Dr KANGFENG YE
6 Years in academia in formal specification and verification of robotics, and cyber-physical systems
8 Years in industry in embedded systems
kangfeng.ye@york.ac.uk

Personal Statement

I am a research associate at the University of York and working on formal verification of robotics and cyber-physical systems using model checking and theorem proving. I am particularly interested in applying mathematics, logic, and model-based techniques to ensure dependability as computer systems, especially safety-critical systems, are becoming increasingly complex.

In my research, I (1) use *mathematical logic* (alphabetised predicate calculus in Unifying Theories of Programming - UTP) to give (probabilistic) *semantics* (denotational semantics and operational semantics) to a domain-specific language (RoboChart) in robotics, with support of modelling time and *probability*, (2) develop *automated verification* tools using modern *model-based* techniques (model transformation, validation, and generation) and *formal verification* (model checking and theorem proving), and (3) apply theoretical semantics and practical tools to a variety of case studies. I am a developer of RoboTool and Isabelle/UTP, the tools developed in our RoboStar group to support modelling and automated verification.

My recent work is summarised in two posters (https://t.co/l0YfbpERtg and https://t.co/v8DIjiIicm) and demonstrated (https://t.co/HgjAnmW9iL, https://t.co/sPVcVjN0FM, and https://t.co/zdfHRvkBec).

Before I moved to academia in 2012 to pursue a PhD, I have eight years of experience as a senior software and firmware leader in industry: R&D in semiconductor equipment and high-end ToR data centre switches. I have seen some major challenges that traditional software and system engineering is facing: for example, dependability and assurance are not guaranteed. This motivated my interest in formal methods.

Education

(Sep 2012 - Nov, 2016) **University of York,** York, UK, PhD in Computer Science
Thesis Title**:** "*Model Checking of State-Rich Formalisms*"
Keywords: Formal Methods, Formal Verification, Model Checking, *Circus*, Z, CSP, CSP || B, UTP
- Also developed a parser and type checker for ISO Standard Z (ISO/IEC 13568:2002)

(2001 - 2004) **ChongQing University,** ChongQing, China, Master of Science in Machine Design (Computer Aided Design)
(1997 - 2001) **ChongQing University,** ChongQing, China, Bachelor of Science in Machine Design

Work Experience

(Dec 2016 - Present) **Research Associate**, **University of York,** York, UK
Worked in four EPSRC-funded projects from 2017
- Development and implementation of a theory for automated (contract-based) reasoning about Simulink diagrams in Isabelle/UTP, an implementation of UTP in Isabelle/HOL. This work is published in this article and the theory is available online.
- Development of probabilistic semantics for RoboChart, a probabilistic property language (based on PCTL*), and Eclipse plugins to verify probabilistic systems automatically using the model checker PRISM. The work is published in this journal paper, detailed in Chapters 5 and 6.2 of the RoboChart Reference Manual, and probabilistic case studies are available online.
- Mechanisation of the theory of UTP probabilistic designs in Isabelle/UTP for automated reasoning about probabilistic programs. The work is published in this article and the theories are available online.
- Development of denotational semantics for a probabilistic programming language to model both epistemic and aleatoric uncertainty and theories in Isabelle/UTP for automated reasoning of probabilistic programs with learning facts. This work isn't published yet and the theories are available online. There is a demonstration online.
- Development of operational semantics for RoboChart and theories in Isabell/UTP to automatically generate Haskell code for sound animation. The work is published in this article and the theories are available online.

Worked in the EU H2020 INTO-CPS project: application of model-based test automation and model checking to several pilot case studies, and verification of a Fan Coil Unit (with discrete controllers + continuous plants) using theorem prover Isabelle/UTP.

(Dec 2012 - Nov 2015) **Part-time Software Engineer**, **Rapita Systems**, York, UK
Development and test of Rapita's on-target worst-case execution time (WCET) and coverage analysis tool (RVS) for embedded systems in Aerospace and Automotive. My responsibility includes regression and qualification kit test support; development support; RTBx (a data collection device) setup, and test; integration support for the PROARTIS project, an FP7 project.

(Oct 2007 - Sep 2012) **Embedded Software and Firmware Lead**, **Celestica R&D Centre**, Shanghai, China
Led an embedded firmware and software team to deliver embedded software solutions to a variety of projects: Voltage-Controlled Optical Filter and 1/10/40G High-End Ethernet switches (Broadcom TR2 and Trident+).

(Dec 2004 - Jul 2007) **Alignment Subsystem Software Lead**, **Shanghai Micro Electronics Equipment**, Shanghai, China
Led an embedded software team to design and develop software for the alignment subsystem in lithography products.

Skills

Items	*Description*
Formal languages	**Z, CSP, Circus**: main languages used in my research and also during my PhD **PRISM**: a deep understanding of its semantics and language features
Semantics Framework	Unifying Theories of Programming (**UTP**): a framework able to unify semantics in different paradigms of programming. Program correctness is through refinement.
Theorem Proving Isabelle/HOL	Used in four research projects, created theories for four languages (discrete part of Simulink, two imperative probabilistic programming languages, and RoboChart) with semantics, proved many algebraic laws, and implemented automated reasoning with case studies
Model checkers	**PRISM**: intensively used it for more than three years to verify several probabilistic reactive systems modelled in RoboChart **FDR**: a refinement model checker for CSP
Model-based techniques	Eclipse Modelling Framework (EMF), Eclipse Xtext and Sirius, and Eclipse Epsilon toolsets for model validation, transformation, and generation.
Functional and logic languages	**Haskell** in my research to develop a parser and type checker for ISO Standard Z (total 15K LOC). Functional languages in **Isabelle/HOL** and **Prolog**.
Programming languages	**C**: More than 100K LOC mainly in embedded OS or RTOS in two large-scale projects **C++**: QT on Linux (30K LOC) and a parser and type checker for Z using C++11 (16K LOC) **Java**: A program (Circus2ZCSP) for translation: AST manipulation (24K LOC + 5K LOC for the test); Eclipse plugins for automated analysis of probabilistic systems (20K LOC)

Awards

- My SoSym paper "Probabilistic modelling and verification using RoboChart and PRISM" is selected as a journal-first paper (a kind of best papers in a year) to be included in a top conference MODELS 2022 to allow me to present our journal paper

Publications

Journals

- Kangfeng Ye, Ana Cavalcanti, Simon Foster, Alvaro Miyazawa, Jim Woodcock. **Probabilistic modelling and verification using RoboChart and PRISM**. S*oftware and Systems Modelling* **21**, 667–716 (2022). https://doi.org/10.1007/s10270-021-00916-8
- Simon Foster, Kangfeng Ye, Ana Cavalcanti, Jim Woodcock. **Automated verification of reactive and concurrent programs by calculation**, Journal of Logical and Algebraic Methods in Programming, Volume 121, 2021, https://doi.org/10.1016/j.jlamp.2021.100681
- Kangfeng Ye and Jim Woodcock, "**Model checking of state-rich formalism Circus by linking to CSP ‖ B** ", International Journal on Software Tools for Technology Transfer, pp. 1–24, 2015. [Online]. Available: http://dx.doi.org/10.1007/s10009-015-0402-1

Conferences

- Kangfeng Ye, Simon Foster, and Jim Woodcock (2022). **Formally Verified Animation for RoboChart using Interaction Trees**. Formal Methods and Software Engineering - ICFEM. https://doi.org/10.1007/978-3-031-17244-1_24
- Kangfeng Ye, Simon Foster, Jim Woodcock (2021). **Automated Reasoning for Probabilistic Sequential Programs with Theorem Proving**. Relational and Algebraic Methods in Computer Science. Available: https://doi.org/10.1007/978-3-030-88701-8_28.
- Jim Woodcock, Simon Foster, Alexandre Mota, Kangfeng Ye (2021). **RoboStar Technology: Modelling Uncertainty in RoboChart Using Probability**. In: Cavalcanti, A., Dongol, B., Hierons, R., Timmis, J., Woodcock, J. (eds) Software Engineering for Robotics. Springer, Cham. https://doi.org/10.1007/978-3-030-66494-7_13

- Kangfeng Ye, Simon Foster, and Jim Woodcock. **Compositional assume-guarantee reasoning of control law diagrams using UTP**. In From Astrophysics to Unconventional Computation, pages 215–254. Springer, 2020.
- Jim Woodcock, Ana Cavalcanti, Simon Foster, Alexandre Mota, Kangfeng Ye (2019). **Probabilistic Semantics for RoboChart - A Weakest Completion Approach**. Unifying Theories of Programming - 7th International Symposium, UTP 2019, Dedicated to Tony Hoare on the Occasion of His 85th Birthday, Porto, Portugal, October 8, 2019, Proceedings.
- Simon Foster, Kangfeng Ye, Ana Cavalcanti, Jim Woodcock (2018). **Calculational Verification of Reactive Programs with Reactive Relations and Kleene Algebra**. Relational and Algebraic Methods in Computer Science.

Thesis
- Kangfeng Ye (2016) **Model Checking of State-Rich Formalisms** (By Linking to Combination of State-based Formalism and Process Algebra). PhD thesis, University of York. [Online]. Available: http://etheses.whiterose.ac.uk/15526/

Conferences and Presentations

- ACM / IEEE 25th International Conference on Model Driven Engineering Languages and Systems (MODELS) 2022 on "Probabilistic modelling and verification using RoboChart and PRISM"
- 23rd International Conference on Formal Engineering Methods, ICFEM2022 on "Formally Verified Animation for RoboChart Using Interaction Trees"
- 19th International Conference on Relational and Algebraic Methods in Computer Science RAMICS 2021 on "Automated Reasoning for Probabilistic Sequential Programs with Theorem Proving"
- Pint of Science 2019 on "Engineering Robotic Swarms"
- Workshop on Modelling, Verification, and Refinement of Evolving Cyber-Physical Systems 2019: one-day tutorial "Isabelle/ UTP Tutorial" to students from Southwest University

Teaching

- Teaching assistant for the practical part of the course "Concurrent System Analysis & Verification (CSAV)" in 2019 and 2020