Use of Program Property Assertions for V&V of ISHM

Lawrence Markosian & Martin Feather

SAS 2008 Workshop on Verification
September 11, 2008

NASA has a long-standing interest in system health management. The context for the work reported here is an ongoing project to improve the reliability and availability of the NASA Constellation Program's manned space systems through application of several ISHM technologies. One of these applications is the Testability Engineering and Maintenance System (TEAMS) from Qualtech Systems, Inc. The TEAMS product family includes a design-time tool (TEAMS Designer) that takes hierarchical functional models of complex systems and related fault information and produces a data structure that is used with a runtime system (TEAMS RT) to diagnose faults. This presentation describes one of our approaches to V&V and certification of TEAMS Designer applications—the use of correctness property assertions to verify, at runtime, that the TEAMS Designer produces a correct runtime environment. The correctness properties are to be understood in the context of the semantics of TEAMS diagnosis. An example property, which in this case should hold for every application, is: "Every failure mode with at least one test that has status Pass has status Good." In addition to these general properties, we expect to include application-specific properties that relate the original schematics, or the input models, to the runtime data structure.

Research described in this paper was carried out at NASA Ames Research Center and at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.