4SECURail Workstream 1
Formal Methods Demonstrator (D2.5)

Franco Mazzanti & Dimitri Belli
ISTI-CNR

23-24/11/2021
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 competitiveness, dependability and efficiency

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

recognize the importance of formal analysis
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? (D2.5)
- Can their adoption be cost effective? How much? (D2.6)
4SECURail: Formal Methods in the Req. Definition

Classical Scenario

Informal Requirements

Rigorous Specification

Product

I.M. Infrastructures are Systems of Systems

RBC

IXL

LX

RBC-IXL

IXL-LX
4SECURail: The Case Study (communications for RBC-RBC handover)

**UNISIG Subset 026**
ETCS/ERTMS
Class 1 System Requirements Specification

**UNISIG Subset 039**
FIS for RBC/RBC Handover

- RBC Handover Transaction
- RBC/RBC Communication Supervision

**UNISIG Subset 098**
RBC-RBC Safe Communication Interface

- Safe Functional Module
- SAI Sublayer
- ER Safety Layer
- Communication Functional Module

**UNISIG Subset 037**
EuroRadio FIS

---

**Handling of Creation/Deletion of Safe Communication lines**

**Exchange of NRBC messages**

**4SECURail Case Study**

- Protection against Delay, Re-sequencing, Deletion, Repetition
- Protection against Corruption, Masquerade, Insertion
- Interface towards the EuroRadio OSI levels

---

**Handling over RBC**

RBC handover protocol (NRBC messages)

**Accepting RBC**

Border balise group

* Support of concurrent RBC/RBC Handover Transactions

* Handling of Creation/Deletion of Safe Communication lines

* Exchange of NRBC messages

---

**UNISIG Subset 039**
FIS for RBC/RBC Handover

---

**UNISIG Subset 098**
RBC-RBC Safe Communication Interface

---

**UNISIG Subset 037**
EuroRadio FIS

---

**UNISIG Subset 026**
ETCS/ERTMS
Class 1 System Requirements Specification
4SECURail: The Approach of the Demonstrator
4SECURail: The Approach of the Demonstrator

- **D2.3 Initial Natural Language Requirements**
  - **Natural Language Requirements revision**
  - **Abstract modelling**
    - Abstract, Semiformal SysML/UML Designs
    - Natural Language Requirements, Assumptions, Guarantees
  - **Executable modelling**
    - Detailed, Executable SysML/UML Designs
    - Formal Models + Formal Properties
  - **Formal modelling and analysis**
4SECURail: Abstract Modelling (freestyle UML)

Initiator CSL

- NOCOMMS Waiting
  - R5 SAI_DISCONNECT.indication /
  - SAI_DISCONNECT.indication /
  - RBC.RBC_User_disconnect_indication
  - [receive timer expired ] /
  - SAI.SAI_DISCONNECT.request;
  - RBC.RBC_User_Disconnect_indication
  - RBC_User_Data.request(userdata) /
  - SAI.SAI_DATA_request (Rbadata,userdata)
  - R8
  - SAI_DATA_indication(msgtype,userdata)
  - [msgtype != lifesign] /
  - RBC.RBC_User_Data_indication(userdata) ;
  - R9
  - R10 SAI_DATA_indication(msgtype,userdata)
  - [msgtype = lifesign] /
  - restart receive timer ;

- NOCOMMS Disconnected
  - R1
  - [connection timer expired ] /
  - R3
  - SAI.SAI_CONNECT.request;
  - start connection timer;

- NOCOMMS Connecting
  - R2
  - [send timer expired ] /
  - SAI.SAI_DATA.request(Life-sign,nodata)
  - R7
  - R4
  - SAI.CONNECT.confirm /
  - RBC.RBC_User_Connect_indication;
  - start send and receive timer;

- COMMS Connected
  - R6
  - R11

Diagram: State transitions and event triggers in the 4SECURail abstract modelling.
4SECURail: The Approach of the Demonstrator

D2.3 Initial Natural Language Requirements

Natural Language Requirements revision

Abstract modelling

Executable modelling

Formal modelling and analysis

modelling and analysis

Abstract, Semiformal SysML/UML Designs

Natural Language Requirements, Assumptions, Guarantees

Detailed, Executable SysML/UML Designs

Formal Models + Formal Properties
4SECURail: The Approach of the Demonstrator

- Abstract modelling
- Executable modelling
- Natural Language Requirements revision
- Formal modelling and analysis

- Abstract, Semiformal SysML/UML Designs
- Natural Language Requirements, Assumptions, Guarantees
- Detailed, Executable SysML/UML Designs
- Formal Models + Formal Properties
ProB encoding

MACHINE ...
VARIABLES

operation = 
PRE ..
END;

operation = 
PRE ..
END;

END

UMC encoding

Class .... Is
Signals ...
Vars ...
Transitions ...
end

Class .... Is
Signals ...
Vars ...
Transitions ...
end

Objects ...

LNT encoding

process P1 ...
end process

process P2 ...
end process

process Main ...
is par
 P1 ..
 || P2...
end par
## 4SECURail: Formal Modelling and Analysis (2)

<table>
<thead>
<tr>
<th>ProB</th>
<th>UMC</th>
<th>LNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Analysis</td>
<td>Static Analysis</td>
<td>Static Analysis</td>
</tr>
<tr>
<td>Reachability Properties</td>
<td>Reachability Properties</td>
<td>Reachability Properties</td>
</tr>
<tr>
<td>Statespace Stats</td>
<td>Statespace Stats</td>
<td>Statespace Stats</td>
</tr>
<tr>
<td>State Invariants</td>
<td>Deadlocks</td>
<td>Deadlocks</td>
</tr>
<tr>
<td>Deadlocks</td>
<td>Runtime Errors</td>
<td>LTLe Model Checking</td>
</tr>
<tr>
<td>LTLe Model Checking</td>
<td>UCTL Model Checking</td>
<td>CTLe Model Checking</td>
</tr>
<tr>
<td>CTLe Model Checking</td>
<td>(state/event based)</td>
<td>(event based)</td>
</tr>
<tr>
<td>...</td>
<td>Custom system observations</td>
<td>Compositional Verification</td>
</tr>
<tr>
<td></td>
<td>Explanations as Message</td>
<td>Strong/ Divbranching/</td>
</tr>
<tr>
<td></td>
<td>Sequence Diagrams</td>
<td>Sharp Minimazations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Powerful scripting language</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>
4SECURail: The Approach of the Demonstrator

- **Abstract modelling**
- **Executable modelling**
- **Formal modelling and analysis**

**D2.3 Initial Natural Language Requirements**

- **Natural Language Requirements revision**
- **Abstract, Semiformal SysML/UML Designs**
- **Natural Language Requirements, Assumptions, Guarantees**
- **Detailed, Executable SysML/UML Designs**
- **Formal Models + Formal Properties**
E.g. Requirements Specification for the *Initiator CSL* Component

**Configuration Parameters ..**
**External Interactions ...**
**External Guarantees ...**
**External Assumptions ...**
**Behavioral Requirements ...**

**E.g.**

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

**R3**: When in **Connecting** state the connTimer expires, the CSL moves to **Disconnected** state.

**R3**

\[
\text{NOCOMMS \_Connecting} \rightarrow \text{NOCOMMS \_Disconnected}
\]

\[
\text{\{ } \text{icsl\_tick \{connectTimer = max\_connectTimer \} / Timer.ok\_icsl \} }
\]
4SECURail: The Demonstrator Results

modelling and analysis

Abstract modelling

Natural Language Requirements revision

Executable modelling

Formal modelling and analysis

Abstract, Semiformal SysML/UML Designs

Natural Language Requirements, Assumptions, Guarantees

Detailed, Executable SysML/UML Designs

Formal Models + Formal Properties
4SECURail: Demonstrator Results

- Abstract UML Designs, Executable UML Designs Revised Natural Language Requirements allow to generate higher quality System Requirements Specifications

- Formal Analysis allows to improve confidence on the correctness of the models for the various components, and of their interoperability.

- Several ambiguities/missing points in the initial requirements have been found.

- Several implementation errors in the executable UML design has been detected by formal analysis.
• The UML subset used in the demonstrator is extremely constrained. How far can this subset be extended, still preserving its clarity, rigor, and easiness of translation towards different formal notations?

• The UMC notation has been mechanically translated into ProB and LNT. Would it be worthwhile to experiment other translations (towards mCRL2, nuXmv, HLL)?

• The mechanical generation of formal models started from the UMC notation. Would it be worthwhile to implement translations from commercial XMI formats (PTC, SPARX-EA, Magic Draw, Raphsody, ...)?

• It is common to find efforts in passing from Natural Language Requirements to Formal Models. Would it be worthwhile the investigate better the viceversa, i.e. «Explainable Formal Models»?
4SECURail: Demonstrator References

- 4SECURail website:  https://4securail.eu

- D2.1 Rationale for demonstrator structure
  https://www.4securail.eu/pdf/4SR-WP2-D2.1-Specification%20of%20formal%20development%20demonstrator-CNR-1.0.pdf

- D2.3 Initial case study requirements definition
  https://www.4securail.eu/pdf/4SR-WP2-D2.3-Case-study-requirements-and-specification-SIRTI-1.0.pdf

- D2.5 The Formal Methods demonstrator experiment

10.5281/zenodo.5541217 revised case study requirements
10.5281/zenodo.5541307 formal models and scenarios
10.5281/zenodo.5541350 model transformation tools
4SECURail: Feedback asked!!!

Please use this survey to evaluate the methodology proposed within the 4SECURail formal method demonstrator. The survey takes less than 5 minutes and all responses are treated anonymously.

Please feed the survey your early impressions:

- is the presented methodology applicable?
- is the presented methodology useful?
- is the presented methodology cost effective?
- is the presented methodology sufficiently mature?

https://tinyurl.com/faer5udc
4SECURail Workstream 1
Cost Benefits Analysis  (D2.6)

Carlo Vaghi
FIT Consulting

23-24/11/2021
Cost-Benefit Analysis in 4SECURAIL

The main objective of 4SECURail WP2 is to experiment a demonstrator of state-of-the-art Formal Methods (FM), evaluate the learning curve and perform a Cost/Benefit Analysis of the adoption of Formal Methods in railway industry.

The Cost-Benefit Analysis (CBA) is due to:

• Select a case study of railway signalling system, due to represent a reference case of formal specification, and for the estimation of benefits from FM use
• Set-up a business case based on the point of view of Infrastructure Managers (IMs), selecting a set of formal tools/methods that can be applied for achieving a rigorous formal specification of the selected systems
• Evaluate costs, benefits and suitable learning curves for the selected approach.
• Identify the economic and societal impact of the implementation of FM against the Baseline Scenario, represented by standard interfaces developed with no use of FM.
4SECURail tackles the adoption of Formal Methods by developing a demonstrator on:

Requirements definition of a railway signalling subsystem

A case study, on which the formal demonstrator prototype is applied, is used to assess costs and benefits of its application.

The definition of the subsystem will include the evaluation of hazards and safety requirements.

The definition of the subsystem will be given by means of standard interfaces.

The identified subsystem is the RBC/RBC handover interface as specified in SUBSET-039 and SUBSET-098 by UNISIG.

[Source: UNISIG SUBSET-039]
4SECURail demonstrator - case study rationale

RBC/RBC interface:

• is a typical product where development processes of different suppliers meet
• is useful to investigate interoperability issues implied by natural language ambiguities
• already supports well established railway operational modes
• offers good opportunities to translate safety related requirements into formally verifiable properties
• is explicitly finalised to connect systems from different suppliers
• offers a reference case for the estimation of formal methods benefits
• more relevant and also more accessible for evaluation than other interfaces (e.g. interface between Interlocking and field objects), the implementation of which is usually proprietary
Stakeholders of the CBA

In line with 4SECURail approach, the CBA is developed from the point of view of the IM. However, the CBA need to include in the picture also stakeholders connected with IMs actions:

- Relevant costs and benefits for IMs (additional against the baseline scenario) have to be assessed.
- IMs provide resources to EULYNX (or any follow-up), by which the definition of “Standard Interface” (SI) in 4SECURail is inspired.
- The role of suppliers is relevant too: additional costs, or benefits in terms of shorter time needed for SW development, are reflected in the price paid by IMs to purchase RBC (of which RBC/RBC interface is a key component).
- Users, i.e. passengers of train services, are included in the chart since they would benefit from the lower probability of service disruption = improved service quality.
- CBA also investigates potential benefits for the society, e.g. in terms of lower accident risks.
The Business Case

A **tender based Business Case** was developed, to properly nest the role of the case study into a rail SW development process, triggered by one IM through a tender. The business case is inspired by X2RAIL-2 business model “Semi-formal methods development”, with some modifications. In 4SECURAIL business case:

a. IM develops the systems with **interoperable Standardised Interfaces**, developed with the use of FM. The formal model is derived from a semi-formal model of the system and associated test cases

b. The IM verifies safety and functional requirements on the formal model

c. **Tender specifications and tender details (for SW supply)** are developed by the IM

d. “Multi-supplier” mode: the same tender specifications are released to many competitor suppliers

e. “Assessors” perform V&V, which costs are borne by suppliers in the “multi-supplier” mode

f. Every change requests triggers the implementation of a new tender
The business case – the «Tender model»

A change request is an update of the system due to:
- New interoperability features (e.g. new ERTMS release)
- New on-board or ground system interfaces
- Other new features

Change requests are implemented through new tenders issued by IMs, facilitated by the adoption of FM

→ Less dependence from a single long-term supplier
Cost and benefit categories

Identification of relevant categories of costs and benefits for the CBA:

Economic items for which a difference between Baseline and FM scenarios is likely occurring, with relevant measurement units

Assumption: savings in development costs fully contribute to reduce SW purchase price

<table>
<thead>
<tr>
<th>Cost/Benefit Item</th>
<th>Meas. unit</th>
<th>Monetary meas unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;EULYNX follow-up&quot; - Costs to issue new guidelines for using FM</td>
<td>Person-days</td>
<td>€/day</td>
</tr>
<tr>
<td>Costs for the definition of SI using issued guidelines</td>
<td>Person-days</td>
<td>€/day</td>
</tr>
<tr>
<td>RBC (or similar device) Purchase price</td>
<td>€/software/year</td>
<td></td>
</tr>
<tr>
<td>Training costs</td>
<td>€/day</td>
<td></td>
</tr>
<tr>
<td>Savings in SW management/assistance</td>
<td>€/day</td>
<td></td>
</tr>
<tr>
<td>Lower development time</td>
<td>€/day</td>
<td></td>
</tr>
<tr>
<td>Learning / personnel training costs</td>
<td>Person-days (2-4)</td>
<td>€/day</td>
</tr>
<tr>
<td>Time to define requirements for RBC/RBC interface supply through FM</td>
<td>Person-days</td>
<td>€/day</td>
</tr>
<tr>
<td>SW Licenses for requirements development through FM</td>
<td>€/software/year</td>
<td></td>
</tr>
<tr>
<td>Costs for RBC acceptance, verification and validation</td>
<td>Person-days</td>
<td>€/day</td>
</tr>
<tr>
<td>Higher maintenance efficiency</td>
<td>Replacement costs</td>
<td>€/year</td>
</tr>
<tr>
<td>Higher availability in case of service disruption (lower penalties from service contracts)</td>
<td># service disruptions/year (prob.)</td>
<td>€/day penalty</td>
</tr>
<tr>
<td>Lower service disruptions</td>
<td># hours saved by users</td>
<td>€/pax*hour</td>
</tr>
<tr>
<td>Lower accident risks</td>
<td>Accidents/year</td>
<td>€/accident (external costs)</td>
</tr>
</tbody>
</table>
The assessment of costs and benefits

The quantitative assessment of costs and benefits is the basis for the calculation of the feasibility and convenience indicators that constitute the outcome of the CBA. Assigning values to the cost and benefit categories is a complex activity, requiring a detailed analysis of different sources. Main barriers:

- Availability of comparable Baseline and Project scenarios, respectively characterised by non-use and use of FM in the development of railway safety components, or railway sector
- Availability of comparable case studies and quantitative information about their results
- Lack of a fully-fledged CBA in FM domain
- Data confidentiality issued by SW developers
- Rather low diffusion of FM adoption cases endowed by quantitative comparisons with the reference scenarios.
Key literature references on FM (FM applications in industry and railway sector) was reviewed:

- 29 relevant records (project reports, scientific papers, surveys, etc.), of which
  - 8 records only include quantitative assessment of costs and benefits

Main outcome:
- FM provide significant benefits in terms of **improved safety**, **requirement quality and reliability**, **reduced time-to-market / cost** (qualitative)
- The 2020 FM survey (Garavel et al.): all experts agree that the improvement of “**system safety**” is one of the main benefits connected to the use of FM, followed by the improvement of SW quality, enhanced cybersecurity, easier certification and easier maintenance. Experts were doubtful about the FM impact in decreasing the cost of SW development
- X2RAIL-2 guesswork estimations:
  - The number of new software releases due to change requests is reduced by 50%.
  - The time to develop software and perform V&V is reduced by 40%.
  - The cost to develop software and perform V&V is reduced by 25%.
Expert survey – main results

In the 1st 4SECURail WP2 workshop (June 2020), some open questions were debated, with a pairwise comparison exercise.

Experts gave some interesting indications, although very few quantitative data:

• Mixed conclusions on relative relevance of cost and benefit categories
• Relevant differences on relevance of RBC purchase price and Lower accident risks
• Cost baseline for the case study: we must rely on baseline available for RBC cost, but not for the RBC/RBC interface (not available as a market price)
Expert survey – main results

Some experts tried to quantitatively assess the differentials between project and Baseline scenario, by cost/benefit item. Range results are controversial

<table>
<thead>
<tr>
<th>Cost-Benefit category</th>
<th>+/- Δ%</th>
<th>+/- Δ%</th>
</tr>
</thead>
<tbody>
<tr>
<td>RBC (or similar device) Purchase price</td>
<td>-5%</td>
<td>+ 10%</td>
</tr>
<tr>
<td>Learning / personnel training costs</td>
<td>-5%</td>
<td>Initially +20% later +/- 0%.</td>
</tr>
<tr>
<td>Time to define requirements for RBC/RBC interface supply through FM</td>
<td>-15% (lower time)</td>
<td>Initially +50% later +/- 0%</td>
</tr>
<tr>
<td>SW Licenses for requirements development through FM</td>
<td>-10%</td>
<td>Depends on tools already used.</td>
</tr>
<tr>
<td>Costs for RBC acceptance, verification and validation</td>
<td>+15%</td>
<td>Acceptance test: 0% V&amp;V-related test: -10%.</td>
</tr>
<tr>
<td>Higher availability in case of service disruption (# service disruptions/year)</td>
<td>+5%</td>
<td>Most likely 0% (random HW failure are not affected by FM), Up to -10% in mass transport UCs</td>
</tr>
<tr>
<td>Higher maintenance efficiency (Lower replacement costs)</td>
<td>+5%</td>
<td>0%</td>
</tr>
<tr>
<td>Lower accident risks</td>
<td>-2%</td>
<td>-5%</td>
</tr>
</tbody>
</table>
Cost and benefit estimation

Learning and tender specification development costs

- Detailed assessment of time-related effort deployed by the IM to learn FM and develop specifications with FM, as observed in the demonstrator (D2.5): 50 requirements excluding 10 non-functional requirements and 12 requirements related to non modelled configuration options.

**LEARNING: Time Required for:**
- Design Language learning
- Design Tools learning
- Formal Modelling Language learning
- Formal Verification Language learning
- Formal verification tool learning

**SPECIFICATION DESIGN:***
- Design
- Debugging
- Formal Modelling
- Tracing the design
- Tracing the Formal Model
- Specifying properties
- Verify properties
- Debug the Formal Model

Demonstrator effort: **1,3 person-month**
«General case»: **2,6 person-month**

Baseline: **2,0 person-month**

Demonstrator effort: **7,0 person-month**
Learning and specification development costs - Assumptions

- Learning costs are borne by IM as CAPEX every 5 years (staff turnover assumed)
- Need to hire “newly skilled” in FM staff (junior-trainees) to side senior engineers
  → 3 staff are deployed to develop specifications through FM in the tendering business model
- Change requests require new tender details. Such specifications are developed with a lower effort (4,0 PM)
- Full staff capacity exploitation scenario: 1 new tender specification + 4 change requests developed per year
- SW licenses costs: assumed 2 “perpetual” licenses (SPARX), renewed every 5 years: 1800 €
Cost and benefit estimation

Savings in SW development and V&V

- Time and costs saved for developing RBC-RBC interface (or case studies having similar complexity) vs Baseline scenario (interface developed without FM-tender specification)

<table>
<thead>
<tr>
<th>Time/cost category</th>
<th>Baseline</th>
<th>+/- Δ</th>
</tr>
</thead>
<tbody>
<tr>
<td>RBC-RBC Interface development</td>
<td>12 PM</td>
<td>-20%</td>
</tr>
<tr>
<td>V&amp;V effort</td>
<td>2-3 PM</td>
<td>-20%</td>
</tr>
<tr>
<td>V&amp;V Assessor costs</td>
<td>6000 €</td>
<td>-3000 €</td>
</tr>
</tbody>
</table>

- What is the business scale for which the higher effort borne by IM is balanced by savings in the development of the interface?

- How much should suppliers save in interface development due to change request to ensure a competitive purchase price (i.e. lower than higher CAPEX and OPEX borne by the IM), over years?
Cost and benefit estimation

- Scenario: 1 tender specification + 4 change requests issued by IM and developed by supplier per year

The break-even between additional costs borne by IM and savings is verified, according to 4SECURail demonstrator input, if the purchase price of SW upon change requests is -40% vs. the baseline.
Cost and benefit estimation

- **Learning curve effects**: scenarios assuming a higher FM learning degree among EU-27 IMs are possible. However, expert survey suggest that the cost decrease due to learning curve would be less intense after the beginning, since “standard” specifications will be more and more customized by IM when defining tender requirements.

- **Higher safety**: the quantitative assessment of lower safety effects with degraded mode (not SIL4) assumed when a component of a safety critical system is unavailable, are hard to predict due to lack of benchmark. However, safety benefits are qualitatively verified since FM decrease the probability of degraded mode running.
Cost and benefit estimation

- **Benefits for rail users**: benefits due to higher maintenance efficiency, higher service availability and time saved for lower probability of service disruption. **However**, service disruptions due to ambiguity of specifications are very rare according to 4SECURail Consortium’s knowledge (0.1% of total cases).

→ Some possible scenarios (two Italian lines), and orders of magnitude of benefits in case cancellations or delays are avoided due to higher maintenance efficiency generated by FM:

- Regional line interruption (one day)
- HS line interruption (one day)
- Regional line trains delay (60’ all day)
- HS line train delay (60’ all day)

**Calculation of penalties IM→RU**
(RFI Performance Regime assumed)

**Delays for passengers**
(EU average VoT for pax categories, from EU HECT)
Costs and benefit estimation

- Costs
- Purchase price savings
- Penalties avoided
- Time saved by passengers

Case-avoided delay 60'-regional

Case-avoided delay 60'-HS

41
Cost and benefit estimation - conclusions

- The CBA has allowed streamlining a micro, bottom-up case based on the point of view of one IM. However, in the case of railway signalling standards, efforts and costs for formal analysis of the system requirements are likely not be distributed among the various entities supporting the standard itself, and not to a single IM.

- Benefits are spread over the entire supply chain, including suppliers, if economies of scale in SW development and the learning curve (i.e. progress in learning FM) are activated among IMs and suppliers.

- The “multi-supplier” mode enabled by FM is likely generating time and cost savings for rail safety industry.

- Benefits for users and society are sensible but hard to quantify, if not by making (realistic) assumptions on the higher maintenance efficiency generated by IMs.