"Program Model Checking Practitioner's Guide" delivered to
Software Assurance Research Program

HIGHLIGHT: The final product of a three-year research initiative, a guidebook called "Program Model Checking: A Practitioner's Guide", was delivered to the Office of Safety and Mission Assurance's Software Assurance Research Program on April 27. This guidebook is directed at software developers and test engineers, and provides an introduction to program model checking technology and the methods and issues in applying it. The examples discussed in the guidebook are primarily NASA mission-critical and safety-critical software applications. The guidebook is available from a SARP website, http://sarpresults.ivv.nasa.gov: search for "program model checking".

BACKGROUND: Program model checking technology has been an area of active research within the Robust Software Engineering (RSE) group at NASA Ames for nearly ten years. It is a verification technology that uses state-space exploration to evaluate large numbers of potential program executions. Program model checking can be effective at detecting critical software errors that are difficult to find through traditional testing. It provides improved coverage over testing by systematically evaluating possible test inputs and possible interleaving of threads in a multithreaded system. Two years ago one of the major research tools for program model checking, Java PathFinder, which was developed in the RSE group, was productized and released under NASA's then-new Open Source license and is available on SourceForge. While the guidebook does not focus on a specific tool, most of the examples are drawn from applications of Java PathFinder and SPIN, the most widely-used model checker, developed by Gerard Holzmann, now at JPL. The case studies include the DS-1 Remote Agent, a Rover Executive, the DEOS operating system, the MER Arbiter, and the Shuttle Abort Flight Manager. The guidebook includes extensive references to the research literature, but the focus of the guidebook itself is on making practical use of the technology, not on the research.

PROGRAM FUNDING: Funding for development of the guidebook was provided by the Software Assurance Research Program (SARP) of NASA's Office of Safety and Mission Assurance (OSMA), and was managed by the NASA Independent Verification and Validation (IV&V) Facility. NASA's Office of Aerospace Technology (OAT) supported the RSE group's underlying research on model checking, via NASA's Information Technology Strategic Research (ITSR) Project; Communication, Information, and Computation Technology (CICT) Program; and Engineering for Complex Systems (ECS) Program. The Constellation Program's Exploration Technology Development Program (ETDP) also supported the underlying research.

TEAM MEMBERS: The authors are members and former members of the Robust Software Engineering Group, headed by Dr. Michael R. Lowry: Masoud Mansouri-Samani, Corina S. Pasareanu, Peter C. Mehlitz, and Lawrence Z. Markosian (Perot Systems Government Services); John J. Penix (Google,

Inc.); Owen O'Malley (Yahoo, Inc.); Willem C. Visser (Seven Networks, Inc.); Guillaume P. Brat (USRA/RIACS); and Thomas T. Pressburger (NASA ARC).

POC: Tom Pressburger, Tom.Pressburger@nasa.gov