Dr Roderick Chapman FIET FBCS

Résumé – March 2019

Roderick Chapman is an independent consultant software engineer. He specialises in the development of safety- and security-critical systems, from requirements engineering, through architectural design and implementation, to verification, audit and assessment.

Following graduation from the University of York, Rod joined Praxis (now Altran UK), and contributed to many of the company's keynote projects, rising to the role of principal engineer for software process and design. He also led the programming language and verification research group at Praxis, leading the technical development, training, sales and marketing of the SPARK product line. More recently, Rod turned his attention to software process, working on merging the discipline of traditional high-integrity processes with more agile approaches such as Scrum, and the philosophy of the Lean Engineering Movement. As part of this work, Rod became the first SEI-certified Personal Software Process (PSP) Instructor in the UK and led the roll-out of the PSP approach within the company's CMMI processes and appraisal.

Rod is a regular speaker at international conferences, and is widely recognized as a leading authority on high-integrity software development, programming language design, and software verification tools. In 2006, he was invited to become a Fellow of the British Computer Society. In 2011, Rod was the joint recipient of the inaugural Microsoft Research Verified Software Milestone Award for his contribution to the Tokeneer project.

In February 2015, Rod was appointed Honorary Visiting Professor in the Department of Computer Science at the University of York, and serves as a member of the department's Industrial Advisory Board.

Education and Qualifications

2005	SEI-Certified PSP Instructor
1995	DPhil in Computer Science, University of York. "Static timing analysis and program proof".
1991	MEng (Hons) 1st Class in Computer Systems and Software Engineering, University of York.

Professional Affiliations

Fellow of the IET (2015), Member of the ACM (2014), Fellow of the British Computer Society (2006), Chartered Engineer (1998)

Employment

February 2015 – present	Honorary Visiting Professor, Department of Computer Science, University of York.
June 2014 – present	Independent consultant and engineer.
2006–May 2014	Principal Engineer with Altran UK.
2001–2006	Senior Engineer with Praxis High Integrity Systems.
1997–2001	Software Engineer with Praxis Critical Systems.
1995–1997	Senior Programmer with Praxis plc., Bath, UK
1991–1995	Research Associate at the British Aerospace Dependable Computing Systems Centre at the University of York, UK

Personal Details

Address for correspondence: 65 Holcombe Close, Bathampton, Bath BA2 6UP.

Telephone: +44 (0)7787 155978

E-mail: rod@proteancode.com

Services, Skills and Technologies

Rod has experience covering the majority of lifecycle phases, and has particular skills in implementation, technologies and training services for teams developing critical software.

Area	Capabilities
Engineering process	Software process design for high-integrity software, incorporating Lean Engineering, Agile approaches, Correctness-by-Construction, Model-Based Design, and Formal Methods. Significant experience with the SEI's CMMI, Team and Personal Software Processes and their application in critical software development.
Architecture and design	Architectural design of systems and software, especially those with safety or security requirements. Verification-driven design.
Implementation technologies	Ada and SPARK (expert level experience, including compiler, runtime, and board-support package design). C and MISRA C. Static analysis and verification technologies, their adoption and deployment.
Standards	Most standards and guidance, including DO-178B, DO-178C, DO-333 (Formal Methods), CENELEC 50128/9, Nuclear, and Security standards.
Audit and Assessment	From basic project/process "health check" to fully formal audit to industry standards.
Training	Rod is an experienced trainer, coach and mentor of software teams. Particular areas include: • SPARK and Ada, their adoption, design, and use in high-integrity projects. • SEI-certified Personal Software Process Instructor.

Publications

I can distribute PDF of the full text of some of these publications. Please email me for details.

Refereed Journals

R. Chapman, N. White, J. Woodcock, "What Can Agile Methods Bring to High-Integrity Software Development?" *Communications of the ACM.* Vol. 60, Number 10. pp. 38-41. DOI:10.1145/3133233

N. White, S. Matthews, R. Chapman, "Formal verification: will the seedling ever flower?" *Phil Trans R Soc A*, vol. 375, no. 2104, Oct 2017, doi: 10.1098/rsta.2015.0402

A. Burns *et. al.* "Ada and the software vulnerabilities project." *ACM SIGAda Ada Letters*, Volume 30 (2), pp. 27-52. 2010.

A. Ireland *et al*, "An integrated approach to high integrity software verification" *J Autom Reasoning*, 36 (4), April 2006, pp. 379–410, doi: 10.1007/s10817-006-9034-1

R. Chapman, "Panellist position statement: some industrial experience with program verification" *Phil Trans R Soc A*, 363 (1835), Oct 2005, pp. 2393–2394, doi: 10.1098/rsta.2005.1652

A. Hall, and R. Chapman "Correctness by construction: building a commercial secure system" *IEEE Software*, 19 (1), Jan/Feb 2002, pp. 18–25, 10.1109/52.976937

Featured in P. Ross "The Exterminators" *IEEE Spectrum*, 42 (9), Sept 2005, pp. 36–41, doi: 10.1109/MSPEC.2005.1502527

S. King *et al*, "Is proof more cost-effective than testing?" *IEEE Trans Software Eng*, 26 (8), Aug 2000, pp. 675–686, doi: 10.1109/32.879807

R. Chapman *et al*, "Combining static worst-case timing analysis and program proof" *Real-Time Systems*, 11 (2), Sept 1996, pp. 145–171, doi: 10.1007/BF00365316

R. Chapman *et al*, "Static worst-case timing analysis of Ada" *ACM Ada Letters*, 14 (5), Sept/Oct 1994, pp. 88–91, doi: 10.1145/192867.192873

Book Chapters

J. Woodcock *et al*, "The Tokeneer Experiments" in *Reflections on the Work on C. A. R. Hoare*. C. B. Jones et al. (Eds), Springer Verlag 2010. pp. 405–430. ISBN 978-1-84882-911-4

Conference & Workshop Papers

R. Chapman, "Sanitizing Sensitive Data: How to Get It Right (or at Least Less Wrong)." *Proc of Reliable Software Technologies – Ada Europe 2017.* Vienna, Austria, June 2017. Springer LNCS Vol. 10300. DOI: 10.1007/978-3-319-60588-3_3. Winner – best presentation award.

R. Chapman, "Industrial experience with Agile in high-integrity software development." *Proc of the 24th Safety Critical Systems Symposium, Brighton, UK*. Safety Critical Systems Club, UK, Feb 2016. pp. 143-154. ISBN 978-1519420077

J. Kanig *et al*, "Explicit Assumptions – A Prenup for Marrying Static and Dynamic Program Verification" *Proc Tests and Proofs 2014*. Springer-Verlag LNCS, vol. 8570, pp. 142 – 157. DOI: 10.1007/978-3-319-09099-3_11.

R. Chapman *et al*, "SPARKSkein: a formal and fast reference implementation of Skein" *Proc 14th Brazilian Symp on Formal Methods*, Sao Paulo, Brazil, Sept 2011. Springer-Verlag LNCS, vol. 7021, pp. 16–27. DOI: 10.1007/978-3-642-25032-3_2.

R. Chapman and T. Jennings "Panellist position statement: OOT, DO-178C and SPARK" *Proc Reliable Software Technologies Conference* (Ada Europe), Edinburgh, UK, June 2011. Springer-Verlag LNCS, vol. 6652, pp. 206–210. DOI: 10.1007/978-3-642-21338-0_18.

V. Klebanov *et al*, "The 1st verified software competition: experience report" *Proc 17th Int'l Symp on Formal Methods*, Limerick, Ireland, June 2011. Springer-Verlag LNCS, vol. 6664, pp. 154–168. DOI: 10.1007/978-3-642-21437-0_14.

Winner – Best paper award

J. Barnes *et al*, "Engineering the Tokeneer enclave protection software" *Proc IEEE Int'l Symp on Secure Software Engineering*, Washington DC, USA, Sept 2006

SPARK team "Languages, ambiguity, and verification" *Proc Verified Software: Theories, Tools, Experiments*, ETH Zürich, Switzerland, Oct 2005

R. Chapman "Correctness by construction: a manifesto for high integrity software" *Proc 10th Australian Workshop on Safety-Related Programmable Systems*, Sydney, Australia, 2005. CRPIT, 55. T. Cant (Ed.) ACS. pp. 43–46

P. Amey *et al*, "Smart certification of mixed criticality systems" *Proc Reliable Software Technologies Conference* (Ada Europe), York, UK, June 2005. Springer-Verlag LNCS, vol. 3555, pp. 144-155

Winner – Best paper award

R. Chapman and A. Hilton "Enforcing security and safety models with an information flow analysis tool" *Proc ACM SIGAda Conference*, Atlanta, USA, Nov 2004

R. Chapman and P. Amey "Static verification and extreme programming" *Proc ACM SIGAda Conference*, San Diego, USA, Dec 2003

P. Amey and R. Chapman "Industrial strength exception freedom" *Proc ACM SIGAda Conference*, Houston, USA, Dec 2002. ISBN 1-58113-611-0, pp. 1–9

R. Chapman "SPARK – A state-of-the-practice approach to the Common Criteria implementation requirements" *Proc Int'l Common Criteria Conference*, Brighton, UK, Sept 2001

R. Chapman and R. Dewar "Re-engineering a safety-critical application using SPARK95 and GNORT" *Proc Reliable Software Technologies Conference* (Ada Europe), Santander, Spain, June 1999. Springer-Verlag LNCS, vol. 1622, pp. 39–51

Winner – Best presentation award

S. King *et al*, "The value of verification: positive experience of industrial proof" *Proc World Congress on Formal Methods*, Toulouse, France, Sept 1999. Springer-Verlag LNCS, vol. 1709, pp. 1527–1545

R. Chapman *et al*, "Regular path algebra applied to non-functional properties of critical software" in *Mathematics of Dependable Systems II* (*Institute of Mathematics and its Application Conference Series)*, V. Stavridou (Ed), Clarendon Press 1997, pp. 95–112. ISBN 978-0198523826

R. Chapman *et al*, "SPATS – A new toolset for high-integrity Ada development" *Proc AdaUK Int'l Conference*, London, UK, 1995. Ada User (Special Issue), vol. 16, no. 3, pp. 123-131

R. Chapman *et al*, "Regular path algebra applied to non-functional properties of critical software" *Proc Mathematics of Dependable Systems Conference*, York, UK, Sept 1995

R. Chapman *et al*, "Integrated program proof and worst-case execution time analysis of SPARK Ada" *Proc ACM Workshop on Language, Compiler and Tool Support for Real-Time Systems*, Florida, USA, June 1994, pp. K1-K11

Invited Conference Presentations and Tutorials

Keynote: "Are We There Yet? 20 Years of Industrial Theorem Proving with SPARK" *Proc Interactive Theorem Proving 2014.* July 2014. Springer-Verlag LNCS, vol 8558, pp. 17 – 26. DOI: 10.1007/978-3-319-08970-6_2

Keynote: "Delivering Agility and Discipline: Experiences with High-Assurance Software Engineering". SEI TSP Symposium, St. Petersburg, Florida, USA, September 2012.

Tutorial: "Static Code Verification: Issues, Problems and Current Technologies" Embedded Systems Conference Silicon Valley, San Jose, California, USA, May 2011.

Presentation: "Tokeneer –An Experiment in High-Assurance Software Engineering" Microsoft Research Software Summit, Paris, France, April 2011.

Tutorial: "SPARK – The Libre Language and Toolset for High-Assurance Software" Reliable Software Technologies (Ada Europe) Conference, Valencia, Spain, June 2010

Presentation: "The SEI's PSP and TSP – Culture and Discipline for High-Assurance Software" Safety Critical Systems Club – Tools and Investment for Optimum Return on Investment. MoD Abbey Wood, Bristol, UK, June 2009

Keynote: "Correctness by Construction: Putting Engineering (back) into Software" ACM SIGAda Conference, Fairfax, Virginia, USA, November 2007

Tutorial: "Security by Construction" ACM SIGAda Conference, Fairfax, Virginia, USA, November 2007

Tutorial: “SPARK - a High-Integrity Programming Language and its Verification Environment” LASER Summer School on Software Engineering, Elba, Italy, September 2007.

Keynote: “Correctness by Construction: Putting Engineering into Software” Reliable Software Technologies (Ada Europe), Porto, Portugal, June 2006

Tutorial: “SPARK – An intensive overview” ACM SIGAda Conference, Houston, Texas, USA, December 2002

Tutorial: “Practical Experiences of Safety-Critical Ada Technologies” Ada Europe, Leuven, Belgium, June 2001

Conference Committee Involvement

2015	FormaliSE Workshop	Programme Committee Member
2002 - 2011	Reliable Software Technologies (Ada Europe)	
	2011	Co-General Chair
	2002 – 2004, 2010, 2011	Programme Committee Member
	2006, 2007, 2009, 2010	Industrial Programme Committee Member
	2005	Exhibition Chair
2001	ACM SIGAda Conference	Programme Committee Member

PhD Examinations

International external examiner for PhD of Kristina Lundqvist, “Distributed Computing and Safety Critical Systems in Ada.” Uppsala University, Sweden, 2000.