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

Franco Mazzanti & Dimitri Belli
ISTI-CNR

23-24/11/2021

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

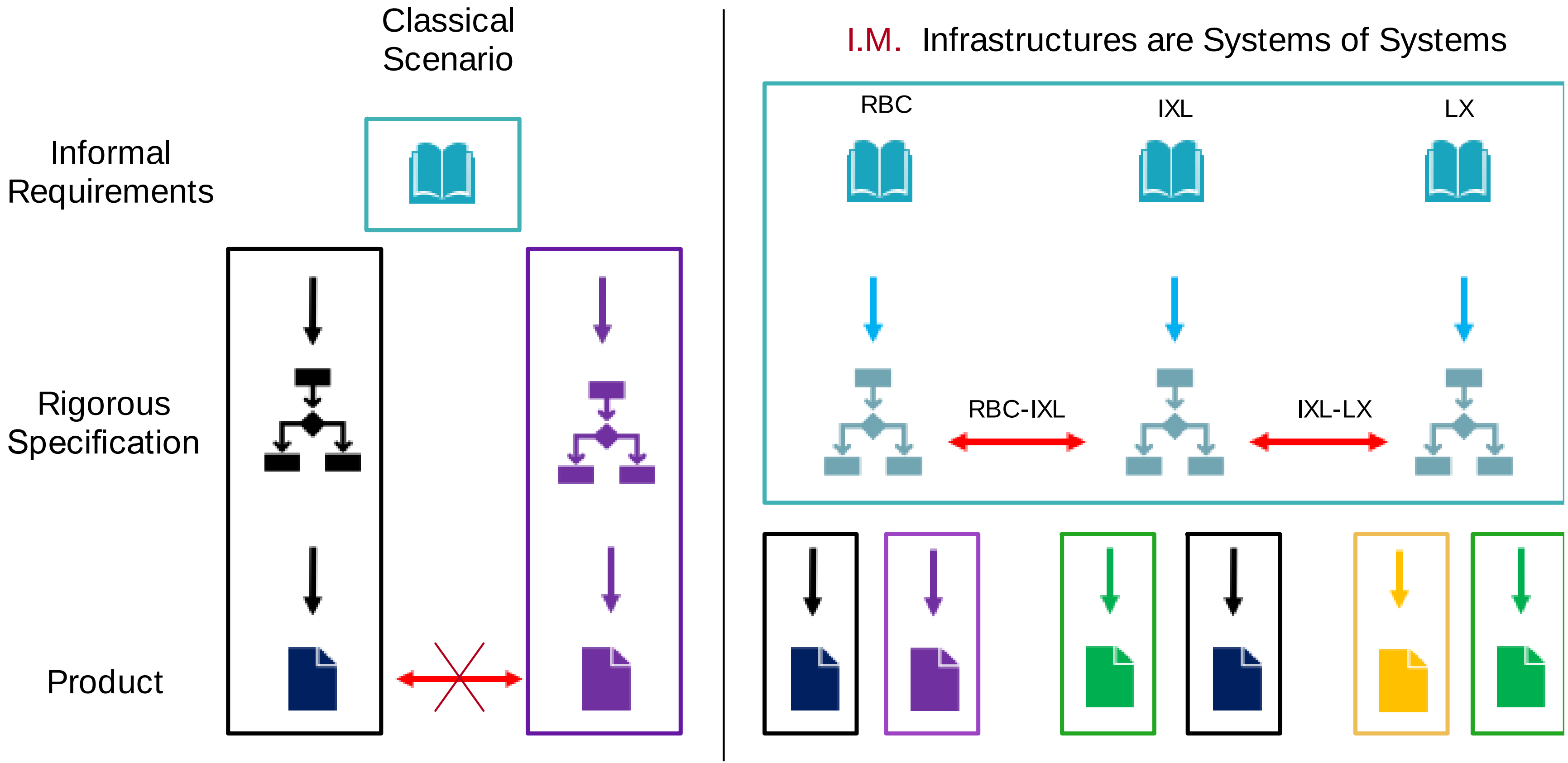
4SECURail: The Demonstrator

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****?* *(D2.5)*

- *Can their adoption be cost effective?* ***How much****?* *(D2.6)*

4SECURail: Formal Methods in the Req. Definition



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

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

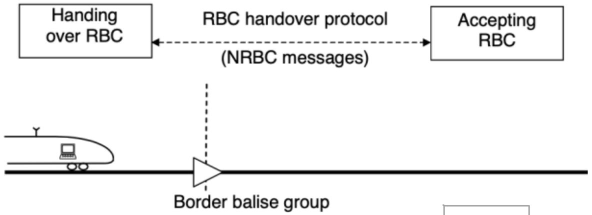
UNISIG Subset 039 — FIS for RBC/RBC Handover

- **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



** Support of concurrent RBC/RBC Handover Transactions* — RBC User

** Handling of Creation/Deletion of Safe Communication lines*
** Exchange of NRBC messages* — CSL

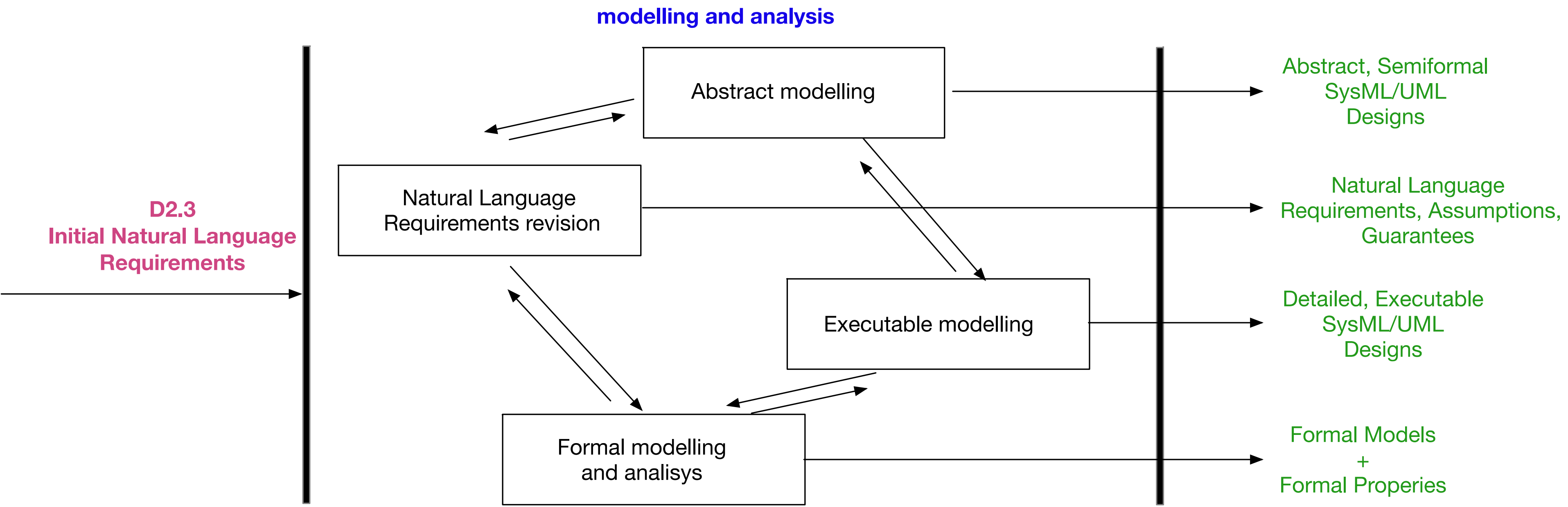
4SECURail Case Study

** Protection agains Delay, Re-sequencing, Deletion, Repetion* — SAI

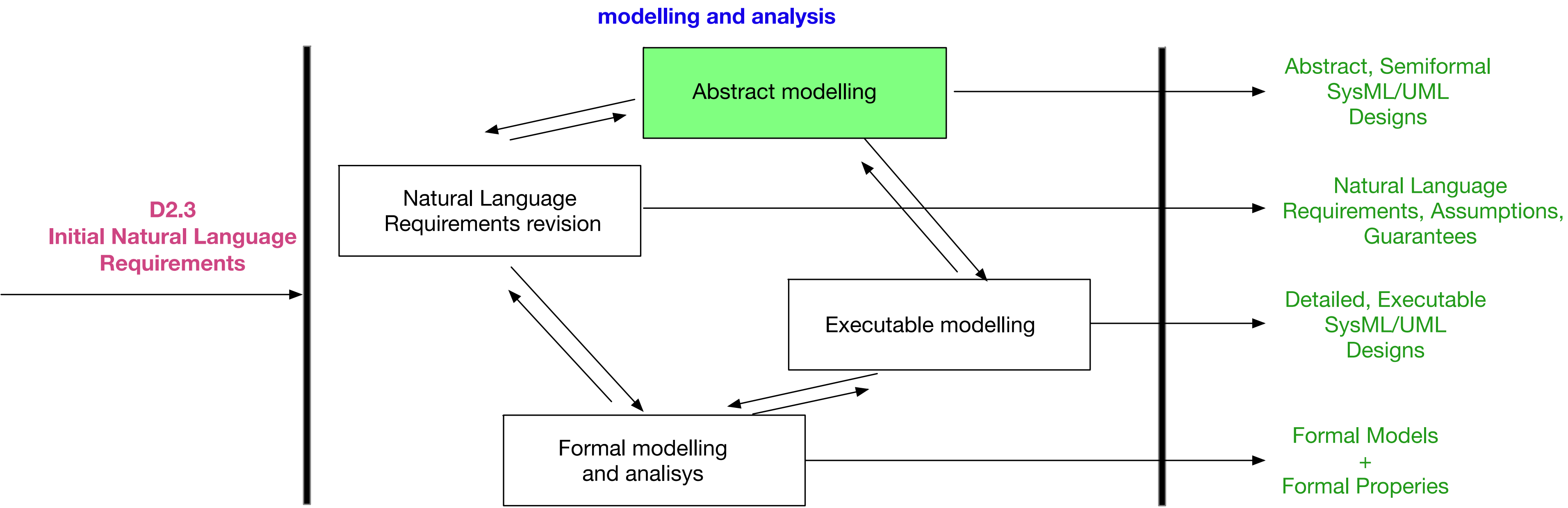
** Protection agains Corruption, Masquerare, Insertion* — ER

** Interface towards the EuroRadio OSI levels*

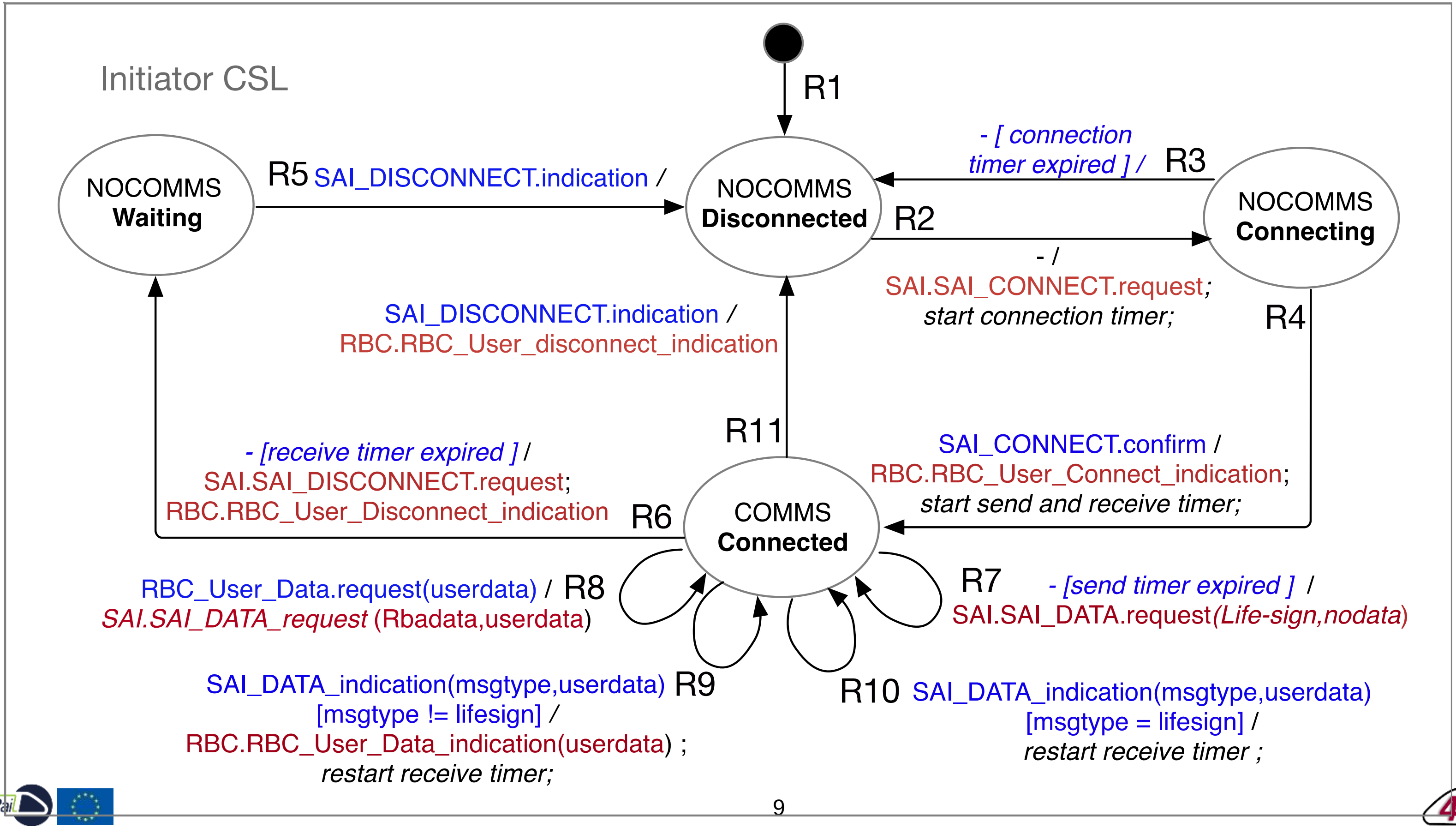
4SECURail: The Approach of the Demonstrator



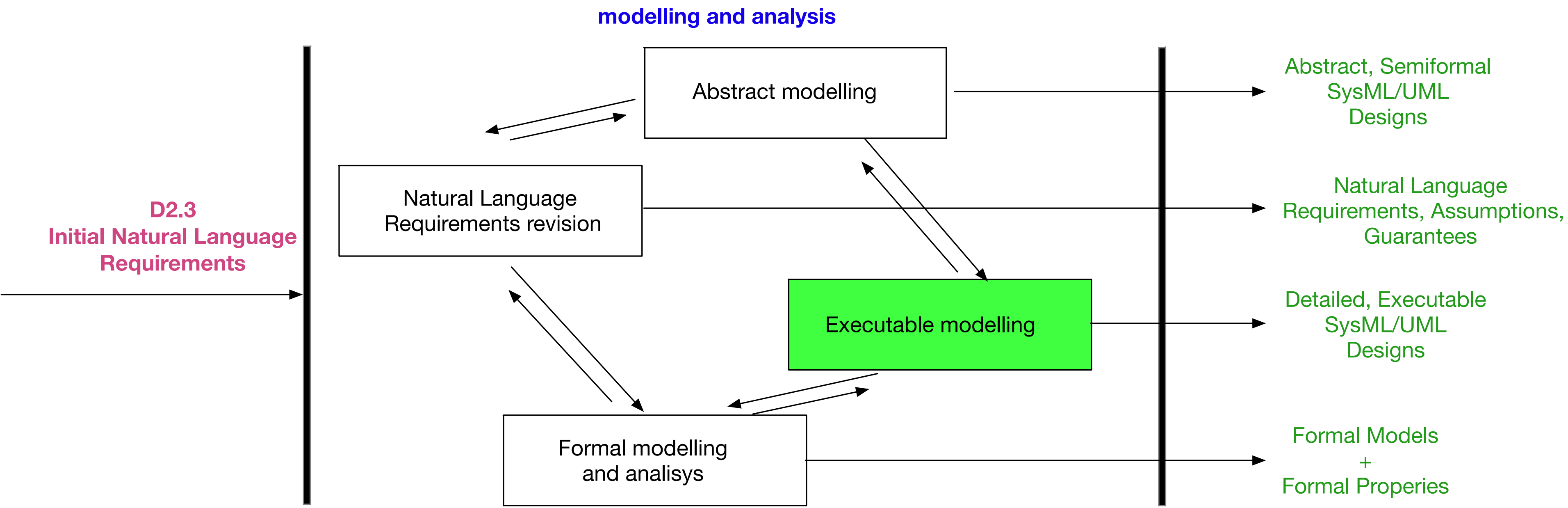
4SECURail: The Approach of the Demonstrator



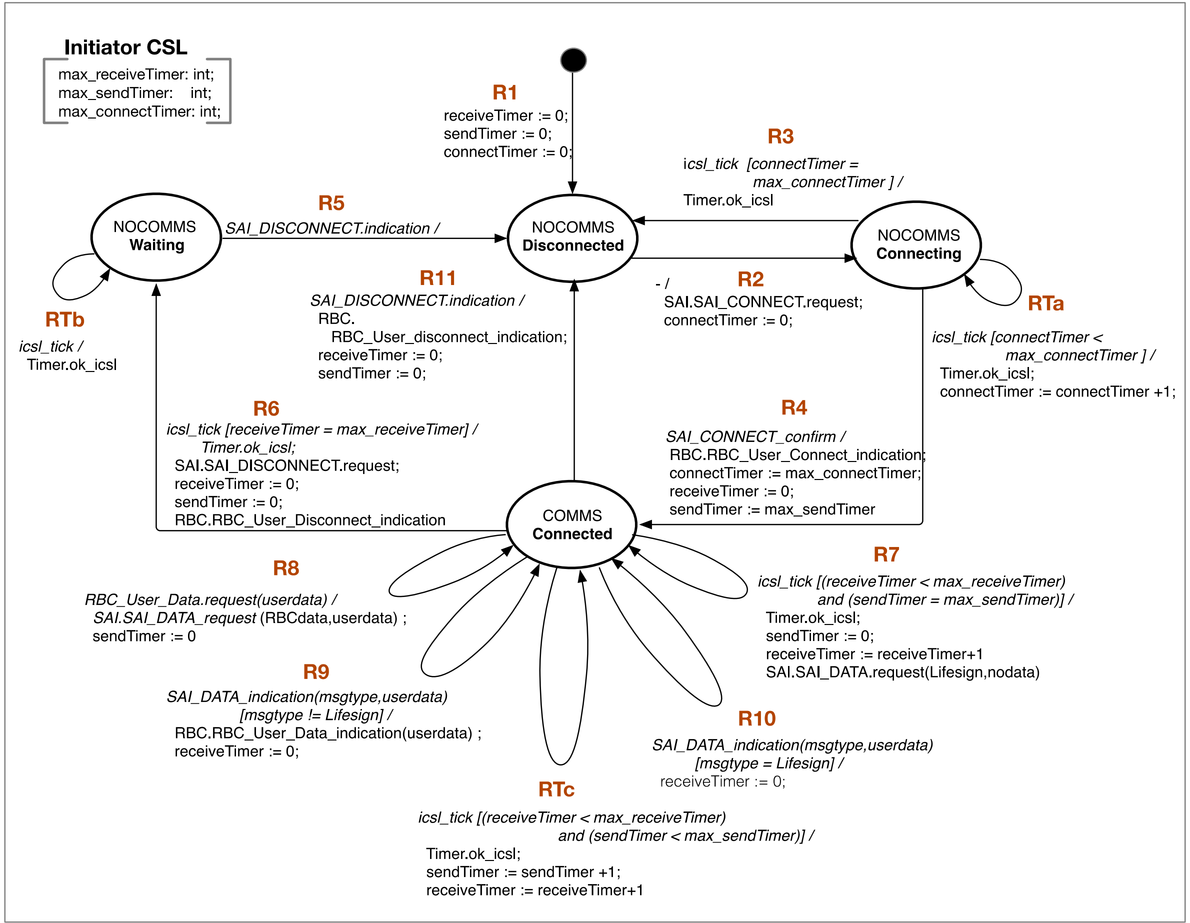
4SECURail: Abstract Modelling (freestyle UML)



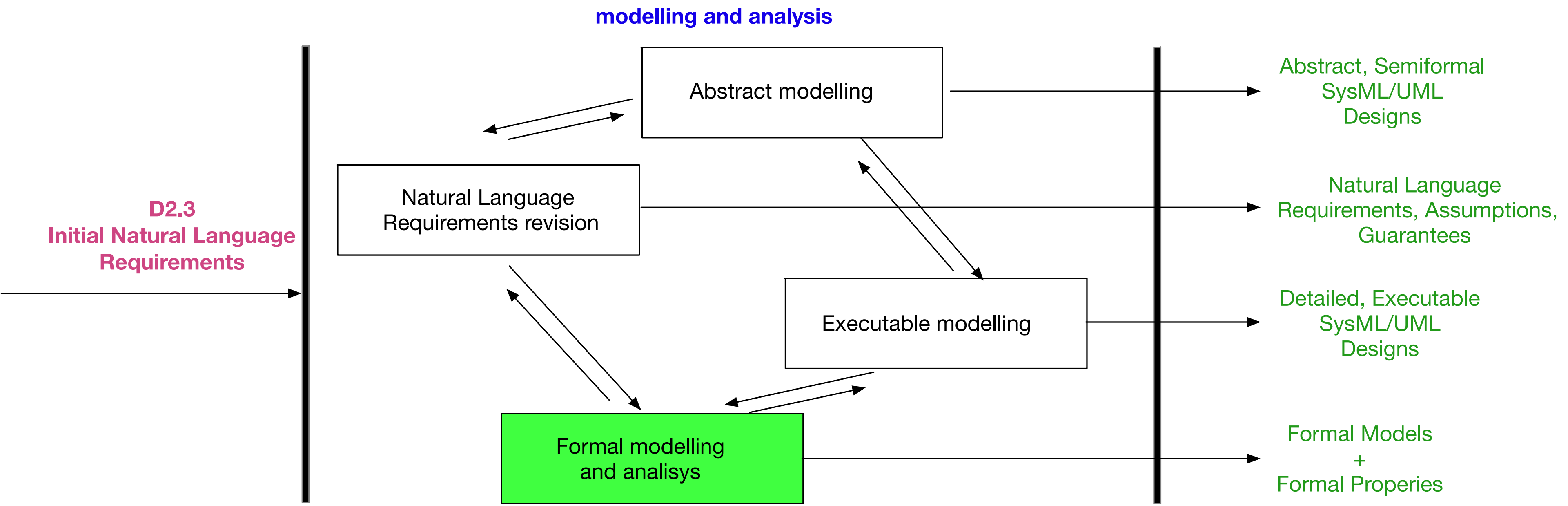
4SECURail: The Approach of the Demonstrator



4SECURail: Executable UML Modelling



4SECURail: The Approach of the Demonstrator



4SECURail: Formal Modelling and Analysis (1)

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)

ProB

- Static Analysis
- Reachability Properties
- Statespace Stats
- State Invariants
- Deadlocks
- LTLe Model Checking
- CTLe Model Checking
- ...

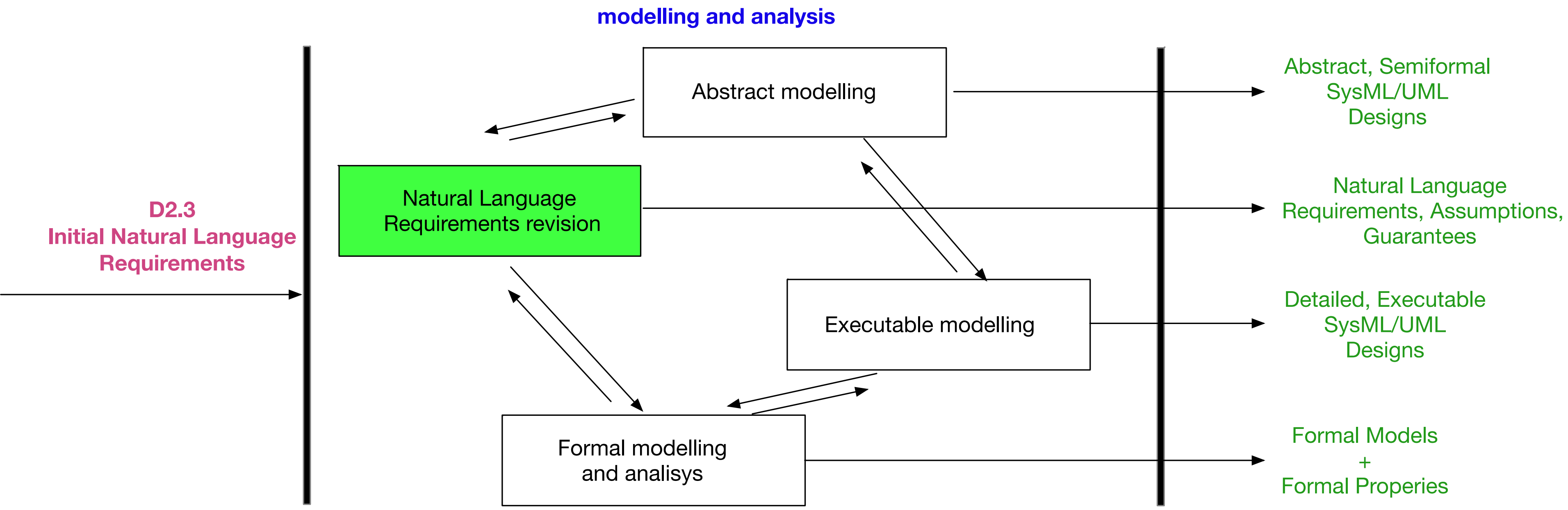
UMC

- Static Analysis
- Reachability Properties
- System Traces Minimization
- Statespace Stats
- Deadlocks
- Runtime Errors
- UCTL Model Checking (state/event based)
- Custom system observations
- Explanations as Message Sequence Diagrams

LNT

- Static Analysis
- Reachability Properties
- Statespace Stats
- Deadlocks
- MCL Model Checking (event based)
- Compositional Verification
- Strong/ Divbranching/ Sharp Minimazations
- Powerful scripting language
- ...

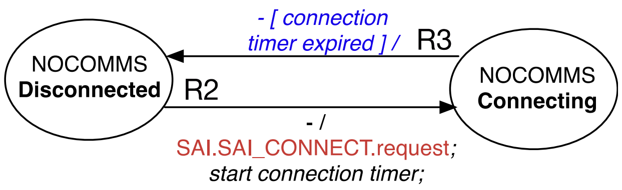
4SECURail: The Approach of the Demonstrator



4SECURail: Natural Language requirements revision

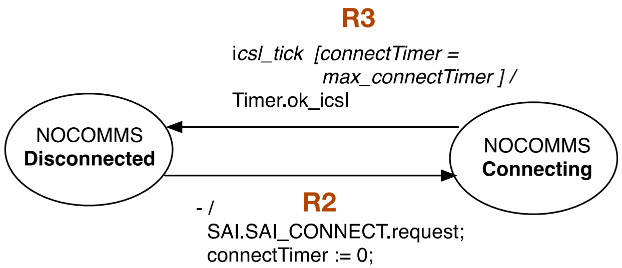
E.g. Requirements Specification for the ***Initiator CSL*** Component

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.

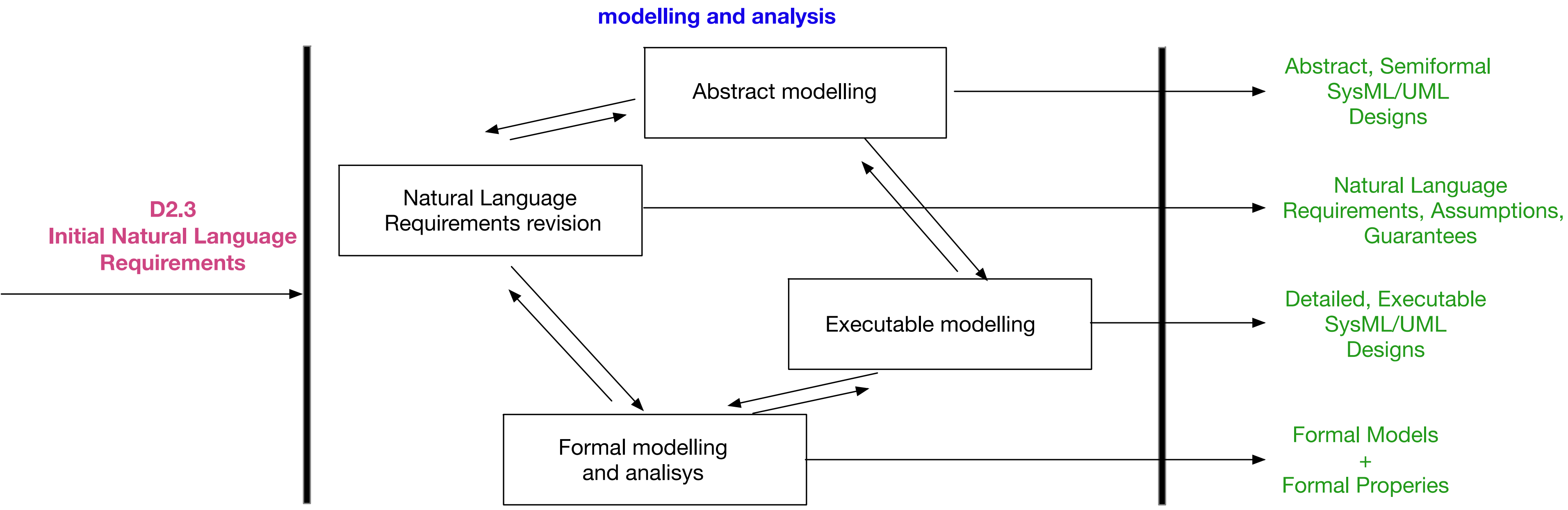


R3: When in Connecting state the connTimer expires, the CSL moves to Disconnected state.

...

R3_ICSL:
NOCOMMS_Connecting -> NOCOMMS_Disconnected
{ *icsl_tick [connectTimer = max_connectTimer*] /
Timer.ok_icsl }

4SECURail: The Demonstrator Results



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.

4SECURail: Further works ...

- 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

  https://www.4securail.eu/pdf/4SR-WP2-D2.5-Formal-development-demonstrator-prototype.final-release-CNR-1.0.pdf

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.

<u>The Cost-Benefit Analysis (CBA) is due to</u>:

- 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 demonstrator - selected case study

4SECURail tackles the adoption of Formal Methods by developing a demonstrator on:

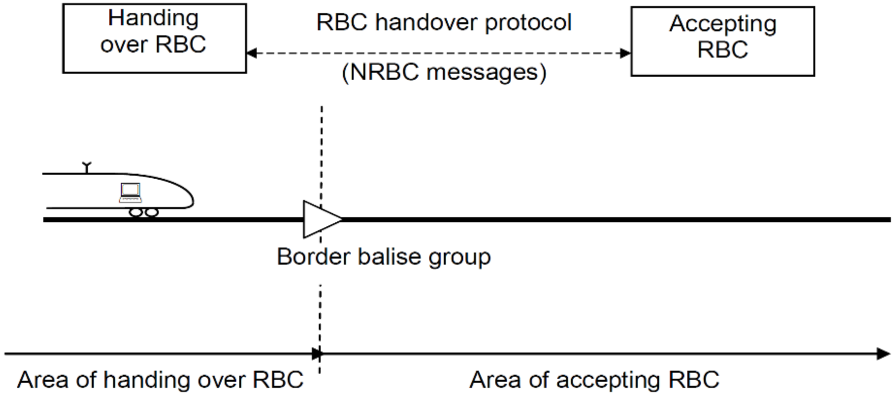
Requirements definition of a railway signalling subsystem

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:

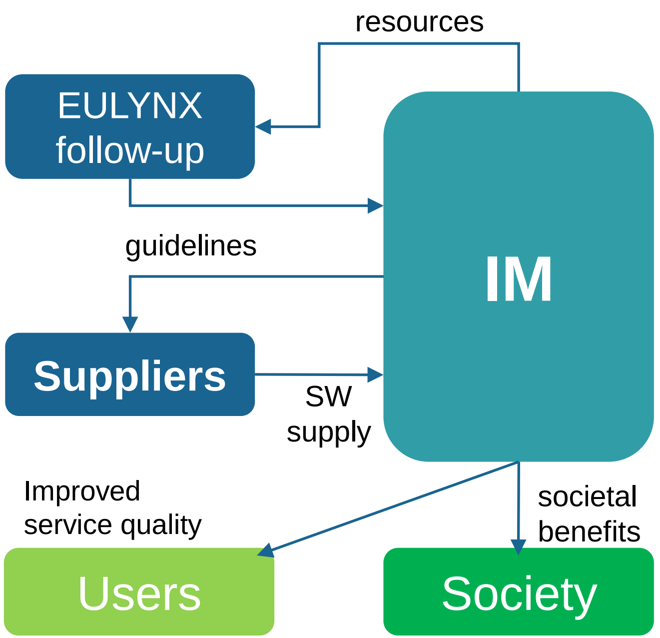
- is a typical product where development processes of **different suppliers** meet
- is useful to investigate **interoperability** issues implied by **natural language ambiguities**
- already supports **well established** railway operational modes
- offers good opportunities to translate **safety related** 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 <u>the point of view of the IM.</u> 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.



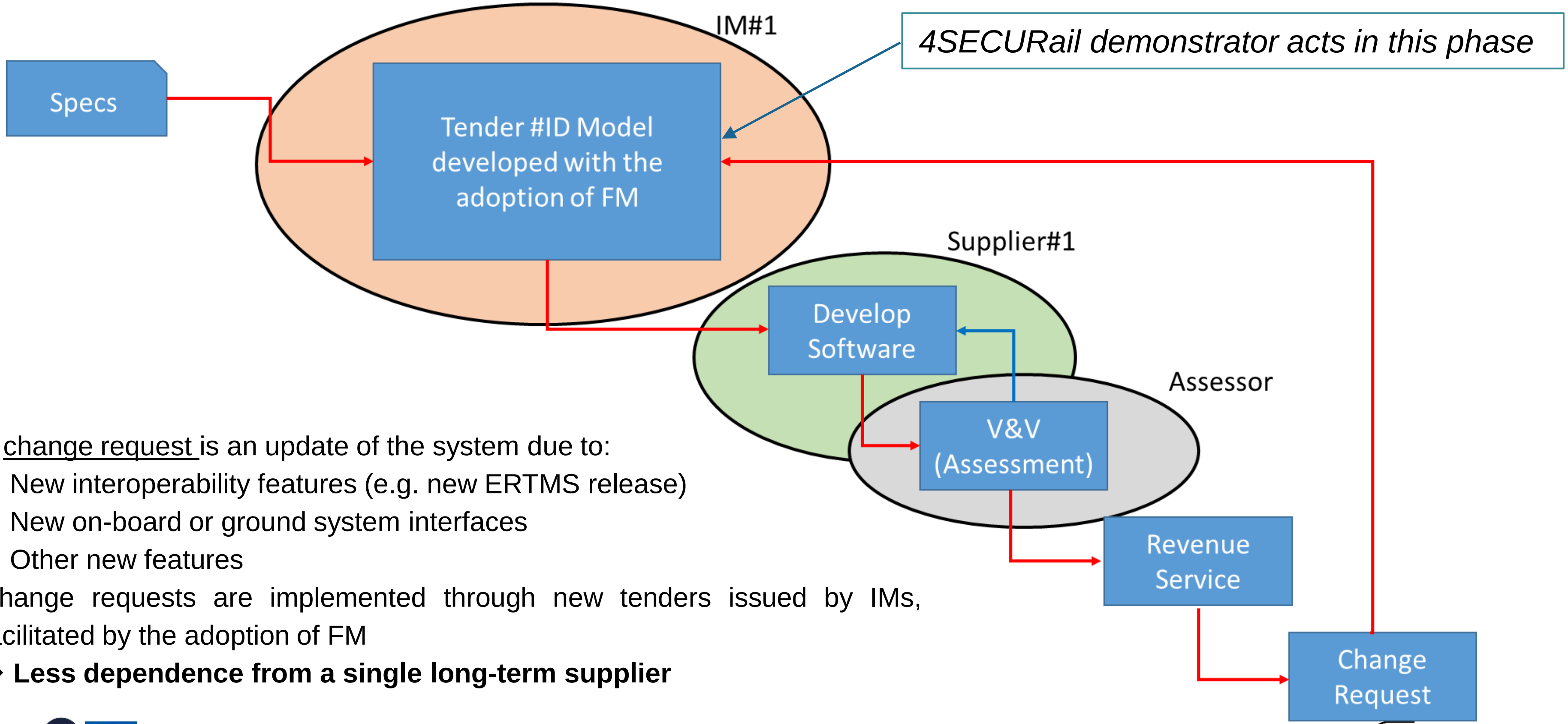
The Business Case

A <u>tender based Business Case</u> 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 <u>interoperable Standardised Interfaces, developed with the use of FM</u>. 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. <u>Tender specifications and tender details (for SW supply) are developed by the IM</u>
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 <u>difference between Baseline and FM scenarios</u> is likely occurring, with relevant measurement units

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

	Cost/Benefit Item		Meas. unit	Monetary meas unit
Investment costs (CAPEX)	"EULYNX follow-up" - Costs to issue new guidelines for using FM Costs for the definition of SI using issued guidelines		Person-days (assumed the deployment of personnel of associated IMs))	€/day
	RBC (or similar device) Purchase price		€/software/year	
		Training costs	Person-days	€/day
		Savings in SW management/assistance	Person-days	€/day
		Lower development time	Person-days	€/day
		Costs for SW verification and validation	Person-days	€/day
	Learning / personnel training costs		Person-days (2-4)	€/day
Operational costs (OPEX)	Time to define requirements for RBC/RBC interface supply through FM		Person-days	€/day
	SW Licenses for requirements development through FM		€/software/year	
	Costs for RBC acceptance, verification and validation		Person-days	€/day
	Higher maintenance efficiency		Replacement costs	€/year
	Higher availability in case of service disruption (lower penalties from service contracts)		# service disruptions/year (prob.)	€/day penalty
Benefits for users	Lower service disruptions		# hours saved by users	€/pax*hour
Externalities	Lower accident risks		Accidents/year	€/accident (external costs)

IM suppliers users society

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:

- <u>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</u>
- 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.

Literature review

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:

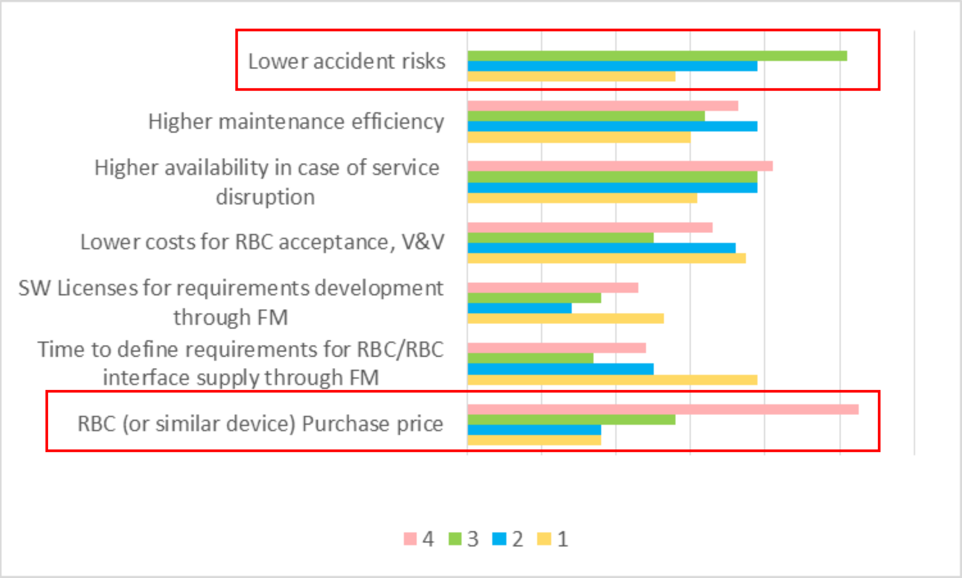
- FM provide significant benefits in terms of improved safety, requirement quality and reliability, reduced time-to-market / cost (qualitative)
- The 2020 FM survey (Garavel et al.): all experts agree that the improvement of "system safety" is one of the main benefits connected to the use of FM, followed 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
- <u>Relevant differences on relevance of RBC purchase price and Lower accident risks</u>
- 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

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

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**

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

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

Demonstrator effort: **7,0 person-month**
Baseline: **2,0 person-month**

Cost and benefit estimation

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)

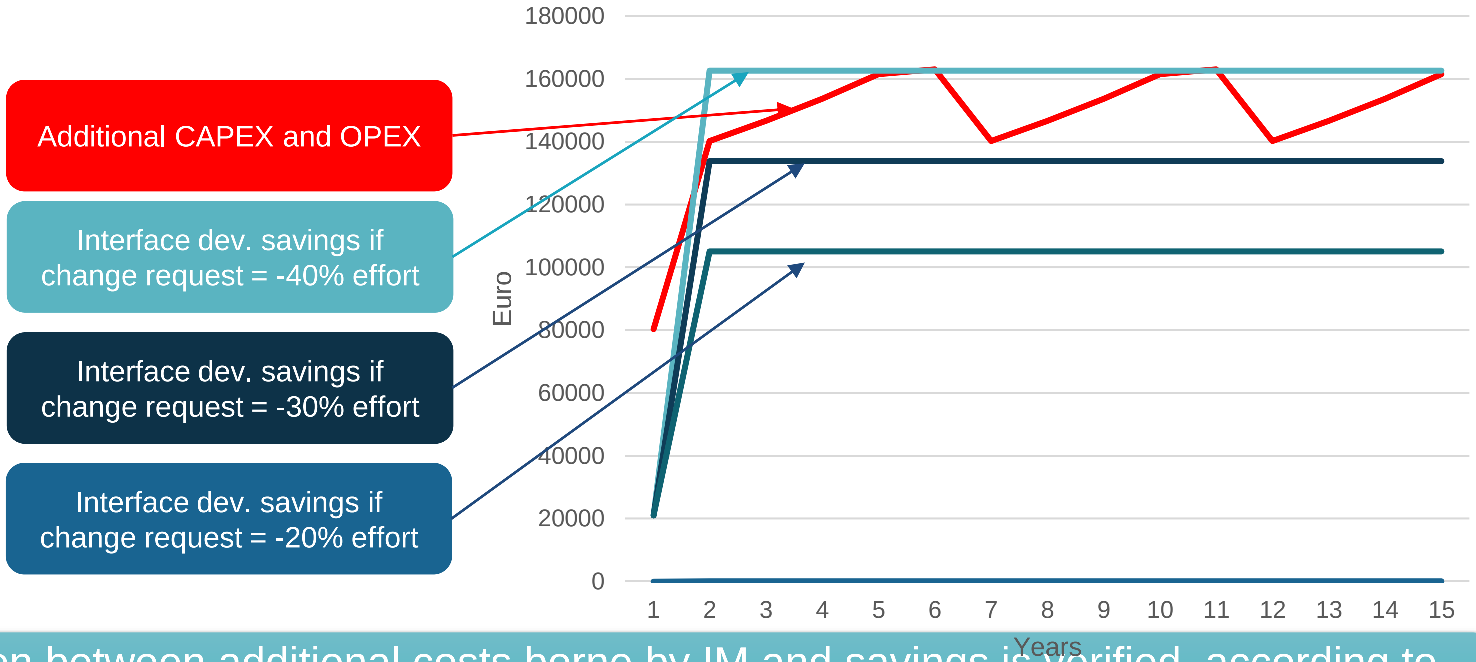
Time/cost category	Baseline	+/- Δ
RBC-RBC Interface development	12 PM	-20%
V&V effort	2-3 PM	-20%
V&V Assessor costs	6000 €	-3000 €

- **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, <u>according to 4SECURail demonstrator input,</u> if the purchase price of SW upon chage 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)

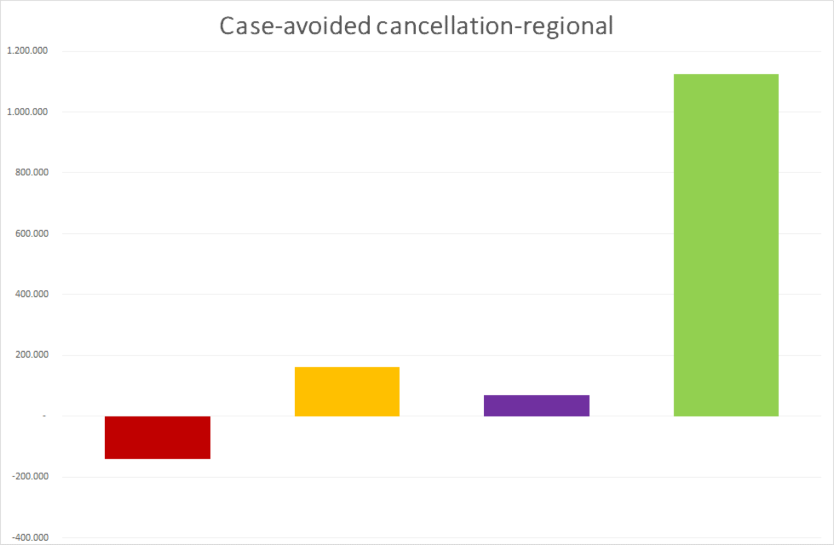
Cost and benefit estimation

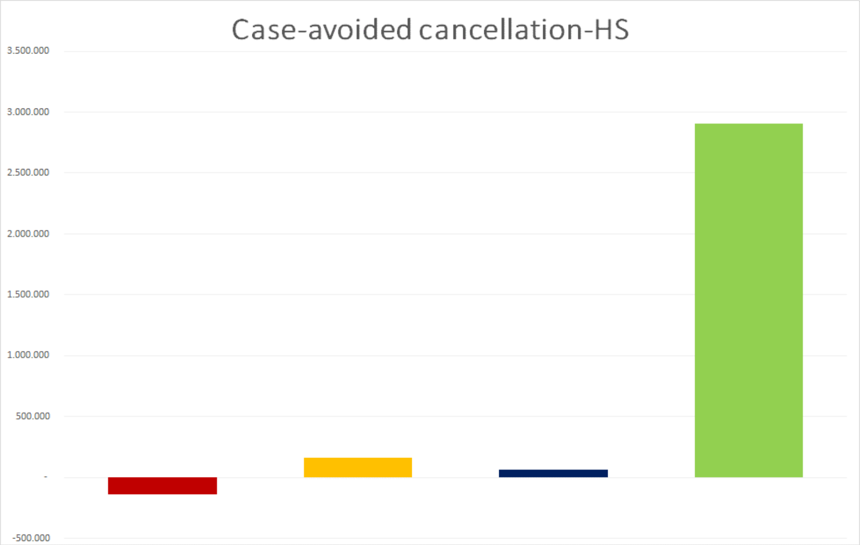
Costs

Purchase price savings

Penalties avoided

Time saved by passengers





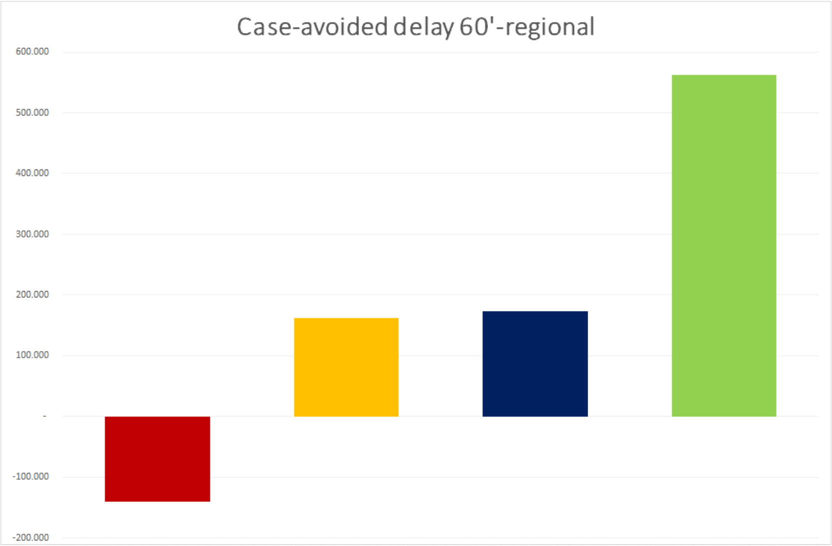
Cost and benefit estimation

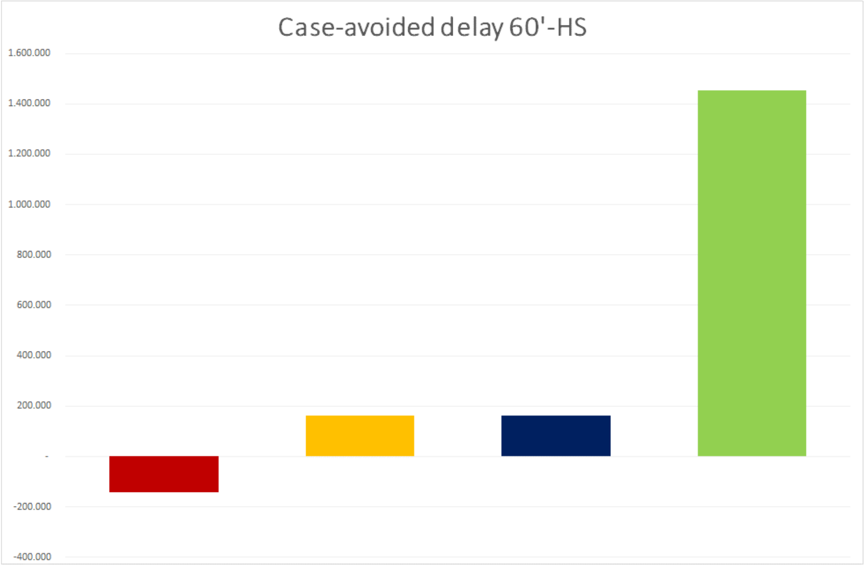
Costs

Purchase price savings

Penalties avoided

Time saved by passengers





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