Model checking for Mission Critical Software Validation

Spacecraft complexity is continually increasing to meet the requirements of ambitious deep space missions. Increasingly the mission capability is implemented in the flight software and the robustness of this software is paramount for mission success. Thus design validation is a major challenge in the software development process. Ideally we strive to ensure the correctness of a design at the earliest stage possible. Traditional software validation methods of simulation and testing are being stretched to the limit. It is becoming increasingly difficult to be cost and schedule-effective to validate mission critical software validation through simulation and test. In some cases it is prohibitive to test all possible paths.

Model checking is emerging as a powerful validation technique that conducts an *exhaustive exploration* of all possible behaviors of a software system design. Model checking has the added advantage that it can be applied to the design specification early on in the development process. Ideally, if the design can be captured by models than the software implementation can be done by automatic code generation and the validation by model checking. To take advantage of these emerging techniques engineers need to be knowledgeable about formal methods and properly trained in the tools and techniques of model checking.

We propose to prototype a formal method model checking process for validation of mission critical software. One modeling technique of capturing the design is with statecharts. This was done for the DS1 Fault Protection using the Stateflow® format. An automatic code generator was then used to produce the software. Our approach is to translate the fault protection statecharts into PROMELA for SPIN model checking.