Optimizing the V&V Process for Critical Systems

James D. Kiper
Department of Computer Science
Miami University
Oxford, OH 45056
James.Kiper@muohio.edu

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

Julian Richardson
Research Institute for Advanced Computer Science,
Moffett Field, CA 94035-1000
julianr@email.arc.nasa.gov

ABSTRACT

In the design of critical systems and software, validation and verification (V&V) that requirements are met is a crucial activity. Since budgets are limited, it is not possible to perform all of the possible V&V activities; a subset must be chosen that maximizes the chances of mission success by reducing risk while meeting budget constraints. By explicitly modeling the contributions that various V&V activities make to reducing risks, and the costs of these activities, we are able to convert this to a classical optimization problem. We then use search, clustering and visualization algorithms to examine the large space of options.

Categories and Subject Descriptors

I.2.8 [**Artificial Intelligence**]: Problem Solving, Control Methods, and Search – *Heuristic methods.*

D.2.4 **[Software Engineering**]: Software/Program Verification – *Validation.*

General Terms

Verification.

Keywords

Simulated annealing, genetic algorithms, clustering.

1. INTRODUCTION

One of the most difficult challenges in the development of spacecraft, or any large system, is assuring quality of the system in a cost effective manner. More precisely, the system should be developed and used in a way which minimizes *risk.* In this context, V&V methods and tools can be seen as one kind of risk reduction activity (*risk mitigation*); other kinds of risk mitigation include introduction of redundancy in system designs or use of procedures to avoid potential problems during operation. Since budgets are always limited and risk mitigation activities incur cost, it is not possible to apply every available risk mitigation. In general, the type and severity of risks varies depending on the project, as does the available budget, so selection of appropriate risk mitigations is an optimization problem [1]. Our approach to this problem has been to model these development risks and costs of mitigating them.

2. OPTIMIZING RISK REDUCTION

The Defect Detection and Prevention (DDP) tool and process have been used at the Jet Propulsion Laboratory in a risk-based approach to system development and technology evaluation. DDP has been applied [2] to individual technologies (e.g., memory devices), designs of entire spacecraft, and programmatic decision making for portfolios of multiple spacecraft missions. The heart of DDP is a model of *objectives* the system must attain, *risks* that threaten them, and *mitigations* that can reduce risks.

3. EXPERIENCES

By modeling designs of complex systems in DDP, we have been able to capture the features of these systems that domain experts view as most important. Models may contain many interrelated requirements, risks and mitigations, resulting in a very large search space of possible mitigation selections. We have used simulated annealing, genetic algorithms, and various visualizations to find the structure in the space.

It is important to realize that in practice users cannot explicitly model *all* system constraints and relationships. Instead of searching for a single optimal solution, we use similarity metrics and clustering to derive and present to the user a set of qualitatively different near optimal solutions to choose among.

4. CONCLUSIONS

In this work, we have shown that V&V of critical systems can be posed as a search problem for which heuristic search techniques are first-rate solutions. By searching for solutions that are near-optimal in the search space represented by the model parameters, the manager is able to focus on those issues for which human experience and judgment is best suited. Experiments on DDP-like models indicate that the V&V recommendations to which these techniques lead are robust in the face of uncertainty in the data [3]. Our experience and experiments suggest that significant gains are achievable by this use of optimization in V&V. In fact, we dare to assert that such model-based optimization used to assist human expertise should be standard practice.

5. REFERENCES

[1] Cornford, S.L., Dunphy, J. and Feather, M.S. “Optimizing the Design of end-to-end Spacecraft Systems using risk as a currency,” *IEEE Aerospace Conference*, Big Sky, MT, March 2002.

[2] Feather, M.S., Cornford, S.L., Hicks, K.A., and Johnson, K.R. “Applications of tool support for risk-informed requirements reasoning”, *Computer Systems Science and Engineering*, 20(1): 5-17, January 2005.

[3] Richardson, J. D. C., Port, D. and Feather, M.S. “Exploring the Robustness of Risk Reduction Strategies,” *IEEE Aerospace Conference*, Big Sky, MT, March 2007.

GECCO'07, July 7–11, 2007, London, England, United Kingdom
ACM 978-1-59593-697-4/07/0007.