Successful Application of Software Reliability Engineering for the NASA Space Shuttle

Ted Keller
Lockheed-Martin Space Mission Systems & Services
1812 Space Park Drive
P.O. Box 58487
Houston, TX 77258
Voice: (281) 335-2168
Fax: (281) 3352390
Email: keller@gwx.sis.lmco.com

Norman F. Schneidewind
Code SM/Ss
Naval Postgraduate School
Monterey, CA 93943, U.S.A.
Voice: (408) 656-2719
Fax: (408) 656-3407
e-mail: schneidewind@nps.navy.mil

Abstract

Space Shuttle Flight Software Application

The Space Shuttle Primary Avionics Software Subsystem (PASS) represents a successful integration of many of the computer industry's most advanced software engineering practices and approaches. Beginning in the late 1970's this software development and maintenance project has evolved one of the world's most mature software processes applying the principles of the highest levels of the Software Engineering Institute's Capability Maturity Model and ISO 9001 Standards. This software process, considered to be a "best practice" by many software industry organizations includes state-of-the-practice software reliability engineering (SRE) methodologies. Life-critical PASS produced by this process is recognized to be among the highest quality and highest reliability software in operation in the world. Using this application, we show how SRE can be applied to: interpret software reliability predictions, support verification and validation of the software, assess the risk of deploying the software, predict the reliability of the software, develop test strategies to bring the software into conformance with reliability specifications, and make reliability decisions regarding deployment of the software.

Reliability predictions are currently used by Lockheed-Martin Space Information Systems to add confidence to established positions regarding low failure probabilities for the
PASS that are based on formal software certification processes. It is the purpose of this case study to share the experience obtained from the use of SRE on this project, since this application is judged by the Lockheed-Martin team to be a successful attempt to apply SRE to this software. The SRE techniques and concepts employed by Lockheed-Martin should be of value for other software systems.

Keywords: Verification and validation, software reliability measurement and prediction, safety critical software, risk analysis.