Institution: Newcastle University

Unit of Assessment: 11 Computer Science and Informatics

Title of case study: Improved processes for the development of dependable systems

1. Summary of the impact

Research at Newcastle University on formal methods for the design of computing systems has had a major impact on the delivery of new high-dependability products by industry. The methods (VDM and Event-B), to which we have made significant contributions, have been embodied in tools (VDMTools, Overture, Rodin) and applied in industry. The reach of the work extends to industries in Europe (e.g. in the rail sector by Siemens, 2011) and Japan (e.g. in firmware design by Sony, 2008). Significance is seen in reported improvements in defect detection rates of up to a factor of 5 over previous processes and the cost-effectiveness of design processes. The “Mobile FeliCa” chip developed using VDMTools is now incorporated into over 200 million mobile phones worldwide. Our approach to disseminating research has engendered lively international and online end-user communities further developing and using the tools today.

2. Underpinning research

This study is founded on Newcastle University’s research from the mid-1990s, on formal engineering of dependable computing systems. The focus is on methods and tools that have a formal semantic basis supporting machine-assisted analysis of models and that can be readily deployed in industry. The formalisms on which advances have been based are the Vienna Development Method (VDM) and Event-B. We describe our work in three phases: *conception*, in which we have uncovered evidence that formal model-based techniques might be used effectively in industry settings if appropriately supported; *development* in which we have worked on the development of appropriate support technology; and *proof of concept*, in which we have worked to achieve industry application and evaluation.

Conception

In the EU project “ConForm” (1994-1995), with partner British Aerospace, *Fitzgerald* (*RA 1991-‘94, Lecturer 1995-2001, Reader 2003-2012, Professor 2012 to date, at Newcastle*) with Larsen (IFAD A/S, Denmark), undertook one of the first documented comparisons between formal and structured methods in an industry setting [P1]. At this time, formal methods were widely regarded as impractical outside of critical software. Crucially, the project provided evidence of strengths of formal modelling in VDM, particularly in requirements specification. It identified needs for (i) robust tool support, for simulation as a means of validation, and (ii) integration with semi-formal development practices, including object-oriented design.

These observations were extended in the work of the EU project “DSoS (2000-2003), in which *Jones (Professor at Newcastle, 1999 to date)* and *Romanovsky (SRA 1998-2003, PRA 2003-2005, Professor 2005 to date, at Newcastle)* developed architectural and fault-tolerance solutions for dependable complex systems formed by integrating otherwise independent systems [P2, P3]. Here it became clear that, in addition to requirements (i) and (ii) identified by Fitzgerald and Larsen, support for formal methods in verifying global dependability properties requires significant advances in (iii) tool support for proof, and (iv) for refinement in order to describe composed architectural structure, notably for error detection and recovery mechanisms.

Development

Requirements (i) and (ii) were implemented for VDM and its tools in work led by Fitzgerald & Larsen resulting in the extended VDM++ language (integrated with the industry-standard UML) and tools (VDMTools). VDMTools was commercialised by IFAD A/S in Denmark and was sold to the large Japanese company, SCSK Corporation, where it has been further developed (www.vdmtools.jp/en/). Requirements (iii) and (iv) were addressed in the EC project RODIN, resulting in the first open toolset for refinement-based modelling with integrated proof support using the Event-B formalism – the “Rodin” platform (www.event-b.org).

Proof of concept

To achieve industry deployment of the simulation-based VDMTools and Overture, work improved accessibility to the language and tools. The VDM++ guide was written up as a text in both English and Japanese (*Validated Designs for Object-oriented Systems*, ISBN: 1-85233-881-4 Springer-Verlag, 2005b & Japanese edition, ISBN 978-1-85233-881-7, SE Shoeisha, 2010) and reported on an application by Japan Future IT Systems reducing trading times in the options market. Results suggested defect densities at integration test were well below industry norms (~0.67 defects per kDSI delivered) and that effort and duration levels were 60% lower than standard estimates. Fitzgerald & Larsen have tracked the state of industry perception and use of formal methods in influential studies since their original work [P6].

The EC project DEPLOY (2008-2012), led by Romanovsky, focussing on the proof/refinement-based Rodin technology included 15 partners from academia and industry (e.g. Systerel & ClearSy). The investigators made substantial advances in improving the tools and methods by working closely with industrial partners (Bosch, SAP, Space System, Siemens) [P4, P5]. The specific results include industry-strength tools and their integration into product development, an evidence repository helping various stakeholders in making decisions about deployment of formal methods, modelling patterns and methodological guidelines and assessment of the cost/benefits for the industrial deployment of refinement-based formal methods.

3. References to the research

[P1] Larsen, P.G., Fitzgerald, J & Brookes, T. *Applying Formal Specification in Industry*, IEEE Software, 13(3):48-56, May 1996. Google Scholar : 117 citations. [*Key ref.]

[P2] Jones, C.B., Romanovsky, A & Welch, I. *A Structured Approach to Handling On-Line Interface Upgrades*. Proc. of 26th International Computer Software and Applications Conference (COMPSAC 2002), 2002, pp. 1000-1005. IEEE CS. ISBN 0-7695-1727-7.

[P3] Tartanoglu, F., Issarny, V., Romanovsky, A. & Levy, N. *Coordinated Forward Error Recovery for Composite Web Services*. Proc. 22nd Symposium on Reliable Distributed Systems (SRDS 2003), 2003, pp. 167-176. IEEE CS. ISBN 0-7695-1955-5. Google Scholar : 95 citations

[P4] Iliasov, A., Troubitsyna, E., Laibinis, L. Romanovsky, A., Varpaaniemi, K., Ilic, D. & Latvala, T., *Developing mode-rich satellite software by refinement in Event-B*, Science of Computer Programming 78(7), 2013, ISSN 0167-6423. 5 year journal impact factor:0.982. [*Key ref.]

[P5] Bryans, J. W., Fitzgerald, J. S., Romanovsky, A. & Roth, A. *Patterns for Modelling Time and Consistency in Business Information Systems*. Proc. 15th IEEE International Conference on Engineering of Complex Computer Systems, (ICECCS 2010), pp. 105-114. IEEE CS. [*Key ref.]

[P6] Woodcock, J. C. P., Larsen, P. G., Bicarregui, J. C. & Fitzgerald, J. S., *Formal Methods: Practice and Experience.* ACM Computing Surveys 41(4), 2009, pp. Google Scholar: 187 citations, 5 year journal impact factor 7.854.

Key research grants

ESSI1, #10670: €159 974, (4 Jan 1994 - 3 May 1995), *A Comparison of Conventional and Formal Methods in the Development of a Secure* System *(ConForm).* Awarded to: British Aerospace (Systems and Equipment) Ltd.

FP5, # IST-1999-11585: € 2 652 872, (1 Apr 2000 - 31 Mar 2003), *Dependable Systems of Systems (DSoS),* Awarded to: Newcastle University. PI: Cliff Jones.

FP6-IST, #511599: € 3 171 000, (1 Sept 2004 - 31 Aug 2007), *Rigorous Open Development Environment for Complex Systems (RODIN)*, Awarded to: Newcastle University. PI: Romanovsky.

FP7-ICT, #214158: € 12 403 399, (1 Feb 2008 - 30 Apr 2012), *Industrial deployment of advanced system engineering methods for high productivity and dependability,(DEPLOY)* Awarded to: Newcastle University. PI: Romanovsky.

4. Details of the impact

In many industrial sectors, the costs of designing for dependability can limit the range of potentially valuable applications that are developed. The proposition underpinning the technology developed in this study is that computer-assisted analysis of system models early in development allows the exploration of trade-offs between design alternatives, and the checking of critical properties related to dependability (including safety and security). This permits early elimination of infeasible or unsatisfactory designs before expensive commitments are made to implementation and test.

Newcastle University research, embodied in tools VDMTools & Rodin, allows improved analysis of system models; they automate processes, manage mathematical complexities and link with existing industrial standards like UML and the Eclipse IDE. The research has had two major impacts: one on business and one social in the educational and developer communities.

Improved product development processes for industry

The advantage to industry is in i) *improved development processes* that ii) *make it more feasible to create dependable applications.* Beneficiaries are not just businesses but the end users provided with new technology. Adoption by practitioners has been wide [E9] e.g. *AeS Group* in Brazil, *Bosch in Germany* and *Space Systems Finland*. We highlight further examples:

- FeliCa Networks, a subsidiary of Sony and NTT DoCoMo, used VDM tools [E1, pg.345, 354] to develop firmware for the “mobile FeliCa” IC chip which allows mobile phones to be used as contactless swipe cards. This chip has many applications, e.g. they may be used to pay for services, used as train tickets or operate as door keys. The chip was incorporated in over 100 million Sony mobile phones in Japan [E1, pg. 343] by 2009, and in over 200 million phones worldwide by 2012 [E7]. The large numbers of users and the social infrastructure this technology supports mean that correctness of design is essential [E1] - the tools make this venture feasible by reducing the chances of errors in the end product.
- The Japanese company (NTT) who have adopted these tools report that using VDMTools improved error detection rates by factors of between 1.5 and 5 over previous processes [E2]. Detecting errors early reduces development and maintenance costs, time to implementation, and take up of systems by users, all of which provide financial and competitive advantages, as the case of Mobile FeliCa above highlights.
- Two French companies (Systerel and ClearSy) [E6, E10] are using the Rodin tools and its plugins for validating large data sets in the railway domain, a venture made more efficient using the tools. Systerel has successfully used the method and the tool to improve the confidence in the specification of automated interlocking.
- Siemens have used the Rodin tools in various industrial projects for developing metro lines and airport shuttles in 2011 & 2012 [E3, E9]; these include the modernisation of ALGER line 1, Sao Paolo line 4, Paris line 1 & Charles de Gaulle Vehicle Automatique Leger. As with the railway system mentioned above, correctness of design is especially important for safety critical systems and any modification would be complex and expensive, making these tools especially important in making such ventures feasible.

Adoption of research results by practitioners and educators

Formal methods techniques, mostly inaccessible without expertise, are widely regarded as impractical outside of critical software analysis research [1]. Our novel tools and approach to disseminating formal methods research has influenced industry to adopt and benefit from these techniques and engendered a lively international community of formal methods end-users. Some indicators & examples:

- The research has had an impact in the Higher Education sector extending beyond Newcastle University and the UK. The “Top SE” programme run by the National Institute of Informatics (NII) in Japan now in its 7th year, is supported by 45 companies, and accepts around 30 students per year, and aims to bridge the academia-industry gap in advanced software technology [E5]. All courses in the Formal Specification series use VDM or Event-B.
- SAP, the world leader in enterprise software with operations in more than 130 countries has integrated the model-based scenario testing features of Rodin into developer kits [E3, E9] used by their large customer base.
- SCSK Systems, one of the largest software houses in Japan is now marketing VDMTools as a commercial toolset for the VDM and VDM++ design methods.
- The online prevalence of blogs, tutorials & other support materials, third party plug-ins and support tools (not created by the researchers) are evidence of a large un-recorded market of users and beneficiaries. Sourceforge.net report over 800,000 downloads of Rodin tools in the impact period from a wide range of countries [E8]. The Overture tool, available online, is an extended open source set of tools for VDM developed by the end-user community.

“I regard the success of the Deploy project as a milestone in progress of formal methods….I am delighted that the continuing legacy of the project includes a form of repository, and a toolset in the public domain”. Sir Tony Hoare (Microsoft) [E4]

5. Sources to corroborate the impact

[E1] Kurita, T. and Nakatsugawa, Y., (2009) “*The Application of VDM to the Industrial Development of Firmware for a Smart Card IC Chip*”, International Journal of Software and Informatics, Vol.3, No.2-3, pp. 343-355, ISSN 1673-7288. (http://www.ijsi.org).

[E2] Kazuya, K. (2011) “*Effectiveness of VDM++ in Removing Defects from Web Application Software*”, in Supplemental Proceedings, Industry Papers Track at IEEE 22nd Intl. Symp. on Software Reliability Engineering.

[E3] Wieczorek, S., Kozyura, V., Wei, W., Roth, A., & Stefanescu, A., (2013) “*Business Information Sector”,* in Industrial Deployment of System Engineering Methods,. Springer. ISBN 978-3-642-33169-5.

[E4] Corroboration from Microsoft.

[E5] Ishikawa, F., Taguchi, K., Yoshioka, N., & Honiden, S. (2009): “*What Top-Level Software Engineers Tackle after Learning Formal Methods: Experiences form the Top SE Project*”, in Gibbons, J.; Oliveira, J. N. (Eds.): “TFM 2009”, LNCS 5846, pp. 57-71, Springer. Doi: 10.1007/978-3-642-04912-5_5.

[E6] Corroboration from ClearSy.

[E7] Press release: “*Sony and Watchdata Announce Agreement to Expand Global Reach for Near Field Communication/FeliCa Technology”* www.sony.net/SonyInfo/News/Press/201212/12-1214E/index.html. (Dec 14, 2012).

[E8] Download statistics: http://sourceforge.net/projects/rodin-b-sharp/files/stats/timeline?dates=2008-01-01+to+2013-06-11.

[E9] Industrial projects, http://wiki.event-b.org/index.php/Industrial_Projects, (2012).

[E10] Corroboration from Systerel.