Model Checking Investigations for Fault Protection System Validation

Authors:	1) Paula J. Pingree	2) Kevin Barltrop
Affiliation:	JPL	
Address:	4800 Oak Grove Drive, Pasadena, CA 91109	
Email:	1) Paula.J.Pingree@jpl.nasa.gov	2) Kevin.J.Barltrop@jpl.nasa.gov
Phone:	1) 818-354-0587	2) 818-354-6412

Abstract:
Proper design validation, which seeks to ensure the correctness of a design at the earliest stage possible, is a major challenge in any responsible software development process. Over the years, the complexity of space missions has dramatically increased with more of the critical aspects of a spacecraft's design being implemented in software. Fault Protection (FP) is autonomous flight software (FSW) that provides the robustness and autonomy needed to ensure survival of a space mission in the event of detected on-board failures. The design and validation of FP software systems is complex and its functionality in flight is critical, thereby making it a good candidate for more design and rigorous methods.

Model checking is a powerful formal methods approach which can detect defects in designs that are typically difficult to discover with conventional testing approaches by conducting an exhaustive exploration of all possible behaviors of a software system design. NASA's Deep Space 1 (DS1) project chose to implement model-based code-generation for the spacecraft system-level Fault Protection software using Stateflow® by The Mathworks. The HiVy Toolset described in this work enables model checking for statechart-based designs by providing a formal method-based capability for automated statechart translation from Stateflow® into Promela, the input language of the SPIN model checker, developed at Bell Labs by Dr. Gerard Holzmann. Spin accepts input of a closed-loop model of the validation article of interest (e.g., the FP design) and specification of correctness properties against which the model can be validated. These validation tools and methods have been prototyped on portions of the DS1 FP design.

Demonstrating the trend toward statechart modeling and auto-code generation, Stateflow® is being used for the FP FSW development on NASA's Deep Impact project, scheduled to launch early in 2004. This formal validation technique is being used to partially validate the system fault protection responses against a set of core behavioral correctness properties. The results of this approach are compared against a traditional test script-based validation using the Matlab® environment. Additional work is in progress to validate the responses in the context of a complete flight system model with its accompanying mission-derived correctness properties. Special attention is given to methods for reducing the model to a form that yields a tractable search space.

The application of these validation methods to two NASA flight projects has provided valuable experience that will facilitate the reliable development of future spacecraft mission designs.