

Verifying Aerospace Software

Willem Visser

Research Institute for Advanced Computer Science (RIACS)
NASA Ames Research Center, Moffett Field, CA 94035, USA
{wvisser}@email.arc.nasa.gov

The talk will focus on the research issues that need to be addressed in order to do efficient verification of aerospace software. The members of the Robust Software Engineering group at NASA Ames, have had the unique opportunity to be involved in a number of efforts to analyze aerospace software over the last few years and in this talk we will highlight some of these activities and what we have learned from them. Unlike the more traditional verification activities each project undertakes, usually centered around functional testing, the approach we followed used state-of-the-art verification techniques and tools, such as model checkers, static analyzers and advanced runtime monitoring systems to find defects.

In the first part of the talk we will highlight two of these verification efforts: analyzing the DEOS real-time operating system from Honeywell that is used in small business aircraft, and, the analysis of the executive of the K9 (prototype) Mars rover. DEOS represents an example of a new generation of aircraft software that shows some of the weaknesses of the FAA software certification process. The K9 analysis was a controlled experiment to determine the capabilities of a number of advanced verification techniques (and tools) in finding seeded errors; the results were compared with a control group that did classic functional testing.

In the second part of the talk we will discuss the lessons learned from the various verification activities and how it is shaping our current research focus. We will also give a brief overview of a ongoing project to determine the risks of using autonomous systems in space exploration and how verification tools can mitigate some of these risks.