Mathematics penetrates mystery of air traffic safety

June 20 2005

Air traffic control is one of the most demanding safety critical distributed systems with an enviable safety record. Using computer modelling researchers developed innovative approaches to handling uncertainty when designing such complex safety critical operations.
It's a scary thought, but air traffic brings with it the chance of a mid-air collision. But the safety record of the air industry is excellent, so obviously it works well.

"The system has grown in an evolutionary way over decades," says Dr Henk Blom of The Netherlands Aerospace Laboratory in Amsterdam, and coordinator of the IST programme-funded Hybridge project. "It works, but nobody really understand why it works so [well]. If you talk to an air traffic controller, he or she can tell you how it works from one perspective, and also about some scary events where things ran out of control."

"Similarly, [other] explanations and experiences can be heard when you talk to a pilot. In combination, their two stories explain how well pilots and controllers collaborate, but it does not explain at all why the safety records are so extremely good. The most likely explanation why it has become so safe is that the air traffic system evolved in small steps over time and each step took advantage of past experience."

There is one big problem, though: "How can you update or automate a system in which the safety records cannot be explained or captured by your design tools?" asks Blom.

That's the question that Hybridge sought to address.

Design-safety tools

The project developed three novel methods and supporting tools to design safety within a distributed system, but in a way that allows pilots and controllers to retain control, since they bear the responsibility in preventing any accidents from occurring.

One novel method allows the designer to analyse and mitigate combinations of small problems at different places in a distributed safety critical system. "In air traffic you have controllers, pilots, planes and mechanical and computer systems. It's complex and highly distributed. And this may result in 'Chinese whisper' kind of effects, which may lead to unnoticed differences in understanding between, for example, a pilot and an air traffic controller.

"When such a difference in understanding remains unrecognised, then the situation may spiral out of control, with potentially catastrophic results," says Blom. "Some of these misunderstandings can be quite sneaky; you can't anticipate them, they simply arise from unfortunate combinations of innocent events." The tools developed by Blom and the Hybridge team seek to identify, and prevent, these potential misunderstandings.

The two other key outcomes are simulation-based approaches. One assesses the risk of collision in a novel air traffic design. You need a massive sample of data to accurately test whether the new design is safe, because collisions occur so rarely in air traffic control.

"Through straightforward simulation it would take a person's life-time to simulate a statistically significant number of collisions for one design," says Blom. "With the novel method you can do it overnight."

That's the power that mathematical modelling can bring to systems' design. What's more, the team developed their simulation to work independently of the system architecture. It's a major advance, because adjusting a simulator for different systems is costly in both time and money.

The third outcome of the project was a simulation-based method, which helps to optimise automation processes in air traffic control, while taking into account the uncertainties that, for example, come from sudden wind speed variations.

Airports would like to automate certain aspects of traffic control, but automation on its own does not take account of unpredictable variables, like wind speed and direction in the Jet stream. "Planes can arrive hours before they are expected if the weather conditions are right," says Blom.

The Hybridge system can factor in such variables to ensure automation runs smoothly and does not get overwhelmed, for example, by the unexpected arrival of several planes ahead of time.

The project finished last December, but work will continue among the partners. Hybridge was simply a proof of principle. Now the partners are looking to develop a full-scale application for advanced air traffic system design.

The project results could also be useful in a wide range of industries, from finance to nuclear power station management, industry, computing and telecommunications management.

"We chose air traffic because it was the most demanding safety critical distributed system we could find, so it was the ultimate test of the methods we developed. We expect it is possible to apply these novel methods to other industries as well," concludes Blom.

Source: IST Results