Validation of a Software-Related Failure Mode Taxonomy

Alice Lee
NASA- Johnson Space Center
Houston, TX, USA

Carol Smidts, Bin Li, Ming Li
Center for Reliability Engineering, University of Maryland
College Park, MD, USA

1 Introduction

Probabilistic Risk Assessment (PRA) is a methodology used to determine the probability of failure or success of a system. PRA results are typically used to make decisions on life extensions, sub-systems upgrades, scheduling of maintenance activities, selection of design concepts, etc. Current PRA methodology accounts for the contributions of hardware systems and in some instances of operating and maintenance crews to risk. However, modern systems are heavily software dependent and this dependency seems to increase. Current PRA methodology neglects the impact of software components on risk. This paper describes initial efforts to address the software issue.

Our current research aims to establish a systematic methodology for integrating software contributions to risk into the classical PRA framework. As a part of this research, UMD (University of Maryland) has established what we believe to be a comprehensive and exhaustive taxonomy of failures related to the software component [1,3]. The taxonomy is based on an understanding of how software functions and interacts with its environment. Essentially, software runs on a computer platform that resides within an environment characterized by parameters such as gravity, humidity, radiation level, etc. Furthermore, the software processes inputs from and produces outputs to other components (other software, humans or hardware) through input and output devices. Failures may therefore originate in the software itself at the input side, the output side or be due to failures of the computer platform. These four categories of failures are further refined in [1,3].

To validate the hypothesis that the taxonomy developed is an acceptable taxonomy of software related failure modes one needs to verify that the taxonomy is complete, consistent, repeatable and applicable [4].

---

1 This research is funded by NASA IV&V and NASA URETI Reusable Launch Vehicle Initiative.
The following questions help further define and assess the criteria and were used throughout this study:

1. Completeness:
   a. Are the failure modes complete enough to apply to aerospace systems of various natures?
   b. Does the taxonomy include failure modes occurring in autonomous real time systems?
   c. Do the taxonomy definitions consider all the failure modes in software?

2. Consistency
   a. Are the taxonomy definitions clear and accurate?
   b. Are the failure mode definitions comprehensive and intuitive?

3. Repeatability
   a. Could different individuals interpret the definition the same way and assign it to the same failure mode?
   b. How much the evaluation of the failure mode dependent on human skill level or on automated process?

4. Applicability
   a. Is data available to validate the UMD developed taxonomy?
   b. Is there flexibility to use alternative data when required data is not available?

The current paper reports on a systematic validation effort of the taxonomy pursued jointly at NASA Johnson Space Center (JSC) and at the University of Maryland (UMD).

The validation process is comprised of four phases shown in Figure 1. The first phase was dedicated to training the JSC team. During the second phase (called JSC Classification), JSC classified around 300 trouble and change reports without any intervention from UMD. During the third phase, UMD will review JSC’s classification and assess its correctness. UMD plans to randomly sample a subset of trouble reports and ascertain the categories to which the failure mode(s) described in the report was (were) assigned. Finally the fourth phase (called JSC/UMD consolidation) is a consensus-building phase where the taxonomy as well as training material and procedures will be finalized.

![Figure 1. Validation Process](image-url)