

SAFE-P: System for Assurance of Flight Executable Procedures

SIFT, LLC

Technical Abstract

NASA operates manned spacecraft according to rigorously-defined standard operating procedures. Unfortunately, operating procedures are often written in different languages. For example, Orion will use automatic procedures written in SCL, the Spacecraft Command Language, while backup manual procedures may be developed in PRL, the Procedure Representation Language. However, procedures developed in different languages may diverge, so that the backup PRL procedures do not operate in the same way as the SCL procedures. This could lead to unintended effects that may range from simply unexpected to inefficient or even catastrophic. We propose to develop the SAFE-P tool, which will use formal model-checking methods to prove that PRL and SCL procedures have the same underlying execution semantics. Our Phase 1 effort validated the effectiveness of our approach; Phase 2 will completely automate the model checking process and integrate with the Procedure Integrated Development Environment (PRIDE). SAFE-P will thus allow procedure authors to easily compare procedures as they are being developed. When differences are found by SAFE-P, they will be highlighted immediately in the PRIDE interface, allowing the operators to either fix problems or annotate the respective procedures to explain the differences. Using SAFE-P, NASA personnel will rapidly and confidently verify that if an automatic SCL program cannot be executed, a backup manual procedure in PRL will be equivalent and safe. Furthermore, as automatic translators are developed to transform procedures in one language into another NASA-relevant language (e.g., Tietronix's current effort to translate PRL into SCL), the SAFE-P tool will provide a critical validation mechanism to double-check the correctness of the translation and highlight areas where the translator makes mistakes (or deliberate approximations that yield different behavior).

Company Contact

David Musliner
(612) 612-9314
musliner@sift.info

Embedding Procedure Assistance into Mission Control Tools

TRAC Labs, Inc.

Technical Abstract

Procedures are the accepted means of commanding spacecraft. Procedures encode the operational knowledge of a system as derived from system experts, testing, training and experience. In current Space Shuttle and ISS operations procedures are displayed using applications separate from the applications used to display commands and telemetry. This means that procedures cannot interact with commands and telemetry to help an operator's situation awareness. This leads to slower procedure performance and greater opportunity for errors. TRAC Labs is building on existing NASA Constellation program technology to combine procedures, commanding and telemetry into a single, consistent framework in which to operate space vehicles. Instead of viewing procedures in static displays, flight controllers will have interactive, reconfigurable procedure displays and assistants that can be tailored for specific situations. The displays will have different views tailored to specific operations, including browsing, assigning, editing, executing and monitoring procedures. A procedure executive automates some procedure execution and provides procedure assistance. Automation is always under the control of the flight controller via level of automation feature. Each step or instruction of a procedure can be labeled as manual, automated or consent. This will increase the efficiency of procedure performance and reduce procedure errors.

Company Contact

David Kortenkamp
(281) 281-7884
korten@traclabs.com