Institution: Swansea University

Unit of Assessment: 11

Title of case study: Improving performance, safety and software development of railway signalling.

Period when the underpinning research was undertaken: 2007-2020

Details of staff conducting the underpinning research from the submitting unit:

Name(s):	**Role(s) (e.g. job title):**	**Period(s) employed by submitting HEI:**
Faron Moller	Professor	August 2000 – present
Markus Roggenbach	Professor	May 2003 - present
Monika Seisenberger	Associate Professor	September 2001 - present
Phillip James	Senior Lecturer	March 2014 - present
Liam O'Reilly	Senior Lecturer	January 2013 - present

Period when the claimed impact occurred: 2014 - 2020

Is this case study continued from a case study submitted in 2014? N

1. Summary of the impact

The implementation of a much-needed update to the UK railway infrastructure has gathered momentum over the past decade. Among the new infrastructure, signalling software is a key technology to increase capacity and automation. However, verifying the safety of this software is a challenge for the railway industry. Swansea University has developed novel safety assurance processes for signalling technologies, using new formal methods that are now in use by Siemens Mobility, a global leader in signalling. Our new processes, which improve error detection, motivated Siemens Mobility to invest in a new verification team in Chippenham to accelerate the development of their next-generation digital interlockings. Similarly, the UK Rail Safety and Standards Board has incorporated our research on formal methods in guidance they provide to their members. Internationally, we have created a new European community of practice on formal methods in railway control.

2. Underpinning research

Since 2007, the Railway Verification Group at Swansea University and Siemens Mobility have been collaborating [**R1 to R6**] to formulate and answer questions concerning safety and network capacity to improve the development of railway signalling software. Swansea's work in this field has grown to enable international collaborations, with the Swansea Railway Verification Group being recognized as an international leader in the verification of signalling systems.

2.1 Engaging with the railway domain

Our sustained collaborations have been pursued using our industry-focused engagement model (Figure 1):

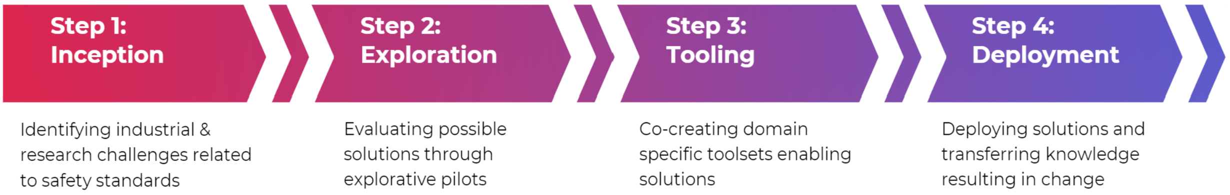

Step 1:
Inception
Identifying industrial & research challenges related to safety standards
Step 2:
Exploration
Evaluating possible solutions through explorative pilots
Step 3:
Tooling
Co-creating domain specific toolsets enabling solutions
Step 4:
Deployment
Deploying solutions and transferring knowledge resulting in change

Figure 1: Swansea Railway Verification Group engagement model.

Collaborating with the following industry partners and standards bodies, the application of this model has identified research problems and led to fundamental computing research (listed in 2.2 below).

- **Siemens Mobility UK (formerly Invensys Rail, formerly Westinghouse)** (Steps 1 - 4)

- **Railway Standards and Strategy Board** (RSSB), who oversee and inform the UK rail industry's work to achieve continuous improvement in safety (Steps 1 - 3),
- **Verified Systems International Germany** (Steps 1 - 2),
- **The State Railway Thailand** (Steps 1 and 4), and
- **Chinese Railway** (Steps 1 - 2).

The Railway Verification Group has also launched (2015), and still chairs, the **European Technical Working Group on Formal Methods in Railway Control**, which brings together academics and industry across Europe to fuel research in this emerging domain. The group's reach is broad and includes 7 universities, 6 companies and industrial bodies (Section 4.3).

2.2 Fundamental computing research

In terms of Computer Science, our work has delivered new research in:

1. Formalization of industrial concepts (domain engineering) [**R3**].
2. Methodology for faithful modelling of industrial concepts [**R3, R4**].
3. Abstractions with soundness proofs allowing for tackling of state space explosion [**R4**].
4. Real world applications of modelling and verification for railways [**R1- R4**].
5. Encapsulating formal methods in user-friendly industry tools [**R3**].
6. Establishing a body of engineering knowledge on formal methods for use for railways.

We have undertaken this research using a wide range of formal methods, e.g., CSP, CSP||B, CASL, Real-time Maude (all in the OnTrack toolset [**R3, R4**]), and SAT based verification algorithms (in the Siemens Ladder Logic Verifier [**R2**]).

2.3 Research within Software Engineering for Railways

Our research has directly addressed the problem of formal safety assurance in an industry that is under pressure to increase capacity and efficiency through the implementation of new automated and autonomous railway networks. Specifically, our research has focused on formally modelling and verifying:

1. **Implementations** of signalling systems at the level of program code written in ladder logic, a programming language standardized as IEC 61131 [**R1- R2**].
2. **Designs** of signalling systems using visual specifications common in industry [**R3 - R5**].
3. **Standards** for control systems (European ERTMS; Chinese CRTMS) replacing fixed, physical signals with dynamic, virtual signalling which utilises radio communication [**R6**].

Concerning **implementations**, Siemens and Swansea University have completed all four steps of the above engagement model. Concerning **designs**, RSSB, Siemens, Network Rail and Swansea University have completed the first three steps of the engagement model. Concerning **standards**, Siemens and Swansea have completed the first step of the engagement model and are working towards completing the second.

3. References to the research

The underpinning research **R1-R6** have been internationally peer reviewed. Papers were supported by funding from external sources such as EPSRC and Siemens Mobility.

[R1]. James, P., Kanso, K., Lawrence, A., Moller, F., Roggenbach, M., Seisenberger, M., Setzer, A., Chadwick, S. (2014) Verification of Solid State Interlocking programs. In: International Conference on Software Engineering and Formal Methods, Springer LNCS, pp. 253-268. https://doi.org/10.1007/978-3-319-05032-4_19

[R2]. Chadwick, S., James, P., Roggenbach, M., Werner, T. (2018) Formal Methods for Industrial Interlocking Verification. In: International Conference in Intelligent Rail Transport, IEEE. https://doi.org/10.1109/ICIRT.2018.8641579

[R3]. James, P., Roggenbach, M. (2014) Encapsulating Formal Methods within Domain Specific Languages: A Solution for Verifying Railway Scheme Plans. Mathematics in Computer Science 8: 11-38. https://doi.org/10.1007/s11786-014-0174-0

[R4]. James, P., Moller, F., Nguyen, N.H., Roggenbach, M., Schneider, S.A., Treharne, H. (2014) Techniques for modelling and verifying railway interlockings. International Journal on Software Tools for Technology Transfer 16:685-71. https://doi.org/10.1007/s10009-014-0304-7

[R5]. Chen, L., James, P., Kirkwood, D., Nguyen, H.N., Nicholson, G.L., Roggenbach, M. (2016) Towards integrated simulation and formal verification of rail yard designs - an experience report based on the UK East Coast Main Line. In: IEEE International Conference on Intelligent Rail Transportation, IEEE, pp. 347-355. https://doi.org/10.1109/ICIRT.2016.7588753

[R6]. Berger, U., James, P., Lawrence, A. Roggenbach, M., Seisenberger, M. (2018) Verification of the European Rail Traffic Management System in Real-Time Maude. Science of Computer Programming 154:61-88. https://doi.org/10.1016/j.scico.2017.10.011

Research Grants:

[G1]. James, P. (PI) (2020). VHDL verification. Siemens Mobility, GBP25,411.
[G2]. James, P. (PI) (2018-2019). Ladder Logic Verifier. Siemens Mobility, GBP119,182.
[G3]. Moller, F. (PI) (2011-2019). Railway Control Systems. Siemens Mobility, GBP126,000.
[G4]. Roggenbach, M. (PI) (2014-2017) Developing Integrated Tools, Techniques and Optimisations (DITTO). Rail Safety and Standard Board (RSSB), GBP1,300,000. Partners: Siemens Mobility, Southampton University, Leeds University.
[G5]. Roggenbach, M. (PI) (2018) Impact Acceleration Award. EPSRC, GBP5,300. Partners: State Railway of Thailand.

Current Additional Fully Funded PhD Projects:

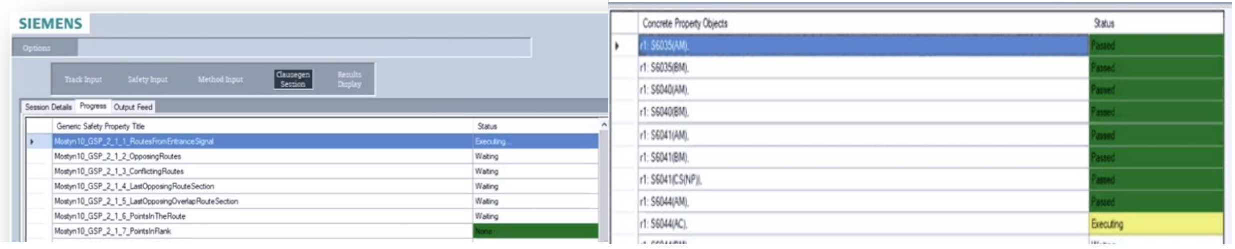
PhD-1. iCase PhD Grant "Formal testing for ERTMS" (2018-2021): Supervisor: M. Roggenbach, Funder: EPSRC/Siemens Mobility.
PhD-2. Center of Doctoral Training PhD Grant "Automated Invariant Finding for Ladder Logic Verification using Machine Learning" (2020-2024): Supervisor: Dr. P. James, Funder: EPSRC/Siemens Mobility.

4. Details of the impact

4.1 Impact within Siemens Mobility *(Steps: inception through deployment)*

> *"Over the past decade our close association with Swansea University and their work on Formal Methods has contributed to a fundamental paradigm shift in our vision for signalling design. We have employed 2 full time verification engineers from Swansea Railway Verification Group to form part of our new verification research team at Chippenham. We have also chosen to integrate Swansea's LLV tool into our interlocking development process, supporting rapid verification, reducing the testing effort and saving time and money."* [Project Manager, Siemens Automation, **C1**]

In the REF period, Swansea University, through the Swansea Railway Verification Group [**C2**] and Siemens have systematically explored novel verification techniques that scale to industrial practice [R1, R2, G3, **C2**] (Steps 1 and 2), as discussed in Sections 2.2 and 2.3. Building on this, through co-creation, a verification toolset was developed [G2] (Step 3). This led to the embedding of Swansea's formal verification techniques into a new signalling system implementation process at Siemens (Step 4).



Generic Safety Property Title	Status
Mostyn10_GSP_2_1_1_RoutesFromEntranceSignal	Executing...
Mostyn10_GSP_2_1_2_OpposingRoutes	Waiting
Mostyn10_GSP_2_1_3_ConflictingRoutes	Waiting
Mostyn10_GSP_2_1_4_LastOpposingRouteSection	Waiting
Mostyn10_GSP_2_1_5_LastOpposingOverlapRouteSection	Waiting
Mostyn10_GSP_2_1_6_PointsInTheRoute	Waiting
Mostyn10_GSP_2_1_7_PointsInFlank	None

Concrete Property Objects	Status
r1: S6035(AM).	Passed
r1: S6035(BM).	Passed
r1: S6040(AM).	Passed
r1: S6040(BM).	Passed
r1: S6041(AM).	Passed
r1: S6041(BM).	Passed
r1: S6041(CS(NP)).	Passed
r1: S6044(AM).	Passed
r1: S6044(AC).	Executing

Figure 2: Siemens-Swansea Ladder Logic Verification tool. Green properties have been proven, the yellow property is currently being checked, and white properties are to be checked.

Our research has led to the following impacts within Siemens [**C1**]:

- ***Tool deployment:*** Swansea's ladder logic verifier LLV [R1, R2] is being used by Siemens Rail staff (Figure 2) as part of their interlocking development process and has verified 4 interlocking systems thus far.
- ***Process change:*** Siemens has changed the way that they test signalling systems in order to include formal methods developed by our team [R2]. Siemens has replaced a highly manual testing process with our automated tools, which enhance software quality by quickly finding errors including those that are often missed with manual testing. The time required for checking over 320 safety properties has been reduced from several weeks to approximately 2 hours using our verification process.
- ***Job creation:*** To support process changes, a new verification team has been formed at Siemens Chippenham, including 2 full-time positions which have been filled by post-graduates from the Swansea Railway Verification Group.
- ***Knowledge Transfer:*** Through a 50% FTE secondment [G2], Dr. Phillip James has been involved in overseeing process change within Siemens.
- ***Innovation diffusion:*** Based on the deployments by Swansea, Siemens is transforming a number of their development methods to include formal methods, e.g., Axel counter control systems (adapting Swansea's LLV tool).

4.2 Impact across the rail industry through the RSSB and Network Rail *(Steps: inception to tooling)*

RSSB, Siemens, Network Rail and Swansea have completed the first three steps of the engagement model. Together in the SafeCap project, we developed new domain engineering [P3] and modelling and verification techniques for real-world designs (e.g., in CSP, CSP||B and CASL [R4]). We were the first to provide proven abstraction techniques including covering [R4] and finitisation (Steps 1 and 2). Continuing this, the DITTO project [G4] embedded these results into a new toolset OnTrack (Step 3). OnTrack allows rail engineers to draw track plans, automatically transform them into a range of formal specifications, and to verify these with a range of provers, thus automating novel model transformations [R5]. These scientific advancements have contributed to a deeper awareness and understanding across the UK Rail Industry, as described below.

Providing new guidance to RSSB on formal methods

> *"An essential part of our strategy for safely increasing capacity is guidance from Swansea University in 2017 on using formal methods for signalling analysis (e.g. in the FuTRO: DITTO Project - Summary of Findings (T1071 Report))"* [Director of Research, RSSB, **C3**]

RSSB maintains the SPARK rail knowledge hub for the rail sector to share knowledge and promote innovation. SPARK has over 16,500 active users from the international rail profession (as of October 2019). In total, Swansea has contributed five articles (2015 to present, **C3**) that have presented scientific arguments for the use of formal methods (see **C4** pgs 7-9 for Swansea's core contribution).

4.3 Co-creating with industry a new body of knowledge in Europe

Swansea is co-creating with other academics and industry a new body of knowledge on applying formal methods to railway systems.

- *Founding a New European Industrial Railway Forum:* The Swansea Railway Verification Group has formed the European Technical Working Group on Formal Methods in Railway Control. We brought together seven European groups and their industry partners, including ProRail (via Eindhoven University of Technology and the University of Twente), Ansaldo STS (via Universita' degli Studi di Firenze), DSB, Verified Systems, VSI (via Technical University of Denmark), Siemens Mobility, Network Rail and RSSB (via Swansea University) and Verified Systems DE (via Swansea University).

  "VSI welcomes Swansea's initiatives to organize and coordinate rail research groups. After a

week-long workshop in 2019 with 5 academics from Swansea University, we were able to strengthen the competitive edge of RT-Tester by applying it to new ERTMS models provided by the working group" [Managing Director VSI, **C5**]

- *Building a Community of Practice:* Swansea is at the centre of the creation of a community of practice, contributing to events by:
    - Hosting a RSSB Futro Board meeting in October 2017.
    - Running a one-week railway verification workshop involving 4 universities (Universita' degli Studi di Firenze, Twente, Coventry, Swansea) in 2017.
    - Hosting an online international railway verification workshop as part of BCTCS 2020, with 50% industrial speakers, and 92 participants from both Europe and Asia.

Swansea has also published a handbook for the engineering domain with an illustration from the Railway Safety Domain [**C6**]

4.4 Impact across international railways (Thailand and China)

Training and Education: The Swansea Railway Verification Group delivered a week-long workshop on the use of formal methods in railways (using Swansea's OnTrack) to upskill 16 senior engineers within the Thailand State Railway. This has changed their procurement process to include formal methods.

"we now take formal methods in account when we are purchasing new signalling systems." [Superintendent Engineer State Railway Thailand, **C7**]

Inception and Exploration: The Swansea Railway Verification Group has collaborated with the Tongkong Institute (Anhui) Ltd, applying Swansea's Ontrack verification toolset on a large Chinese railway design with the intention to roll out Swansea's technology.

"From Swansea we have learned the benefits of formal methods, in particular for error checking of scheme plans, and plan to apply them to further designs in 2020/2021, with the ultimate aim of having Swansea formal methods integrated into our design tools for the Chinese railway" [Board Chair, Tongkong Institute, **C8**]

4.5 Public Outreach

The Swansea Railway Verification Group regularly engages with railway enthusiasts and the general public. The group has developed a model railway exhibition that shows how formal methods can solve safety problems. This has been an educational resource for the Didcot Railway Centre [**C9**], the British Science Festival 2016, Science days (2017-2019) for the National Museum of Wales, school visits and Technocamps in their outreach activities to all schools across Wales.

"It was impressive to see that no matter how young children interactively controlled trains using 3D printed controllers, Swansea's methods for ensuring safety always stopped the trains from colliding thanks to the verified control system". [Swindon Panel Society Chairman, **C9**]

5. Sources to corroborate the impact

[C1]. Testimonial Letter from Siemens Mobility Limited, UK.
[C2]. Website http://cs.swansea.ac.uk/rail.
[C3]. Testimonial Letter from the Rail Strategy and Standards Board, UK.
[C4]. Guidelines published by RSSB [PDF].
[C5]. Testimonial Letter from Verified Systems International, Germany.
[C6]. On the construction of Engineering Handbooks with an illustration from the Railway domain. https://doi.org/10.1007/978-3-030-44648-2
[C7]. Testimonial Letter from the State Railway of Thailand.
[C8]. Testimonial Letter from the Tongkong Institute (Anhui) Ltd, China.
[C9]. Testimonial Letter from an organiser of the Swindon Panel Opening Event.