Building a Safety Case for a Safety-Critical NASA Space Vehicle Software System

Martin S. Feather
Jet Propulsion Laboratory,
California Institute of Technology
Pasadena, USA
Martin.S.Feather@jpl.nasa.gov

Lawrence Markosian
SGT Inc., NASA Ames Research Center
Moffett Field, USA
Lawrence.Z.Markosian@nasa.gov

Abstract—We describe our development of a key portion of a safety case for a safety-critical piece of NASA software designed to operate on a NASA launch vehicle. The software’s purpose is to make real-time determinations of the presence of catastrophic failure conditions of that vehicle and react accordingly. We show how our safety case development applies a series of generic software considerations instantiated on the specifics of the NASA software system. We conclude that this approach is applicable to a wide range of NASA software systems.

Software safety; safety cases; V&V