Formal Methods and Tools in Railways

Anne's Impact and Future Challenges

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

Formal Methods and Tools Lab

Consiglio Nazionale delle Ricerche

Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"

AH65 colloquium, DTU, Denmark, February 19$^{\text{th}}$, 2026

Who am I?

Formal Methods and Tools Lab

- Member of FMT lab at CNR–ISTI since ’03, lab head since ’19
- MSc (’96) and PhD (’03) degrees from Leiden University (NL)
- Positions in HU (’95-’96,’02), BE (’05), IT (’00-’01), NL (’12-’13,’15)

Who am I? What do I work on?

- Member of FMT lab at CNR–ISTI since ’03, lab head since ’19
- MSc (’96) and PhD (’03) degrees from Leiden University (NL)
- Positions in HU (’95-’96,’02), BE (’05), IT (’00-’01), NL (’12-’13,’15)
- Formal methods, SPL, team automata, railway systems, . . .

Who am I? What's my connection with Anne?

- Member of FMT lab at CNR–ISTI since '03, lab head since '19
- MSc ('96) and PhD ('03) degrees from Leiden University (NL)
- Positions in HU ('95-'96,'02), BE ('05), IT ('00-'01), NL ('12-'13,'15)
- Formal methods, SPL, team automata, railway systems, ...
- FAC, FM, RSSRail, ISoLA, Festschrifts, DTU, ...

Outline

- Railway research
  - Sustainable mobility
  - Industrial standards
  - Anne's impact
- Formal methods and tools
  - Formal methods in railways
  - Anne's impact
  - Formal tools in railways
- Success stories
  - Anne's impact
- Future challenges
  - Anne's impact
- Concluding remarks
  - Lessons learned
  - Anne's impact

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)

Railway 200: on September 27$^{\text{th}}$, 1825 the first Railway between Stockton and Darlington opened to the public `https://railway200.co.uk/`

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)

Railway 200: on September 27$^{\text{th}}$, 1825 the first Railway between Stockton and Darlington opened to the public `https://railway200.co.uk/`

China State Key Laboratory of Rail Traffic Control and Safety

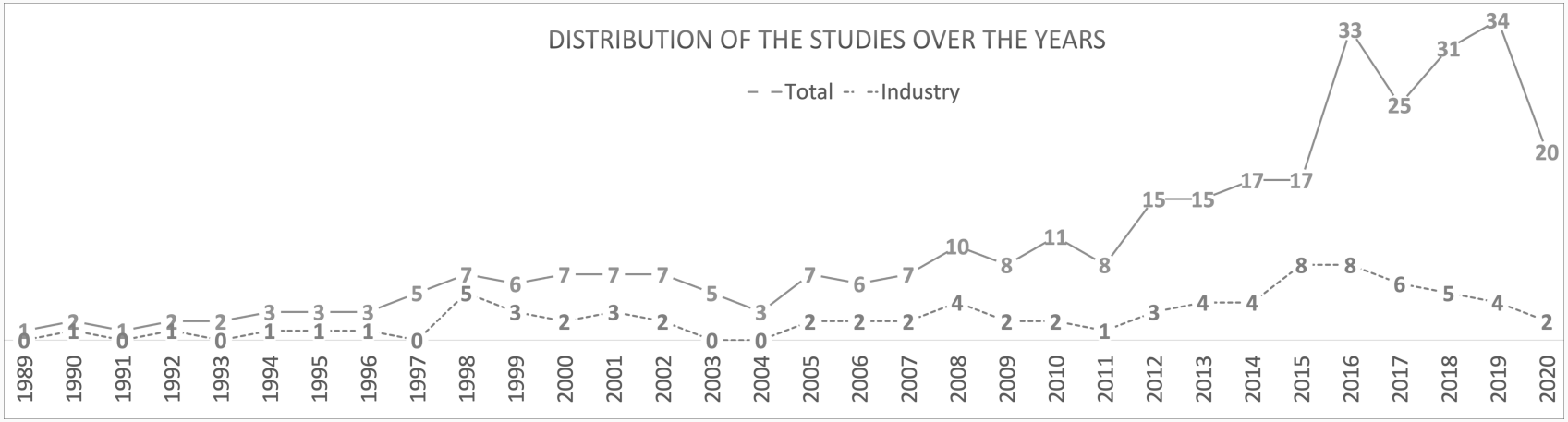
CENELEC EN 50128

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

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

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



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

Anne's impact

Anne E. Haxthausen

Associate Professor of Computer Science, Technical University of Denmark
Verified email at dtu.dk

Formal Methods Semantics Safety Railways #dtusse

rail 1/63

	All
Citations	2552
h-index	26
i10-index	60

Safety Monitoring for Future Train Control Systems J Peleska, AE Haxthausen Journeys Between Formal Methods and the Railway Industry: Essays Dedicated …		2026
A domain-specific language for generic interlocking models and their properties LH Vu, AE Haxthausen, J Peleska International Conference on Reliability, Safety and Security of Railway …	24	2017
Model checking geographically distributed interlocking systems using UMC A Fantechi, AE Haxthausen, MBR Nielsen 2017 25th Euromicro international conference on parallel, distributed and …	23	2017
Formal Modeling and Verification of Interlocking Systems Featuring Sequential Release LH Vu, AE Haxthausen, J Peleska	105	2014
Applied Bounded Model Checking for Interlocking System Designs AE Haxthausen, J Peleska, R Pinger Towards a Formal Methods Body of Knowledge for Railway Control and Safety …	60	2013
Formal development of a tool for automated modelling and verification of relay interlocking systems AE Haxthausen, AA Kjær, M Le Bliguet International Symposium on Formal Methods, 118-132	26	2011
Modelling and verification of relay interlocking systems AE Haxthausen, M Le Bliguet, AA Kjær Monterey Workshop, 141-153	54	2008
Automated verification for train control systems J Peleska, D Große, AE Haxthausen, R Drechsler FORMS/FORMAT, 296-303	29	2004

Formal methods in railways

Formal methods in railways: research questions

Systematic mapping study of formal methods for railway signalling systems

K. Petersen, S. Vakkalanka & L. Kuzniarz, Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology* (2015)

Formal methods in railways: research questions

Systematic mapping study of formal methods for railway signalling systems

K. Petersen, S. Vakkalanka & L. Kuzniarz, Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology* (2015)

RQ1 *How is research demographically and empirically characterized in the field of applications of formal methods in the railway domain?*

RQ2 *What formal methods are used in the railway domain?*

- **RQ2.1** *What is the degree of formality?*
- **RQ2.2** *What formal techniques are used?*
- **RQ2.3** *Which specification languages?*
- **RQ2.4** *Which tools?*

RQ3 *In which way are formal methods applied to railway system development?*

RQ-I *What are the characteristics of the studies reporting industrial applications?*

RQ-T : *What are the emerging trends of the last 5 years?*

Formal methods in railways: search process

Search String

Inclusion Criteria (*Abstract/Title*)

	ACM Digital Library			IEEE Xplore			Science Direct			SpringerLink - CS			SpringerLink - ENG		
Primary Search	I	II	III	I	II	III	I	II	III	I	II	III	I	II	III
Retrieved	72	9	321	631	88	205	321	86	141	1780	243	318	124	4	3
Included	34	0	6	163	15	28	74	12	8	298	22	55	8	1	0

Exclusion Criteria (*Full Text*)

Quality Criteria

Primary Search	I (X - 2017)	II (2017-2018)	III (2018 - 2020)	**Secondary Search**
Selected	198	27	67	36

	TOTAL
Retrieved	4346
Included	724
Selected	**328**

Formal methods in railways: search process

Search String

Inclusion Criteria (*Abstract/Title*)

	ACM Digital Library			IEEE Xplore			Science Direct			SpringerLink - CS			SpringerLink - ENG		
Primary Search	I	II	III	I	II	III	I	II	III	I	II	III	I	II	III
Retrieved	72	9	321	631	88	205	321	86	141	1780	243	318	124	4	3
Included	34	0	6	163	15	28	74	12	8	298	22	55	8	1	0

Exclusion Criteria (*Full Text*)

Quality Criteria

Primary Search	I (X - 2017)	II (2017-2018)	III (2018 - 2020)	**Secondary Search**
Selected	198	27	67	36

	TOTAL
Retrieved	4346
Included	724
Selected	**328**

"formal" OR "model check*" OR "model based" OR "model driven" OR "theorem prov*" OR "static analysis"

AND

"railway*" OR "CBTC" OR "ERTMS" OR "ETCS" OR "interlocking" OR "automatic train" OR "train control" OR "metro" OR "CENELEC"

Formal methods in railways: selection process

Search String

Inclusion Criteria (*Abstract/Title*)

	ACM Digital Library			IEEE Xplore			Science Direct			SpringerLink - CS			SpringerLink - ENG		
Primary Search	I	II	III	I	II	III	I	II	III	I	II	III	I	II	III
Retrieved	72	9	321	631	88	205	321	86	141	1780	243	318	124	4	3
Included	34	0	6	163	15	28	74	12	8	298	22	55	8	1	0

Exclusion Criteria (*Full Text*)

Quality Criteria

Primary Search	I (X - 2017)	II (2017-2018)	III (2018 - 2020)	**Secondary Search**
Selected	198	27	67	36

	TOTAL
Retrieved	4346
Included	724
Selected	**328**

Selected papers: read the full-text of the included papers, and apply the exclusion criteria, plus the quality checklist. A ternary scale (Yes $= 1$, Partial $= 0.5$, No $= 0$) was used to grade the papers on each question in the checklist. The quality score is the sum of the grades. If a paper does not not reach a quality score higher than 6 out of 10, exclude the paper from the selection.

Formal methods in railways: Anne's impact

Search String

Inclusion Criteria (*Abstract/Title*)

	ACM Digital Library			IEEE Xplore			Science Direct			SpringerLink - CS			SpringerLink - ENG		
Primary Search	I	II	III	I	II	III	I	II	III	I	II	III	I	II	III
Retrieved	72	9	321	631	88	205	321	86	141	1780	243	318	124	4	3
Included	34	0	6	163	15	28	74	12	8	298	22	55	8	1	0

Exclusion Criteria (*Full Text*)

Quality Criteria

Primary Search	I (X - 2017)	II (2017-2018)	III (2018 - 2020)	**Secondary Search**
Selected	198	27	67	36

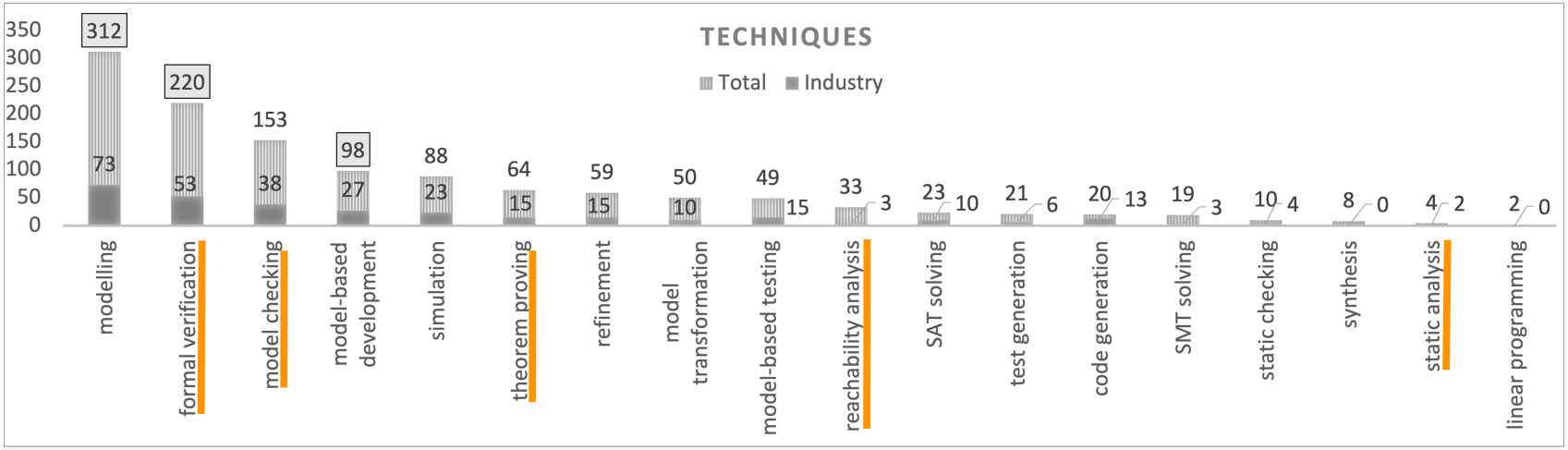
	TOTAL
Retrieved	4346
Included	724
Selected	**328**

Selected papers by Anne: 21 papers (6,5% of a total of 328) were co-authored by Anne. As a matter of fact, 5 of her papers received top grades, and the average grade of her papers is excellent (8.4). These papers moreover span 20+ years, starting with her well-cited FM'99/TSE papers with long-time collaborator Jan Peleska

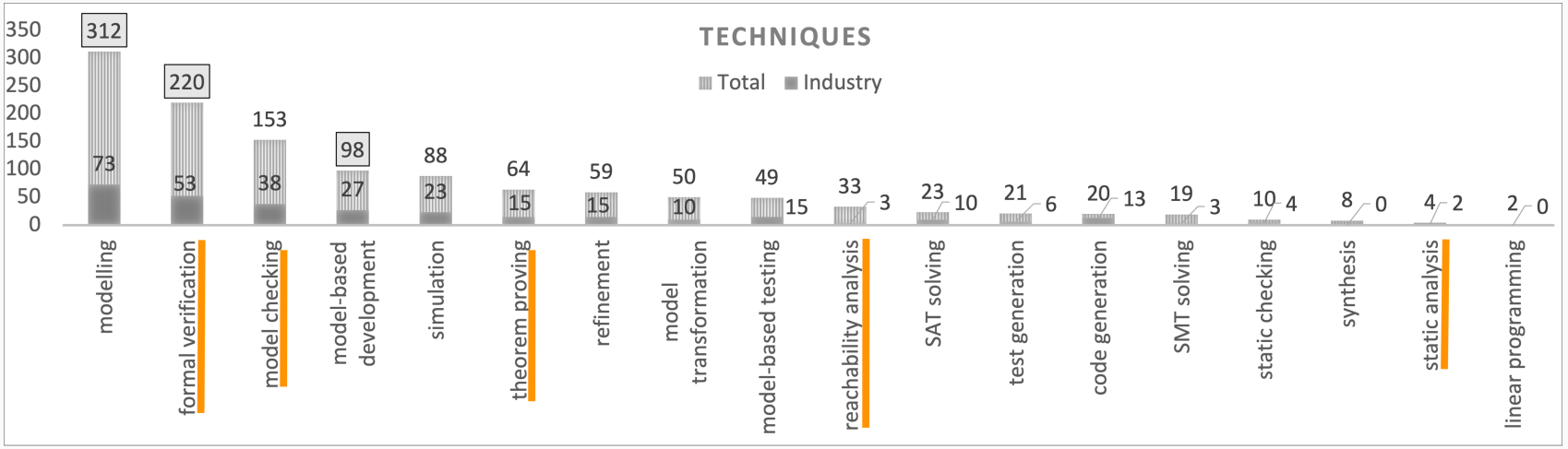
Formal development and verification of a distributed railway control system — 182 — 2000
AE Haxthausen, J Peleska
Software Engineering, IEEE Transactions on 26 (8), 687-701

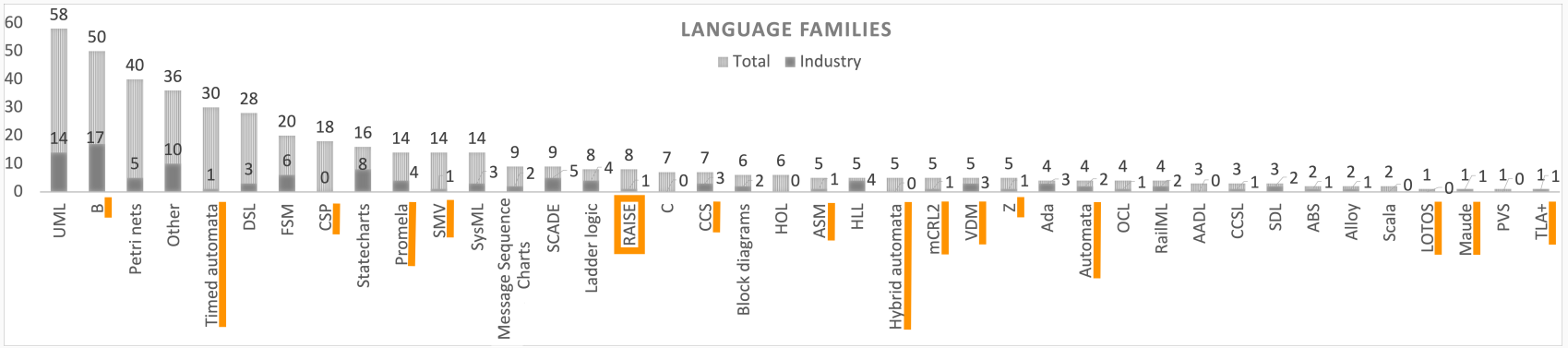
Formal development and verification of a distributed railway control system — 27 — 1999
AE Haxthausen, J Peleska
International Symposium on Formal Methods, 1546-1563

Formal methods & tools are at the basis!

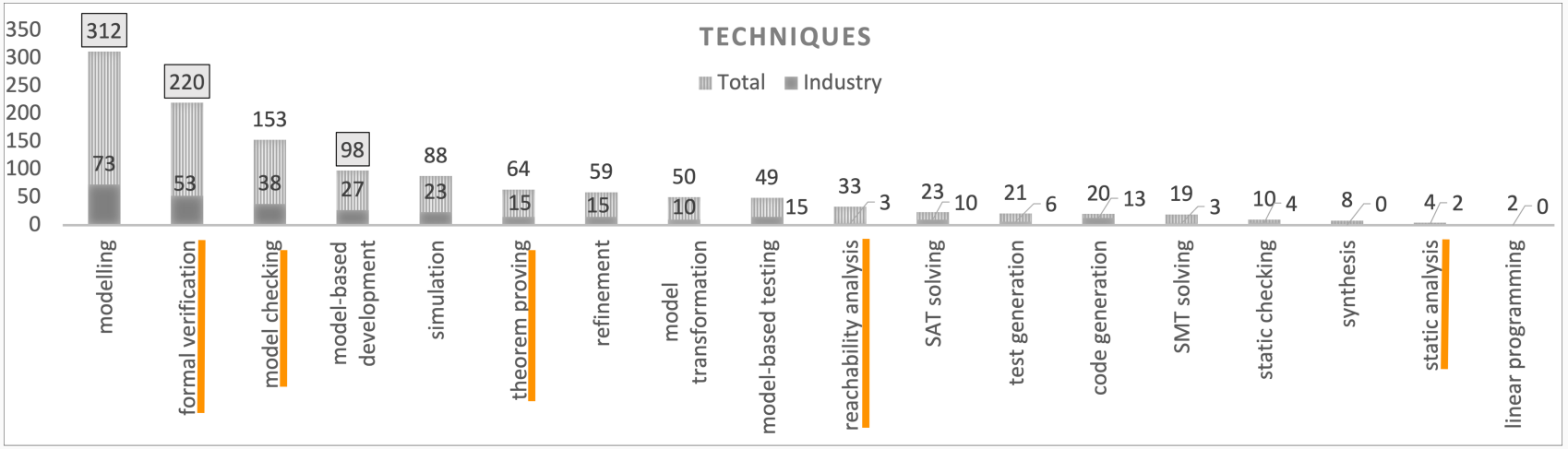


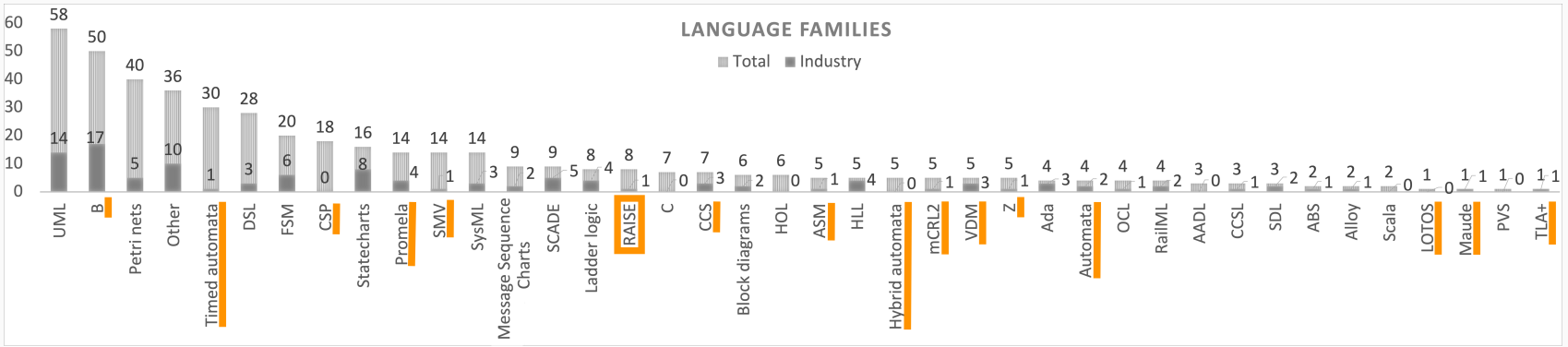
Formal methods & tools are at the basis!

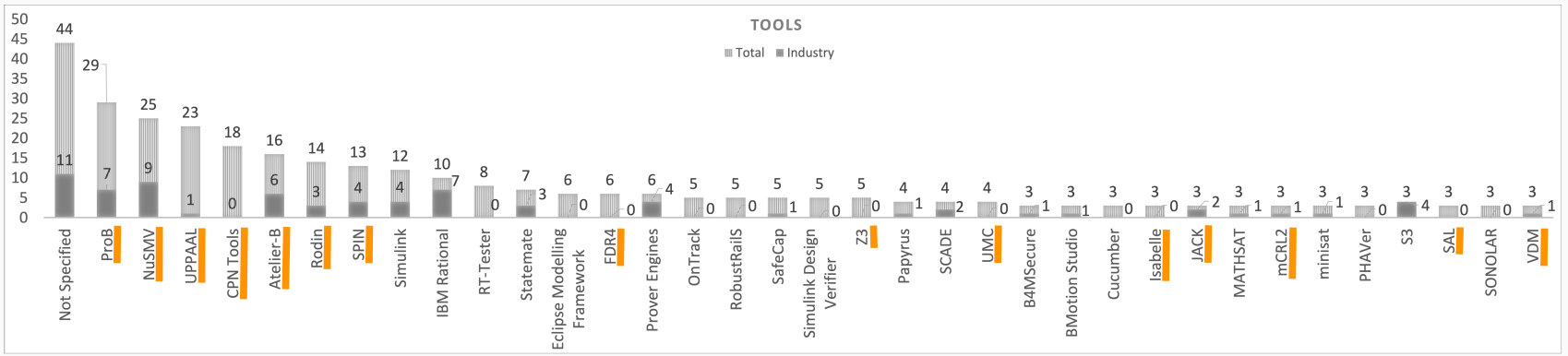




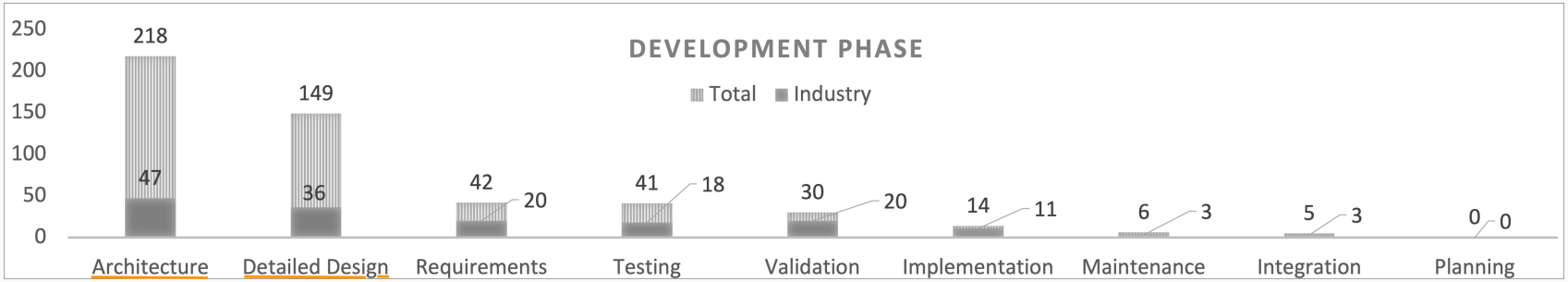
Formal methods & tools are at the basis!



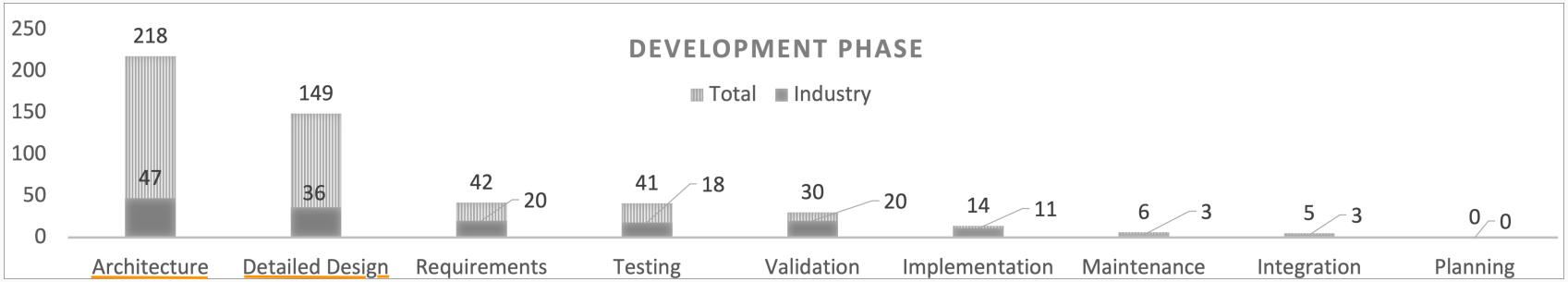




Indeed, at the basis!



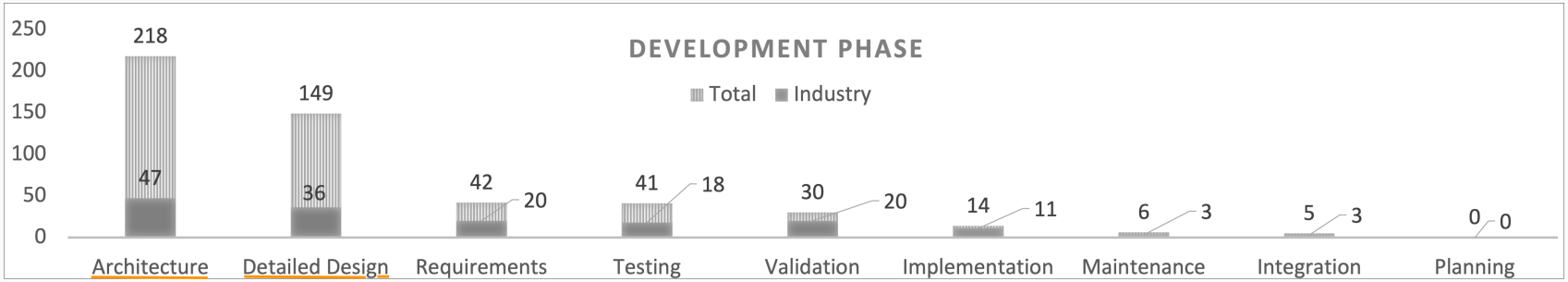
Results



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

Formal tools in railways: research questions

Systematic evaluation of formal tools for system design in railways

B. Kitchenham, S. Linkman & D. Law, DESMET: A methodology for evaluating software engineering methods and tools. *Computing & Control Engineering Journal* (1997)

Formal tools in railways: research questions

Systematic evaluation of formal tools for system design in railways

B. Kitchenham, S. Linkman & D. Law, DESMET: A methodology for evaluating software engineering methods and tools. *Computing & Control Engineering Journal* (1997)

RQ1 *Which are the features to consider for evaluating formal tools?*

RQ2 *How do different tools compare with respect to these features?*

RQ3 *How do different tools compare with respect to their usability?*

[TSE22] A. Ferrari, F. Mazzanti, D. Basile & M.H. ter Beek, Systematic Evaluation and Usability Analysis of Formal Methods Tools for Railway Signaling System Design. *IEEE Transactions on Software Engineering* (2022)

[ICSE20] A. Ferrari, F. Mazzanti, D. Basile, M.H. ter Beek & A. Fantechi, Comparing Formal Tools for System Design: a Judgment Study @ ICSE'20

Formal tools in railways: research questions

Systematic evaluation of formal tools for system design in railways

B. Kitchenham, S. Linkman & D. Law, DESMET: A methodology for evaluating software engineering methods and tools. *Computing & Control Engineering Journal* (1997)

RQ1 *Which are the features to consider for evaluating formal tools?*

RQ2 *How do different tools compare with respect to these features?*

RQ3 *How do different tools compare with respect to their usability?*

[TSE22] A. Ferrari, F. Mazzanti, D. Basile & M.H. ter Beek, Systematic Evaluation and Usability Analysis of Formal Methods Tools for Railway Signaling System Design. *IEEE Transactions on Software Engineering* (2022)

[ICSE20] A. Ferrari, F. Mazzanti, D. Basile, M.H. ter Beek & A. Fantechi, Comparing Formal Tools for System Design: a Judgment Study @ ICSE'20

Selected tools? Top ranked ones in a survey among railway practitioners

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

Characteristics and expertise of study participants

ID	Role in Study	Milieu	Main Function	Age	Sex	Years of Experience in		
						Formal Methods (FM)	Railway Industry	FM in Railways
1	assessor	academic	workpackage leader	39	M	> 13	3	13
2	assessor	academic	tool developer	62	M	> 20	0	9
3	assessor	academic	researcher	36	M	> 6	0	4
4	expert	academic	group leader	48	M	> 15	0	9
5	expert	academic	project leader	66	F	> 30	0	> 25
6	expert	academic	professor	65	M	> 30	0	> 25
7	expert	industry	system engineer	NA	M	0	> 10	0
8	expert	industry	system engineer	52	M	0	> 10	0
9	expert	industry	system engineer	48	M	0	> 10	0
10	expert	industry	software developer	43	M	0	> 10	0
11	expert	industry	product manager	NA	M	0	> 10	0
12	expert	industry	system engineer	48	M	0	> 10	0
13	expert	industry	innovation engineer	NA	M	0	> 10	0
14	expert	industry	software developer	45	M	0	> 10	0
15	expert	industry	innovation engineer	NA	F	0	3 to 10	0

Feature elicitation

Workshop with assessors, academic and industry experts: 33 features

Feature elicitation

Workshop with assessors, academic and industry experts: 33 features

The assessors produced an evaluation sheet for each tool based on:

1. install and run the tool
2. consult the tool's website for official documentation
3. search for additional documentation
4. consult the papers on formal methods and railways from the literature review to check for the tool's application in railways
5. perform tool trials to confirm claims from the documentation, and assign value to those features requiring hands-on activity
6. report the evaluation, with notes and links to documentation

Feature elicitation

Workshop with assessors, academic and industry experts: 33 features

The assessors produced an evaluation sheet for each tool based on:

1. install and run the tool
2. consult the tool's website for official documentation
3. search for additional documentation
4. consult the papers on formal methods and railways from the literature review to check for the tool's application in railways
5. perform tool trials to confirm claims from the documentation, and assign value to those features requiring hands-on activity
6. report the evaluation, with notes and links to documentation

Revision during face-to-face meetings to align visions and balance judgements, and reviewed externally as part of a project deliverable

Feature evaluation table

Category	Name	SPIN	Simulink	nuXmv	ProB	Atelier B	UPPAAL	FDR4	CPN Tools	CADP	mCRL2	SAL	TLA+	UMC
Development Functionalities	Specification / Modeling	TEXT	GRAPH	TEXTIM	TEXT	TEXT	GRAPH	TEXTIM	GRAPH	TEXTIM	TEXT	TEXTIM	TEXT	TEXT
	Code Generation	NO	YES	NO	NO	YES	NO	NO	NO	YES	NO	NO	NO	NO
	Documentation / Report Generation	PARTIAL	YES	NO	PARTIAL	PARTIAL	PARTIAL	PARTIAL	NO	PARTIAL	PARTIAL	NO	NO	PARTIAL
	Requirements Traceability	NO	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Project Management	NO	YES	NO	YES	YES	NO	NO	NO	NO	NO	NO	NO	NO
Verification Functionalities	Simulation	TEXT	GRAPH	TEXT	MIX	NO	GRAPH	TEXT	GRAPH	TEXT	TEXT	TEXT	NO	TEXT
	Formal Verification	MC-L	MC-O	MC-L,MC-B	MC-L,MC-B,RF	TP	MC-L,RF	RF	MC-B	MC-B,RF	MC-B,RF	MC-L,TP	MC-L,TP	MC-B
	Large-scale Verification Technique	FLY,POR,PAR	BMC	BMC,SYM	SCT	SCT	SMC,SYM	COM,POR	BMC	COM,PAR	COM	PAR,SCT	SYM,SCT	FLY
	Model-based Testing	NO	YES	NO	YES	NO	YES	NO	NO	YES	NO	YES	NO	NO
Language Expressiveness	Non-determinism	INT	EXT	INT,EXT	INT,EXT	INT,EXT	INT,EXT	INT,EXT	INT	INT,EXT	INT,EXT	INT,EXT	INT	INT
	Concurrency	ASYNCH	NO	SYNCH	NO	NO	SYNCH	ASYNCH	ASYNCH	ASYNCH	ASYNCH	A/SYNCH	ASYNCH	A/SYNCH
	Timing Aspects	NO	YES	YES	NO	NO	YES	YES	YES	NO	YES	YES	NO	NO
	Stochastic or Probabilistic Aspects	NO	NO	NO	NO	NO	YES	NO	NO	NO	YES	NO	NO	NO
	Modularity of the Language	HIGH	HIGH	MEDIUM	LOW	LOW	MEDIUM	HIGH	HIGH	HIGH	HIGH	MEDIUM	MEDIUM	HIGH
	Supported Data Structures	BASIC	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX
	Float Support	NO	YES	YES	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO
Tool Flexibility	Backward Compatibility	LIKELY	LIKELY	LIKELY	LIKELY	MODERATE	LIKELY	MODERATE	LIKELY	LIKELY	LIKELY	MODERATE	MODERATE	MODERATE
	Standard Input Format	OPEN	PARTIAL	OPEN	OPEN	OPEN	PARTIAL	OPEN	PARTIAL	STANDARD	OPEN	OPEN	OPEN	STANDARD
	Import / Export vs. Other Tools	MEDIUM	LOW	MEDIUM	HIGH	MEDIUM	LOW	MEDIUM	MEDIUM	HIGH	HIGH	MEDIUM	LOW	MEDIUM
	Modularity of the Tool	LOW	HIGH	LOW	HIGH	MEDIUM	HIGH	LOW	LOW	HIGH	MEDIUM	LOW	LOW	MEDIUM
	Team Support	NO	NO	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO	NO
Maturity	Industrial Diffusion	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	MEDIUM	MEDIUM	MEDIUM	MEDIUM	LOW	MEDIUM	LOW
	Stage of Development	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	PROTOTYPE
Usability	Availability of Customer Support	PARTIAL	YES	PARTIAL	YES	YES	YES	PARTIAL	PARTIAL	PARTIAL	PARTIAL	PARTIAL	PARTIAL	PARTIAL
	Graphical User Interface	LIMITED	YES	NO	PARTIAL	PARTIAL	YES	LIMITED	PARTIAL	LIMITED	PARTIAL	NO	LIMITED	PARTIAL
	Mathematical Background	MEDIUM	BASIC	MEDIUM	MEDIUM	ADVANCED	MEDIUM	ADVANCED	MEDIUM	ADVANCED	ADVANCED	ADVANCED	ADVANCED	MEDIUM
	Quality of Documentation	GOOD	EXCELLENT	GOOD	GOOD	EXCELLENT	GOOD	EXCELLENT	GOOD	GOOD	GOOD	GOOD	GOOD	LIMITED
Company Constraints	Cost	FREE	PAY	MIX	FREE	FREE	MIX	MIX	FREE	MIX	FREE	FREE	FREE	FREE
	Supported Platforms	ALL	ALL	ALL	ALL	ALL	ALL	ALL	Windows	ALL	ALL	ALL	ALL	ALL
	Complexity of License Management	EASY	ADEQUATE	EASY	EASY	EASY	MODERATE	MODERATE	EASY	MODERATE	EASY	EASY	EASY	EASY
	Easy to Install	YES	YES	YES	YES	YES	YES	YES	YES	PARTIAL	YES	YES	YES	YES
Railway-specific Criteria	CENELEC Certification	NO	PARTIAL	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO	NO
	Integration in the CENELEC Process	MEDIUM	YES	MEDIUM	YES	YES	MEDIUM	MEDIUM	MEDIUM	MEDIUM	LOW	LOW	LOW	MEDIUM
		SPIN	Simulink	nuXmv	ProB	Atelier B	UPPAAL	FDR4	CPN Tools	CADP	mCRL2	SAL	TLA+	UMC

Feature evaluation table

Category	Name	SPIN	Simulink	nuXmv	ProB	Atelier B	UPPAAL	FDR4	CPN Tools	CADP	mCRL2	SAL	TLA+	UMC
Development Functionalities	Specification / Modeling	TEXT	GRAPH	TEXTIM	TEXT	TEXT	GRAPH	TEXTIM	GRAPH	TEXTIM	TEXT	TEXTIM	TEXT	TEXT
	Code Generation	NO	YES	NO	NO	YES	NO	NO	NO	YES	NO	NO	NO	NO
	Documentation / Report Generation	PARTIAL	YES	NO	PARTIAL	PARTIAL	PARTIAL	PARTIAL	NO	PARTIAL	PARTIAL	NO	NO	PARTIAL
	Requirements Traceability	NO	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
	Project Management	NO	YES	NO	YES	YES	NO	NO	NO	NO	NO	NO	NO	NO
Verification Functionalities	Simulation	TEXT	GRAPH	TEXT	MIX	NO	GRAPH	TEXT	GRAPH	TEXT	TEXT	TEXT	NO	TEXT
	Formal Verification	MC-L	MC-O	MC-L,MC-B	MC-L,MC-B,RF	TP	MC-L,RF	RF	MC-B	MC-B,RF	MC-B,RF	MC-L,TP	MC-L,TP	MC-B
	Large-scale Verification Technique	FLY,POR,PAR	BMC	BMC,SYM	SCT	SCT	SMC,SYM	COM,POR	BMC	COM,PAR	COM	PAR,SCT	SYM,SCT	FLY
	Model-based Testing	NO	YES	NO	YES	NO	YES	NO	NO	YES	NO	YES	NO	NO
Language Expressiveness	Non-determinism	INT	EXT	INT,EXT	INT,EXT	INT,EXT	INT,EXT	INT,EXT	INT	INT,EXT	INT,EXT	INT,EXT	INT	INT
	Concurrency	ASYNCH	NO	SYNCH	NO	NO	SYNCH	ASYNCH	ASYNCH	ASYNCH	ASYNCH	A/SYNCH	ASYNCH	A/SYNCH
	Timing Aspects	NO	YES	YES	NO	NO	YES	YES	YES	NO	YES	YES	NO	NO
	Stochastic or Probabilistic Aspects	NO	NO	NO	NO	NO	YES	NO	NO	NO	YES	NO	NO	NO
	Modularity of the Language	HIGH	HIGH	MEDIUM	LOW	LOW	MEDIUM	HIGH	HIGH	HIGH	HIGH	MEDIUM	MEDIUM	HIGH
	Supported Data Structures	BASIC	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX	COMPLEX
	Float Support	NO	YES	YES	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO
Tool Flexibility	Backward Compatibility	LIKELY	LIKELY	LIKELY	LIKELY	MODERATE	LIKELY	MODERATE	LIKELY	LIKELY	LIKELY	MODERATE	MODERATE	MODERATE
	Standard Input Format	OPEN	PARTIAL	OPEN	OPEN	OPEN	PARTIAL	OPEN	PARTIAL	STANDARD	OPEN	OPEN	OPEN	STANDARD
	Import / Export vs. Other Tools	MEDIUM	LOW	MEDIUM	HIGH	MEDIUM	LOW	MEDIUM	MEDIUM	HIGH	HIGH	MEDIUM	LOW	MEDIUM
	Modularity of the Tool	LOW	HIGH	LOW	HIGH	MEDIUM	HIGH	LOW	LOW	HIGH	MEDIUM	LOW	LOW	MEDIUM
	Team Support	NO	NO	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO	NO
Maturity	Industrial Diffusion	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	MEDIUM	MEDIUM	MEDIUM	MEDIUM	LOW	MEDIUM	LOW
	Stage of Development	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	MATURE	PROTOTYPE
Usability	Availability of Customer Support	PARTIAL	YES	PARTIAL	YES	YES	YES	PARTIAL	PARTIAL	PARTIAL	PARTIAL	PARTIAL	PARTIAL	PARTIAL
	Graphical User Interface	LIMITED	YES	NO	PARTIAL	PARTIAL	YES	LIMITED	PARTIAL	LIMITED	PARTIAL	NO	LIMITED	PARTIAL
	Mathematical Background	MEDIUM	BASIC	MEDIUM	MEDIUM	ADVANCED	MEDIUM	ADVANCED	MEDIUM	ADVANCED	ADVANCED	ADVANCED	ADVANCED	MEDIUM
	Quality of Documentation	GOOD	EXCELLENT	GOOD	GOOD	EXCELLENT	GOOD	EXCELLENT	GOOD	GOOD	GOOD	GOOD	GOOD	LIMITED
Company Constraints	Cost	FREE	PAY	MIX	FREE	FREE	MIX	MIX	FREE	MIX	FREE	FREE	FREE	FREE
	Supported Platforms	ALL	ALL	ALL	ALL	ALL	ALL	ALL	Windows	ALL	ALL	ALL	ALL	ALL
	Complexity of License Management	EASY	ADEQUATE	EASY	EASY	EASY	MODERATE	MODERATE	EASY	MODERATE	EASY	EASY	EASY	EASY
	Easy to Install	YES	YES	YES	YES	YES	YES	YES	YES	PARTIAL	YES	YES	YES	YES
Railway-specific Criteria	CENELEC Certification	NO	PARTIAL	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO	NO
	Integration in the CENELEC Process	MEDIUM	YES	MEDIUM	YES	YES	MEDIUM	MEDIUM	MEDIUM	MEDIUM	LOW	LOW	LOW	MEDIUM
		SPIN	Simulink	nuXmv	ProB	Atelier B	UPPAAL	FDR4	CPN Tools	CADP	mCRL2	SAL	TLA+	UMC

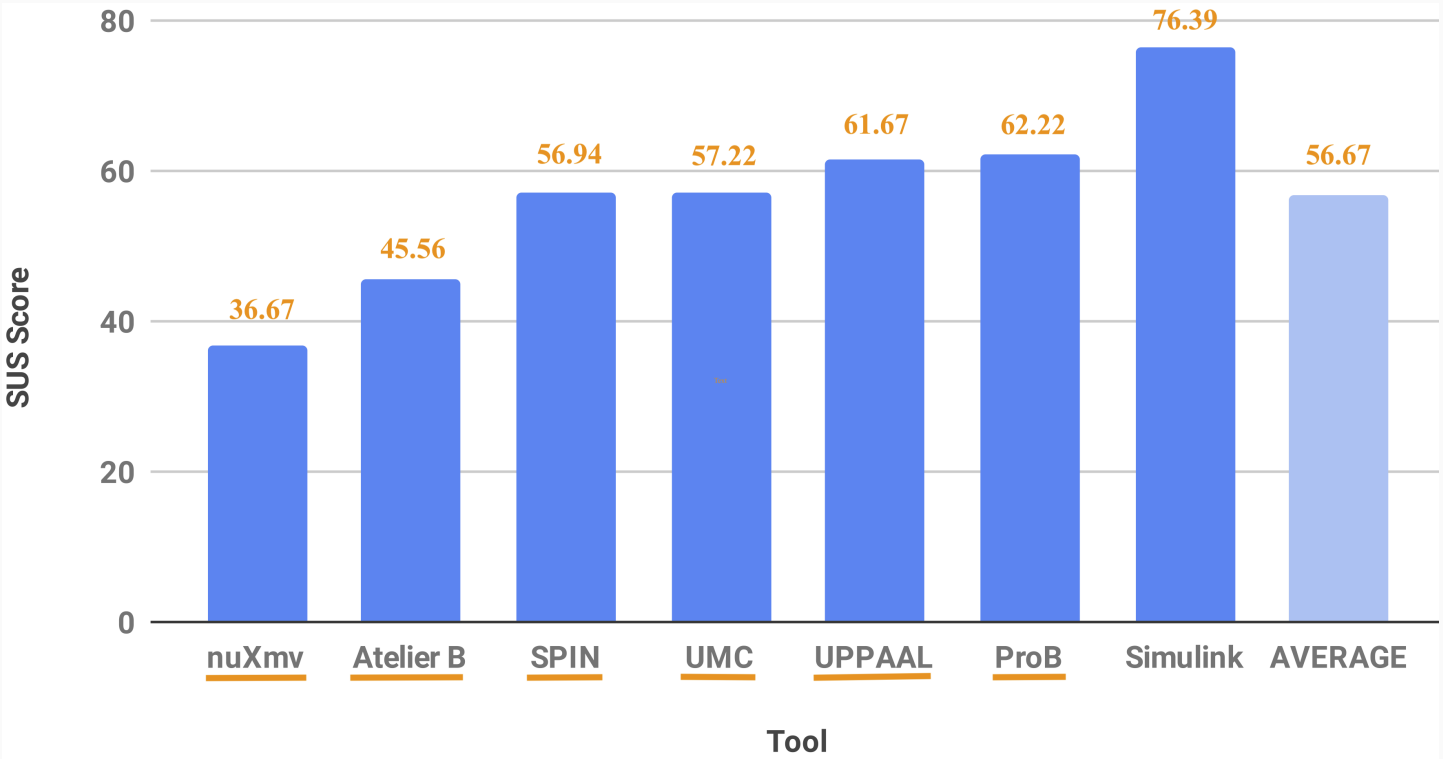
e.g. ProB and Atelier-B both stand out for project management and score well on tool flexibility, maturity and usability; TLA+ much less

System Usability Scale (SUS) evaluation

Tool demos presented in meeting with experts: structure, opening, navigating and describing the predeveloped moving block model, followed by guided simulation and formal verification session; after each tool presentation, the experts filled a usability questionnaire

System Usability Scale (SUS) evaluation

Tool demos presented in meeting with experts: structure, opening, navigating and describing the predeveloped moving block model, followed by guided simulation and formal verification session; after each tool presentation, the experts filled a usability questionnaire



J. Brooke,
SUS: A 'quick and dirty' usability scale. Usability Evaluation in Industry (1996)
SUS: A retrospective. *Journal of Usability Studies* (2013)

Take-away messages

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

Results

Take-away messages

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

Formal methods & tools in railways: Success stories

Well-known success stories

Formal Methods and Tools Lab

Using B

- **B** Automatic Train Protection (ATP) system of Paris RER Line A
- **B** Subway Speed Control System (SSCS) of the Calcutta subway
- **B** Paris Metro Line 14 and its derivatives, like NY Canarsie line 1
- **B** Alstom's U400 system (in use in $\pm$ 100 metro lines worldwide)
- **B** Driverless Paris–Roissy Airport shuttle

Well-known success stories

Using B, Simulink/Stateflow, NuSMV, SPIN, AADL, UPPAAL, ...

- **B** Automatic Train Protection (ATP) system of Paris RER Line A
- **B** Subway Speed Control System (SSCS) of the Calcutta subway
- **B** Paris Metro Line 14 and its derivatives, like NY Canarsie line 1
- **B** Alstom's U400 system (in use in $\pm$ 100 metro lines worldwide)
- **B** Driverless Paris–Roissy Airport shuttle

- Metro control system of Rio de Janeiro
- Movement Authority (MA) scenario of Chinese Train Control System Level 3 (CTCS-3)
- Autonomous Positioning System (APS) of Florence tramways

Well-known success stories

Using B, Simulink/Stateflow, NuSMV, SPIN, AADL, UPPAAL, ...

- **B** Automatic Train Protection (ATP) system of Paris RER Line A
- **B** Subway Speed Control System (SSCS) of the Calcutta subway
- **B** Paris Metro Line 14 and its derivatives, like NY Canarsie line 1
- **B** Alstom's U400 system (in use in ± 100 metro lines worldwide)
- **B** Driverless Paris–Roissy Airport shuttle

- Metro control system of Rio de Janeiro
- Movement Authority (MA) scenario of Chinese Train Control System Level 3 (CTCS-3)
- Autonomous Positioning System (APS) of Florence tramways

ERTMS/ETCS standard, e.g., ERTMS/ETCS Hybrid Level 3 → ABZ 2018 case study; M. Bartholomeus, B. Luttik & T.A.C. Willemse, Modelling and Analysing ERTMS Hybrid Level 3 with the mCRL2 Toolset @ FMICS'18

...

A History of Formal Methods in Railways

MAURICE H. TER BEEK*, CNR–ISTI, Italy
ALESSANDRO FANTECHI, University of Florence, Italy
ALESSIO FERRARI, University College Dublin, Ireland
STEFANIA GNESI, CNR–ISTI, Italy
ANNE E. HAXTHAUSEN, Technical University of Denmark, Denmark
THIERRY LECOMTE, CLEARSY Systems Engineering, France

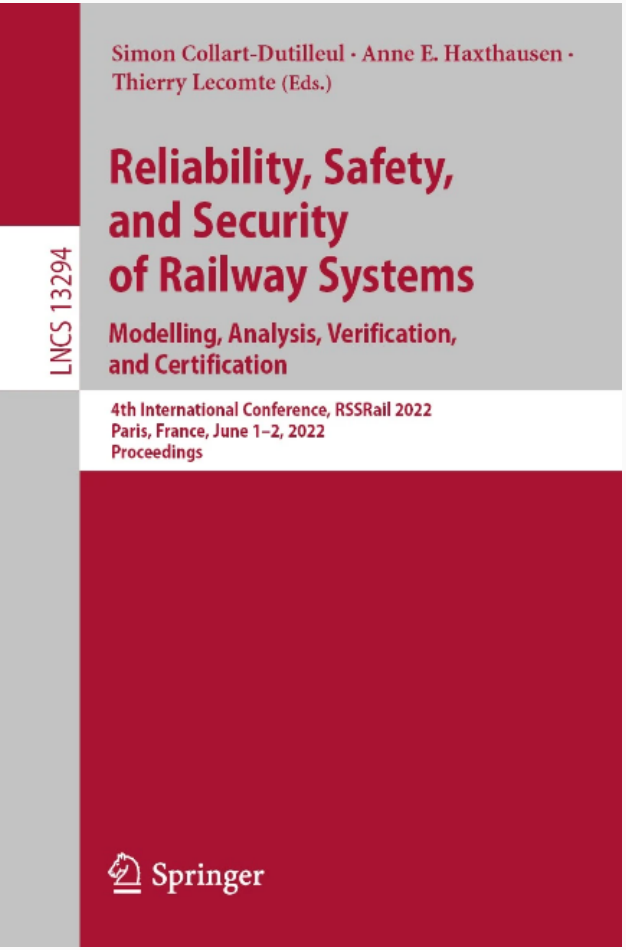
The engineering of industrial systems, particularly in safety-critical domains such as railways, demands rigorous verification and validation processes to ensure system dependability. Formal methods have emerged as powerful tools to complement traditional software engineering practices. In the railway sector, which increasingly relies on complex, distributed, and cyber-physical control systems, formal methods have demonstrated particular value for many decades now. In this paper, we provide a retrospective overview of the application of formal methods and tools in the railway domain, with emphasis on two prominent verification approaches and one frequently verified railway system: modeling and validation with the B method and tools and formal verification of interlocking systems by model checking. We explore their role in the design and development of key railway systems, highlighting both academic research and industrial success stories, as witnessed by international projects and initiatives. We conclude with an outlook on the potential of integrating AI and formal methods to enhance the efficiency of next-generation railway systems.

CCS Concepts: • **Software and its engineering** → **Formal methods**; • **Social and professional topics** → **History of computing**.

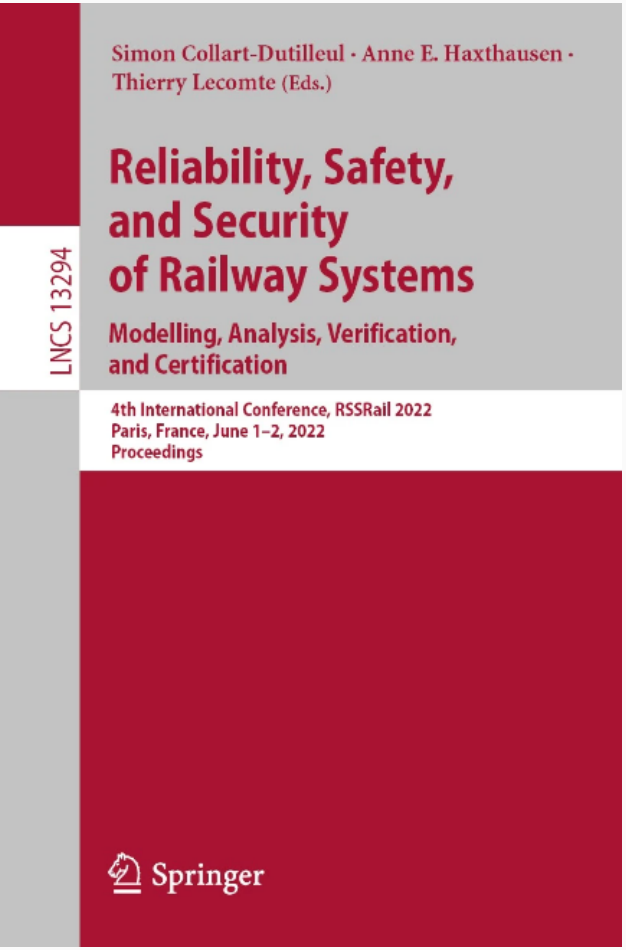
Additional Key Words and Phrases: Formal Methods, Railways

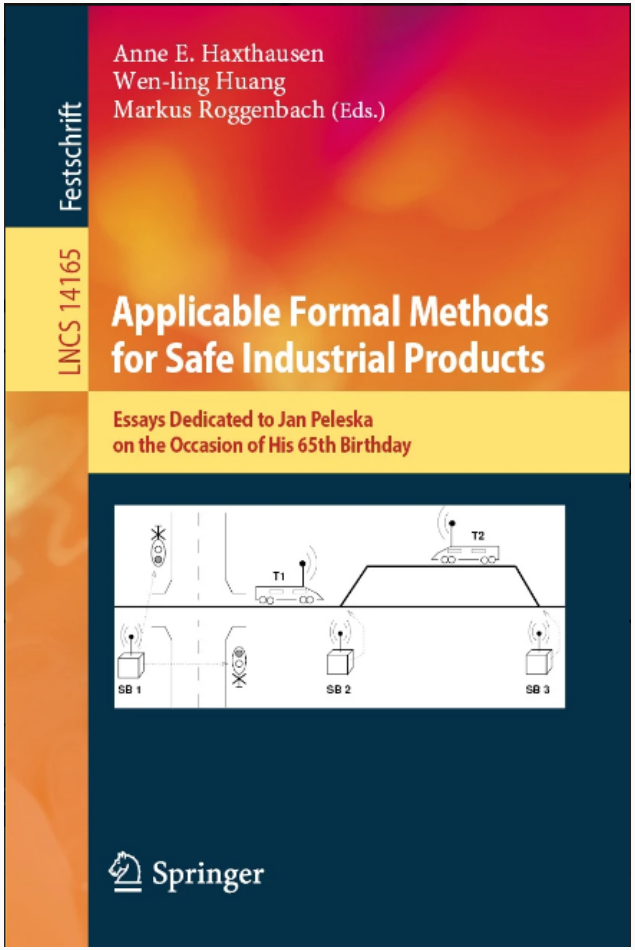
ACM Reference Format:
Maurice H. ter Beek, Alessandro Fantechi, Alessio Ferrari, Stefania Gnesi, Anne E. Haxthausen, and Thierry Lecomte. 2026. A History of Formal Methods in Railways. *Form. Asp. Comput.* XX, Y (July 2026), 31 pages. https://doi.org/10.1145/ZZZ

Some of Anne's success stories: RSSRail

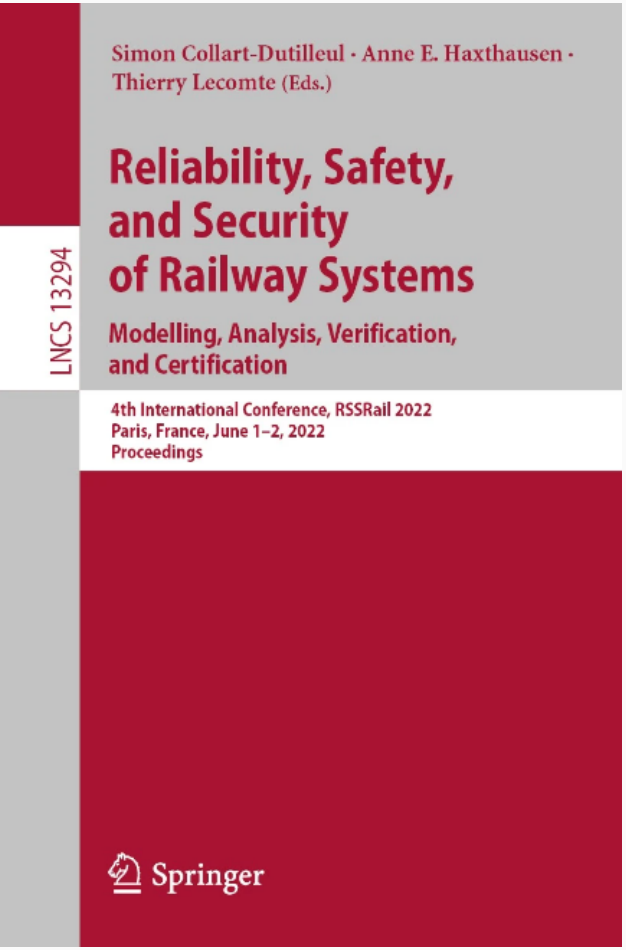


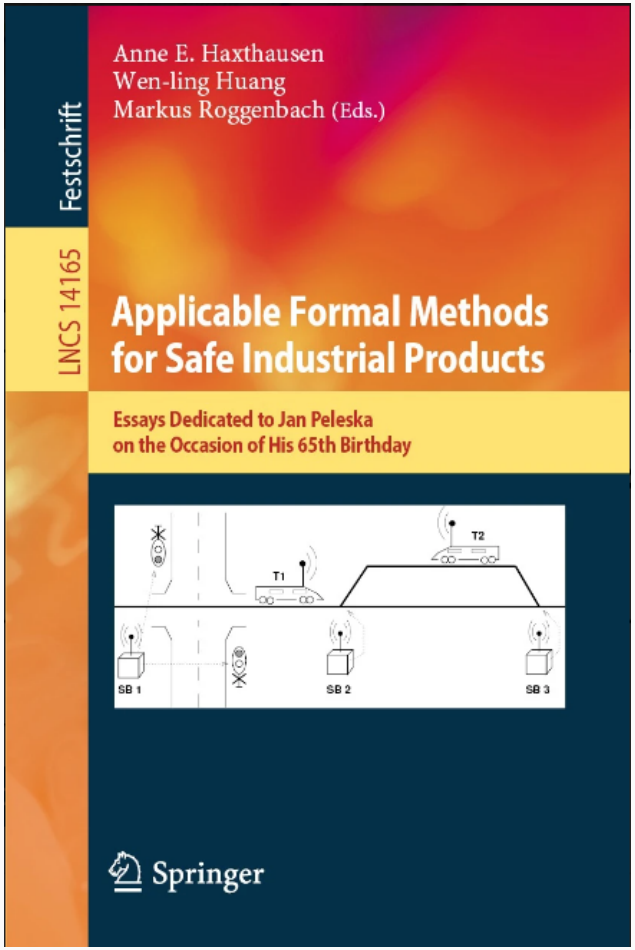
Some of Anne's success stories: RSSRail + Festschrift

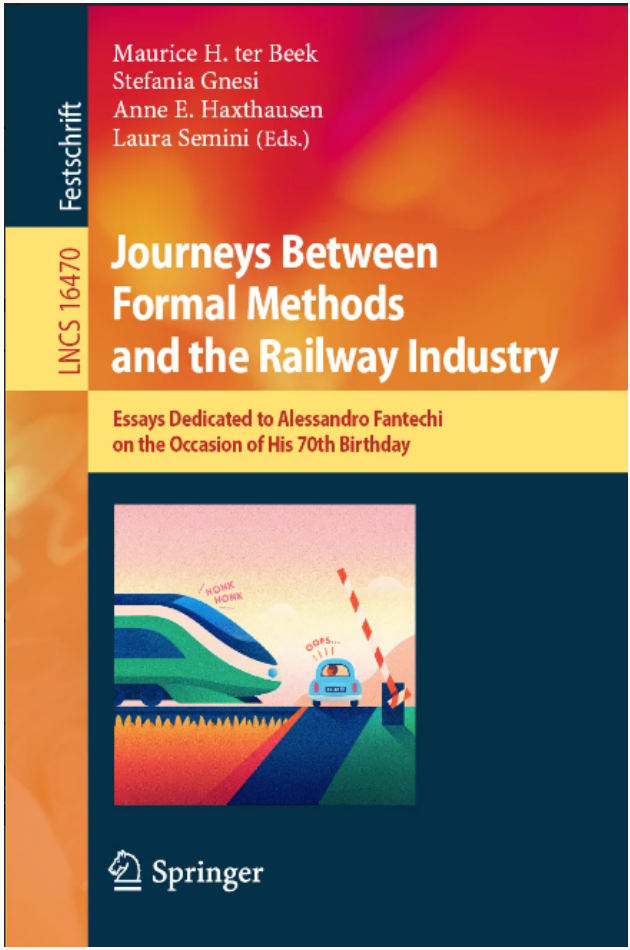




Some of Anne's success stories: RSSRail + Festschrifts







Some of Anne's success stories: RSSRail + Festschrifts

Some of Anne's success stories: ISoLA + DisCoRail

Formal Methods and Tools Lab

2024

- [c49] Alessandro Fantechi, Stefania Gnesi, Anne E. Haxthausen: **Formal Methods for Distributed Computing in Future Railway Systems.** ISoLA (5) 2024: 109-111
- [c48] Christophe Limbrée, Anne E. Haxthausen, Gloria Gori, Alessandro Fantechi: **Formal Verification of Railway Interlockings: a Compositional Approach Based on a Library of Pre-verified Components.** ISoLA (5) 2024: 127-141

2022

- [c44] Alessandro Fantechi, Stefania Gnesi, Anne E. Haxthausen: **Formal Methods for Distributed Control Systems of Future Railways.** ISoLA (4) 2022: 243-245
- [c43] Monika Seisenberger, Maurice H. ter Beek, Xiuyi Fan, Alessio Ferrari, Anne E. Haxthausen, Phillip James, Andrew Lawrence, Bas Luttik, Jaco van de Pol, Simon Wimmer: **Safe and Secure Future AI-Driven Railway Technologies: Challenges for Formal Methods in Railway.** ISoLA (4) 2022: 246-268
- [c42] Jan Peleska, Anne E. Haxthausen, Thierry Lecomte: **Standardisation Considerations for Autonomous Train Control.** ISoLA (4) 2022: 286-307

2020

- [c40] Alessandro Fantechi, Stefania Gnesi, Anne E. Haxthausen: **Formal Methods for Distributed Computing in Future Railway Systems.** ISoLA (3) 2020: 389-392
- [c39] Per Lange Laursen, Van Anh Thi Trinh, Anne E. Haxthausen: **Formal Modelling and Verification of a Distributed Railway Interlocking System Using UPPAAL.** ISoLA (3) 2020: 415-433
- [c38] Signe Geisler, Anne E. Haxthausen: **Model Checking a Distributed Interlocking System Using k-induction with RT-Tester.** ISoLA (3) 2020: 449-466

2016

- [c29] Anne E. Haxthausen, Jan Peleska: **On the Feasibility of a Unified Modelling and Programming Paradigm.** ISoLA (2) 2016: 32-49
- [c28] Anne E. Haxthausen, Peter H. Østergaard: **On the Use of Static Checking in the Verification of Interlocking Systems.** ISoLA (2) 2016: 266-278
- [c27] Hugo Daniel Macedo, Alessandro Fantechi, Anne E. Haxthausen: **Compositional Verification of Multi-station Interlocking Systems.** ISoLA (2) 2016: 279-293

2012

- [c19] Anne E. Haxthausen: **Automated Generation of Safety Requirements from Railway Interlocking Tables.** ISoLA (2) 2012: 261-275

Some of Anne's success stories: ISoLA + DisCoRail

Formal methods for DIStributed COmputing in future RAILway systems (DisCoRail)

Organizers:

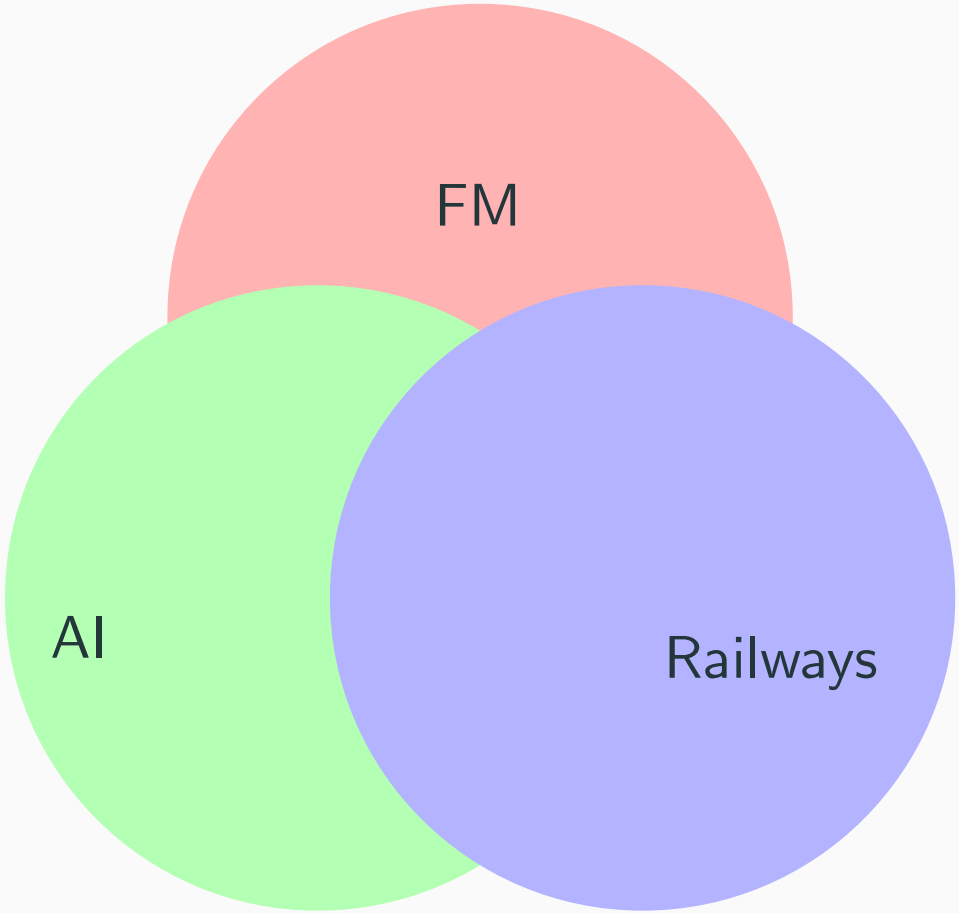
- Alessandro Fantechi (Università di Firenze, IT)
- Stefania Gnesi (Institute of Information Science and Technologies ISTI-CNR, IT)
- Anne Haxthausen (Technical University of Denmark, DK)

Some of Anne's success stories: ISoLA + DisCoRail

Some of Anne's success stories: ISoLA + DisCoRail

Future challenges

FM & AI in Railways?



"Every good talk should include a Venn diagram" – Einar (Lima, Peru, 2023)

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

Big data analytics: predictive maintenance

Aim: detect failures before they actually occur

?! how's the data collected and exploited to implement prognostics:

model-based use the provided input data on a previously defined physical or mathematical model

data-driven-based use a statistical model inferred from the data available at the time of training the prognostics application

knowledge-based use domain knowledge (e.g., ontologies) or expertise of the system

digital twin-based use a real-time digital representation of the physical system to generate data imitating the real events

Big data analytics: predictive maintenance

Aim: detect failures before they actually occur

?! how's the data collected and exploited to implement prognostics:

model-based use the provided input data on a previously defined physical or mathematical model

data-driven-based use a statistical model inferred from the data available at the time of training the prognostics application

knowledge-based use domain knowledge (e.g., ontologies) or expertise of the system

digital twin-based use a real-time digital representation of the physical system to generate data imitating the real events

$\Rightarrow$ development of effective and efficient predictive maintenance solutions for railways is a challenging and emerging research field: 24 papers in the literature for the period 2016–2021

M. Binder, V. Mezhuyev & M. Tschandl, Predictive Maintenance for Railway Domain: A Systematic Literature Review. *IEEE Engineering Management Review* 51, 2 (2023), 120–140.

Improved digitalisation: formal methods

To increase safety, security, reliability and comfort levels in railways, formal methods and tools need to cope with AI-based systems

Improved digitalisation: Anne's impact

To increase safety, security, reliability and comfort levels in railways, formal methods and tools need to cope with AI-based systems

Safe and Secure Future AI-Driven Railway Technologies: Challenges for Formal Methods in Railway

Monika Seisenberger[1( )], Maurice H. ter Beek[2], Xiuyi Fan[3], Alessio Ferrari[2], Anne E. Haxthausen[4], Phillip James[1], Andrew Lawrence[5], Bas Luttik[6], Jaco van de Pol[7], and Simon Wimmer[7]

[1] Swansea University, Swansea, UK
m.seisenberger@swansea.ac.uk
[2] ISTI–CNR, Pisa, Italy
[3] Nanyang Technological University, Singapore, Singapore
[4] Technical University of Denmark, Kongens Lyngby, Denmark
[5] Siemens Mobility Chippenham, Chippenham, UK
[6] Eindhoven University of Technology, Eindhoven, The Netherlands
[7] Aarhus University, Aarhus, Denmark

Improved digitalisation: Anne's impact

To increase safety, security, reliability and comfort levels in railways, formal methods and tools need to cope with AI-based systems

Improved digitalisation: Anne's impact

To increase safety, security, reliability and comfort levels in railways, formal methods and tools need to cope with AI-based systems

[ISoLA22] M. Seisenberger, M.H. ter Beek, X. Fan, A. Ferrari, A.E. Haxthausen, et al., Safe and Secure Future AI-Driven Railway Technologies: Challenges for Formal Methods in Railway @ ISoLA'22

Safe and Secure Future AI-Driven Railway Technologies: Challenges for Formal Methods in Railway

Monika Seisenberger[1(✉)], Maurice H. ter Beek[2], Xiuyi Fan[3], Alessio Ferrari[2], Anne E. Haxthausen[4], Phillip James[1], Andrew Lawrence[5], Bas Luttik[6], Jaco van de Pol[7], and Simon Wimmer[7]

[1] Swansea University, Swansea, UK
m.seisenberger@swansea.ac.uk
[2] ISTI–CNR, Pisa, Italy
[3] Nanyang Technological University, Singapore, Singapore
[4] Technical University of Denmark, Kongens Lyngby, Denmark
[5] Siemens Mobility Chippenham, Chippenham, UK
[6] Eindhoven University of Technology, Eindhoven, The Netherlands
[7] Aarhus University, Aarhus, Denmark

Improved digitalisation: Anne's impact

To increase safety, security, reliability and comfort levels in railways, formal methods and tools need to cope with AI-based systems

[ISoLA22] M. Seisenberger, M.H. ter Beek, X. Fan, A. Ferrari, A.E. Haxthausen, et al., Safe and Secure Future AI-Driven Railway Technologies: Challenges for Formal Methods in Railway @ ISoLA'22

- Integrate AI-based systems into the CENELEC standards

Improved digitalisation: Anne's impact

To increase safety, security, reliability and comfort levels in railways, formal methods and tools need to cope with AI-based systems

[ISoLA22] M. Seisenberger, M.H. ter Beek, X. Fan, A. Ferrari, A.E. Haxthausen, et al., Safe and Secure Future AI-Driven Railway Technologies: Challenges for Formal Methods in Railway @ ISoLA'22

- Integrate AI-based systems into the CENELEC standards
- Equip verification tools with certificate generation in case of a "yes"-answer, to achieve improved trustworthiness (e.g., by *explainability* or *certified model checking*)

Explainability is one of the 10 principles of *applicable formal methods*

M. Gleirscher, J. van de Pol & J. Woodcock, A manifesto for applicable formal methods. *Software and Systems Modeling* 22, 6 (2023), 1737–1749.

Concluding remarks

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

Academia: 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

Academia: researchers with different and complementary expertise

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

Road to success:

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

Academia: researchers with different and complementary expertise

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

Road to success: ask Anne 🤭

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:

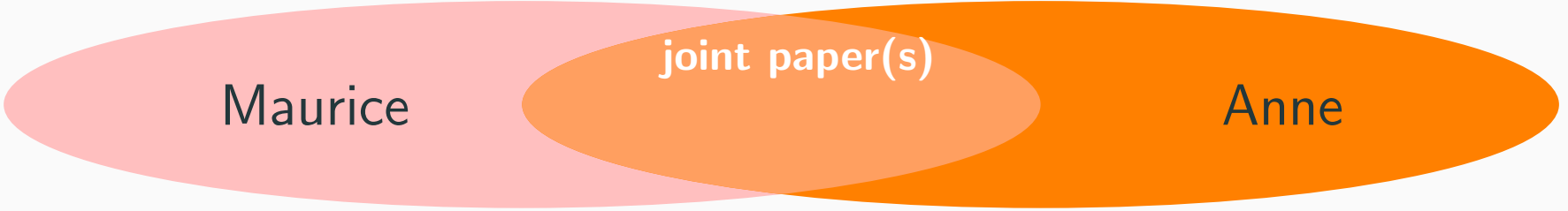
- requires modelling in a different input language
- expert knowledge of different analysis technique

Academia: researchers with different and complementary expertise

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

Road to success:

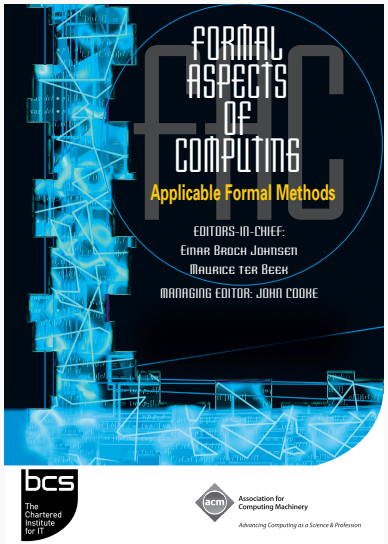
- capacity to abstract
- pick the right tool based on the industry input and requirements at hand


joint paper(s)
Maurice
Anne

Maurice

joint paper(s)
FAC RSSRail

Anne



2025

- [j18] Robert Sachtleben, Anne E. Haxthausen, Jan Peleska: **Mechanised Safety Verification for a Distributed Autonomous Railway Control System.** Formal Aspects Comput. 37(2):

2023

- [j16] Simon Collart Dutilleul, Anne E. Haxthausen, Thierry Lecomte, Jim Woodcock: **Introduction to the Special Section on Reliability, Safety, and Security of Railway Systems.** Formal Aspects Comput. 35(1): 1:1-1:2 (2023)
- [j15] Anne Elisabeth Haxthausen, Alessandro Fantechi: **Compositional Verification of Railway Interlocking Systems.** Formal Aspects Comput. 35(1): 4:1-4:46 (2023)

2021

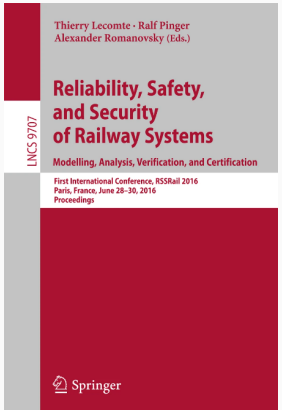
- [j14] Signe Geisler, Anne Elisabeth Haxthausen: **Stepwise development and model checking of a distributed interlocking system using RAISE.** Formal Aspects Comput. 33(1): 87-125 (2021)
- [j13] Alessandro Fantechi, Anne E. Haxthausen, Jim Woodcock: **Editorial.** Formal Aspects Comput. 33(6): 923-924 (2021)
- [j12] Jan Peleska, Niklas Krafczyk, Anne E. Haxthausen, Ralf Pinger: **Efficient data validation for geographical interlocking systems.** Formal Aspects Comput. 33(6): 925-955 (2021)

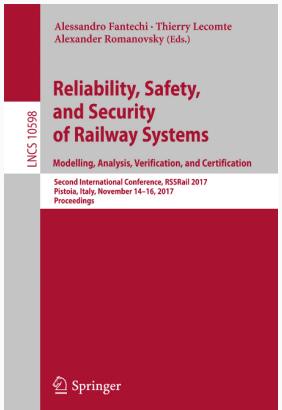
2011

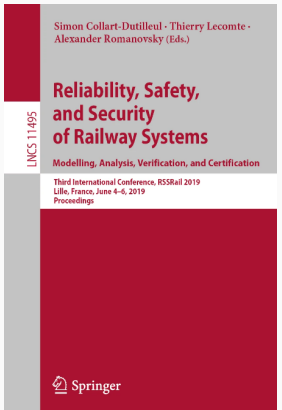
- [j9] Anne E. Haxthausen, Jan Peleska, Sebastian Kinder: **A formal approach for the construction and verification of railway control systems.** Formal Aspects Comput. 23(2): 191-219 (2011)

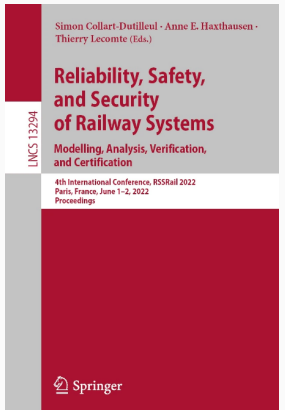
2008

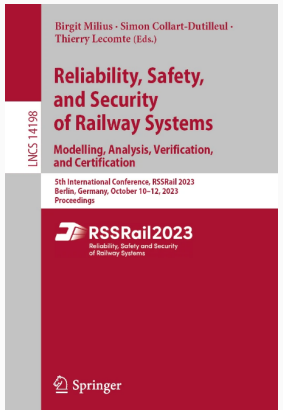
- [j7] Chris George, Anne E. Haxthausen: **Specification, proof, and model checking of the Mondex electronic purse using RAISE.** Formal Aspects Comput. 20(1): 101-116 (2008)

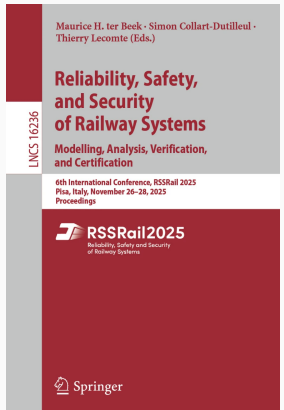








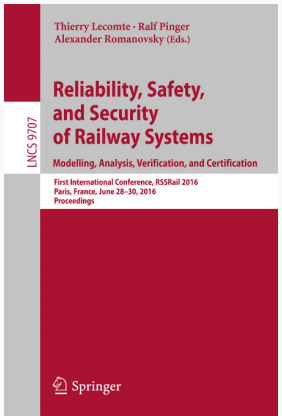


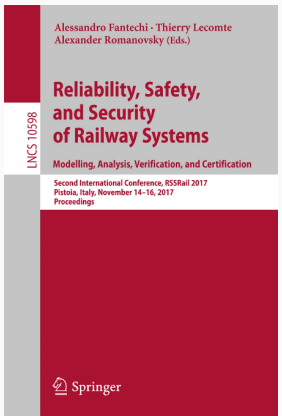


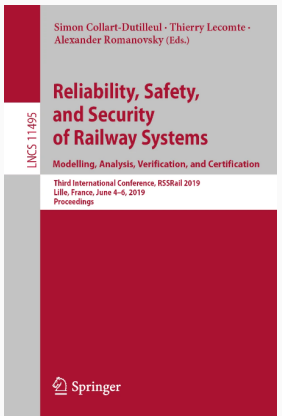
Maurice

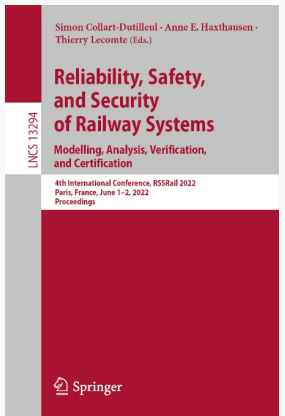
joint paper(s)
FAC RSSRail
ISoLA

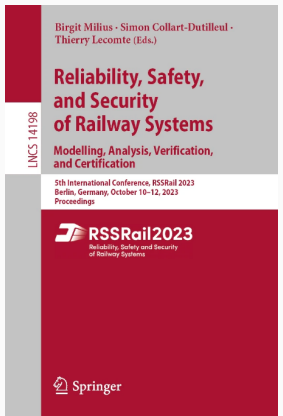
Anne

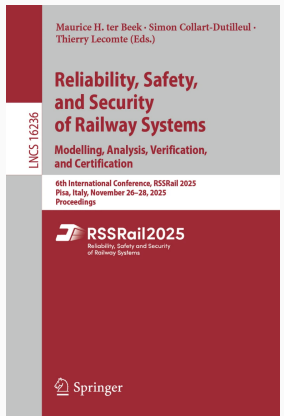








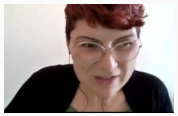


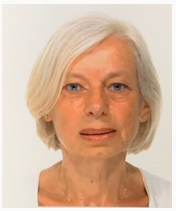


Acknowledgements

Thanks to all the co-authors of my work on railways:

Formal Methods and Tools Lab





Sirti
building the future

PROVER

mermec
AN ANGEL COMPANY

TRENORD

. . .

. . . and thanks to Alessandro for some of the photos!