

Verification and Validation of Advanced Fault Detection, Isolation and Recovery for a NASA Space System

Mark A. Schwabacher, Martin S. Feather, and Lawrence Z. Markosian

I. INTRODUCTION

NASA has a long-standing interest in system health management[1]. The context for the work reported herein is an ongoing project to improve the reliability and availability of the NASA Constellation Program's manned space systems through health management technologies that perform system-wide integration and analysis of health data. One example, described in this abstract, is the application of advanced fault detection, isolation and recovery (FDIR) technologies during preparation and test of a space system during the several weeks prior to launch. The project plan calls for this software to be fed actual data from the sensors located both on the space system itself, and on the Ground Support Equipment (GSE) used to prepare and test the space system, and to execute, in real time, on computing platforms located at the launch facility. From this sensor data the software is to perform all the traditional functions of FDIR. Some especially stringent requirements on reliability and availability for launch motivate the need for the advanced FDIR technologies that this project will deploy, since they offer the potential to speed up fault detection, diagnosis and recovery, and thus avoid launch slips without compromising safety. Since the FDIR system will ultimately be used to make launch control decisions affecting manned space vehicles, it will need to be certified to the highest integrity standards, those defined in the NASA Human Rating Requirements[2].

This abstract reviews the requirements refinement process for the FDIR software; describes the V&V challenges and approaches posed by the innovative technologies being employed; and discusses additional certification

Manuscript received Aug 10th, 2008. Research described in this paper was carried out at NASA Ames Research Center and at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

M. S. Feather is with the Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA 91109 USA (corresponding author to provide phone: 818-354-1194; fax: 818-393-1362; e-mail: Martin.S.Feather@jpl.nasa.gov).

M. A. Schwabacher is with NASA Ames Research Center, Moffett Field, CA 94035 (email: Mark.A.Schwabacher@nasa.gov)

L. Z. Markosian, is with Perot Systems Government Services at NASA Ames Research Center, Moffett Field, CA 94035 USA (e-mail: Lawrence.Z.Markosian@nasa.gov).

considerations. The FDIR project software is currently under development. Two related prototypes are being developed: one for the Ares I-X vehicle and its GSE[3], scheduled for launch 2nd quarter of 2009, and one for Ares I.

II. REQUIREMENTS REFINEMENT PROCESS

The initial deployments will be prototypes that will demonstrate the advanced FDIR technologies being applied. These technologies include (a) The Inductive Monitoring System (IMS), a NASA-developed tool for anomaly detection based on a clustering algorithm; (2) TEAMS-RT, a tool from Qualtech Systems, Inc. (QSI) for diagnosis that uses model-based reasoning; and (3) a rule-based reasoning tool, Spacecraft Health INference Engine (SHINE), from JPL, which may be employed both in anomaly detection and in fault recovery.

Overall requirements on the FDIR prototype include a very low false alarm rate and a low missed detection rate for anomaly detection and fault diagnosis, and a high "correctness" rate for diagnosis. These are the principal requirements of interest here.

Each of the overall requirements was refined to one or more requirements on the performance of the individual tools. For example, the higher-level requirement on diagnosis was refined to a requirement on the TEAMS-RT tool that it must provide a correct diagnosis for any possible inputs.

As is typically the case in systems engineering at NASA, each requirement must have a corresponding "verification requirement", which is a description of the test, analysis, demonstration, or inspection procedure that will be used to verify the corresponding requirement. Developing the verification requirements posed a number of challenges, and resulted in a reworking of the original requirements, usually because the concepts of "anomaly", "fault", "false alarm rate", etc. were not precise enough to allow definition of the verification procedure.

An example requirement on anomaly detection, and a corresponding verification requirement, are given below.

R1: The prototype shall have a false alarm rate for anomaly detection of no more than xx%.

VR: The requirement shall be verified by test. The test shall consist of inputting historical nominal shuttle data into the

prototype to detect anomalies. The historical shuttle data used shall not contain any anomalies. The test will be considered successful when the prototype has a false alarm rate that does not exceed xx% with a minimum of yy time steps.

III. V&V CHALLENGES AND APPROACHES

A major challenge in specifying verification requirements for the prototypes is that the prototypes will be used to analyze data from new spacecraft that is currently under development. Real data from this new spacecraft will not be available before the prototypes are deployed. We therefore specified that four types of data shall be used to test the prototypes before deployment:

1. **Historical data from a similar spacecraft:** The new spacecraft is based in part on the Space Shuttle, and is similar to the Space Shuttle in several ways. We specified in the verification requirements that historical Space Shuttle data be used to test the prototype. There is a risk that the historical Space Shuttle data will not be sufficiently similar to the data from the new spacecraft. Also, there are very few failures in the historical data, so it is not possible to adequately test the ability of the prototype to detect failures using the historical data. The Space Shuttle data can, however, be used both for verification of the false positive rate and for stress testing.
2. **Simulated data:** We specified that a certain number of scripts be written to simulate various failure modes. These scripts will combine simulated data with real historical Space Shuttle data, and will be used to detect the ability of the prototype to detect these failure modes. Unfortunately, there is no physics-based simulator available to serve as a test oracle. Thus, the scripts will require an engineering expert, particularly to serve as a test oracle. Developing these scripts is labor intensive, which limits how many scripts can be developed.
3. **Random data:** We specified that the prototype shall be tested using a large amount of randomly generated data. This testing will not verify that the prototype produces the correct diagnosis; it will only be used to verify that the system does not crash.
4. **All possible inputs:** For a realistic system, the number of possible inputs is much too large to perform exhaustive testing. However, we have also developed a simplified model of the system that only has six Boolean inputs. We specified that the prototype shall be tested using all 64 possible inputs to this simplified model.

IV. ADDITIONAL CONSIDERATIONS FOR CERTIFICATION

We are also considering developing reference implementations that can serve as test oracles. This is particularly appropriate for IMS, which uses a relatively simple algorithm to identify anomalies and generate a corresponding anomaly measure. A reference algorithm ideally should be written as a specification that can be executed directly (or compiled and executed). An alternative is to use a

high level language that can be more readily verified, possibly by inspection and analysis, than the actual implementation, which, because of optimizations and other implementation constraints, poses a much greater V&V challenge.

Also under consideration is a reference implementation for the model-based reasoning system. This is complicated by the fact that the TEAMS product line includes a “compiler”, TEAMS Designer, that takes engineering schematics, FMEA, fault propagation information, and other input to produce a data structure used by the runtime component, TEAMS-RT, to perform diagnosis. A reference implementation for TEAMS-RT is under consideration, and a reference implementation for the relevant “compiler” subset of TEAMS Designer is a possibility.

Other certification challenges are discussed in [4].

V. CONCLUSION

Conventional wisdom recommends considering testability of requirements at the time they are written as a way to achieve high quality requirements. For example, considering how to identify whether a test has “passed” or “failed” a requirement may help weed out an ambiguous expression of that requirement. Our experience reinforces this—we were led to iterate the statements of many of our requirements. In addition, our experience also gave us key insights into the V&V challenges posed by certification to the particularly stringent standards that this application calls for. Conventional wisdom also indicates that V&V to attain stringent certification may well consume significant resources – in some cases, more than the cost of the original development. Thus early insight into the V&V challenges – in our case, lack of relevant historical data to cover off-nominal cases – is itself of great benefit, by guiding us towards tasks (e.g., development of reference implementations) to be performed in parallel with the application development.

VI. ACKNOWLEDGEMENT

The research described in this paper was carried out at NASA Ames Research Center and at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. The authors thank the entire FDIR development team for their insights and advice, and especially for their patience with our many questions.

REFERENCES

- [1] First International Forum on Integrated System Health Engineering and Management in Aerospace Nov 7-10 , 2005, Napa, CA: <http://ti.arc.nasa.gov/projects/ishem/index.php>
- [2] *NASA Human-Rating Requirements for Space Systems*. NPR 8705.2B, 2008.
- [3] M.A. Schwabacher and R. Waterman, “Pre-Launch Diagnostics for Launch Vehicles,” *Proc. of the IEEE Aerospace Conf.*, Big Sky, MT, March, 2008.
- [4] M.S. Feather and L.Z. Markosian, “Towards Certification of a Space System Application of Fault Detection and Isolation,” *Int. Conf. Prognostics and Health Management*, Denver, CO, October, 2008.