Simon Foster

+44 (0)1904 325424
simon.foster@york.ac.uk
http://www.cs.york.ac.uk/~simonf
http://uk.linkedin.com/in/simondfoster
https://orcid.org/0000-0002-9889-9514

Personal	**Full Name** Dr. Simon David Foster **Date of Birth** 25th of August, 1983 **Nationality** British **Current Role** Post-Doctoral Research Fellow, University of York **Department** Computer Science **Date of Appointment** 13/03/2012
Academic Qualifications	*Jan 2010* **PhD, Computer Science,** University of Sheffield (Viva: 30/07/2009) *Sep 2005* **MComp (Hons) Computer Science** (First Class), University of Sheffield
Statement	*"I am an experienced postdoctoral researcher with 10 years of experience, and can evidence my skills, including research (with impact), publication, teaching, research proposal writing, and project administration. My specialist area is the development of automated software verification tools via formal denotational semantic models in the Isabelle/HOL proof assistant. I have applied our verification platform,* ***Isabelle/UTP****, in verification of concurrent, cyber-physical, and systems of systems. Our technology is widely applicable, and we seek to transfer these results to verification of real world industrial safety assurance problems. I have recently been awarded a UKRI Innovation Fellowship by EPSRC, a project which will help me firmly establish my research field."*
Education & Employment	*June 2018 – present* **PI on UKRI EPSRC Fellowship EP/S001190/1. "***CyPhyAssure***: *Compositional Safety Assurance for Cyber-Physical Systems".* University of York. https://www.cs.york.ac.uk/circus/CyPhyAssure/ *Jan 2018 – May 2018* **Research Fellow, EPSRC Project EP/M025756/1.** *"A Calculus for Software Engineering of Mobile and Autonomous Robots" (RoboCalc).* University of York. PI: Prof. Ana Cavalcanti, https://www.cs.york.ac.uk/circus/RoboCalc/ *Apr 2015 – Dec 2017* **Research Fellow, EU H2020 ICT-1 Project.** *"Integrated Tool Chain for Model-based Design of Cyber-Physical Systems" (INTO-CPS).* University of York. PI: Prof. Jim Woodcock, http://into-cps.au.dk *Oct 2014 – Mar 2015* **Research Associate, QinetiQ sponsored. "***Modular Safety Cases for the Generic Vehicle Architecture".* University of York. PI: Prof. Tim Kelly *Mar 2012 – Sep 2014* **Research Associate, EU FP7 Project 287829. "***Comprehensive Modelling for Advanced Systems of Systems" (COMPASS).* University of York. PI: Prof. Jim Woodcock. http://www.compass-research.eu *2009 – 2012* **Research Associate, EPSRC Project EP/G031711/1.** *"Higher Order Refinement Techniques for the Model Driven Architecture".* University of Sheffield. PI: Prof. John Derrick *Summer 2009* **Research Assistant on "Bridging the Gaps" investigation** *"Resource optimisation for modular speech recognition systems" .* PI: Dr. Thomas Hain *2005 – 2009* **PhD, University of Sheffield.** *"A Compositional Semantic Theory for Service Composition".* Supervisor: Dr. Mike Stannett *2001 – 2005* **MComp (Hons) Computer Science,** University of Sheffield
Funding	**CyPhyAssure: Compositional Safety Assurance for Cyber-Physical Systems.** Principal Investigator. EPSRC UKRI Innovation Fellowship. Period: June 2018 – May 2021. Value: £562,549

	Mechanised Assume-Guarantee Reasoning for Control Law Diagrams via Circus. Co-Investigator. GCHQ funded under UK Research Institute in Verified Trustworthy Software Systems (VeTSS). Period: September 2017 – March 2018. Value: £81,956
Publications	S. Foster, M. Gleirscher, R. Calinescu. **Towards Deductive Verification of Control Algorithms for Autonomous Marine Vehicles.** 25th Intl. Conf. on Engineering of Complex Computer Systems (ICECCS 2020). October 2020. S. Foster, J. Baxter, A. Cavalcanti, J. Woodcock, F. Zeyda. **Unifying Semantic Foundations for Automated Verification Tools in Isabelle/UTP.** Science of Computer Programming, volume 197. October 2020. S. Foster, Y. Nemouchi, C. O'Halloran, N. Tudor, K. Stephenson. **Formal Model-Based Assurance Cases in Isabelle/SACM: An Autonomous Underwater Vehicle Case Study.** Proc. 8th Intl. Conf. on Formal Methods in Software Engineering (FormaliSE 2020). ACM. October 2020. S. Foster, J. Baxter. **Automated Algebraic Reasoning for Collections and Local Variables with Lenses.** 18th Intl. Conf. on Relational and Algebraic Methods in Computer Science (RAMiCS 2020). LNCS 12062. Springer. October 2020. S. Foster, J. J. H. Munive, G. Struth: **Differential Hoare Logics and Refinement Calculi for Hybrid Systems with Isabelle/HOL.** 18th Intl. Conf. on Relational and Algebraic Methods in Computer Science (RAMiCS 2020). LNCS 12062. Springer. October 2020. S. Foster, A. Cavalcanti, S. Canham, J. Woodcock, F. Zeyda. **Unifying theories of reactive design contracts.** Theoretical Computer Science journal, volume 802. January 2020. Y. Nemouchi, S. Foster, M. Gleirscher. **Isabelle/SACM: Computer-Assisted Assurance Cases with Integrated Formal Methods.** Proc. 15th Intl. Conf. on Integrated Formal Methods (iFM 2019). LNCS 11918. December 2019. S. Foster, F. Zeyda, et al. **Isabelle/UTP: Mechanised Theory Engineering for Unifying Theories of Programming.** Archive of Formal Proofs (AFP 2019). S. Foster. **Hybrid Relations in Isabelle/UTP.** In Proc. 7th Intl. Symp. on Unifying Theories of Programming (UTP 2019). LNCS 11885. October 2019. J. Woodcock, A. Cavalcanti, S. Foster, A. Mota, K. Ye. **Probabilistic Semantics for RoboChart: A Weakest Completion Approach.** In Proc. 7th Intl. Symp. on Unifying Theories of Programming (UTP 2019). LNCS 11885. October 2019. M. Gleirscher, S. Foster, and Y. Nemouchi. **Evolution of Formal Model Based Assurance Cases for Autonomous Robots.** Proc. 17th Intl. Conf. on Software Engineering and Formal Methods (SEFM 2019). September 2019. M. Gleirscher, S. Foster, J.Woodcock. **New Opportunities for Integrated Formal Methods.** Accepted for publication in ACM Computing Surveys, August 2019. S. Foster, J. Baxter, A. Cavalcanti, A. Miyazawa, J. Woodcock. **Automating Verification of State Machines with Reactive Designs and Isabelle/UTP.** In Proc. 16th Intl. Conf. on Formal Aspects of Component Software (FACS 2018). LNCS

11222.

S. Foster, K. Ye, A. Cavalcanti, J. Woodcock. **Calculational Verification of Reactive Programs with Reactive Relations and Kleene Algebra.** In Proc. 17th Intl. Conf. on Relational and Algebraic Methods in Computer Science (RAMICS 2018). LNCS 11194.

S.Foster, S. Canham, A. Cavalcanti, J. Woodcock, F. Zeyda. **Unifying Theories of Reactive Design Contracts.** Submitted to Theoretical Computer Science, December 2017. Preprint: http://arxiv.org/abs/1712.10233.

S. Foster, A. Cavalcanti, J. Woodcock, F. Zeyda. **Unifying Theories of Time with Generalised Reactive Processes.** Information Processing Letters 135:47-52. July 2018.

F. Zeyda, J. Ouy, S. Foster, and A. Cavalcanti. **Formalising Cosimulation Models.** 1st Workshop on Formal Co-simulation of Cyber-Physical Systems (CoSim-CPS). September 2017. LNCS 10729.

S. Foster and F. Zeyda. **Optics in Isabelle/HOL.** Archive of Formal Proofs. 2017.

S. Foster and J. Woodcock. **Towards Verification of Cyber-Physical Systems with UTP and Isabelle/HOL.** Concurrency, Security, and Puzzles. 2017. LNCS 10160.

S. Foster, F. Zeyda, and J. Woodcock: **Unifying Heterogeneous State-Spaces with Lenses.** Proc. 13th Intl. Colloq. on Theoretical Aspects of Computing (ICTAC). October 2016. LNCS 9965.

P. G. Larsen, J. Fitzgerald, J. Woodcock, R. Nilsson, C. Gamble, S. Foster: **Towards Semantically Integrated Models and Tools for Cyber-Physical Systems Design.** Proc. 7th Intl. Symp. on Leveraging Applications of Formal Methods (ISoLA). 2016. LNCS 9952.

J. Woodcock, S. Foster, and A. Butterfield: **Heterogeneous Semantics and Unifying Theories.** Proc. 7th Intl. Symp. on Leveraging Applications of Formal Methods (ISoLA). 2016. LNCS 9952.

J. Woodcock and S. Foster: **UTP by Example: Designs.** 2nd Intl. School on Engineering Trustworthy Software Systems (SETSS). 2016. LNCS 10215.

S. Foster, B. Thiele, A. Cavalcanti, and J. Woodcock: **Towards a UTP Semantics for Modelica.** Proc. 6th Intl. Symp. on Unifying Theories of Programming (UTP). 2016. LNCS 10134.

F. Zeyda, S. Foster, and L. Freitas: **An Axiomatic Value Model for Isabelle/UTP.** Proc. 6th Intl. Symp. on Unifying Theories of Programming (UTP). 2016. LNCS 10134.

S. Foster and G. Struth: **On the Fine-Structure of Regular Algebra.** Journal of Automated Reasoning 54:2. February 2015.

J. Woodcock, A. Cavalcanti, J. Fitzgerald, S. Foster, P. G. Larsen: **Contracts in CML.** 6th International Symposium on Leveraging Applications of Formal Methods, Verification, and Validation (ISoLA). LNCS 8803. October 2014.

S. Foster, F. Zeyda, and J. Woodcock: **Isabelle/UTP: A Mechanised Theory**

	Engineering Framework. 5th International Symposium on Unifying Theories of Programming. LNCS 8963. May 2014. S. Foster, A. Miyazawa, J. Woodcock, A. Cavalcanti, J. Fitzgerald, P. G. Larsen: **An approach for managing semantic heterogeneity in systems of systems engineering.** IEEE 9th International System of Systems Engineering Conference. June 2014. S. Foster and G. Struth: **Regular Algebras.** Archive of Formal Proofs. 2014. L. D. Couto, S. Foster, and R. Payne: **Towards Verification of Constituent Systems through Automated Proof.** Workshop on Engineering Dependable Systems of Systems (EDSoS). April 2014. S. Foster and J. Woodcock: **Unifying Theories of Programming in Isabelle.** ICTAC School on Software Engineering. 2013. LNCS 8050. S. Foster and G. Struth: **Automated Analysis of Regular Algebra.** 6th International Joint Conference on Automated Reasoning (IJCAR). 2012. LNCS 7364. S. Foster, O. Rypáček, and G. Struth: **Correctness of Object Oriented Models by Extended Type Inference.** 9th Intl. Colloquium on Theoretical Aspects of Computing (ICTAC). 2012. LNCS 7521. A. Armstrong, S. Foster and G. Struth: **Dependently Typed Programming Based on Automated Theorem Proving.** 11th Intl. Conference on Mathematics of Program Construction (MPC). 2012. LNCS 7342. S. Foster, G. Struth, and T. Weber: **Automated Engineering of Relational and Algebraic Methods in Isabelle/HOL.** Proc. 12th Intl. Conf. on Relational and Algebraic Methods in Computer Science (RAMiCS). 2012. LNCS 6663. S. Foster, G. Struth: **Integrating an Automated Theorem Prover into Agda**. 3rd NASA Formal Methods Symposium (NFM). 2011. LNCS 6617. B. Norton, S. Foster, Andrew Hughes: **A Compositional Operational Semantics for OWL-S.** Intl. Workshop on Web Services and Formal Methods (WS-FM). 2005. LNCS 3670.
Teaching	I have lectured and/or provided demonstration support for the following modules: **Formal Specification** (Lecturer, University of York). This course trains students in the use of the Z notation for formally specifying and verifying systems. **Programming: Correctness by Construction** (Demonstrator, University of York). A course on the use of the Z and CSP notations for formal verification. **Foundations of Computer Science** (Demonstrator, University of Sheffield). First year foundation course in propositional logic, set theory, algebra, and proof. **Abstract Datatypes** (Lecturer, University of Sheffield). Module on various aspects of functional programming in Haskell, with a particular slant on abstract data types. **Theory of Distributed Systems** (Demonstrator, University of Sheffield). Module on theoretical representation and verification of concurrent systems in Process Algebra. I have also lectured in several postgraduate schools at ICTAC 2013, FM 2014,

	Marktoberdorf 2014, and INTO-CPS 2017, teaching on Unifying Theories of Programming and Isabelle/HOL. This included live demonstrations using Isabelle.
Training & Experience	*Apr 2018* **"Making a Difference" award recipient for services to University of York** *Mar 2018* **Interviewer for UCAS Open Days** *Dec 2017* **Proposal writing and administrative support for EPSRC VeTSS2 project** *Nov 2017* **Presenter at INTO-CPS plenary meeting**. University of Aarhus, Denmark. *July 2017* **Proposal writing and administrative support for EPSRC VeTSS project** *July 2017* **Lecturer, INTO-CPS Summer School**: "Mechanised proof support for CPS", at "Lucian Blaga" University of Sibiu, Romania. *Jun 2017* **Presenter and industrial collaboration at INTO-CPS plenary meeting**. United Technologies Research Centre (UTRC), Cork, Ireland. *March 2017* **Undergraduate Lecturer:** "Programming: Correctness by Construction", University of York. Lecturing on automated proof technology. *Feb 2017* **EU project review in Brussels.** Work Package Deliverables (accepted). *Nov 2016* **INTO-CPS Industry Follow Group and Plenary Meeting**. Presentation and industrial engagement. SOFTEAM Headquarters, Paris. *October 2016* **Lecturer at ICTAC Tutorial Series,** National Taiwan University. *Jan-Feb 2015* **Lecturing on "Formal Specification" (FMSP) Masters Module.** *Jan 2015* **Proposal writing on two bids under JLR-EPSRC TASCC scheme.** *Nov 2014* **EU project review in Brussels, Refinement Tool Deliverable** (accepted). *Sep 2014* **Headed a EU H2020 FET-Open project bid** (*"CyVeriPhy"*). *Aug 2014* **Assistant Lecturer at Marktoberdorf Summer School on Dependable Software Systems Engineering.** Co-lecturing *"Electronic UTP: Mechanised Unifying Theories of Programming"* with Prof. Jim Woodcock. *July 2014* **Dissemination of COMPASS project results** to PICASSOS industrial consortium at National Railway Museum. *May 2014* **Lecturer at FM Tutorial Series, Singapore.** Co-lecturing *"Unifying Theories of Programming in Isabelle/HOL"* with Prof. Jim Woodcock. *Jan-Apr 2014* **Proposal writing and administrative support for two EU H2020 proposals under ICT1** (INTO-CPS was a successful bid - *€7m funded, €950k to York*) *Jan 2014* **Presenter, Industrial Outreach Event,** COMPASS Interest Group, Amsterdam *Nov 2013* **EU project review in Brussels,** Theorem Prover Deliverable (accepted) *Aug 2013* **Lecturer at ICTAC School on Software Engineering.** ECNU, Shanghai. *Aug 2011* **Visiting Researcher at McMaster University.** Host: Dr. Wolfram Kahl. *Apr 2006 and 2007* **Midlands Graduate School in Foundations of Computer Science** *Jun 2006* **Visiting Researcher at Knowledge Media Institute, Open University**
Notable Presentations	*"Integrating Formal Methods into Assurance Cases with SACM and Isabelle"* – presentation a Safety Critical Systems Club, March 2019 *"Foundations for Simulink diagrams in UTP"* – presentation at joint workshop with IIIT Bangalore and Mathworks in Bangalore, India, May 2017 *"Unifying Heterogeneous State-spaces with Lenses"* – guest seminar at University of

	Sheffield, February 2017 *"Towards Verification of Cyber-Physical Systems with UTP and Isabelle*" – guest seminar at University Paris-Sud, November 2016 *"Isabelle/HOL and UTP"* – INTO-CPS tutorial in Aarhus, Denmark, September 2016 *"The COMPASS Modelling Language"* - COMPASS Interest Group tutorial, Jan 2014. *"Towards a theorem prover for CML"* - COMPASS tutorial in Trieste, Italy, Mar 2013. *"CML tutorial"* - tutorial on COMPASS Modelling Language, Bremen, Feb 2013. *"Applying Agda in Model Driven Design"* - invited talk, McMaster University, Aug 2011. *"Reflective Equational Proofs in Agda"* - Agda meeting, 2011 at Chalmers University. *"A Compositional Semantic Theory for Service Composition"* - group seminar, 2009. *"Service Composition Algebra"* - Invited talk at Leicester University, Oct 2007. *"Behavioural Types for Service Composition"* - Invited talk, University of Bamberg, 2007. *"A Formal Model for Web Service Composition"* - British Colloquium for Theoretical Computer Science (BCTCS 2006), 04-2006
Services to Research Community	*March 2019* **Organiser of and Lecturer at CyPhyAssure Spring School in York** *April 2016* **Organiser of INTO-CPS Workshop in York** *September 2015* **Conference Co-organiser:** SEFM in York *March 2010* **Co-organiser of Midlands Graduate School in Sheffield** *2005 and 2007* **Sheffield Theory Special Interest Group organiser** *2006* **Organiser for International Workshop on Hypercomputation** (HyperTrends). **Peer review:** Formal Aspects of Computing; Theoretical Computer Science; SEFM 2018; FM 2018; ICFEM 2017; ITP 2017; RAMiCS 2011; Software Testing, Verification and Reliability; SEEFM 2009

References available upon request.