Formal Approaches to Ensuring the Safety of Space Software

Ewen Denney

1NASA Ames Research Center, Moffett Field, CA 94035 - USA
edenney@email.arc.nasa.gov

Abstract. The size, complexity, and safety criticality of software in space missions is increasing exponentially. The consequence of these trends has been an increase in the likelihood of catastrophic failure due to a software bug. I will describe ongoing work in the Robust Software Engineering Group at the NASA Ames Research Center on the application of formal methods to ensure ultra-reliable space software. We have developed customized tools that exploit both classical verification and code generation techniques that are applicable at different stages of the software lifecycle. After giving a survey of the range of tools we have developed, I will concentrate on recent work on reliable code generation.