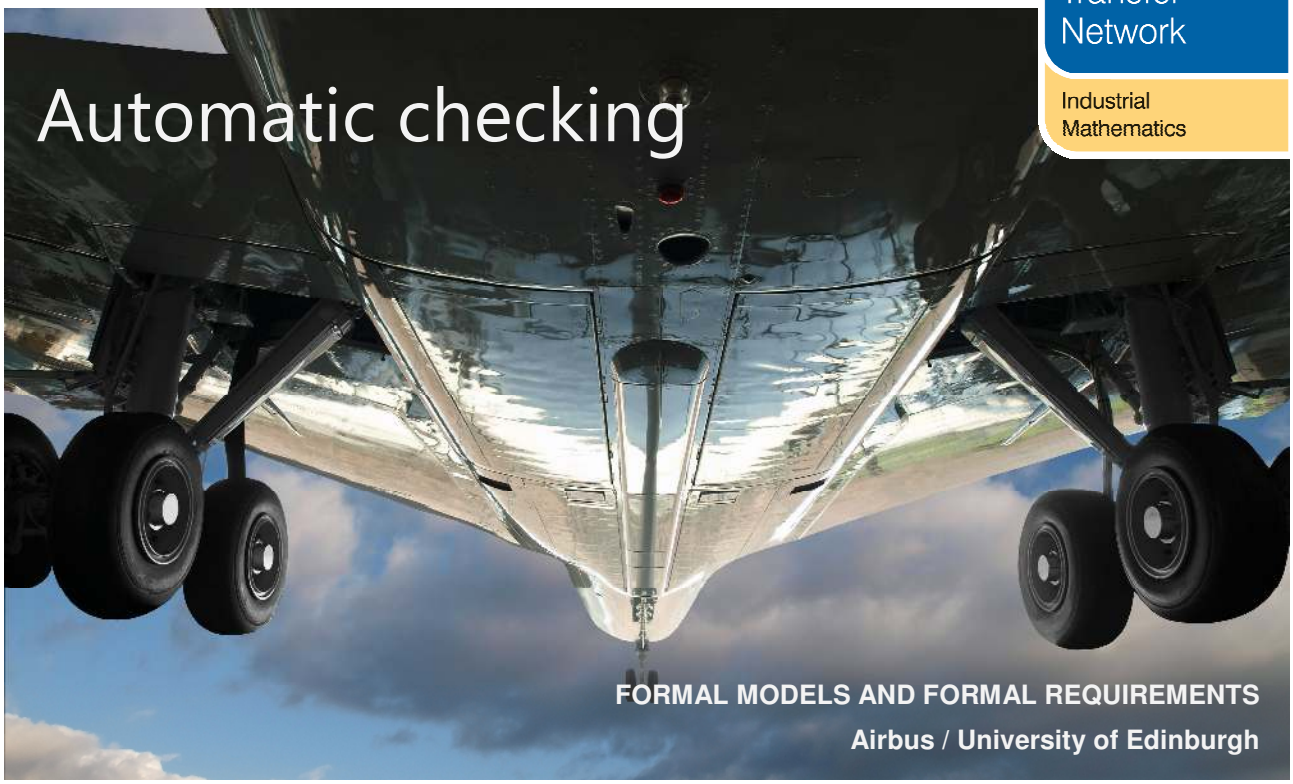
Technology Strategy Board
Driving Innovation

Knowledge Transfer Network
Industrial Mathematics

Automatic checking



FORMAL MODELS AND FORMAL REQUIREMENTS

Airbus / University of Edinburgh

The need

Airbus specifies, designs and implements complex mechatronic functions into systems featuring analogue and digital data and signals.

Currently, computers cannot be relied upon to resolve ambiguities that are naturally present in human-generated engineering specifications. Sometimes, those ambiguities are an inevitable consequence of the medium used (e.g. the English language, block diagrams), but sometimes they could be avoided if a more standardised approach to design and requirement engineering were adopted.

This exploratory work illuminates the most common sources of ambiguity and provides partial solutions and tools for coping with it.

The outcomes

The main aim was to explore the potential for automated verification of hybrid designs. Formalising engineering specifications features prominently in this work, because it is a prerequisite for any kind of automated analysis. Hybrid designs have interacting continuous and discrete features, which cannot be ignored in design, validation and implementation.

The project used the Airbus A350 autobrake model as a case study. The work formalisation (a) hybrid system designs, using diagrams generated by the Simulink software tool, and (b) engineering requirements, beginning with the original set of functional requirements for the A350 braking system. The two strands then merged into a common formal basis, which was analysed using the formal verification tool HySAT and the mathematical theory of hybrid satisfiability.

The HySAT analysis was found to verify most of the requirements, and otherwise provided insights into the model and the requirements themselves. A notable outcome of the project was a jointly authored paper, "Formal assessment of hybrid functions", which was accepted for publication and oral presentation at the Embedded Real-Time Software 2010 Conference.

"We are very pleased to report that Marek Kwiatkowski was a great addition to our team and produced some excellent work. Marek's work enabled us to make significant progress in our broader research programme."

Sanjiv Sharma
Airbus

Technical summary

The first major topic of this work was formalisation of Simulink diagrams as HySAT models. More specifically, it was necessary to embed the models in a suitable state space (the DECL section of a HySAT input file), determine the initial state(s) of the model (the INIT section) and the relationships between present and future states (TRANS). We used the A350 autobrake design as the driving example for this task.

A variable was assigned to every signal in a Simulink model. The types and ranges of these variables were obtained by manually setting them for the input variables and then automatically propagating them through the model. This kind of inference was automatically performed for the entire diagram, resulting in setting the types and ranges of 81% of signals. The remaining 19% were involved in feedbacks, where the described method fails, and they were treated as real numbers with wide ranges. This data was then appropriately formatted as a DECL section of a HySAT input file.

An association table linking the textual and the formal descriptions of basic system properties (for example, “the autobrake is disarmed" would be linked to a formula such as “AB ARMED = false"). This was then used to automatically translate the structured requirement to a HySAT formula, where the connectives and their nesting would be determined by the structure of the requirement, and their arguments (operands) would correspond to the formal descriptions of basic properties. The resulting formulae formed the TARGET section of a HySAT input file.

Several requirements were translated in this way, and the HySAT code was run to verify them. In most cases the requirements were satisfied; when they were not, insights into the model and the requirements themselves were the result.

“The internship gave me the opportunity to meet some of the finest industrial R&D minds. Perhaps the most valuable experience I gained from interacting with them is the appreciation of the differences in industrial and academic approaches to research and the realisation that the purest route is not always the shortest one.”

Marek Kwiatkowski, University of Edinburgh

This project was part of the programme of industrial mathematics internships managed by the Knowledge Transfer Network (KTN) for Industrial Mathematics. The KTN works to exploit mathematics as an engine for innovation. It is supported by the Technology Strategy Board, in its role as the UK’s national innovation agency, and the Engineering and Physical Sciences Research Council, in its role as the main UK government agency for funding research and training in engineering and the physical sciences.

EPSRC
Engineering and Physical Sciences Research Council

Project Details

Partners
Airbus
University of Edinburgh

Project investment
£14,000

Intern
Marek Kwiatkowski

For further details on the technology:
Sanjiv Sharma
Airbus
sanjiv.sharma@airbus.com

For further information on internships and other collaborations:
Lorcán Mac Manus
Industrial Mathematics KTN
lbmm@industrialmaths.net
+44 (0) 1483 579108