# Applying Formal Methods to NASA Projects: Transition from Research to Practice

Bill Othon
NASA Johnson Space Center
Houston, TX

**Abstract**

NASA project managers attempt to manage risk by relying on mature, well-understood process and technology when designing spacecraft. In the case of crewed systems, the margin for error is even tighter and leads to risk aversion. But as we look to future missions to the Moon and Mars, the complexity of the systems will increase as the spacecraft and crew work together with less reliance on Earth-based support. NASA will be forced to look for new ways to do business. Formal methods technologies can help NASA develop complex but cost effective spacecraft in many domains, including requirements and design, software development and inspection, and verification and validation of vehicle subsystems. To realize these gains, the technologies must be matured and field-tested so that they are proven when needed. During this discussion, current activities used to evaluate FM technologies for Orion spacecraft design will be reviewed. Also, suggestions will be made to demonstrate value to current designers, and mature the technology for eventual use in safety-critical NASA missions.

E. Denney, D. Giannakopoulou, C.S. Păsăreanu (eds.); The First NASA Formal Methods Symposium, pp. 2-2