From Proof to Practice: Formal Methods and Tools in Railways

Maurice ter Beek
FMT, CNR–ISTI, Pisa, Italy







DIA Summit 2026, Pisa, Italy, October 13$^{\text{th}}$, 2026

Outline

- Railway research
  - Sustainable mobility
  - Industrial standards
- Formal methods and tools
  - Formal methods in railways
  - Formal tools in railways
- Some success stories
  - NextGen Railway signalling
  - Smart railways and stations
- Future challenges: AI
  - Predictive maintenance
- Concluding remarks

Railway research

Global community effort for green transportation



EU green deal initiative

→ H2020 Shift2Rail Joint Undertaking (JU): €920 million (2014–2020)

"*formal methods are fundamental for safe and reliable technological advances to increase the competitiveness of the European rail industry*"

→ Horizon Europe Europe's Rail JU: €1.2 billion (2020–2027)

"*to ensure the safety, quality, and applicability of specifications, formal methods can provide significant benefits. Therefore, formal methods will be used for [. . .] to build the necessary confidence in the systems*"



Global community effort for green transportation



EU green deal initiative

→ H2020 Shift2Rail Joint Undertaking (JU): €920 million (2014–2020)

"*formal methods are fundamental for safe and reliable technological advances to increase the competitiveness of the European rail industry*"

→ Horizon Europe Europe's Rail JU: €1.2 billion (2020–2027)

"*to ensure the safety, quality, and applicability of specifications, formal methods can provide significant benefits. Therefore, formal methods will be used for [. . .] to build the necessary confidence in the systems*"

UK Rail Research and Innovation Network (UKRRIN)



Global community effort for green transportation



EU green deal initiative

→ H2020 Shift2Rail Joint Undertaking (JU): €920 million (2014–2020)

"*formal methods are fundamental for safe and reliable technological advances to increase the competitiveness of the European rail industry*"

→ Horizon Europe Europe's Rail JU: €1.2 billion (2020–2027)

"*to ensure the safety, quality, and applicability of specifications, formal methods can provide significant benefits. Therefore, formal methods will be used for [. . .] to build the necessary confidence in the systems*"

UK Rail Research and Innovation Network (UKRRIN)



China State Key Laboratory of Rail Traffic Control and Safety

FMT involved in EU, national and regional projects

Sustainable Mobility Center: Rail Transportation (NextGen, 2022–26)

→ Learning formal models for predictive monitoring and maintenance

Formal methods and CSIRT for the railway sector (H2020, 2019–21)

→ Demonstrator to evaluate cost, benefits and required learning curve of using formal methods for rigorous specification of a railway signalling infrastructure

SAtellite-based Signalling and Automation SysTems on Railways along with Formal Method and Moving Block Validation (H2020, 2017–19)

→ Requirements analysis plus safety, hazard and performance analyses of moving block signalling scenarios with the most suitable formal methods and tools

FMT involved in EU, national and regional projects

MOST CENTRO NAZIONALE PER LA MOBILITÀ SOSTENIBILE Sustainable Mobility Center: Rail Transportation (NextGen, 2022–26)

→ Learning formal models for predictive monitoring and maintenance

4SECURail Formal methods and CSIRT for the railway sector (H2020, 2019–21)

→ Demonstrator to evaluate cost, benefits and required learning curve of using formal methods for rigorous specification of a railway signalling infrastructure

ASTRail SAtellite-based Signalling and Automation SysTems on Railways along with Formal Method and Moving Block Validation (H2020, 2017–19)

→ Requirements analysis plus safety, hazard and performance analyses of moving block signalling scenarios with the most suitable formal methods and tools

ADV.E.N.T.U.R.E. ADVancEd iNtegraTed evalUation of Railway systEms (PRIN, 2023–26)

FMT involved in EU, national and regional projects

Sustainable Mobility Center: Rail Transportation (NextGen, 2022–26)

→ Learning formal models for predictive monitoring and maintenance

Formal methods and CSIRT for the railway sector (H2020, 2019–21)

→ Demonstrator to evaluate cost, benefits and required learning curve of using formal methods for rigorous specification of a railway signalling infrastructure

SAtellite-based Signalling and Automation SysTems on Railways along with Formal Method and Moving Block Validation (H2020, 2017–19)

→ Requirements analysis plus safety, hazard and performance analyses of moving block signalling scenarios with the most suitable formal methods and tools

ADVancEd iNtegraTed evalUation of Railway systEms (PRIN, 2023–26)

SmaRIERS: Smart Railway Infrastructures: Efficiency, Reliability and Safety (RT, 2021–23)

STINGRAY: SmarT station INtelliGent RAilwaY (RT, 2018–21)

CENELEC EN 50128

EU standard for the development of software for the railway industry: highly recommends formal methods for the design and verification of products that need to meet the highest Safety Integrity Levels

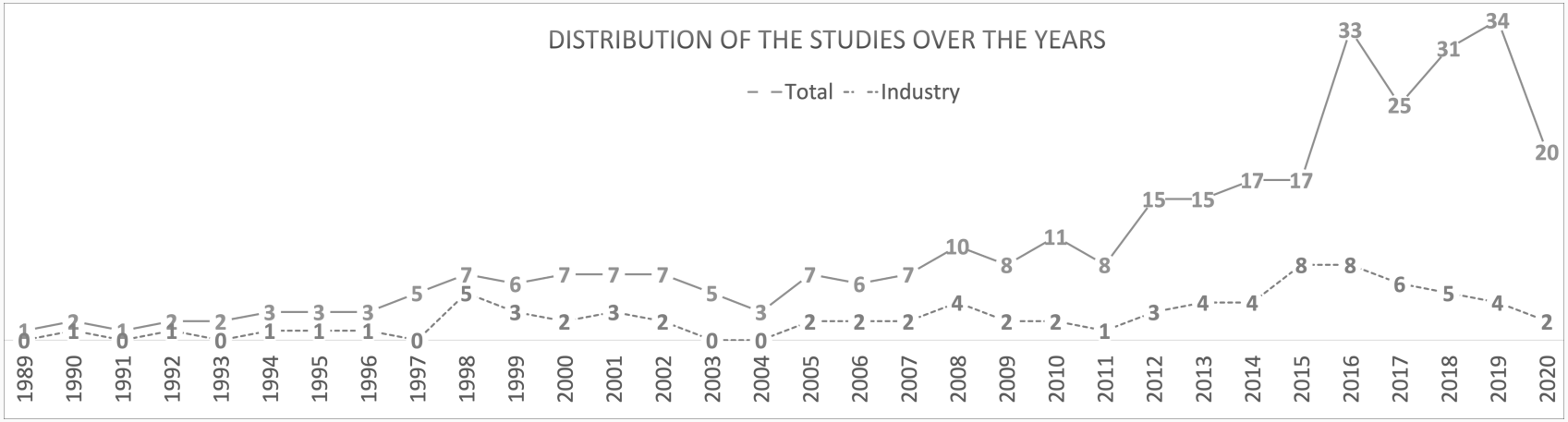
CENELEC EN 50128, being replaced by 50716

EN 50716 extends this to all Safety Integrity Levels from SIL 1 to 4; this marks a decisive shift: formal modeling and verification is now a baseline expectation across the entire railway software domain

CENELEC EN 50128, being replaced by 50716

EN 50716 extends this to all Safety Integrity Levels from SIL 1 to 4; this marks a decisive shift: formal modeling and verification is now a baseline expectation across the entire railway software domain

In fact, formal methods in railways is a thriving research field with strong industrial ties: 143 studies (44% of a total of 328) published solely in the last 5 years, while 79 studies (24%) involved industry



[CSUR23] A. Ferrari & M.H. ter Beek, Formal Methods in Railways: A Systematic Mapping Study. *ACM Computing Surveys* (2023)

Formal methods in railways

Formal methods . . .

Formal methods are rigorous mathematics-based techniques and tools for the specification (modelling) and manual or automated verification (analysis) of software or hardware systems (designs)

Formal methods . . .

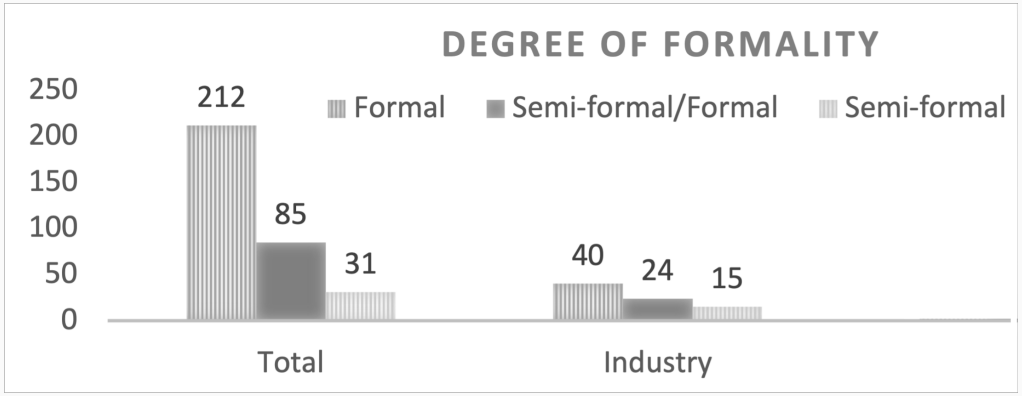
Formal methods are rigorous mathematics-based techniques and tools for the specification (modelling) and manual or automated verification (analysis) of software or hardware systems (designs)

Formal verification concerns verifying (e.g., by model checking) that functional properties (e.g., absence of deadlocks) or critical system properties related to safety are satisfied

Formal methods . . .

Formal methods are rigorous mathematics-based techniques and tools for the specification (modelling) and manual or automated verification (analysis) of software or hardware systems (designs)

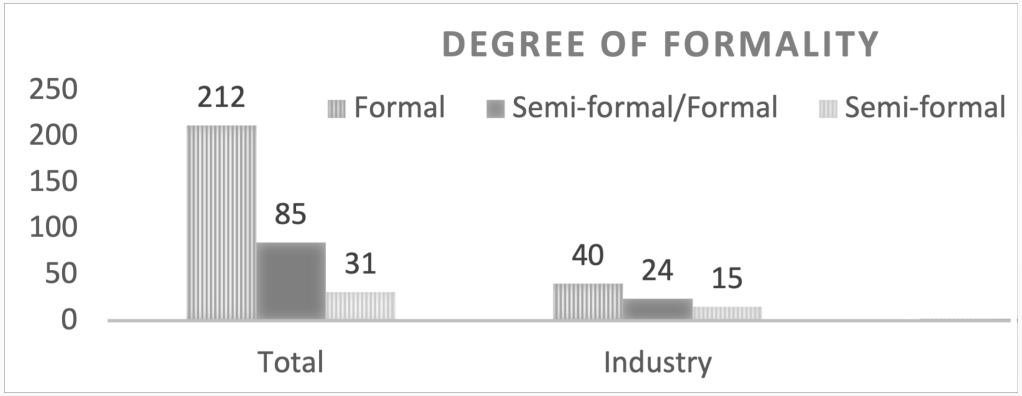
Formal verification concerns verifying (e.g., by model checking) that functional properties (e.g., absence of deadlocks) or critical system properties related to safety are satisfied $\Rightarrow$ requires formal models **with a precise semantics**



Formal methods . . .

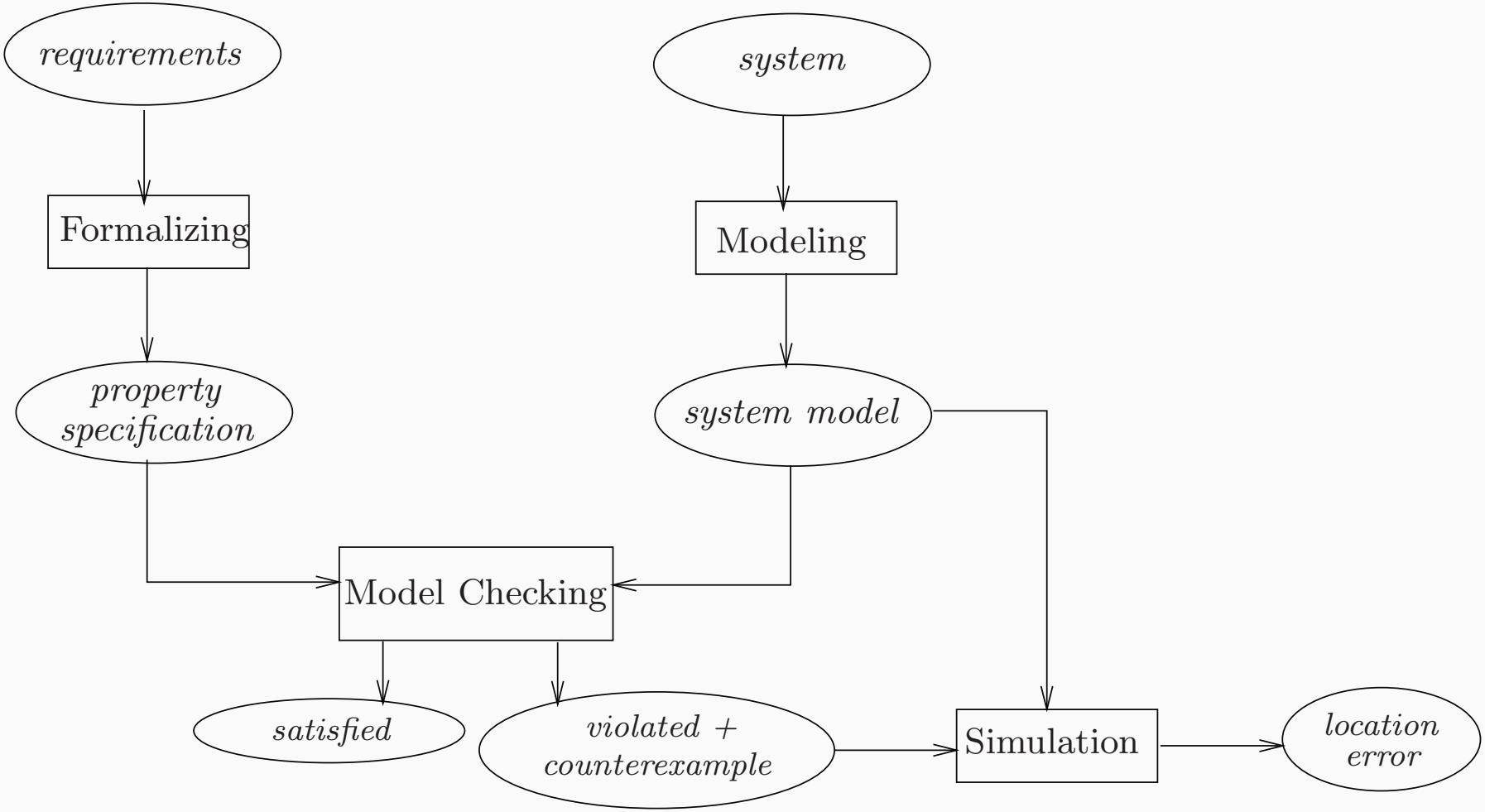
Formal methods are rigorous mathematics-based techniques and tools for the specification (modelling) and manual or automated verification (analysis) of software or hardware systems (designs)

Formal verification concerns verifying (e.g., by model checking) that functional properties (e.g., absence of deadlocks) or critical system properties related to safety are satisfied $\Rightarrow$ requires formal models **with a precise semantics**



"testing can be used to show the presence of bugs,
but never to show their absence!" – Edsger W. Dijkstra

. . . and (model-checking) tools



C. Baier & J.-P. Katoen, *Principles of Model Checking*, MIT, 2008

Strengths and weaknesses

- General verification approach, applicable to a wide range of applications (e.g., embedded systems, software engineering, hardware design)
- Supports partial verification, i.e. properties can be checked individually, allowing to focus on essential properties first (no complete requirement specification needed)
- Not vulnerable to likelihood that an error is exposed; this contrasts with testing and simulation that are aimed at tracing the most probable defects
- Provides diagnostic info in case a property is invalidated: very useful for debugging
- **Potentially a "push-button" technology**, requiring neither a high degree of user interaction nor a high degree of expertise
- Enjoys a rapidly increasing interest by industry: several companies have started their in-house verification labs (e.g., Amazon), frequent job offers with required skills in model checking, and commercial model checkers have become available
- Easy integration in existing development cycles: its learning curve is not very steep, empirical studies indicate that it may lead to shorter development times
- Sound and mathematical underpinning, based on theory of graph algorithms, data structures and logic

Strengths and weaknesses

- General verification approach, applicable to a wide range of applications (e.g., embedded systems, software engineering, hardware design)
- Supports partial verification, i.e. properties can be checked individually, allowing to focus on essential properties first (no complete requirement specification needed)
- Not vulnerable to likelihood that an error is exposed; this contrasts with testing and simulation that are aimed at tracing the most probable defects
- Provides diagnostic info in case a property is invalidated: very useful for debugging
- **Potentially a "push-button" technology**, requiring neither a high degree of user interaction nor a high degree of expertise
- Enjoys a rapidly increasing interest by industry: several companies have started their in-house verification labs (e.g., Amazon), frequent job offers with required skills in model checking, and commercial model checkers have become available
- Easy integration in existing development cycles: its learning curve is not very steep, empirical studies indicate that it may lead to shorter development times
- Sound and mathematical underpinning, based on theory of graph algorithms, data structures and logic

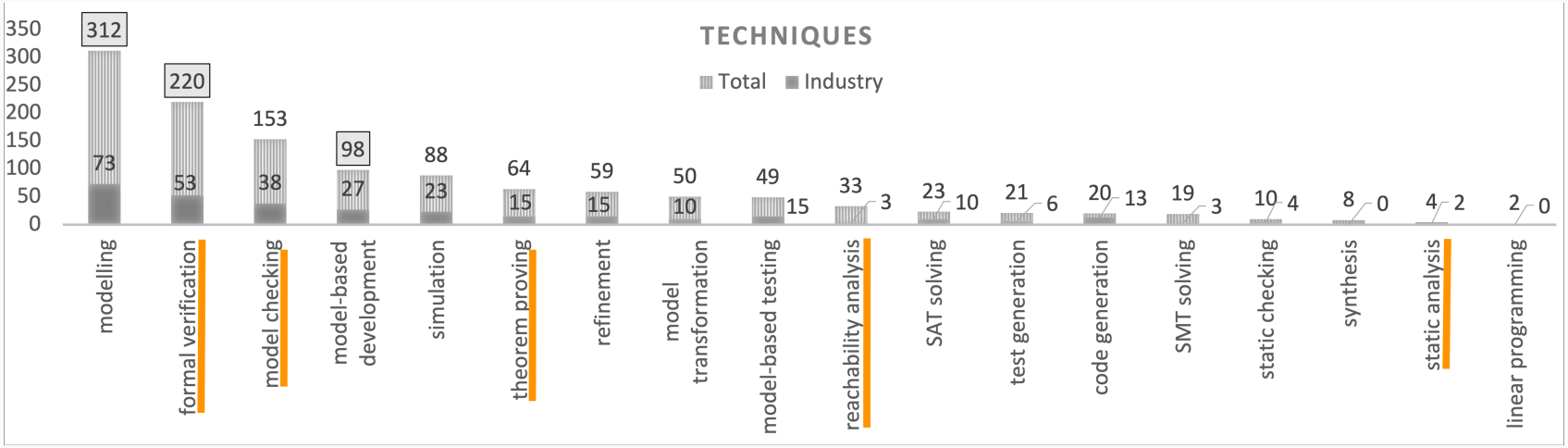
Strengths and weaknesses

- Mainly appropriate to control-intensive applications and less suited for data-intensive applications as data typically ranges over infinite domains
- Applicability subject to decidability issues: for infinite-state systems or reasoning about abstract data types (which requires undecidable or semi-decidable logics), model checking is in general not effectively computable
- Verifies a system model, and not the actual system (product or prototype) itself: **any obtained result is thus as good as the system model** (need complementary techniques, like testing, to find fabrication faults (for HW) or coding errors (for SW)
- Checks only stated requirements, i.e. **no guarantee of completeness**, since the validity of properties that are not checked cannot be judged
- Suffers from state space explosion problem: number of states needed to model the system accurately may easily exceed the amount of available computer memory (despite the development of several very effective methods to combat this problem, models of realistic systems may still be too large to fit in memory)
- Its usage requires some **expertise** in finding appropriate abstractions to obtain smaller system models and to state properties in the logical formalism used
- Correct results not guaranteed: like any tool, it may contain software defects
- Does not allow checking generalizations: in general, checking systems with an arbitrary number of components, or parameterized systems, cannot be treated

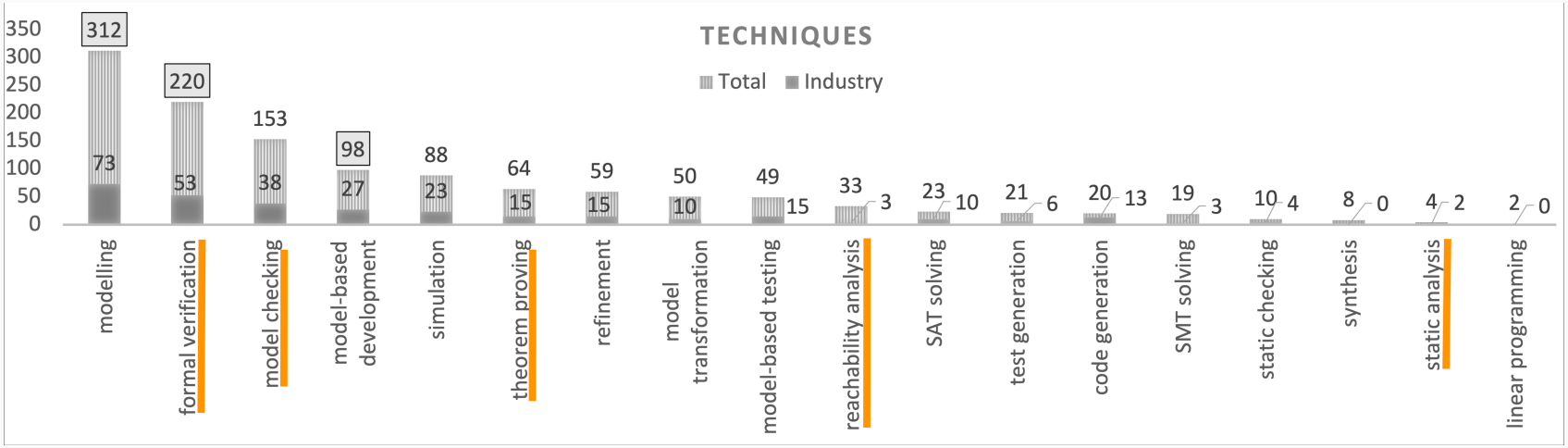
Strengths and weaknesses

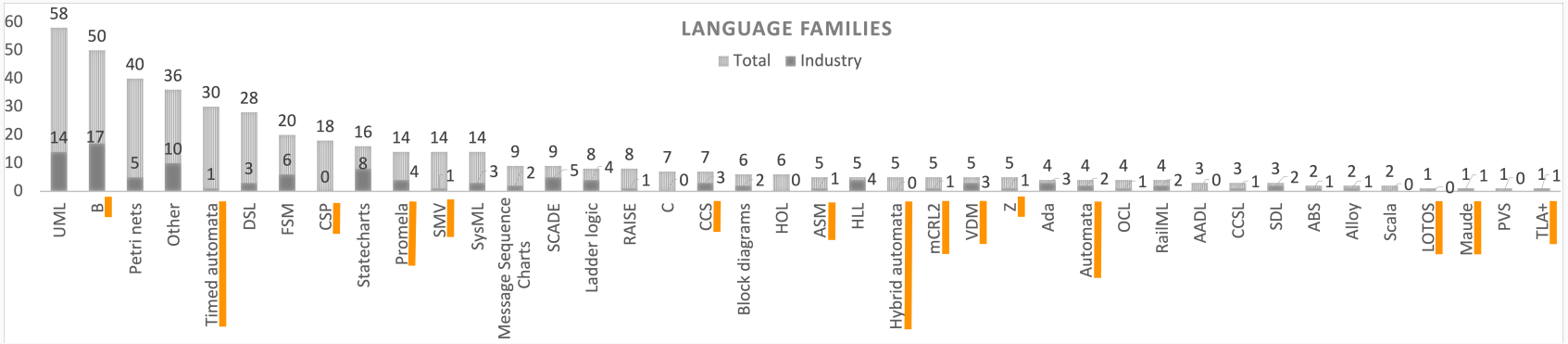
- Mainly appropriate to control-intensive applications and less suited for data-intensive applications as data typically ranges over infinite domains
- Applicability subject to decidability issues: for infinite-state systems or reasoning about abstract data types (which requires undecidable or semi-decidable logics), model checking is in general not effectively computable
- Verifies a system model, and not the actual system (product or prototype) itself: **any obtained result is thus as good as the system model** (need complementary techniques, like testing, to find fabrication faults (for HW) or coding errors (for SW)
- Checks only stated requirements, i.e. **no guarantee of completeness**, since the validity of properties that are not checked cannot be judged
- Suffers from state space explosion problem: number of states needed to model the system accurately may easily exceed the amount of available computer memory (despite the development of several very effective methods to combat this problem, models of realistic systems may still be too large to fit in memory)
- Its usage requires some **expertise** in finding appropriate abstractions to obtain smaller system models and to state properties in the logical formalism used
- Correct results not guaranteed: like any tool, it may contain software defects
- Does not allow checking generalizations: in general, checking systems with an arbitrary number of components, or parameterized systems, cannot be treated

Formal methods and tools are at the basis!

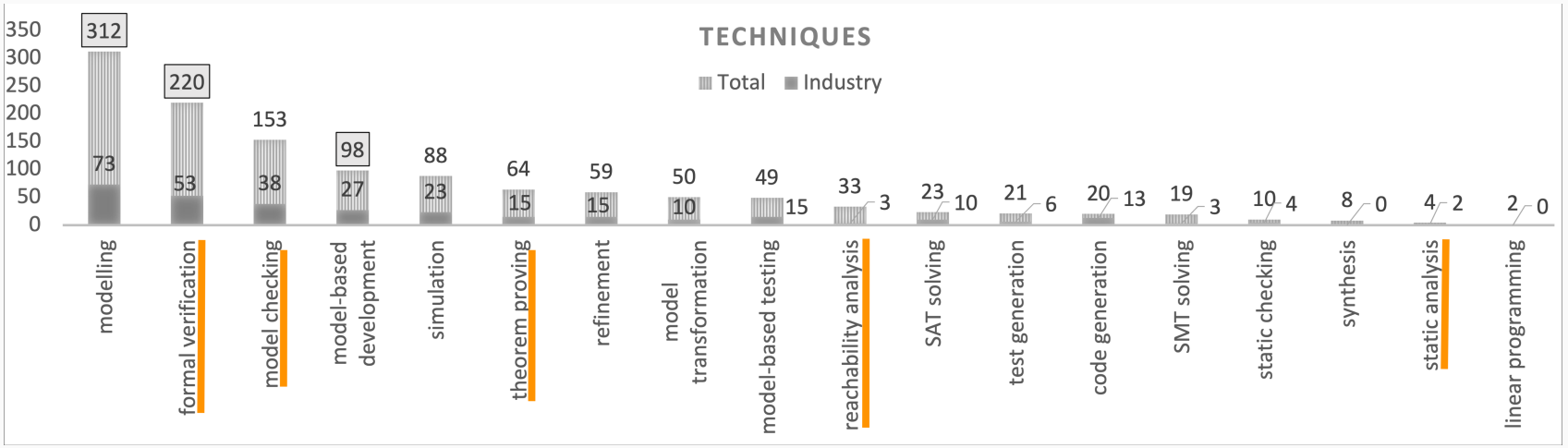


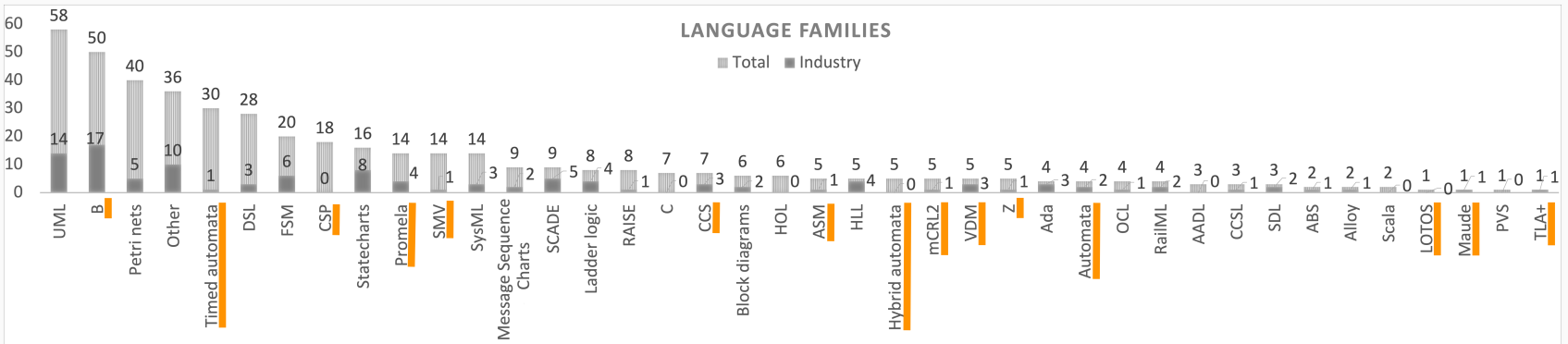
Formal methods and tools are at the basis!

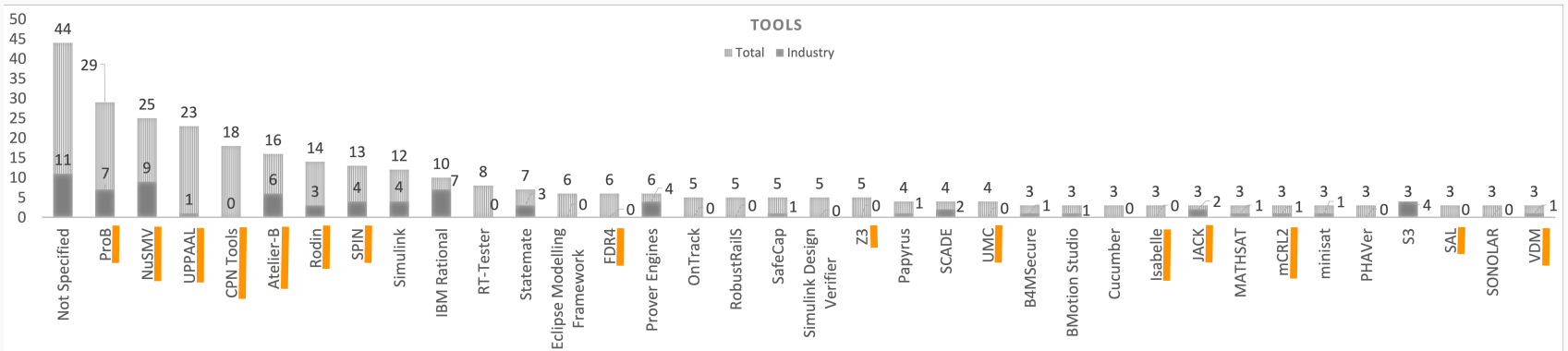




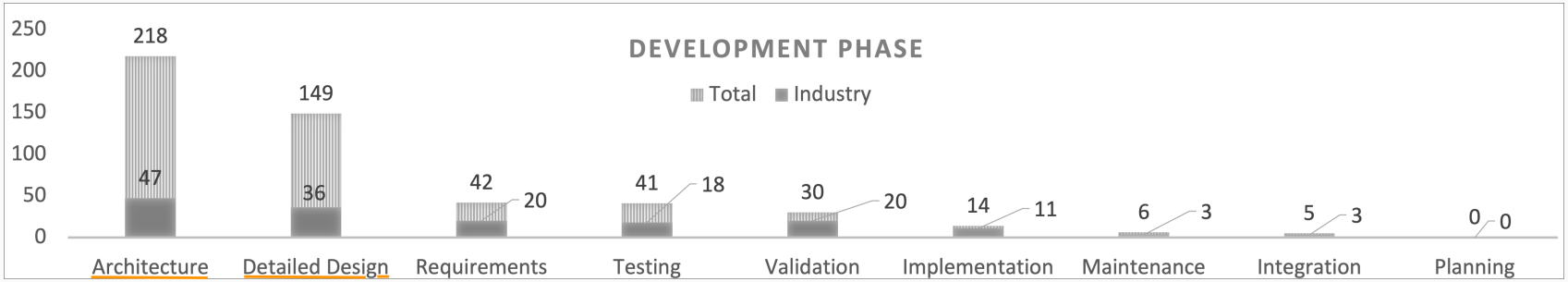
Formal methods and tools are at the basis!



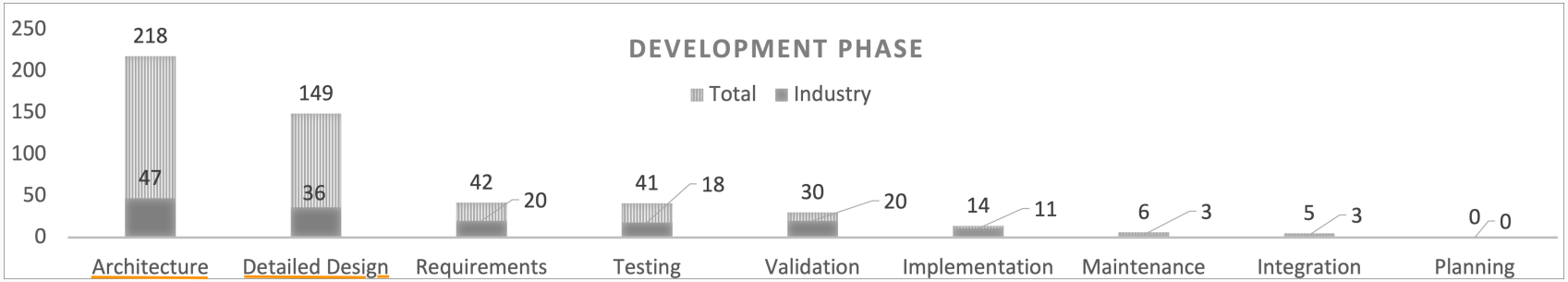




Indeed, at the basis!



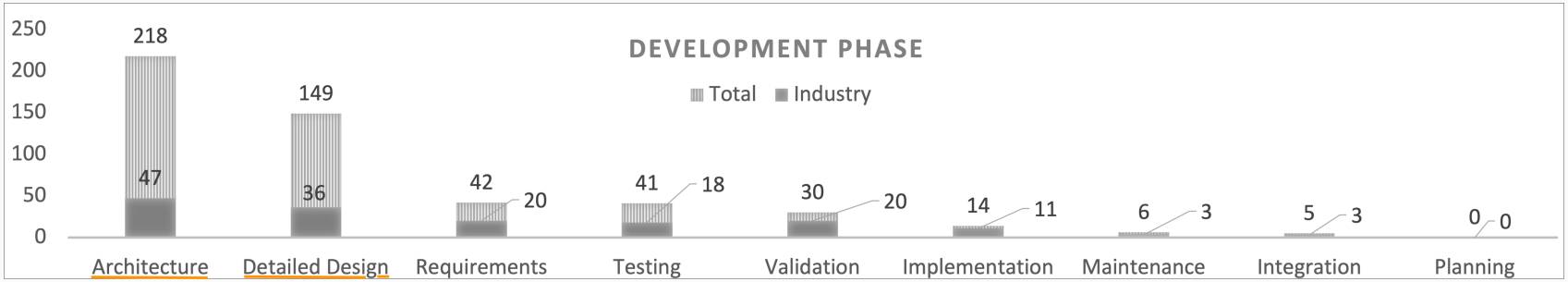
Results



Take-away messages

- Later development phases, in particular testing, implementation and validation, are currently not sufficiently addressed
- Formal methods are typically applied on abstract, high-level models, and source code is only marginally considered

Results



Take-away messages

- Later development phases, in particular testing, implementation and validation, are currently not sufficiently addressed
- Formal methods are typically applied on abstract, high-level models, and source code is only marginally considered
+ UML is typically used for high-level models, which are then translated into input languages of the formal methods tools
+ Almost all core railway development phases can be addressed by formal methods, in line with CENELEC recommendation

Formal tools in railways

Take-away messages

- Many of the formal tools lack support for development features and process-integration aspects
- Most formal tools are independent ecosystems, with unique, non-standard languages and specialised verification features

Results

Take-away messages

- − Many of the formal tools lack support for development features and process-integration aspects
- − Most formal tools are independent ecosystems, with unique, non-standard languages and specialised verification features
- + Formal tools are mature, as highly desired by the railway industry [iFM18,FM19]
- + Most usability aspects appear to be low in principle, but, when the formal tools are assessed by railway practitioners, usability is considered acceptable

[iFM18] D. Basile, M.H. ter Beek, et al., On the Industrial Uptake of Formal Methods in the Railway Domain: A Survey with Stakeholders @ iFM'18

[FM19] M.H. ter Beek et al., Adopting Formal Methods in an Industrial Setting @ FM'19

Formal methods and tools in railways: Success stories

Some of our success stories

A taste of FMT's railway research in projects with industrial partners over the last 10 years:

- Deadlock avoidance in train scheduling
- Next generation railway signalling systems
- Synthesis of autonomous driving strategies
- Smart railway systems & stations of the future







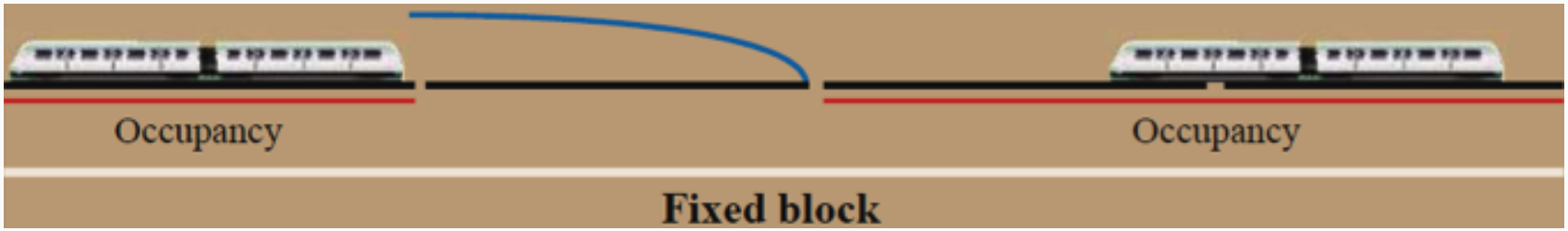
...

Success story 2

Next generation railway signalling systems

Current ERTMS / ETCS signalling systems max. level 2:

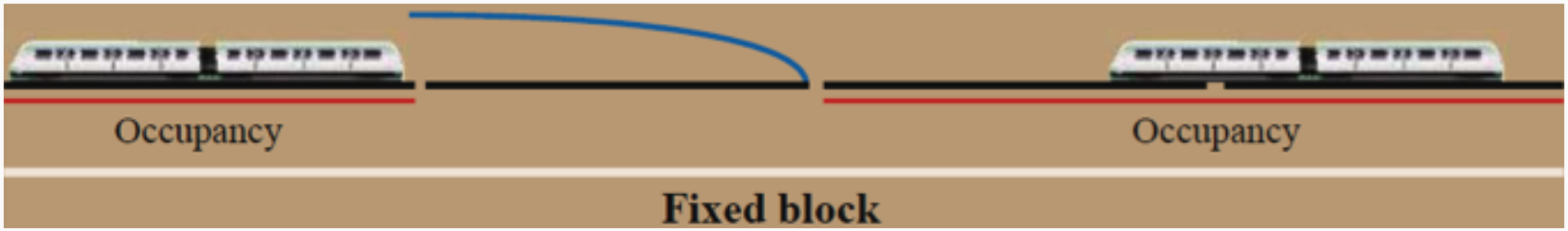
- fixed blocks: based on line's speed limit, train's speed/braking, . . . , thus faster trains imply longer blocks imply lower track occupancy
- trackside equipment for train positioning, with costly maintenance



Next generation railway signalling systems

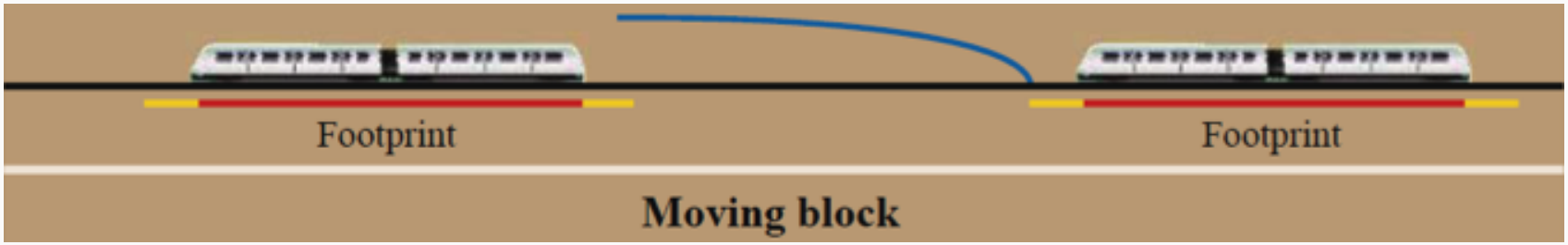
Current ERTMS / ETCS signalling systems max. level 2:

- fixed blocks: based on line's speed limit, train's speed/braking, . . . , thus faster trains imply longer blocks imply lower track occupancy
- trackside equipment for train positioning, with costly maintenance



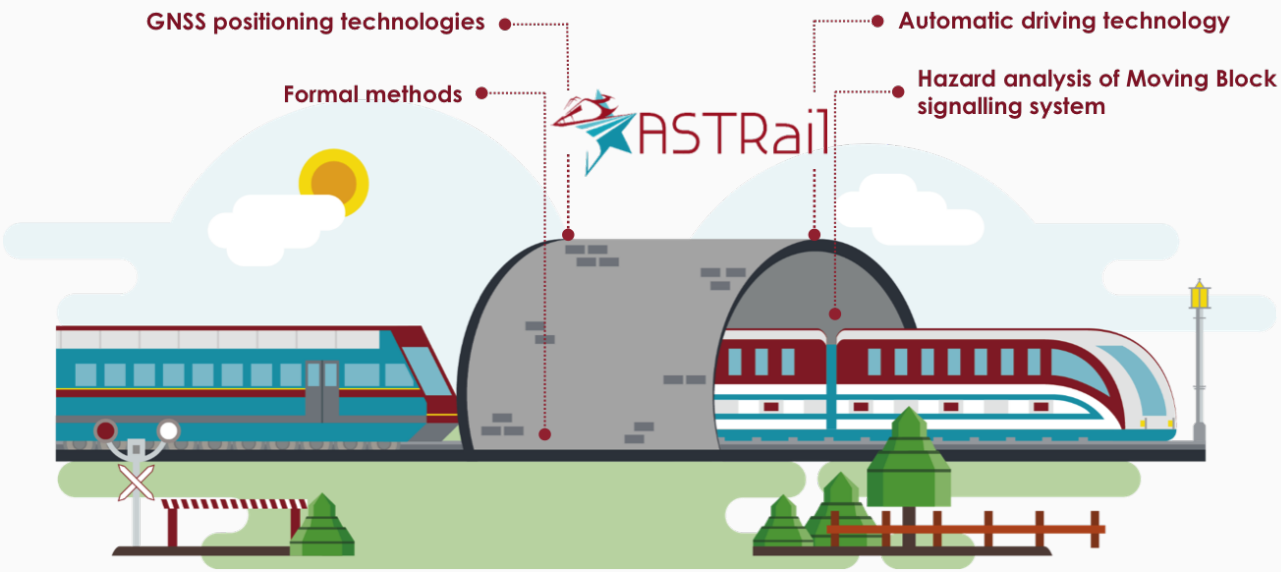
Next generation railway signalling systems from level 3:

- moving blocks: safe zone based on rear position of train ahead, thus reducing trains' headways, in principle to braking distance
- onboard odometry for train positioning (no trackside equipment)



Safety analysis of moving block signalling system

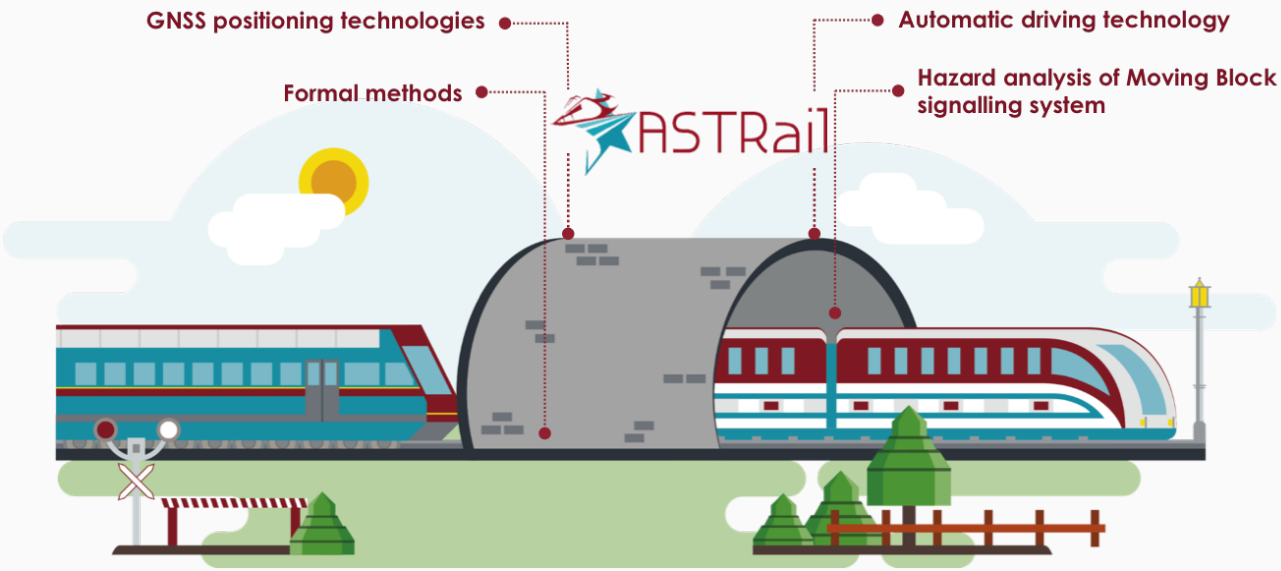
Challenge: effective, precise moving block signalling systems by GNSS-based satellite positioning, leveraging on an integrated solution for signal outages (e.g. tunnels) and multipath interference in dense urban areas



Safety analysis of moving block signalling system

Challenge: effective, precise moving block signalling systems by GNSS-based satellite positioning, leveraging on an integrated solution for signal outages (e.g. tunnels) and multipath interference in dense urban areas

Aim: analyse suitability of formal methods in transitioning to the next generation of ERTMS/ETCS railway signalling systems, with satellite-based positioning, moving block distancing, and automatic driving



Safety analysis of moving block signalling system

Challenge: effective, precise moving block signalling systems by GNSS-based satellite positioning, leveraging on an integrated solution for signal outages (e.g. tunnels) and multipath interference in dense urban areas

Aim: analyse suitability of formal methods in transitioning to the next generation of ERTMS/ETCS railway signalling systems, with satellite-based positioning, moving block distancing, and automatic driving

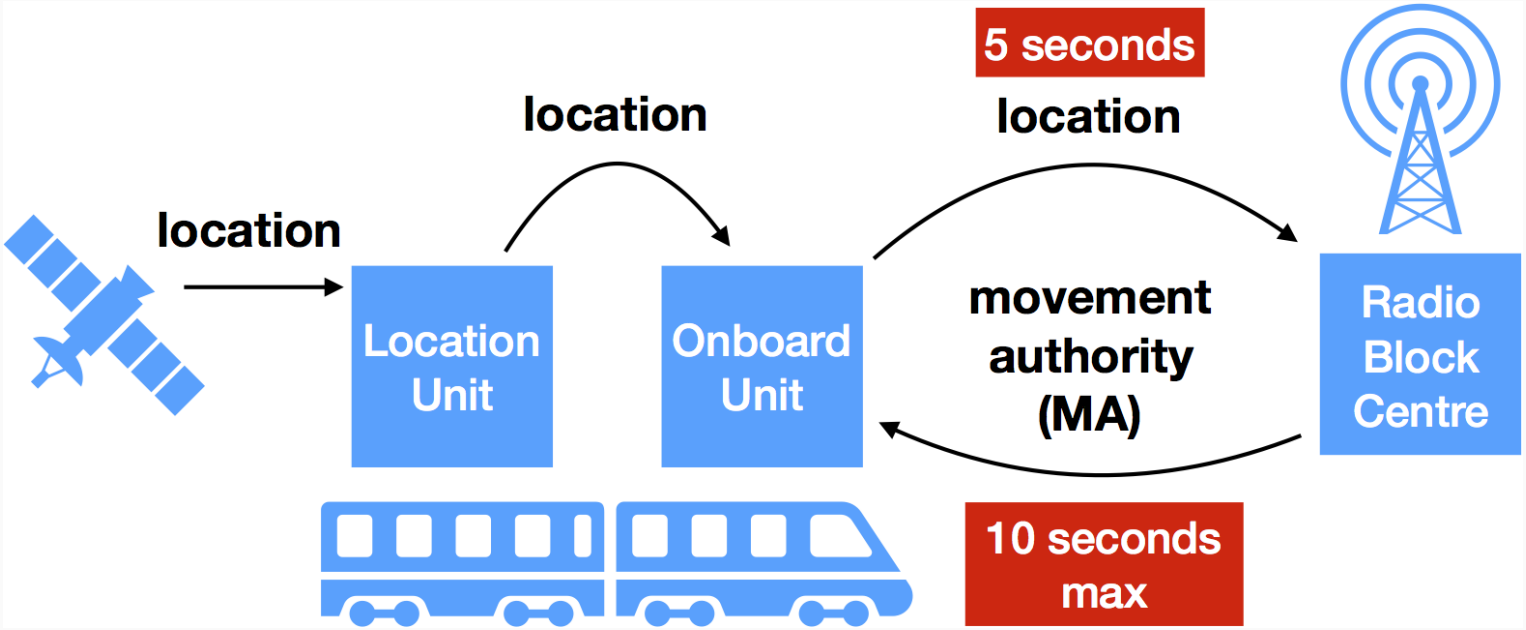
[STTT22] D. Basile, M.H. ter Beek, A. Ferrari & A. Legay, Exploring the ERTMS/ETCS full moving block specification: An experience with formal methods. *International Journal on Software Tools for Technology Transfer* (2022)

[FORTE20] D. Basile, M.H. ter Beek & A. Legay, Strategy Synthesis for Autonomous Driving in a Moving Block Railway System with Uppaal Stratego @ FORTE'20

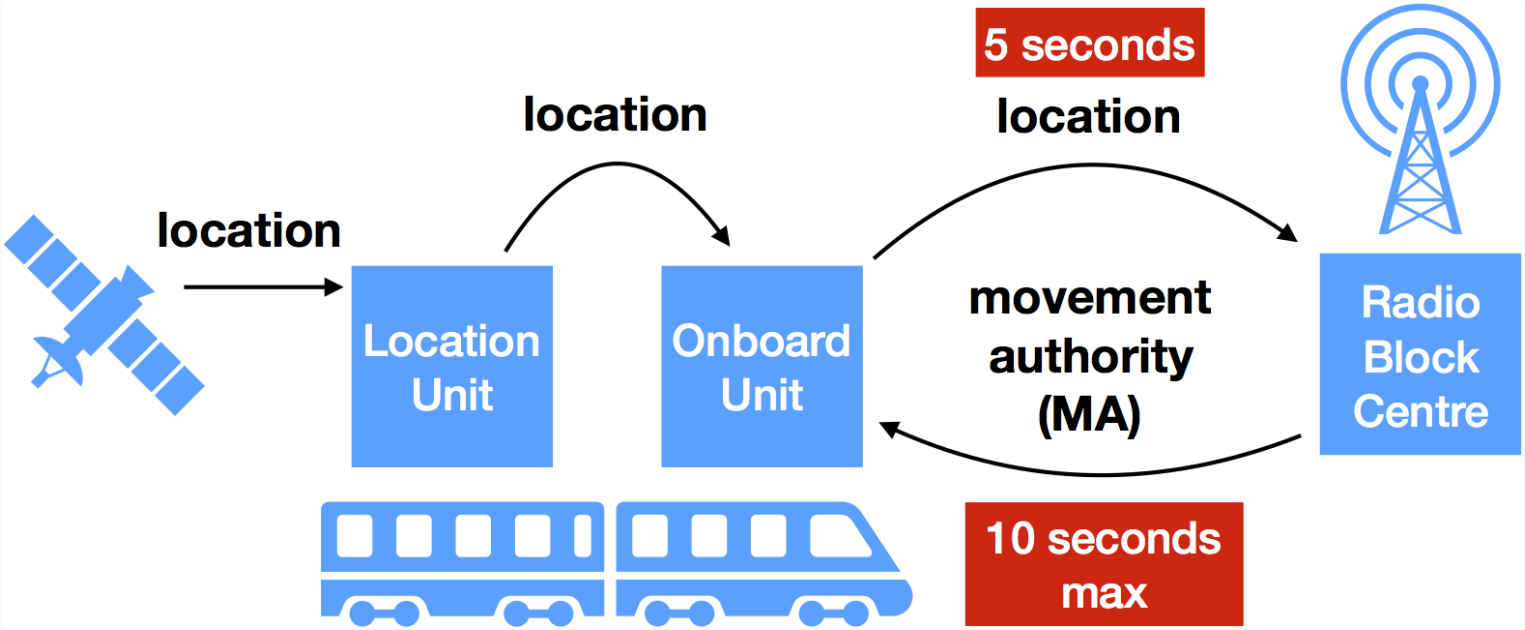
[FMICS19] D. Basile, M.H. ter Beek, A. Ferrari & A. Legay, Modelling and Analysing ERTMS L3 Moving Block Railway Signalling with Simulink and UPPAAL SMC @ FMICS'19

[ISoLA18] D. Basile, M.H. ter Beek & V. Ciancia, Statistical Model Checking of a Moving Block Railway Signalling Scenario with Uppaal SMC @ ISoLA'18

Moving block system architecture



From semi-formal models to formal models



Input: Real-Time UML (RT UML) and Simulink models obtained from/upon requirements elicitation and refinement with industrial partners

Output: UPPAAL SMC model

- capable of natively accommodating both real-time and probabilistic aspects
- ± UML state machine diagrams, easing understanding by industrial partners

Preliminary hazard analysis by industrial partners

Goal: evaluate safety level of a moving block signalling system

Procedure: identify and analyse hazards (e.g. GNSS-related errors, communication failures, faulty states)

- risk assessment: probability of occurrence of a hazard and severity of its consequences
- risk qualifying according to CENELEC EN 50126 standard (RAMS: Reliability, Availability, Maintainability and Safety)

Outcome: hazard log

Examples from the hazard log

Requirements:

"Communication between RBC and OBU must be safe and continuously supervised, if the connection is lost an alarm must be triggered."

"OBU device must be SIL 4 device. Once OBU receives the alarm [. . .] it must immediately send an alarm to RBC."

Mitigation: "In case of communication loss enter in safe state mode."

Examples from the hazard log

Requirements:

"Communication between RBC and OBU must be safe and continuously supervised, if the connection is lost an alarm must be triggered."

"OBU device must be SIL 4 device. Once OBU receives the alarm [. . .] it must immediately send an alarm to RBC."

Mitigation: "In case of communication loss enter in safe state mode."

Safety Related Application Conditions:

"If train position cannot be received within the maximum time limit, the OBU shall generate an alarm and must transit to degraded mode."

"If Train Integrity cannot be confirmed within the maximum time limit, the train shall be stopped."

Analyses with UPPAAL SMC

1 It must always be the case that eventually either a MA is received or the train enters a safe state `Stop`:

$$A \Diamond (\texttt{ReplyMA.ReplyRequest} \parallel \texttt{Controlling.Stop})$$

UPPAAL SMC reports that this (reachability) property (expressed in CTL) holds

Analyses with UPPAAL SMC

1 It must always be the case that eventually either a MA is received or the train enters a safe state `Stop`:

$$A \Diamond (\texttt{ReplyMA.ReplyRequest} \parallel \texttt{Controlling.Stop})$$

UPPAAL SMC reports that this (reachability) property (expressed in CTL) holds

2 Probability that the train enters a safe state `Stop` upon a `timeout`:

$$\mathbb{P}_M(\Diamond_{\leq(\texttt{timeout})}\, \texttt{Controlling.Stop})$$

UPPAAL SMC reports that this probability is in interval [0,9.99994e-005], with confidence 0.995 and obtained from 59912 runs in ± 5 min.

Success story 4

Smart energy consumption: energy efficiency vs. dependability

Smart railway systems and stations of the future

Smart energy consumption: energy efficiency vs. dependability

- Smart deicing system: railroad switch heaters for correct working of switches in case of ice / snow

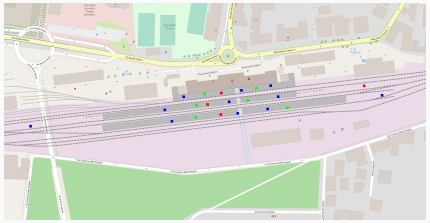


Smart railway systems and stations of the future

Smart energy consumption: energy efficiency vs. dependability



- Smart deicing system: railroad switch heaters for correct working of switches in case of ice / snow
- Smart station lighting: reduce illumination whenever (time) and wherever (space) possible, guaranteeing legal minimum levels





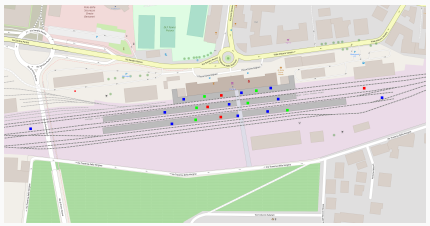

Smart railway systems and stations of the future

Smart energy consumption: energy efficiency vs. dependability

- Smart deicing system: railroad switch heaters for correct working of switches in case of ice / snow



- Smart station lighting: reduce illumination whenever (time) and wherever (space) possible, guaranteeing legal minimum levels






[ISoLA20] D. Basile, M.H. ter Beek, F. Di Giandomenico, A. Fantechi, S. Gnesi & G.O. Spagnolo, 30 Years of Simulation-Based Quantitative Analysis Tools: A Comparison Experiment Between Möbius and Uppaal SMC @ ISoLA'20

[FMICS21] M.H. ter Beek, V. Ciancia, D. Latella, M. Massink & G.O. Spagnolo, Spatial Model Checking for Smart Stations: Research Challenges @ FMICS'21

Current challenges

Lessons learned

Closing the gap:

semi-formal models popular and suitable to communicate with industry

formal models required to apply analysis tools in safety-critical domains (e.g., railways)

Lessons learned

Closing the gap:

semi-formal models popular and suitable to communicate with industry

formal models required to apply analysis tools in safety-critical domains (e.g., railways)

Each formal tool:

- requires modelling in a different input language
- expert knowledge of different analysis technique

Lessons learned

Closing the gap:

semi-formal models popular and suitable to communicate with industry

formal models required to apply analysis tools in safety-critical domains (e.g., railways)

Each formal tool:

- requires modelling in a different input language
- expert knowledge of different analysis technique

FMT: researchers with different and complementary expertise

Industry: in-house formal methods expertise rare (AWS, ASML, . . .)

Lessons learned

Closing the gap:

semi-formal models popular and suitable to communicate with industry

formal models required to apply analysis tools in safety-critical domains (e.g., railways)

Each formal tool:

- requires modelling in a different input language
- expert knowledge of different analysis technique

FMT: researchers with different and complementary expertise

Industry: in-house formal methods expertise rare (AWS, ASML, . . .)

Road to success:

- capacity to abstract
- pick the right tool based on the industry input and requirements at hand

Future challenges

Future challenges: AI

EU Sustainable and Smart Mobility Strategy:

Putting European transport on track for the future

https://transport.ec.europa.eu/system/files/2021-04/2021-mobility-strategy-and-action-plan.pdf

Future challenges: AI

EU Sustainable and Smart Mobility Strategy:
Putting European transport on track for the future

`https://transport.ec.europa.eu/system/files/2021-04/2021-mobility-strategy-and-action-plan.pdf`

Railways is expected to contribute by improved digitalisation and big data analytics:

R. Tang, L. De Donato, N. Bešinović, F. Flammini, R.M.P. Goverde, Z. Lin, R. Liu, T. Tang, V. Vittorini & Z. Wang, A literature review of Artificial Intelligence applications in railway systems. *Transportation Research Part C: Emerging Technologies* 140 (2022).

Future challenges: AI

EU Sustainable and Smart Mobility Strategy:
Putting European transport on track for the future

`https://transport.ec.europa.eu/system/files/2021-04/2021-mobility-strategy-and-action-plan.pdf`

Railways is expected to contribute by improved digitalisation and big data analytics:

R. Tang, L. De Donato, N. Bešinović, F. Flammini, R.M.P. Goverde, Z. Lin, R. Liu, T. Tang, V. Vittorini & Z. Wang, A literature review of Artificial Intelligence applications in railway systems. *Transportation Research Part C: Emerging Technologies* 140 (2022).

$\Rightarrow$ AI research in railways still in its early stages, yet major efforts dedicated to the use of AI for innovating rail maintenance policies (not surprising: promises the minimisation of equipment downtime thus reducing the high operational costs characteristic of railways)

Big data analytics: predictive maintenance

Aim: detect failures before they actually occur

Our approach (collaboration with Trenord)

$\Rightarrow$ Data-driven strategies for on-board equipment, focusing on local commuter trains Traction Control Unit (TCU) and Door CU (DCU)

Our approach (collaboration with Trenord)

$\Rightarrow$ Data-driven strategies for on-board equipment, focusing on local commuter trains Traction Control Unit (TCU) and Door CU (DCU)

TCU: adherence to acceleration/deceleration values from regulations

Our approach (collaboration with Trenord)

$\Rightarrow$ Data-driven strategies for on-board equipment, focusing on local commuter trains Traction Control Unit (TCU) and Door CU (DCU)

TCU: adherence to acceleration/deceleration values from regulations

DCU: related to safety, security and efficiency of railway operations, implying that its failure can lead to operational disruptions/delays that may propagate, thus causing economic loss and bad reputation (DCU responsible for 30% – 60% of total failures in railway vehicles)

Our approach (collaboration with Trenord)

$\Rightarrow$ Data-driven strategies for on-board equipment, focusing on local commuter trains Traction Control Unit (TCU) and Door CU (DCU)

TCU: adherence to acceleration/deceleration values from regulations

DCU: related to safety, security and efficiency of railway operations, implying that its failure can lead to operational disruptions/delays that may propagate, thus causing economic loss and bad reputation (DCU responsible for 30% – 60% of total failures in railway vehicles)

Goal: identify operational anomalies and potential defects in the data logs of these on-board units, to be able to schedule the maintenance

Our approach (collaboration with Trenord)

⇒ Data-driven strategies for on-board equipment, focusing on local commuter trains Traction Control Unit (TCU) and Door CU (DCU)

TCU: adherence to acceleration/deceleration values from regulations

DCU: related to safety, security and efficiency of railway operations, implying that its failure can lead to operational disruptions/delays that may propagate, thus causing economic loss and bad reputation (DCU responsible for 30% – 60% of total failures in railway vehicles)

Goal: identify operational anomalies and potential defects in the data logs of these on-board units, to be able to schedule the maintenance

Data-driven as opposed to model-based approaches:

− Require huge amounts of data to correctly infer a statistical model

+ Domain-agnostic nature guarantees instant applicability on the data

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

MOST
CENTRO NAZIONALE PER LA MOBILITÀ SOSTENIBILE

WP3: Digitization of railway transport

Maurice ter Beek (CNR-ISTI, Pisa)

MOST SP4 | evento finale

Politecnico di Milano

7 novembre 2025



Maurice ter Beek (CNR) | WP3 Leader

Tasks & Partners

T3.1: **Learning formal models for predictive maintenance** (leader: Maurice ter Beek, CNR–ISTI)
Partners: CNR, UNIFI, UNINA, UNIPR, UNIRM1, ACCENTURE, HRI, LUTECH, TRENORD

T3.2: **On board monitoring systems for rolling stock and infrastructure** (leader: Riccardo Licciardello, UNIRM1)
Partners: CNR, POLIMI, UNIFI, UNINA, UNIRM1, ANGEL

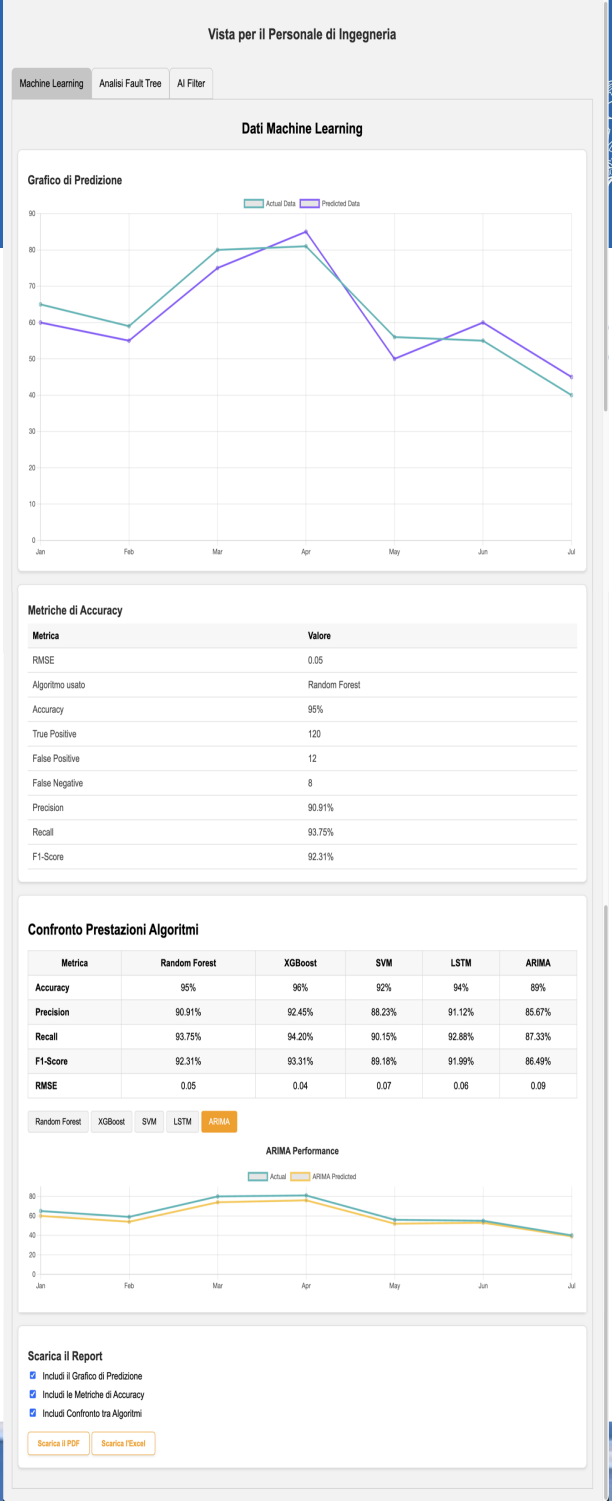
T3.3: **Way side monitoring systems for rolling stock and infrastructure** (leader: Vito Renò, CNR–STIIMA)
Partners: CNR, POLIMI, UNINA, UNIPR, UNIRM1, ISP, ANGEL

T3.4: **Drone for autonomous infrastructure inspection** (leader: Davide Tarsitano, POLIMI)
Partners: CNR, POLIMI, UNIFI, ACCENTURE, FSI-RFI

T3.1: Learning formal models for predictive maintenance

Development and improvement of TRENORD's remote diagnostics platform

- 4 years of diagnostic data from TRENORD of traction control units of 4 TSR trains and of corrective and scheduled maintenance activities
- 4 predictive maintenance approaches from 4 project partners: supervised machine learning (ML) [CNR], fault-tree analysis [UNIFI], data filtering techniques [UNINA] & ML-based forecasting [LUTECH]



Ministero dell'Università e della Ricerca

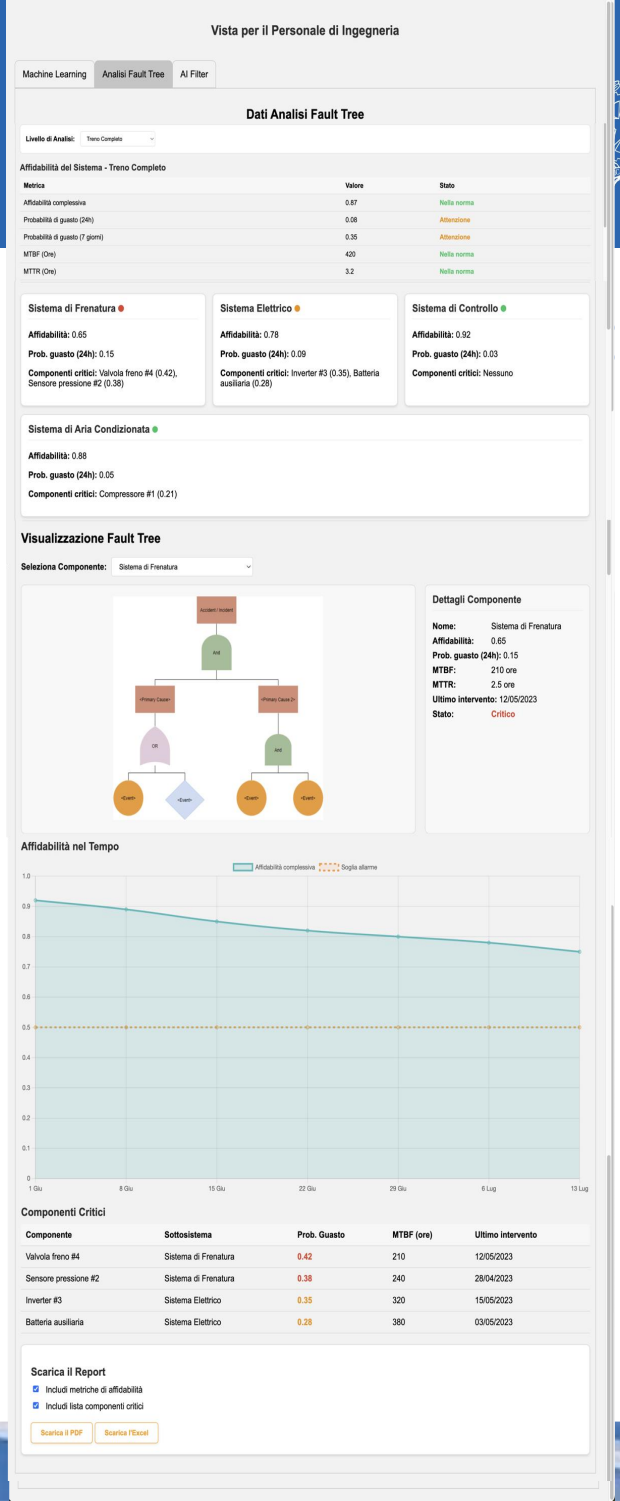
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

MOST
CENTRO NAZIONALE PER LA MOBILITÀ SOSTENIBILE

Learning formal models for predictive maintenance

Development and improvement of TRENORD's remote diagnostics platform

- 4 years of diagnostic data from TRENORD of traction control units of 4 TSR trains and of corrective and scheduled maintenance activities
- 4 predictive maintenance approaches from 4 project partners: supervised machine learning (ML) [CNR], fault-tree analysis [UNIFI], data filtering techniques [UNINA] & ML-based forecasting [LUTECH]



Ministero dell'Università e della Ricerca

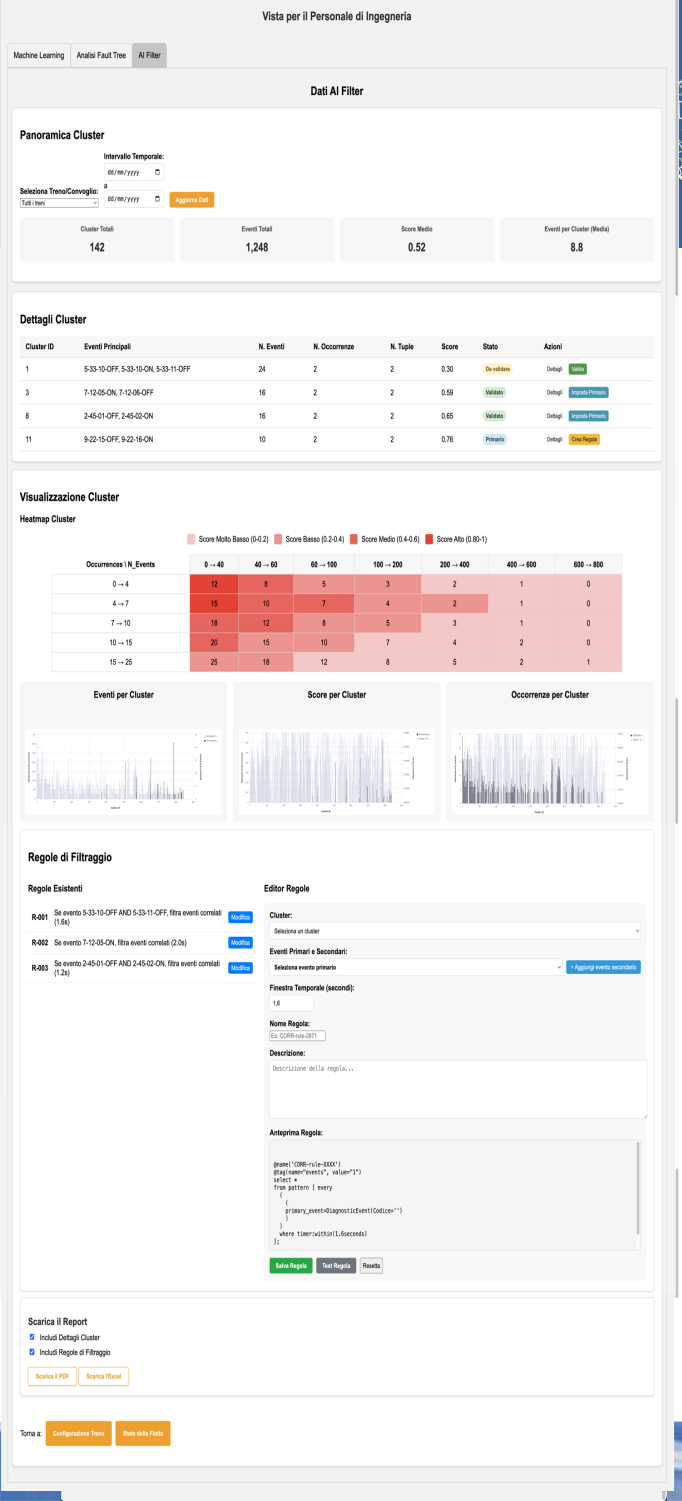
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

MOST
CENTRO NAZIONALE PER LA MOBILITÀ SOSTENIBILE

Learning formal models for predictive maintenance

Development and improvement of TRENORD's remote diagnostics platform

- 4 years of diagnostic data from TRENORD of traction control units of 4 TSR trains and of corrective and scheduled maintenance activities
- 4 predictive maintenance approaches from 4 project partners: supervised machine learning (ML) [CNR], fault-tree analysis [UNIFI], data filtering techniques [UNINA] & ML-based forecasting [LUTECH]



Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

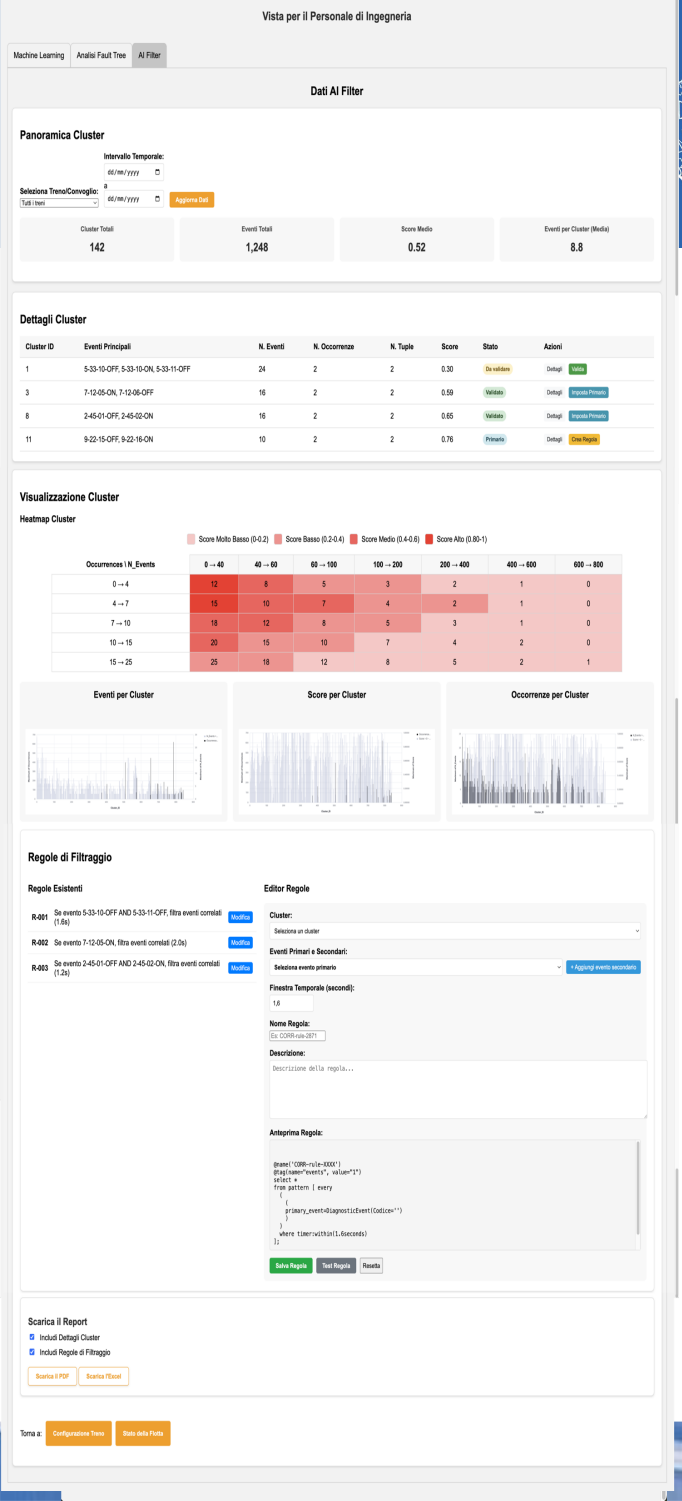
MOST
CENTRO NAZIONALE PER LA MOBILITÀ SOSTENIBILE

Learning formal models for predictive maintenance

Development and improvement of TRENORD's remote diagnostics platform

- 4 years of diagnostic data from TRENORD of traction control units of 4 TSR trains and of corrective and scheduled maintenance activities
- 4 predictive maintenance approaches from 4 project partners: supervised machine learning (ML) [CNR], fault-tree analysis [UNIFI], data filtering techniques [UNINA] & ML-based forecasting [LUTECH]

Maurice ter Beek (CNR) | WP3 Leader



Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

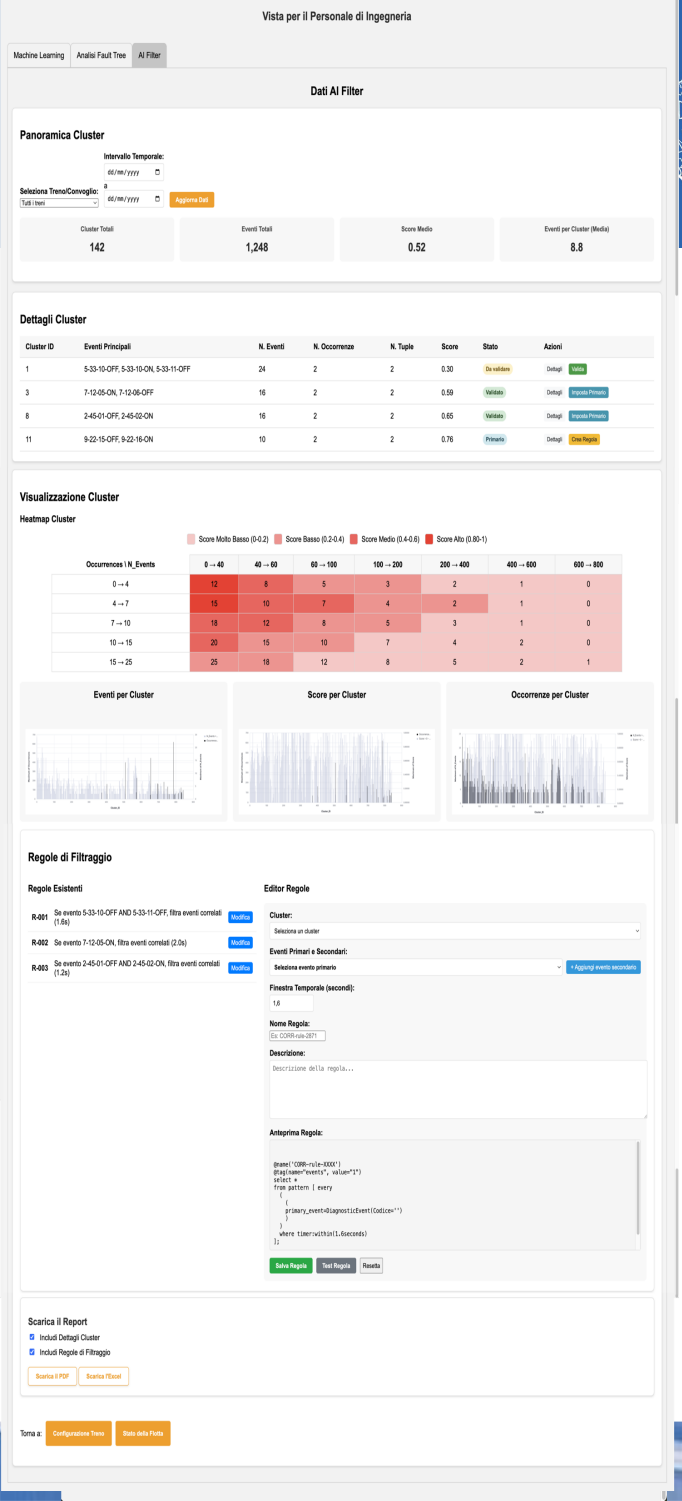
MOST
CENTRO NAZIONALE PER LA MOBILITÀ SOSTENIBILE

Learning formal models for predictive maintenance

Development and improvement of TRENORD's remote diagnostics platform

- 4 years of diagnostic data from TRENORD of traction control units of 4 TSR trains and of corrective and scheduled maintenance activities
- 4 predictive maintenance approaches from 4 project partners: supervised machine learning (ML) [CNR], fault-tree analysis [UNIFI], data filtering techniques [UNINA] & ML-based forecasting [LUTECH]

NOME CONVOGLIO	NUMERO TRENO	CHECK NUMERO TRENO	LINEA	ALLARME PIÙ GRAVE	ALLARMI ROSSI	ALLARMI GIALLI	ALLARMI AZZURRI
R3001 - R5067	24527	✓	S5 - Varese-Milano Passante-Treviglio		0	4	9
R3003 - R5038	24526	✓	S5 - Varese-Milano Passante-Treviglio		0	0	0
R3004					0	0	1
R3006					0	0	2



Ministero dell'Università e della Ricerca

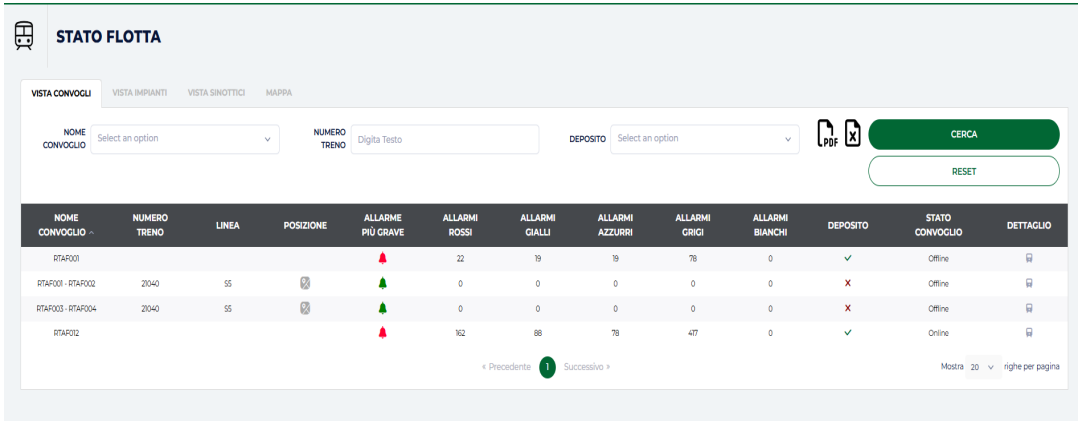
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

MOST
CENTRO NAZIONALE PER LA MOBILITÀ SOSTENIBILE

Learning formal models for predictive maintenance

Development and improvement of TRENORD's remote diagnostics platform

- 4 years of diagnostic data from TRENORD of traction control units of 4 TSR trains and of corrective and scheduled maintenance activities
- 4 predictive maintenance approaches from 4 project partners: supervised machine learning (ML) [CNR], fault-tree analysis [UNIFI], data filtering techniques [UNINA] & ML-based forecasting [LUTECH]



Maurice ter Beek (CNR) | WP3 Leader

Vista per il Personale di Ingegneria

Machine Learning | Analisi Fault Tree | AI Filter

Dati AI Filter

Panoramica Cluster

Intervallo Temporale: gg/mm/yyyy a gg/mm/yyyy Aggiorna Dati

Seleziona Treno/Convoglio: Tutti i treni

Cluster Totali	Eventi Totali	Score Medio	Eventi per Cluster (Media)
142	1,248	0.52	8.8

Dettagli Cluster

Cluster ID	Eventi Principali	N. Eventi	N. Occorrenze	N. Tuple	Score	Stato	Azioni
1	5-33-10-OFF, 5-33-10-ON, 5-33-11-OFF	24	2	2	0.30	Da validare	Dettagli Valida
3	7-12-05-ON, 7-12-06-OFF	16	2	2	0.59	Validato	Dettagli Imposta Primario
8	2-45-01-OFF, 2-45-02-ON	16	2	2	0.65	Validato	Dettagli Imposta Primario
11	9-22-15-OFF, 9-22-16-ON	10	2	2	0.76	Primario	Dettagli Crea Regola

Visualizzazione Cluster

Heatmap Cluster

Score Molto Basso (0-0.2) Score Basso (0.2-0.4) Score Medio (0.4-0.6) Score Alto (0.80-1)

Occurrences \ N_Events	0 → 40	40 → 60	60 → 100	100 → 200	200 → 400	400 → 600	600 → 800
0 → 4	12	8	5	3	2	1	0
4 → 7	15	10	7	4	2	1	0
7 → 10	18	12	8	5	3	1	0
10 → 15	20	15	10	7	4	2	0
15 → 25	25	18	12	8	5	2	1

Eventi per Cluster | Score per Cluster | Occorrenze per Cluster

Regole di Filtraggio

Regole Esistenti

R-001 Se evento 5-33-10-OFF AND 5-33-11-OFF, filtra eventi correlati (1.6s) Modifica

R-002 Se evento 7-12-05-ON, filtra eventi correlati (2.0s) Modifica

R-003 Se evento 2-45-01-OFF AND 2-45-02-ON, filtra eventi correlati (1.2s) Modifica

Editor Regole

Cluster: Seleziona un cluster

Eventi Primari e Secondari: Seleziona evento primario + Aggiungi evento secondario

Finestra Temporale (secondi): 1.6

Nome Regola: Es: CORR-rule-2871

Descrizione: Descrizione della regola...

Anteprima Regola:

```
@name("CORR-rule-XXXX")
@tag(name="events", value="1")
select *
from pattern [ every
    (
    primary_event=DiagnosticEvent(Codice='')
    )
    ->
    (
    where timer:within(1.6seconds)
];
```

Salva Regola | Testi Regola | Resetta

Scarica il Report

Includi Dettagli Cluster

Includi Regole di Filtraggio

Scarica il PDF | Scarica l'Excel

Torna a: Configurazione Treno | Stato della Flotta

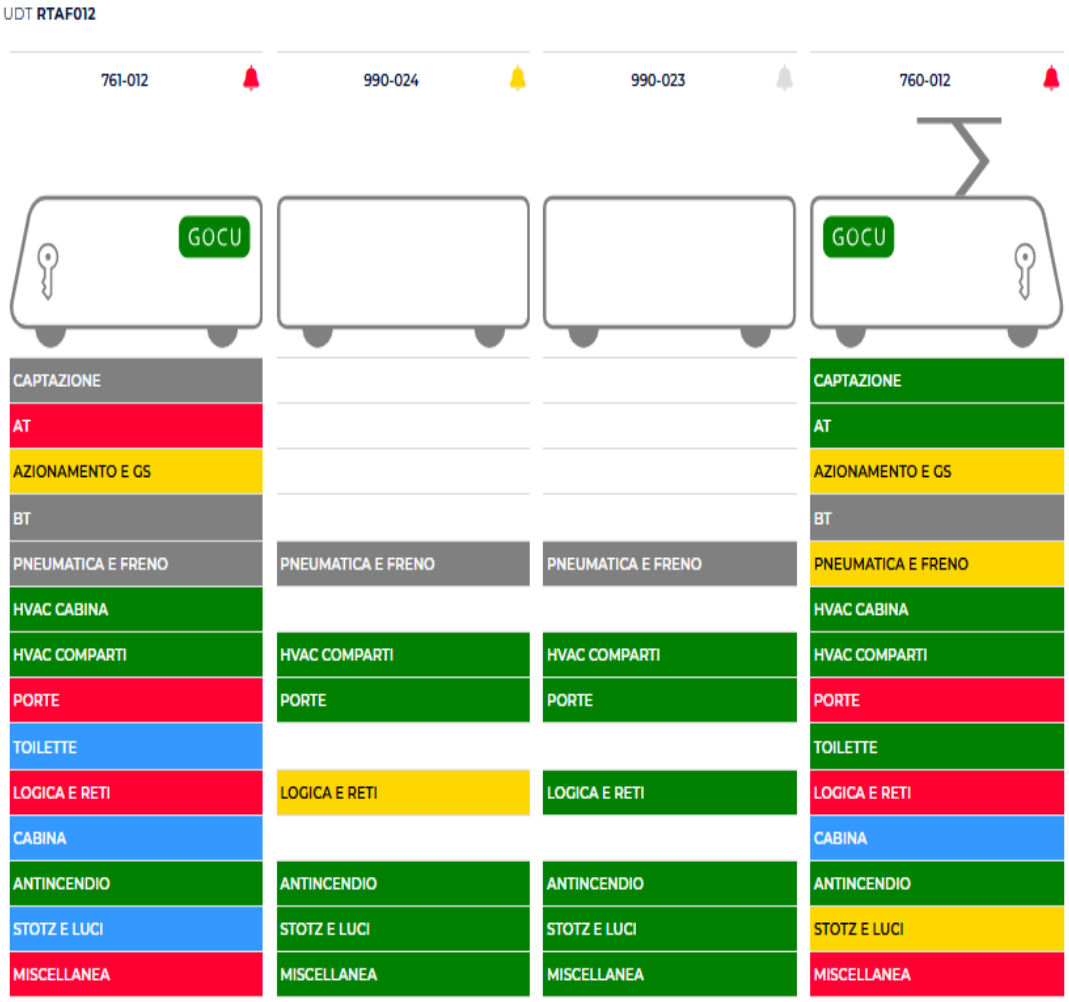
Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

MOST
CENTRO NAZIONALE PER LA MOBILITÀ SOSTENIBILE

Learning formal models for predictive maintenance

Development and improvement of TRENORD's remote diagnostics platform



Leader

Thanks for your attention!