Annual Progress Report
Grant No. NAG-1-260 Supp. No. 7
January 1, 1987 - February 14, 1988

THE IMPLEMENTATION AND USE OF ADA ON DISTRIBUTED SYSTEMS WITH HIGH RELIABILITY REQUIREMENTS

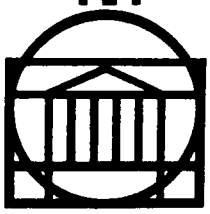
Submitted to:

Mr. C. Michael Holloway
ISD M/S 125
NASA Langley Research Center
Hampton, VA 23665

Submitted by:

J. C. Knight
Associate Professor

Report No. UVA/528213/CS88/112
March 1988



SCHOOL OF ENGINEERING AND APPLIED SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

UNIVERSITY OF VIRGINIA
CHARLOTTESVILLE, VIRGINIA 22901

An Annual Progress Report
Grant No. NAG-1-260 Supp. No. 7
January 1, 1987 - February 14, 1988

THE IMPLEMENTATION AND USE OF ADA ON DISTRIBUTED SYSTEMS WITH HIGH RELIABILITY REQUIREMENTS

Submitted to:

Mr. C. Michael Holloway
ISD M/S 125
NASA Langley Research Center
Hampton, VA 23665

Submitted by:

J. C. Knight
Associate Professor

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

Report No. UVA/528213/CS88/112
March 1988

Copy No. 5

TABLE OF CONTENTS

SECTION 1

INTRODUCTION

The primary goal of this grant is to investigate the use and implementation of Ada* in distributed environments in which reliability is the primary concern. In particular, we are concerned with the possibility that a distributed system may be programmed entirely in Ada so that the individual tasks of the system are unconcerned with which processors they are executing on, and that failures may occur in the software or underlying hardware. A secondary interest is in the performance of Ada systems and how that performance can be gauged reliably.

Over the next decade, it is expected that many aerospace systems will use Ada as the primary implementation language. This is a logical choice because the language has been designed for embedded systems. Also, Ada has received such great care in its design and implementation that it is unlikely that there will be any practical alternative in selecting a programming language for embedded software.

The reduced cost of computer hardware and the expected advantages of distributed processing (for example, increased reliability through redundancy and greater flexibility) indicate that many aerospace computer systems will be distributed. The use of Ada and distributed systems seems like a good combination for advanced aerospace embedded systems.

A distributed system is only as reliable as its weakest node. For example, if each of three computers in a system will operate correctly 99 percent of the time, the complete system will function, on average, only approximately 97 percent of the time. If a node has failed, however, a distributed system has the potential to continue providing service since some hardware facilities

* Ada is a trademark of the U.S. Department of Defense

remain. Continuation will make these systems *more* reliable than single-processor architectures. In order to be truly useful from a reliability standpoint, however, distributed systems must be safe: they should provide a level of service after failure which reflects the reduction in computing power and does not jeopardize the fundamental purpose of the application. Post-failure operation could take the form either of ongoing but reduced service (as in an aircraft control system) or of a timely, controlled shutdown (as in a nuclear power plant).

Such real-time control applications as are found in the defense and aerospace industries often require very high reliability, so toleration of hardware failures can be extremely important. We designate such applications to be *crucial* in that their failures may cause human lives to be endangered or enormous sums of money to be wasted.

Another concern that is emerging is the performance that might be achieved from Ada implementations. Initial performance measures indicate that there is considerable variability between implementations and between different types of program on the same implementation. Programmers have expressed concern that, although Ada may allow software to be developed with fewer faults, the execution-time performance may make the use of Ada impractical. We have developed a system that allows system designers to build benchmarks that can be used to evaluate implementations prior to implementation to ensure that performance will be adequate for the application under consideration.

During the grant reporting period our primary activities have been:

(1) Analysis of the original approach to recovery in distributed Ada programs using the ATOPS example.

(2) Review and assessment of the original approach which was found to be capable of improvement.

(3) Preparation and presentation of a paper describing this work at the 1987 Washington DC Ada Symposium.

(4) Development of a refined approach to recovery that has been applied to the ATOPS example.

(5) Design and development of a performance assessment scheme for Ada programs based on a flexible user-driven benchmarking system.

(6) Preparation of a paper describing the work on benchmarking that will be presented at the Third International IEEE Conference On Ada Applications and Environments, Manchester, New Hampshire, May 1988.

In section 2 of this report, our activities in the area of distributed Ada are summarized briefly. Section 3 is an overview of our benchmarking project. A list of papers and reports prepared under this grant, other than the annual and semi-annual progress reports, is presented in the Appendix.

SECTION 2

DISTRIBUTED Ada

In previous work under this grant we have shown the general inadequacy of Ada for programming systems that must survive processor loss. We have also proposed a solution to the problem in which there are no syntactic changes to Ada. We felt confident that the solution was adequate but could not be sure until the solution was tested. A major goal of this grant, therefore, was to evaluate the approach using a full-scale, realistic application. The application we used was the Advanced Transport Operating System (ATOPS), an experimental computer control system developed at NASA Langley for a modified Boeing 737 aircraft. The ATOPS system is a full authority, real-time avionics system providing a large variety of advanced features.

The preliminary evaluation lead us to conclude that the approach was indeed workable. We documented the preliminary results in a paper presented at the 1987 Washington DC Ada symposium. That paper has been supplied to the sponsor under separate cover.

Although workable, various deficiencies in style and flexibility were noted and a new approach was devised that is far more useful than the original. A preliminary discussion of that approach was presented in the 1987 Semi-Annual report for this grant. A more detailed report will be supplied to the sponsors under separate cover.

SECTION 3

Ada IMPLEMENTATION PERFORMANCE

In a somewhat different area of research under this grant we have designed and prototyped a system to provide performance analysis of Ada implementations. Our goal is to supply the system designer with tools that will allow a rational decision to be made about whether a particular implementation can support a given application early in the design cycle.

A commitment to the use of Ada is viewed as a substantial risk by most project managers mainly because of unknown performance, and if this risk could be reduced it would enhance the use of Ada considerably. The problem with traditional benchmarks as performance predictors is that they lack relevance to particular applications. A given Ada implementation may work one way with an existing benchmark but work differently with a specific application because of differences that may appear minor between the benchmark and the application.

The benchmarking system we have designed and prototyped allows a system designer to tailor a benchmark to the characteristics of the system he expects to build and to do parametric studies around the operating point. Tis latter facility helps build credibility in the implementation because it does not require that the benchmark be particularly accurate. Since a range of performance figures is obtained, a confidence interval of performance data can be obtained.

A discussion of this project on performance has been supplied to the sponsor under separate cover. That discussion will appear as a paper in the Third International Conference on Ada Applications and Environments to be held in Nashua, NH, in May of 1988.

APPENDIX

REPORT LIST

The following is a list of papers and reports, other than progress reports, prepared under this grant.

(1) Knight, J.C. and J.I.A. Urquhart, "Fault-Tolerant Distributed Systems Using Ada", Proceedings of the *AIAA Computers in Aerospace Conference*, October 1983, Hartford, CT.

(2) Knight, J.C. and J.I.A. Urquhart, "The Implementation And Use Of Ada On Fault-Tolerant Distributed Systems", *Ada LETTERS*, Vol. 4 No. 3 November 1984.

(3) Knight, J.C. and J.I.A. Urquhart, "On The Implementation and Use of Ada on Fault-Tolerant Distributed Systems", *IEEE Transactions on Software Engineering*. May, 1987.

(4) Knight J.C. and S.T. Gregory, "A Testbed for Evaluating Fault-Tolerant Distributed Systems", Digest of Papers FTCS-14: *Fourteenth Annual Symposium on Fault-Tolerant Computing*, June 1984, Orlando, FL.

(5) Knight J.C. and S.T. Gregory, "A New Linguistic Approach To Backward Error Recovery", Digest of Papers FTCS-15: *Fifteenth Annual Symposium on Fault-Tolerant Computing*, June 1985, Ann Arbor, MI.

(6) Gregory, S.T. and J.C. Knight, "Concurrent System Recovery" in *Resilient Computing Systems, Volume 2* edited by T. Anderson, Wiley, 1987.

(7) Knight, J.C. and M.E. Rouleau, "Analysis Of Ada For A Crucial Distributed Application", Proceedings of the Fifth National Conference On Ada Technology,

Washington DC, March, 1987.

(8) Knight, J.C. and R.H. Crowe, "A System for Evaluating Ada Implementations Using Benchmarks", Proceedings of the Third International Conference on Ada Applications and Environments, Nashua NH, May, 1988.

(9) Knight, J.C. and J.I.A. Urquhart, "Difficulties With Ada As A Language For Reliable Distributed Processing", Unpublished.

(10) Knight, J.C. and J.I.A. Urquhart, "Programming Language Requirements For Distributed Real-Time Systems Which Tolerate Processor Failure", Unpublished.

DISTRIBUTION LIST

Copy No.	
1 - 3	Mr. C. Michael Holloway ISD M/S 125 NASA Langley Research Center Hampton, VA 23665
4	Mr. J. F. Royall, Jr. Grants Officer, M/S 126 NASA Langley Research Center Hampton, VA 23665
5 - 6*	NASA Scientific and Technical Information Facility P.O. Box 8757 Baltimore/Washington International Airport Baltimore, MD 21240
7 - 8	J. C. Knight, CS
9	R. P. Cook, CS
10 - 11	E. H. Pancake, Clark Hall
12	SEAS Publications Files

* reproducible copy

JO#1071:ph

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 560. There are 150 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 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 16,400), 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.