Scientists develop method for verifying safety of computer-controlled devices

April 20 2009

Researchers at Carnegie Mellon University's School of Computer Science have developed a new method for systematically identifying bugs in aircraft collision avoidance systems, high-speed train controls and other complex, computer-controlled devices, collectively known as cyber-physical systems (CPS).

The approach, developed by University Professor of Computer Science Edmund M. Clarke and Andre Platzer, assistant professor of computer science, already has detected a flaw in aircraft collision avoidance maneuvers —since corrected — that could have caused mid-air collisions. It also has verified the soundness of the European Train Control System. Ultimately, the method could be used on other cyber-physical systems, such as robotic surgery devices and nano-level manufacturing equipment.

"Engineers increasingly are relying on computers to improve the safety and precision of physical systems that must interact with the real world, whether they be adaptive cruise controls in automobiles or machines that monitor critically ill patients," Clarke said. "With systems becoming more and more complex, mere trial-and-error testing is unlikely to detect subtle problems in system design that can cause disastrous malfunctions. Our method is the first that can prove these complex cyber-physical systems operate as intended, or else generate counterexamples of how they can fail using computer simulation."

In the case of aircraft collision avoidance systems, for instance, Platzer

and Clarke used their method to analyze so-called roundabout maneuvers. When two aircraft are on rapidly converging paths, one technique for avoiding collisions is for the system to order each pilot to turn right and then circle to the left until the aircraft can safely turn right again to resume their original paths. It's as if the aircraft are following a large traffic circle, or rotary, in the sky. But analysis by the Carnegie Mellon researchers identified a counterexample: when aircraft approach each other at certain angles, the roundabout maneuver actually creates a new collision course that, in the few seconds remaining before their paths cross, the pilots might not have time to recognize.

Like Model Checking, a method pioneered by Clarke that today is the most widely used technique for detecting and diagnosing errors in complex hardware and software design, the new method analyzes the logic underlying the system design, much as a mathematician uses a proof to determine that a theorem is correct. Clarke shared the 2007 A.M. Turing Award, generally considered the computer science equivalent of the Nobel Prize, for his role in developing Model Checking.

A crucial difference, however, is that Model Checking can examine every possible state of a discrete finite-state system, such as a new circuit design for a computer chip; that's not possible for a CPS that must interact with the infinitely variable real world. Even if the differential equations that govern these systems can be solved — and they often can't — it usually is impossible to use the results to predict the behavior of the system, Platzer said. Instead, he and Clarke have developed algorithms that decompose the systems until they produce differential invariants — mathematical descriptions of parts of the system that always remain the same. These differential invariants, in turn, can be used to prove the global logic of the CPS.

"When the system design is sound, as we found in the case of the

European control system for train traffic or the repaired flight controller, our method can provide conclusive proof," Platzer said. Likewise, when flaws exist, the method reliably generates counterexamples. "Finding the counterexamples is actually the easy part," he added. "Proving that they are fixed is hard."

The demand for methods that can prove a CPS or hybrid system operates as intended will only increase as these systems become more numerous and more crucial for everyday life, Platzer said. "Bugs in complex cyber-physical systems like cars, aircraft, chips or medical devices are expensive to fix and may endanger human life," he explained. "In transportation, the percentage of development cost spent on design and testing new control software is already well above 50 percent and is steadily rising."

The National Science Foundation (NSF) has identified the design and verification of CPS as a key area of research. The increasing use of robotic devices, the growth of sensor networks, the proposed creation of a "smart grid" for delivering electrical power, a greater reliance on automated war fighting and growing use of efficient, "zero-net-energy" buildings are all examples of a growing reliance on computer control systems that are tightly coupled to physical systems. This work was sponsored, in part, by the NSF and the German Research Council.

Source: Carnegie Mellon University (news : web)