An Annual Progress Report
Grant No. NAG-1-1123

April 1, 1991 - March 31, 1992

DEVELOPMENT AND VALIDATION OF TECHNIQUES FOR IMPROVING SOFTWARE DEPENDABILITY

Submitted to:

National Aeronautics and Space Administration
Langley Research Center
Hampton, VA 23665

Attention:

Dr. D. E. Eckhardt, Jr., ISD
M/S 478

Submitted by:

John C. Knight
Associate Professor

Report No. UVA/528344/CS92/102
June 1992

DEPARTMENT OF COMPUTER SCIENCE

SCHOOL OF
ENGINEERING
& APPLIED SCIENCE

University of Virginia
Thornton Hall
Charlottesville, VA 22903

UNIVERSITY OF VIRGINIA
School of Engineering and Applied Science

The University of Virginia's School of Engineering and Applied Science has an undergraduate enrollment of approximately 1,500 students with a graduate enrollment of approximately 600. There are 160 faculty members, a majority of whom conduct research in addition to teaching.

Research is a vital part of the educational program and interests parallel academic specialties. These range from the classical engineering disciplines of Chemical, Civil, Electrical, and Mechanical and Aerospace to newer, more specialized fields of Applied Mechanics, Biomedical Engineering, Systems Engineering, Materials Science, Nuclear Engineering and Engineering Physics, Applied Mathematics and Computer Science. Within these disciplines there are well equipped laboratories for conducting highly specialized research. All departments offer the doctorate; Biomedical and Materials Science grant only graduate degrees. In addition, courses in the humanities are offered within the School.

The University of Virginia (which includes approximately 2,000 faculty and a total of full-time student enrollment of about 17,000), also offers professional degrees under the schools of Architecture, Law, Medicine, Nursing, Commerce, Business Administration, and Education. In addition, the College of Arts and Sciences houses departments of Mathematics, Physics, Chemistry and others relevant to the engineering research program. The School of Engineering and Applied Science is an integral part of this University community which provides opportunities for interdisciplinary work in pursuit of the basic goals of education, research, and public service.

An Annual Progress Report
Grant No. NAG-1-1123

April 1, 1991 - March 31, 1992

DEVELOPMENT AND VALIDATION OF TECHNIQUES FOR IMPROVING SOFTWARE DEPENDABILITY

Submitted to:

National Aeronautics and Space Administration
Langley Research Center
Hampton, VA 23665

Attention:

Dr. D. E. Eckhardt, Jr., ISD
M/S 478

Submitted by:

John C. Knight
Associate Professor

Department of Computer Science
SCHOOL OF ENGINEERING AND APPLIED SCIENCE
UNIVERSITY OF VIRGINIA
CHARLOTTESVILLE, VIRGINIA

Report No. UVA/528344/CS92/102
June 1992

Copy No.____

TABLE OF CONTENTS

OVERVIEW

During the grant reporting period, the research carried out has been in a number of areas. Specifically:

- Previous work on modelling of error detection mechanisms has been completed, documented in a technical report, and submitted for publication.

- Previous work on software inspection has been continued. The process, known as *Phased Inspection* has been refined, the support toolset extended, and the process evaluated by experimentation. The results have been documented as a technical report and submitted for publication.

- A study of the use of formal specifications as a source of test cases has been completed and reported at the annual Computer Assurance Conference (COMPASS).

- An introductory explanation of formal methods has been written and documented as a technical report.

- A draft version of the Magnetic Stereotaxis System safety specifications has been prepared.

- A draft version of the Magnetic Stereotaxis System system fault trees has been prepared.

- A toolset for injecting synthetic faults into software has been built. The research surrounding that toolset is underway and progress is reported in a working document.

All of the documents referred to above have been supplied to the sponsor under separate cover.

PUBLICATIONS

Below are listed the various publications resulting form this funding.

Title

The Effect Of Imperfect Error Detection on Software Reliability Estimation.

Authors

P.E. Ammann, S.S. Brilliant, and J.C. Knight.

Disposition

University of Virginia Technical Report Number TR-92-16.
Submitted to the IEEE Transactions on Software Engineering.

Abstract

Measurement of software reliability by life testing involves executing the software on large numbers of test cases and recording the results. The number of failures observed is used to bound the failure probability even if the number of failures observed is zero. Most analyses assume that all failures will be observed but in practice this will rarely be the case. In this paper we examine the effect of imperfect error detection, *i.e.*, the situation in which a failure of the software may not be observed. If the conventional analysis associated with life testing is used, the confidence in the bound on the failure probability is optimistic. Our results show that imperfect error detection does not necessarily limit the ability of life testing to bound the probability of failure to the very low values required in critical systems. However, we show that the confidence level associated with a bound on failure probability cannot necessarily be made as high as desired unless very strong assumptions are made about the error detection mechanism. Such assumptions are unlikely to be met in practice, and so life testing is likely to be useful only for situations where very high confidence levels are not required.

Title

An Improved Software Inspection Technique And An Empirical Evaluation Of Its Effectiveness.

Authors

E.A. Myers and J.C. Knight.

Disposition

University of Virginia Technical Report Number TR-92-15.
Submitted to the Communications of the ACM.

Abstract

Inspection of software work products is common practice and has been shown to be a valuable tool for the software engineer. However, we believe that the technology is not being exploited as fully as possible. We define an enhanced inspection technique called *Phased Inspection* that addresses the deficiencies of existing inspection techniques. This technique is designed to permit the inspection process to be rigorous, tailorable, efficient in its use of resources, and heavily computer supported. The Phased Inspection process is designed to permit the engineer to trust the results of a specific inspection and to ensure that inspection results are repeatable. Phased Inspections inspect the work product in a series of small inspections termed phases each of which is designed to ascertain whether the work product possesses some desirable property. The skills of the staff performing a phase are tailored to the goals of the phase, and the checking that is performed during a given phase is defined precisely and computer supported. An important goal of Phased Inspection is computer support and we present details of a toolset that supports Phased Inspection by providing the inspector with extensive computer assistance and by checking for compliance with the required process. A preliminary evaluation of Phased Inspection is also presented.

Title

Using Z Specifications in Category Partitioning Testing

Authors

N. Amla and P.E. Ammann

Disposition

Proceedings COMPASS '92.

Abstract

The application of specification-based test methods to informal functional specifications requires considerable analysis on the part of the test engineer. We hypothesize that a large portion of this analysis is already present in formal functional specifications. In this paper we examine this hypothesis by analyzing a particular variety of formal specifications, namely Z specifications, in the context of a general specification-based testing method known as Category Partition testing. The paper presents general guidelines to derive Category Partition test specifications from Z functional specifications. The relationship between a Z specification and steps in the Category Partition method is broadly defined and illustrated with an example.

Title

A Tourists' Guide To Formal Methods

Author

D.M. Kienzle

Disposition

University of Virginia Technical Report Number TR-92-17.

Abstract

The term *formal methods* conjures up images of entirely cryptic proofs, rife with mathematical mysticism and understandable only by the few initiates of that bizarre sect.

In actuality, that image could not be further from the truth. Formal methods are the basis of all aspects of computer science. Rather than a simple demarcation between formal and informal, formal methods encompass a spectrum of approaches, from the almost entirely informal, to the strictly formal. The question practitioners must ask is not whether to use formal methods, but what degree of formality is required and what is most cost effective. The basic issues are not religious, but economic.

This paper attempts to disperse some of the fog that still enshrouds formal methods, surveying many of todays existing approaches. The emphasis is not on converting others to the formal methods camp, but on identifying the level of formality suitable for the individual reader's needs.

Title

Software Safety Specifications For The Magnetic Stereotaxis System

Authors

D.M. Kienzle, J.C. Knight, and K.G. Wika

Disposition

Working draft document.

Abstract

This document contains a draft of the safety specification for the Magnetic Stereotaxis System. The specification is written in Z. It is considered to be only a draft because it has not be formally reviewed or verified and it has received no formal approval.

Title

System Fault Trees For The Magnetic Stereotaxis System

Authors

D.M. Kienzle, J.C. Knight, and K.G. Wika

Disposition

Working draft document.

Abstract

This document contains a draft of the system fault trees for the Magnetic Stereotaxis System. The trees are presented in a textual representation rather than the more traditional graphic form to facilitate manipulation. It is considered to be only a draft because it has not be formally reviewed or verified and it has received no formal approval.

Title

On The Creation Of Synthetic Software Faults

Authors

K.G. Wika and J.C. Knight

Disposition

Working draft document.

Abstract

A critical problem in the development of improved software test methods is the lack of any standard empirical assessment technique. The goal of the research outlined in this report is the development of concepts and tools necessary for evaluating software testing strategies. Research has focused on developing fault-injected programs appropriate for the analysis of test methods. A fault injection tool has been implemented to generate the faulty programs. Using a test harness, the erroneous programs have been evaluated with respect to selected fault quality metrics developed as a component of the research. Initial analysis has also been performed to understand the types of alterations that are most likely to result in high quality faults.

DISTRIBUTION LIST

1 - 3 National Aeronautics and Space Administration
Langley Research Center
Hampton, VA 23665

Attention: Dr. D. E. Eckhardt, Jr., ISD
M/S 478

4 - 5 * National Aeronautics and Space Administration
Scientific and Technical Information Facility
P. O. Box 8757
Baltimore/Washington International Airport
Baltimore, MD 21240

6 National Aeronautics and Space Administration
Acquisition Division
Langley Research Center
Hampton, VA 23665

Attention: Mr. Richard J. Siebels
Grants Officer, M/S 126

7 - 8 E. H. Pancake, Clark Hall

9 - 10 J. C. Knight, CS

11 A. K. Jones, CS

12 SEAS Preaward Administration Files

*One reproducible copy

JO#4505:ph