Institution: **University of Oxford**

Unit of Assessment: **11 Computer Science and Informatics**

Title of case study: **Automated Verification and Validation for Defence, Aerospace and Automotive Embedded Software (7)**

1. Summary of the impact (indicative maximum 100 words)

QinetiQ's Systems Assurance Group (SAG) collaborated with the UoA from the early 1990s on the use of their research, such as Communicating Sequential Processes (CSP) and the verification tool FDR. SAG applied these to MOD projects, assessing the dependability of software systems, such as Plug & Play Weapons architectures and Eurofighter avionics, up until 2012. In 2012, core people from SAG set up the company D-RisQ. D-RisQ obtained a license from QinetiQ enabling them to take the UoA's technology forward and commercialise it. The core of this impact relates to safety-case analysis for legacy systems.

2. Underpinning research (indicative maximum 500 words)

D-RisQ's technology (like its predecessors created at QinetiQ) is based on Failures Divergences Refinement (FDR). FDR is a model checker which itself uses Communicating Sequential Processes (CSP), a process algebra designed to help understand and analyse how systems interact with each other [1]. While the initial development of CSP dates back to the 1970s, it continues to be researched and developed within the UoA [2].

The second, heavily updated and completely re-written version, FDR2, became available in 1994. Throughout its history, the key designer of FDR and its algorithms has been Professor Bill Roscoe from the UoA, although until 2007 the program was released and maintained by Oxford Spin-out Formal Systems. FDR development has been entirely the responsibility of the UoA since 2008 with releases of FDR2 up to 2.94 in 2012, and the completely re-written FDR3 in 2013. FDR's main function is to verify or refute refinement relations over a variety of semantic models—essentially it establishes that abstract specifications are satisfied by concrete programs. FDR is an extremely powerful process-algebra based model checker, and as such has been widely used in research and industry.

Most of the current funding for the development of FDR3 comes from the DARPA HACMS programme under a proposal concentrating on the further development of D-RisQ's technology on system-of-system applications in autonomous systems.

DERA, QinetiQ, and latterly D-RisQ, have sponsored and/or collaborated in a significant amount of research in the UoA relating to CSP and FDR in the period since 1994. They have sponsored doctoral students such as Sadie Creese (inductive verification) who worked there before becoming Professor of Cyber Security at Warwick and now Oxford. They have sponsored work and collaborated on topics such as security [1,4] (cryptographic protocols, including the development of the FDR chase operator, information flow, and ad hoc security), the state explosion problem including induction [3] and symmetry reduction [5], assumption-guarantee methods, and Statechart verification [6]. All of this and more has been relevant to the impact story told below.

Aside from this, the applications of FDR and CSP referred to below depend on a wide range of CSP work done at the UoA since 1993 including FDR's compressions, lazy abstraction, *tock*-CSP, and data independence, all reported in [1,2].

3. References to the research (indicative maximum of six references)

The three asterisked outputs best indicate the quality of the underpinning research.

***[1] A.W. Roscoe. *The Theory and Practice of Concurrency*, Prentice-Hall 1997.** http://dl.acm.org/citation.cfm?id=550448

*[2] **A.W. Roscoe. *Understanding Concurrent Systems*, Springer 2010.** http://www.springer.com/computer/swe/book/978-1-84882-257-3

The above are both major books on CSP and FDR describing many of the CSP techniques and theories, and FDR function and algorithms, used by DERA/QinetiQ and D-RisQ.

***[3] S. J. Creese, AW Roscoe. Data independent induction over structured networks. In International Conference on Parallel and Distributed Processing, 2000.**

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.35.8274&rep=rep1&type=pdf

DERA sponsored work on verification that was the basis of a number of projects in DERA/QinetiQ.

[4] S Creese, M Goldsmith, A W Roscoe, I Zakiuddin. Authentication for pervasive computing. Security in Pervasive Computing, pp439-488, 2004.

http://www.cs.ox.ac.uk/people/bill.roscoe/publications/87.ps

Reports agenda-setting collaboration on security between Oxford and QinetiQ.

[5] N. Moffat, M. Goldsmith, A.W Roscoe. A Representative Function Approach to Symmetry Exploitation for CSP Refinement Checking. Formal Methods and Software Engineering: 10th International Conference on Formal Engineering Methods, ICFEM 2008, Kitakyushu-City, Japan, October 27-31, 2008: proceedings. Pages 258-277. Springer-Verlag New York Inc.

DOI: 10.1007/978-3-540-88194-0_17

Reports collaborative work between QinetiQ and Oxford (Moffat was QinetiQ employee doing a part-time Oxford doctorate) which was key to the scalability of some of the FDR analysis done in QinetiQ.

[6] AW Roscoe, Z Wu. Verifying Statemate statecharts using CSP and FDR**.** Formal Methods and Software Engineering, 324-341. 2004.

doi:10.1007/11901433_18

QinetiQ-sponsored continuation of Roscoe's work on verifying Statecharts in CSP/FDR: model for translating notations into CSP, important to ModelWorks, as is the Statechart model.

4. Details of the impact (indicative maximum 750 words)

The period of 2008-July 2013 provides a window on an impact story that was already well established at the start of it, and has multiple aspects continuing at the end of it. Understanding the story prior to 2008 is important in understanding the route to the in-period impact. The long-standing research relationship, set out in Section 2, is itself the primary route to impact. The impact described below should be set against the fact that, while there have been many attempts to use formal verification tools such as model checkers such as FDR (which explore the state space of an implementation trying to eliminate the possibility of errors) for certifying large-scale software systems, comparatively few have been successful.

The exploitation of the UoA's research in CSP and FDR was carried out by the Systems Assurance Group (SAG) within DERA (later QinetiQ) from the 1990s up until 2012. The exploitation took the form of building models of high profile third party software based components and systems in order to check independently derived safety or security requirements on behalf of the MOD. Independent measurements [J] indicated the potential for 60-80% savings on time and cost when used the approach was used as part of a system's development due to reductions in testing and automation of re-work due to requirements change. More importantly it enabled the MOD to accept systems for use when testing was not a viable option, e.g. to prove a negative such that a dangerous behaviour could never occur. The importance of this is that it enabled new military capabilities to be exploited that reduced the risk to life of service personnel in operations. For example the MOD was able to use the Typhoon aircraft, instead of more vulnerable aircraft, because of the direct contribution of CSP and FDR to its military airworthiness. The process of transferring such a system from the procurement part of MOD to the Services for military operations is called “Release to Service”. The successful application of formal methods to systems of this scale is unusual, and we believe that in legacy systems it is probably unique. Success can also be judged by the safety record of such a complex safety critical software system. The importance of Oxford’s work is shown in a quote from [C] below:

‘Oxford's research has been central to the Systems Assurance Group's project support activities, up until 2012, and now D-RisQ Ltd. Research outputs from Oxford were applied to give bespoke solutions to difficult assurance issues and then turned into commoditised services that were used to reduce the cost of assuring third party systems. Conversely challenging assurance issues were fed back to Oxford to stimulate research whose outputs were again applied. The result of this collaboration was the creation of a unique capability to assess third party systems. The key to the capability was the exploitation of non-determinism to model uncertainty about claimed system behaviour and Oxford's contribution to this was to provide tractable analysis methods.’

FDR first became widely used within DERA in the late nineties, after it was used to analyse the safety of inserting the US Tomahawk Land Attack Missile system into the Royal Navy’s legacy systems [A,B]. This, and much of the subsequent work, depended crucially on FDR *chase*, discovered and developed at Oxford during DERA-sponsored security work as described in Part 2. Further models for assessing the safety of systems procured by the MOD were developed [D], as well as methods for scaling the analysis, for example using compression [1,2 above], induction [2,3] and symmetry reduction [5].

MOD project support led to the development of a generic library of CSP models that could be re-used, enabling more MOD procurements to be supported. For example, various fault tolerant architectures have been modelled and used to assess different MOD avionics systems, as shown in the following quote from [C], which demonstrates clear impact within the REF period:

‘*A notable application of FDR2 was to check Code Level Analysis Objectives (which link lower level safety objectives to high level aircraft safety requirements) for Eurofighter Typhoon's avionics systems. The exploitation of FDR2 on providing evidence for the Release To Service recommendation for Eurofighter finished in 2010. The Systems Assurance Group developed a tool called ModelWorks that compiles higher level descriptions of systems into efficient machine readable CSP for checking specified properties by FDR2. In 2011 - 2012 two notable applications of ModelWorks and FDR2 took place. The first application was to check safety properties of a System of Systems based upon Service Oriented Architectures. The second application of FDR2 was to check safety properties for a Plug and Play Architecture for Weapon Systems that is being developed by a consortium called Weapons Integration UK under a task called Software Auto-code and Auto-proof.’*

Reference to the “Software Auto-code and Auto-proof” work can be found in [E]; details of ModelWorks can be found at [F]. ModelWorks was the main means by which FDR has been exploited since 2008. The Plug and Play project is a direct descendant of the earlier work on cruise missiles described above.

A further economic impact has been the formation of a company to further develop and commercially exploit the tools and methods described above, both in their established domain in the defence sector and beyond. In May 2012 the start-up D-RisQ Ltd was set up [F]. D-RisQ has licensed FDR, and IP from QinetiQ, such as ModelWorks, that utilises the UoA's research. It aims to provide assurance evidence that is at least 60% cheaper than current practice in the areas of automotive, defence, and aerospace through standards such as ISO 26262, 00-56, and DO178-C.

This represents a significant personal financial risk to the founding directors of approximately £500K to start up the company and created 9 high tech jobs in an area hit by redundancies in high tech firms. D-RisQ's promise was recognised in a recent competition for start-ups [G]. At 31 July 2013, D-RisQ is six months into a project with Blue Bear Systems Research [H] to develop and certify a vehicle with entry level autonomy using FDR, with some oversight by the Civil Aviation Authority. Similarly they are engaged with the automotive sector in the application of FDR through ModelWorks being taken forward in 2013 through the Advanced Manufacturing Supply Chain Initiative for commercial exploitation by D-RisQ in partnership with Ricardo Ltd [I], to improve cost efficiency across the UK.

5. Sources to corroborate the impact (indicative maximum of 10 references)

[A] C. O'Halloran. *Assessing Safety Critical COTS Systems*. Journal of Hazard Prevention, Volume 35. Pages 14-19, 1999. System Safety Society, Inc.
One of two papers as a result of the analysis of the safety of inserting the US Tomahawk Land Attack Missile system into the Royal Navy's legacy systems.

[B] I. Zakiuddin, N. Moffat, C. O'Halloran, P. Ryan. *Chasing events to certify a critical system.* Technical report, UK Defence Evaluation and Research Agency, 1998.
One of two papers as a result of the analysis of the safety of inserting the US Tomahawk Land Attack Missile system into the Royal Navy's legacy systems.

[C] Email from D-RisQ Business Director (N. Tudor) to Bill Roscoe on the use of FDR for assessing MOD avionics systems. *Held on file.*

[D] I. Zakiuddin, N. Moffat, M. Goldsmith, T. Whitworth. *Property-based compression strategies.* Proceedings of Second Workshop on Automated Verification of Critical Systems (AVoCS 2002).
This paper describes the creation of models in FDR for assessing the safety of systems.

[E] http://aerosociety.com/Assets/Docs/Events/710/4)%20Stephen%20Michie%20[Compatibility%20Mode].pdf
Reference to "Software Auto-code and Auto-proof" work on page 5.

[F] D-RisQ Flyer held on record 'D-Risq Modelworks - Systems of Systems Analysis' describes the use of Modelworks for analysis techniques

[G] http://www.cambridgenetwork.co.uk/news/winners-of-uk-discovering-start-ups-2012-announced/
Shows details of the start-up company recognition for D-RisQ.

[H] http://www.bbsr.co.uk/blog/2013/10/collaboration-between-blue-bear-and-d-risq-in-the-tsbs-novel-autonomous-robotics-call/
Press release from Blue Bear on their collaboration with D-RisQ..

[I] http://www.ricardo.com/en-GB/News--Media/Press-releases/News-releases1/2013/Ricardo-led-consortium-wins-UK-government-funding-for-safety-critical-systems-development/
Shows details of the recent project with Ricardo to commercially exploit Modelworks for Manufacturing Supply Chain Management.

[J] N. Tudor. *Benefits of QinetiQ Architecture Analysis.* Report Reference QINETIQ/10/02472. 14/12/2010. Delivered to Jaguar/Land Rover under the TSB Validation of Complex Systems programme.
Report by a QinetiQ employee, indicating the savings achieved by using Modelworks.