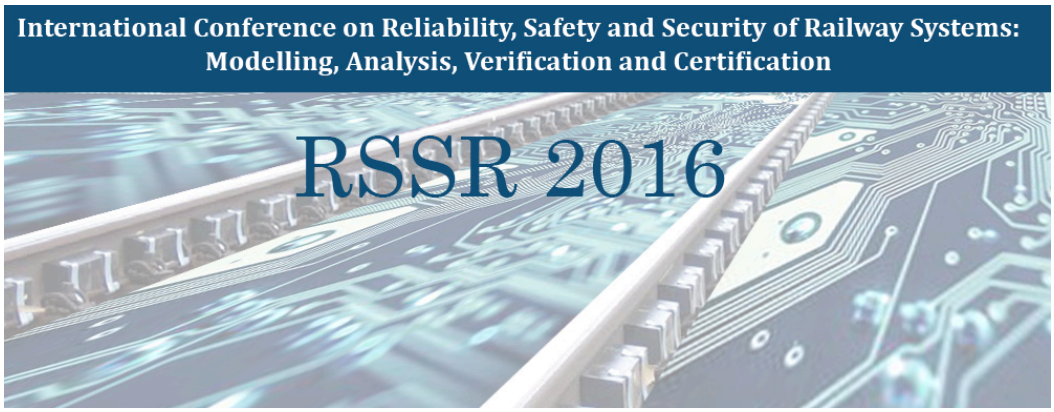
International Conference

Reliability, Safety and Security of Railway Systems:

Modelling, Analysis, Verification and Certification

Programme



28th – 30th June 2016

Espace du Centenaire, Maison de la RATP

Paris, France

© – RATP – Bruno Marguerite

Safety and development work on the Paris Metro at Château de Vincennes

Greetings from the Conference Chairs

We look forward to welcoming participants at the first RSSRail event, to be held in June 2016 in Paris. The conference is hosted by RATP, and will be held in the main auditorium at their head office in Paris, adjacent to the Gare de Lyon rail station. We wish to express our cordial thanks to RATP for their support and sponsorship of this event.

The Organising Committee of RSSRail 2016 warmly invites you to attend this new international conference. We have an exciting and innovative programme at a superb venue. We hope that you will also join us for a drinks reception on Tuesday evening (hosted by AdaCore, based here in Paris), and to take advantage of a very special conference dinner to be held in the famous – and wonderfully decorated – restaurant *Le Train Bleu* on Wednesday evening.

Thierry Lecomte, ClearSy, France
Ralf Pinger, Siemens Mobility, Germany
Alexander Romanovsky, Newcastle University, UK

Conference Overview

The conference programme comprises two and a half days of technical presentations, from Tuesday 28 June to Thursday 30 June, accompanied by a poster display and a vendor exhibition.

The technical programme includes a presentation from the Head of Rail Transport for RATP, three invited keynote presentations from leading investigators, plus 15 refereed and selected papers.

Tuesday 28th June

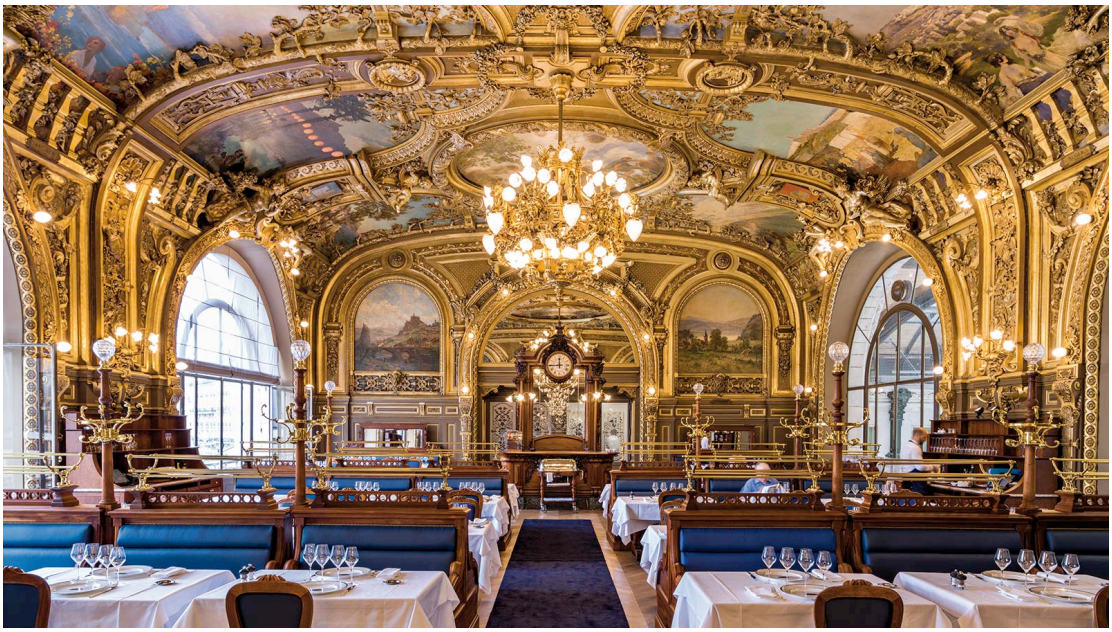
Registration will be available from 12.00 and the conference will open at 13.00. After four talks, including the first keynote presentation, the technical programme ends at 17.00. This will be followed by an opportunity for networking at a drinks and canapé reception at the Café Barge, which is moored on the river Seine only a very short walk from the conference venue.

Wednesday 29th June

Starting at 0900, day two of the conference offers nine talks, including our second keynote presentation and a special invited talk from the head of rail transport at RATP. These talks will conclude at 17.30, to be followed at 19.30 by a pre-dinner drink and the conference dinner; the banquet dinner will be held at the magnificent restaurant Le Train Bleu, very conveniently located in the Gare de Lyon, adjacent to the event venue.

Thursday 30th June

Starting at 0930, day three of the conference offers a further six talks, including the third keynote presentation. At 15.15 the event concludes with a short wrap-up session and the event will close at 15.30.



Sumptuous decoration sets the scene for gourmet dining at Le Train Bleu

Tuesday 28th June

12.00 Registration and Coffee

13.00 Welcome from RATP and the Conference Chairs

Session Chair: Alexander Romanovsky

13.10 **Keynote 1: Robin Bloomfield** (Adelard LLP & City University, UK)
The risk assessment of ERTMs-based railway systems from a cyber perspective: methodology and lessons learned

14.10 **Coffee break**

Session: Security. Chair: Ralf Pinger

14.40 **Joeri de Ruiter, Richard J Thomas & Tom Chothia** (University of Birmingham, UK)
Formal Security Analysis of ERTMS train to Trackside Protocols

15.20 **Po-Chi Huang & Birgit Milius** (Technische Universität Braunschweig, Germany)
Operational Security – A Coming Evolution of Railway Operational Procedures under the IT security Threat

16.00 **Florent Pépin & Maria Grazia Vigliotti** (RSSB, UK)
Risk Assessment of the 3Des in the ERTMS

16.40 **Close of Day 1**

17.30 Conference reception – Café Barge

Wednesday 29th June

08.30 Coffee

Session Chair: Thierry Lecompte

09.00 **Keynote 2: Denis Sabatier** (ClearSy, France)
Using formal proof and B method at system level for industrial projects

Session: Systems 1. Chair: Aryldo Russo

10.00 **Xiao Han, Tao Tang, Jidong Lv & Haifeng Wang** (Beijing Jiaotong University, China)
Failure Analysis of Chinese Train Control System Level 3 Based on Model Checking

10.40 **Coffee break**

Wednesday 29th June (continued)

11.10 **Marco Filax, Tim Gonschorek & Frank Ortmeier** (Otto-von-Guericke-Universität, Germany)
Correct Formalization of Requirement Specifications: A V-Model for Building Formal Methods

11.50 **Alexei Iliasov, Paulius Stankaitis & David Adjepon-Yamoah** (CSR, University of Newcastle, UK)
Static verification of railway scheme and interlocking design data

12.30 **Lunch**

Session Chair: Alexander Romanovsky

13.30 **Invited presentation: Claude Andlauer** (Head of Rail Transport for RATP, France)
Formal methods as part of RATP's DNA

Session: Systems 2. Chair: Véronique Delebarre

14.15 **Christophe Limbrée, Quentin Cappart, Charles Pecheur** (Université catholique de Louvain, Belgium)
& Stefano Tonetta (Fondazione Bruno Kessler, Italy)
Verification of railway interlocking – Compositional approach with OCRA

14.55 **Coffee break**

Session: Systems 3. Chair: Michael Leuschel

15.30 **Paulius Stankaitis & Alexei Iliasov** (CSR, Newcastle University, UK)
Safety Verification of Heterogeneous Railway Networks

16.10 **Anne Elisabeth Haxthausen** (Technical University of Denmark), **Hoang Nga Nguyen** (Centre for Mobility and Transport, UK) **& Markus Roggenbach (**Swansea University, UK)
Comparing formal verification approaches of interlocking systems

16.50 **Luke Martin** (CSR, Newcastle University, UK)
Predictive Reasoning and Machine Learning for the Enhancement of Reliability in Railway Systems

17.30 **Close of day 2**

19.30 Conference Dinner – Le Train Bleu

YouTube has a video of the restaurant, but it is not a guide to good behaviour: https://www.youtube.com/watch?v=p-2isH-SgHA

Thursday 30th June

9.00 Coffee

Session Chair: Ralf Pinger

09.30 **Keynote 3: Jan Peleska**
(University of Bremen & Verified Systems, Germany)
A novel approach to HW/SW integration testing of route-based interlocking system controllers

Session: V&V 1. Chair: Alessandro Fantechi

10.30 **Daniel Kästner & Christian Ferdinand** (AbsInt GmbH, Germany)
Applying Abstract Interpretation to Verify EN-50128 Software Safety Requirements

11.10 **Coffee Break**

11.40 **Nazim Benaissa, David Bonvoisin, Abderrahmane Feliachi & Julien Ordioni** (RATP, France)
The PERF Approach for Formal Verification

12.20 **Lunch**

Session: V&V 2. Chair: Kenji Taguchi

13.20 **Claire Dross & Yannick Moy** (AdaCore, France)
Abstract Software Specifications and Automatic Proof of Refinement

14.00 **Nicolas Breton & Yoann Fonteneau** (Systerel, France)
S3: Proving the Safety of Critical Systems

14.40 **Sylvain Conchon** (Université Paris-Sud, France) **& Mohammed Iguernlala** (OCamlPro SAS, France)
Increasing Proofs Automation Rate of Atelier-B Thanks to Alt-Ergo

15.20 **Wrap-up and closing remarks**

15.30 Close of Conference

Keynote Speakers

Prof Robin Bloomfield, *Adelard LLP & City University, London*

The risk assessment of ERTMS based railway systems from a cyber perspective: methodology and lessons learnt

Abstract: The impact that cyber issues might have on the safety and resilience of railway systems has been studied for nearly a decade by industry specialists and government agencies. This talk/paper presents some of the work lead by Adelard, starting with an analysis of vulnerabilities in ERTMS specifications through to a high level preliminary system risk assessment followed by detailed analyses of particular systems on behalf of UK industry. The focus of the paper will be on the issue of security informed safety, the development of cyber informed hazard analyses and overall methodology. High level results will be presented but, of course, many details remain proprietary or sensitive and cannot be published.

Denis Sabatier, *ClearSy*

Using formal proof and B method at system level for industrial projects

Abstract: Over several years, ClearSy has driven large projects about using formal proofs at system level. The fundamental goal in these projects is to extract the rigorous reasoning that establishes that the system under consideration ensures its requested properties, and to assert that this reasoning is correct and fully expressed. In this paper, we give feedback about the methodology used in all these projects, about the differences made by whether the concerned system is currently under design or already existing, and about the benefits obtained. The formal proofs are performed using Event-B, with the Atelier-B toolkit.

Jan Peleska, University of Bremen & Verified Systems

A novel approach to HW/SW integration testing of route-based interlocking system controllers

Abstract: Recent progress in bounded model checking and inductive reasoning has shown that the fully automated verification of route-based interlocking system designs of realistic "real-world" complexity is both possible and ready for industrial application. In this paper, we present a new model-based testing strategy for interlocking system controllers that exploits the fact that the design has already been verified, so that it can be used as a reference model for test case and test oracle generation. Our special interest lies in the field of complete testing strategies that are able to uncover every implementation error, provided that the implementation behaviour is captured in a pre-specified fault domain. Despite their guaranteed test strength, these strategies have two well-known disadvantages: (1) applied in a naive way, they often result in an infeasible amount of test cases, and (2) the hypothesis that the real implementation behaviour is captured by a member of the fault domain can rarely be justified in a convincing way. We describe a new combination of compositional reasoning and input equivalence class generation techniques that removes problem (1). For coping with disadvantage (2), we suggest a combination of equivalence class and random testing that – while not being able to guarantee complete fault coverage for implementations outside the fault domain – results in a test strength that is significantly higher than heuristic test approaches for interlocking system controllers. Estimates are presented that show how application of this novel strategy reduces the effort for HW/SW integration testing, while simultaneously increasing the fault coverage in comparison with more conventional testing approaches.

Invited Presentation

Claude Andlauer, *Head of Rail Transport for RATP, France*
Formal methods as part of RATP's DNA

Abstract: From the very first introduction of software in applications that were critical for safety on the railway, RATP has addressed the problem of demonstrating that safety was maintained. At an early stage it was recognised that formal methods could offer an effective and suitable approach for such a demonstration. From initial trials by internal RATP teams, formal methods have become an industrial technique that supports enhancement of the RATP network. Since then, RATP has continued to improve and enhance the associated methods and tools, working with its traditional partners. The experience gained, plus increased knowledge of the formal techniques, has both broadened the range of suitable application areas and made them available to a much wider community of practitioners.

Poster Programme – Displayed in the exhibitor area.

Barbara Gallina & Mattias Nyberg. An EN5012x-compliant OSLC-based Safety Case Generator

Giacomo Bersano, Mathieu Ramondou, Sergio Recio & Nicolas Ayache. A New Method to Address Security Issues of Railway Systems

Alexei Iliasov, Paulius Stankaitis, Luke Martin & Roberto Palacin. The SafeCap Platform for Modelling and Verification of Railway Networks

Dominik Hansen, Michael Leuschel & Nader Nayeri. Validation of Engineering Rules with B and ProB

Giovanni Neglia, Sara Alouf, Abdulhalim Dandoush, Sebastien Simoens, Pierre Dersin, Alina Tuholukova, Jerome Billion & Pascal Derouet. Performance Evaluation of Train Moving-Block Control

Subeer Rangra, Mohamed Sallak, Walter Schön & Frédéric Vanderhaegen. Human reliability analysis for railway operations: a framework for integration of human factors in risk analysis

Alessandro Fantechi, Stefania Gnesi, Anne Haxthausen, Jaco van de Pol, Marco Roveri & Helen Treharne. SaRDIn - A Safe Reconfigurable Distributed Interlocking.

Conference Sponsors and Exhibitors

Sincere thanks and appreciation go to our conference sponsors:

AdaCore
The GNAT Pro Company

isograph

CLEARSY
SYSTEM ENGINEERING

Newcastle University
UK | Malaysia | Singapore

RATP

SIEMENS

systerel
Safe real-time solutions