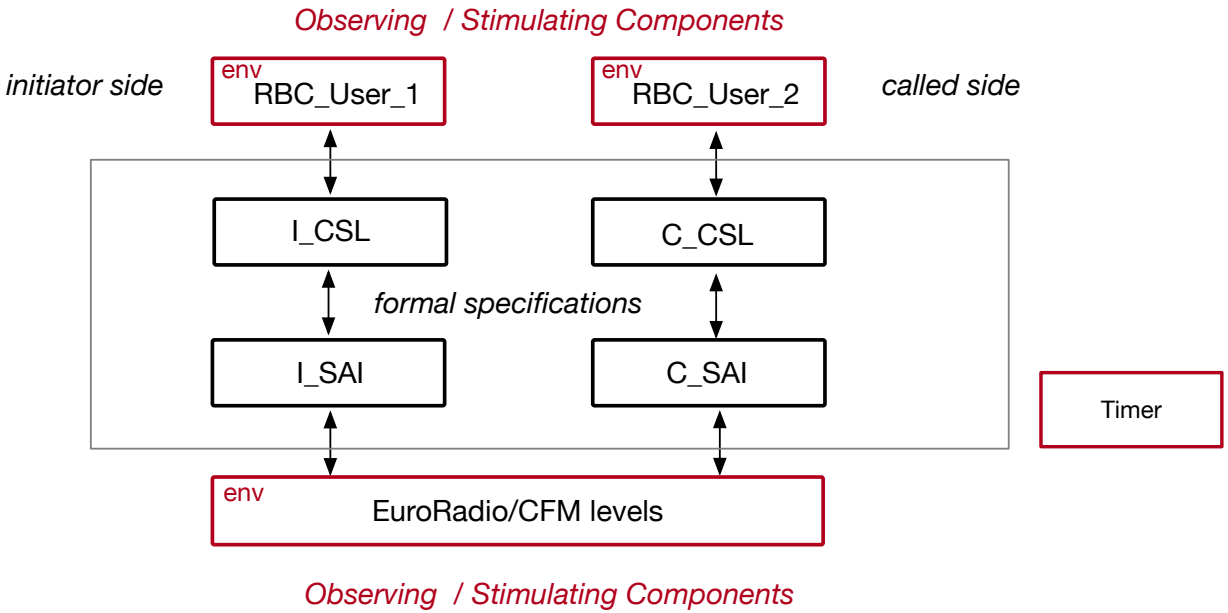



```
NOCOMMSdisconnected -> NOCOMMSconnecting
    { - / SAI.ISAI_CONNECT_request;
      connectTimer := 0; }
```

- Used an **extremely** limited UML subset,
  - with a very clear semantics
  - easy to translate into other formal notations

4SECURail: more on formal modellling (2/4)

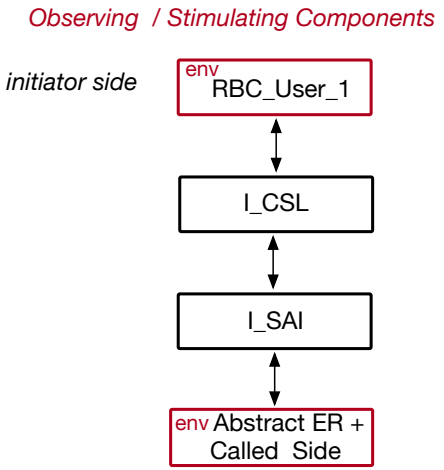
Specified CSL and SAI components to be complemented by necessary environment components



- Environment components still modelled as state machines

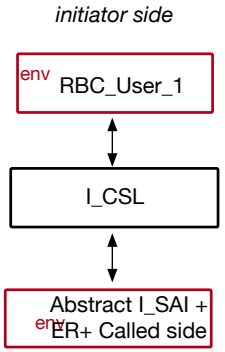
4SECURail: more on formal modellling (3/4)

Property-driven constructions of analysis scenarios (varying the environment)



All messages sent by the RBC are forwarded to the ER

connection_timeout = ..
send_timeout = ...
receive_timeout =..
...
...
...



The initiator CSL, when connected, continuously sends RBC messages or Lifesign messages

4SECURail: more on formal modellling (4/4)

Formal frameworks

- Not just UMC (academic research / teaching oriented tool)
  But also ProB and LNT + CADP (mature, industry ready)

- ProB / LNT models mechanically generated from UML / UMC

- Achieving formal methods diversity
  (robustness of the modelling)

- More complete static analysis,
  different verification techniques expoitable

4SECURail: results

Demonstrator results:

Artefacts: Better documentation for the developers
Semiformal designs, formal designs, natural language requirements
(more clear and rigorous than the initial ones)

Feedback: Detection of dangerous ambiguities in the initial requirements
(especially in the form of missing requirements and
hidden assumptions on the environment components)

4SECURail: Cost / Benefit analysis

Detailed, financial, economic Cost / Benefit analysis still in progress

Observed demonstrator Costs: licenses, training, effort

Observed demonstrator Benefits:

higher quality specs:

- easier to implement
- less prone to raise interoperability problems

4SECURail: references

- 4SECURail website: https://4securail.eu
- Final event (free registration!): https://www.4securail.eu/news-and-events.html

- D2.1 Rationale for demonstrator structure
- D2.3 Initial case study requirements definition
- D2.5 The Formal Methods demonstrator experiment

- D2.4 Preliminary CBA structure
- D2.6 Final CBA (due end of November 2021)

10.5281/zenodo.5541217 revised case study requirements
10.5281/zenodo.5541307 formal models and scenarios
10.5281/zenodo.5541350 model transformation tools

4SECURail

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 881775

Call identifier: H2020-S2RJU-2019
Topic: S2R-OC-IP2-01-2019 - Demonstrator development for the use of Formal Methods in railway environment and Support to implementation of CSIRT to the railway sector

Ardanuy
Moving innovation
Sirti building the future
hitrail european railway IT & data communications
uic
TREE TECHNOLOGY