Institution: University of Southampton		
Unit of Assessment: 11 Computer Science and Informatics		
Title of case study: 11-09 Cost-effective assurance for industrial software systems through open source formal modelling and verification tools		
Period when the underpinning research was undertaken: 2000 – 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:**
Professor Michael Butler	Professor of Computer Science	1995 – present
Dr Thai Son Hoang	Lecturer	2015 – present
Dr Colin Snook	Senior Research Fellow	2000 – present
Professor Michael Leuschel	Professor of Computer Science	1997 – 2005
Period when the claimed impact occurred: January 2014 – July 2020		
Is this case study continued from a case study submitted in 2014? N		

1. Summary of the impact

Researchers at the University of Southampton have developed open source formal modelling and verification tools supporting the B and Event-B formal methods. These tools – **ProB** (model checker for B), **UML-B** (graphical front-end for B) and **Rodin** (formal verification for Event-B) – are used by industry worldwide for software validation and verification. Since 2014 they have led to:

1.1 Reduced costs and improved quality of data validation of engineering processes, including a 100-fold increase in verification speed for CLEARSY (France) and significant use in automated validation of railway control systems by Thales (Germany), leading to cost reductions.

1.2 Verification of model-based design processes, with rigorous, early-stage, automated verification achieved in deployments by Thales (Austria), AWE (UK), Sandia National Laboratories (USA) and Deutsche Bahn (Germany).

1.3 More than GBP600,000 of commercial income for industrial training and adoption services through UoS consultancy company ECS Partners Ltd.

1.4 A widely downloaded open source toolset with global developer/user communities. The 2018 version of Rodin has been downloaded over 10,000 times, predominantly in France, China, UK, Germany and USA, for free research, teaching and commercial use. The 7th global Rodin workshop was hosted by Southampton in June 2018.

2. Underpinning research

Reliance on software for effective operation and safety of high-end systems in the transportation, aerospace, and defence industries is increasing. Engineers use *formal methods* – a range of mathematical techniques for modelling and reasoning about the design of hardware and software – to detect and prevent errors at every stage of system lifecycles. Existing formal methods provide rich mathematical languages for modelling and reasoning about correct system behaviour. However, it is difficult to scale them for complex systems in which software-based controllers manage many features or control a large proportion of a system's functions – for example, a control system that supervises a large volume of traffic on a rail network. Another issue with formal methods approaches is slow uptake in industry, where the potential improvements in reliability, and savings in testing and reworking costs, are not always recognised and the techniques are perceived as being inaccessible to non-academic engineers.

Research since 2000 led by Professor Michael Butler of Southampton's Cyber-Physical Systems Research Group has developed more 'engineer friendly' formal methods and tools that have saved industry time and effort and boosted innovation. Applying formal methods to complex distributed systems, Butler has worked with several Southampton colleagues: Dr Thai Son Hoang, Dr Colin Snook, and Professor Michael Leuschel (moved to University of Düsseldorf, Germany in 2005).

Since 2000 Butler and his team focused on securing uptake of the B and Event-B formal methods and tools by industry. An existing commercial tool for the B Method, called Atelier-B, was the closest fit but had two weaknesses: lack of automated model checking capabilities and lack of support for graphical modelling notations. This led to two major research and development contributions from Southampton: ProB, a model checker, and UML-B, a graphical front-end for B.

Originally developed at Southampton by Leuschel and Butler, ProB [**3.1**] is a powerful model-checking engine that exploits constraint logic programming and can be used to automatically find errors in B models. ProB has been further developed to be used for data validation of industrial scale systems. In the mid-2000s Snook and Butler designed UML-B [**3.2**], providing an engineer-friendly graphical front-end to B, based on the UML notation popular in industry. UML-B includes a concept of layered refinement, and the team developed a method and tool for translating UML-B into B models. This allowed the Atelier-B and ProB analysis tools to be applied to UML-B models.

In the early 2000s Butler collaborated with independent French consultant Jean-Raymond Abrial, originator of the B method. The result was a new generation of the B method, known as Event-B [**3.3**]. It also led to further elaborations of Butler's method of refinement of distributed systems in Event-B [**3.4**, **3.5**]. Event-B spurred the development of the open-source Rodin toolset to support practical application of Event-B [**3.3**]. Rodin uses a range of custom-built and off-the-shelf verification tools to enable engineers to apply formal reasoning to large Event-B models. In addition, both ProB and UML-B were integrated into the Rodin toolset, enabling engineers to use combined features, including graphical modelling, model-checking, animation and verification, on the same Event-B models in a single design environment. Rodin is a collaborative project involving several European universities and SMEs, with Southampton playing a leading role in the toolset's design and promotion. The Rodin toolset was developed initially as part of the RODIN EU FP6 Project (2004-2007), and further enhanced in a series of EU and UK projects (see list of grants). Butler and Hoang worked closely with Abrial and others to turn the theoretical framework into a practical method and tool [**3.3**].

3. References to the research

3.1 Leuschel, M. and Butler, M. (2003) ProB: A model checker for B. FME2003: Formal Methods. https://doi.org/10.1007/978-3-540-45236-2_46

3.2 Snook, C. and Butler, M. (2006) UML-B: Formal modelling and design aided by UML. ACM Transactions on Software Engineering and Methodology, 15 (1). https://doi.org/10.1145/1125808.1125811

3.3 Abrial, J. R., Butler, M., Hallerstede, S., Hoang, T. S., Mehta, F. and Voisin, L. (2010) Rodin: An Open Toolset for Modelling and Reasoning in Event-B. International Journal on Software Tools for Technology Transfer. https://doi.org/10.1007/s10009-010-0145-y

3.4 Butler M. (2002) A system-based approach to the formal development of embedded controllers for a railway. Design Automation for Embedded Systems 6 (4), 355-366. https://doi.org/10.1023/A:1016503426126

3.5 Butler, M. (2009) Decomposition Structures for Event-B. In: Integrated Formal Methods iFM2009, Springer, LNCS 5423. https://doi.org/10.1007/978-3-642-00255-7_2

4. Details of the impact

The University of Southampton's formal modelling and verification technology is providing impact on practitioners, covering industrial software engineering processes, economic impact, benefit to industrial end-users and commercial contracts, and international community impact through an open source toolset and university education.

4.1 ProB for data validation of engineering processes at CLEARSY and Thales Germany

A safety critical system often contains many data parameters which are instantiated differently for each particular installation of the system. Data validation involves checking that all the data values for the installation satisfy safety rules. Data validation for railway installations is an important business area for **CLEARSY**, a French safety systems and software company who initially used a manual data validation process for this purpose. This typically led to painful, error-prone, long-term activities requiring several months to check manually up to 100,000 items of data against

1,000 rules. From 2014, CLEARSY started using ProB for automated data validation on several client railway projects and this has helped major customers to obtain considerable savings (up to a factor of 100) in their data validation activities while improving the quality process [**5.1**]. Example industrial projects in which CLEARSY exploited ProB are:

- Data validation for Alstom's URBALIS Computer-Based Train Control system. Data validation has been used for various lines since 2014 in Mexico, Toronto, Sao Paulo and Panama.
- Alstom and SNCF: data validation of European Train Control System (ETCS) Level 1 software in 2018
- ATOS and SNCF: for MISTRAL NG (new centralized command/control rail management system) since 2017
- Siemens Automated Train System in 2018

The Activity Director at CLEARSY testified to the vastly improved validation performance with ProB:

> "*The formal approach with ProB is up to 100x faster than a pure human verification and a few hours are enough for validating a complete railway project. Furthermore, it removes human errors, as it makes use of certified formal techniques."*

Based on this experience, CLEARSY have integrated ProB into a generic validation tool called CLEARSY Data Solver (CDS) and in 2019 CDS was T2 qualified for use in safety-critical certification according to the European standard for railway control and protection systems (EN50128). CDS has since been used on client projects with Thales Toronto [text removed for publication]. CLEARSY have also integrated ProB with their commercial Atelier-B tool to extend its proof capability.

Since 2014, **Thales Transportation Germany** have used ProB for validation of installations of their flagship RBC (Radio Block Centre) product line for railway control, achieving significant cost reduction in validation compared with conventional validation [**5.2**]. Thales now express the rules in the B language and use ProB to automate the verification of the rules. Compared with the previous methods used by Thales, ProB provided a more exhaustive validation process of higher quality with better feedback to engineers. This resulted in reduced costs for encoding and checking RBC engineering rules. Thales have built a custom rule checker, called RUBIN, on top of ProB that has been qualified to class T2 of the EN50128 standard. RUBIN is now used routinely by Thales for rule validation on industrial projects including several RBC installations.

4.2 UML-B and Rodin for model-based design process at Thales, AWE, Sandia and Deutsche Bahn.

Engineers in companies worldwide are successfully using UML-B and Rodin in the early-stage model-based design and validation of computer-based control systems. These organisations were already using industry-standard model-based software design methods, including UML, SysML and Statecharts. However these methods lack the formal verification capabilities provide by the Rodin toolset. Our UML-B technology is providing these companies with a bridge between the industry-standard model-based design languages and the powerful verification capabilities of Rodin. The resulting toolchains are helping them uncover potential design problems earlier in the development of new systems, contributing to safer system design and avoiding expensive reworkings.

In 2017 **Thales Austria** used UML-B and Rodin to verify and validate the *Hybrid ERTMS/ETCS Level 3* specification [**5.3**]. ERTMS (European Rail Traffic Management System) is the EU system of standards for management and interoperation of signalling for railways. Hybrid ERTMS/ETCS Level 3 increases the throughput of trains on a conventional rail network by dividing a physical block into multiple virtual blocks. In parallel with the Thales Austria work, **Thales Germany** integrated ProB with the Deutsche Bahn field demonstrator rail system allowing a B model of ERTMS to be used as a runtime controller-in-the-loop for in-the-field validation. Both of these formal modelling and validation projects identified issues in the original ERTMS standard and these findings were fed back to the standardisation work, leading to improvements in the revised standard [**5.4**].

> *"To sum up, using formal methods improves verification and validation efficiency and helps with detecting design flaws at an early stage of the development."* Thales Austria [**5.3**]

AWE engineers deployed the Rodin toolset on an internal system engineering project during 2014 to 2018. To facilitate this, the Southampton team developed a Rodin plugin called CODA in 2014-2015 which augments UML-B state machines with support for hierarchical communicating components [**5.5**]. AWE report that the use of the Rodin technology, including CODA, is demonstrating a positive impact on the quality of the specifications and designs for their products [**5.6**]. A significant impact for AWE is that potential design problems are being uncovered early in the development cycle thus saving expensive reworking of designs and implementations later in development. AWE have released CODA as open source under an MOD licence in 2017.

Facilitated by UoS collaboration with AWE, engineers at **Sandia National Laboratories** in the USA have deployed Rodin technology to support design verification. Sandia already used an industry-standard Statechart format (SCXML) for modelling. To enable exploitation of Rodin formal verification capabilities, Sandia and Southampton developed a Rodin plugin in 2018-2019 to automatically translate SCXML models to UML-B models [**5.5**]. This provided the basis for 'engineer friendly' formal methods for high consequence embedded system design and verification and has given Sandia engineers access to formal verification without forcing them to abandon familiar concepts and tools [**5.7**]. The Southampton work allowed Sandia to exploit a correspondence between State Charts and Event-B which allowed them to develop sound, usable tools for high-consequence electronic control systems. Sandia confirmed that the development of their Statechart based design method supporting refinement and allowing such rigorous verification was made possible by Event-B and UML-B.

Deutsche Bahn (DB) successfully used UML-B as a route to formal verification of digital Railway Command Control and Signalling (CCS) system specifications during 2019-2020. The CCS specifications were developed using the industry standard SysML language and translated to UML-B. DB evaluated several verification approaches and determined that UML-B provided a very effective route for verification of their SysML models [**5.7**]. Using UML-B and Rodin in this way allowed DB to identify and remove errors and gaps in models, providing formal verification that their railway component specifications are safe and helping to ensure that the implementations of the components are interoperable and fit for purpose. DB report that the use of UML-B provided a very effective route to formal verification of their SysML models [**5.8**].

To support adoption of Rodin tools by industry, since 2014 Butler and colleagues have given training to over 30 industrial users on Event-B, UML-B and Rodin technology to help them adopt the technology. Courses have been given to engineers in AWE, Sandia Labs (USA), Imagination Technologies, Atkins Rail, Thales (Austria, Germany, Romania, Spain), Deutsche Bahn. Leuschel has provided ProB training to Thales (Germany), CLEARSY (France), Witz (Japan) and Aisin (Japan).

4.3 Commercial contracts for ECS Partners

Through ECS Partners, a University of Southampton consultancy company, since 2014 the Southampton team have had commercial contracts with AWE, Cobham, Sandia National Labs, Critical Software Technologies, Thales, Hitachi Ltd, Imagination technologies and Atkins Rail worth a total of over GBP600,000. During 2014-2017, AWE contracted ECS Partners to adapt the Rodin toolset to support their in-house process for embedded system design; their engineers have used the resulting toolset since [**5.6**]. During 2018-20019 Sandia contracted ECS Partners to adapt the Rodin toolset to support integration of industry-standard Statechart models with Rodin [**5.7**].

4.4 Widely used open source tools and worldwide developer/user community

Rodin is an open source toolset. The source code and executables are available on SourceForge and it is available for Windows, Mac and Linux. It is free to use for research, teaching and commercial purposes. Version 3.4 (Jan 2018) has been downloaded over 10,000 times. The top 5 download countries are France, China, UK, Germany and USA. Southampton hosts the main website for the Rodin toolset (www.event-b.org) which includes a heavily used wiki providing user and developer support. ProB is available both as a standalone application for Windows, Mac and Linux and as a plug-in for Rodin [**5.9**].

Southampton organised the first Rodin User and Developer Workshop in Southampton in 2009 with participants for a range of European countries as well as Australia, Brazil and Canada. The success of this led to the Rodin Workshop becoming a regular event with the most recent (7th in the series) being held in Southampton in June 2018. There were 40 attendees including presentations from **Thales** (Tomas Fischer) and **Airbus** (Martin Kubisch) [**5.10**]. This Rodin workshop series helps to sustain the international community of Rodin users and developers. The 2020 workshop was postponed to 2021 due to Covid-19 restrictions.

The Rodin toolset is used for undergraduate and postgraduate teaching in a number of universities worldwide. We are aware of it being used in the following universities: Southampton, Newcastle, Bristol, Surrey, Düsseldorf, Aabo Akademi (Finland), Universidade Federal do Rio Grande do Norte (Brazil), University of New South Wales, York University (Canada), National Institute of Informatics Tokyo, IIT Mumbai, IIT Bhubaneswar, University Putra (Malaysia), Prince of Songkla University (Thailand). These universities use the Rodin and ProB websites which include tutorials and training material [**5.11**].

5. Sources to corroborate the impact

5.1 Testimonial from CLEARSY.

5.2 Testimonial from Thales Transportation Germany

5.3 https://www.thalesgroup.com/en/austria/news/future-oriented-research-programme-relies-railway-expertise-thales

5.4 Demonstration of ETCS Level 3 by Deutsch Bahn including ProB simulation https://www.youtube.com/watch?v=FjKnugbmrP4 (The console visible 2mins30 into the video is a visualisation of ProB executing a B model that is controlling two trains.)

5.5 https://www.uml-b.org/caseStudies.html

5.6 Testimonial from AWE, https://sourceforge.net/projects/rodin-b-sharp/files/Plugin_CODA

5.7 Testimonial from Sandia, https://doi.org/10.1007/978-3-030-12988-0_8

5.8 Testimonial from Deutsche Bahn

5.9 https://www3.hhu.de/stups/prob/index.php/Main_Page

5.10 http://wiki.event-b.org/index.php/Rodin_Workshop_2018

5.11 Rodin: http://www.event-b.org; ProB: https://prob.hhu.de