TECHNIQUES FOR THE DESIGN AND IMPLEMENTATION OF HIGHLY RELIABLE MULTI-PROCESSING SYSTEMS

D. C. Luckham

MAY 1985

RFOSR-TR-85-8693
AFOSR-85-0355

UNCLASSIFIED
During this research period several significant accomplishments were obtained. The completion of implementation of a prototype runtime monitor for detecting deadness errors in Ada tasking was accomplished. The work on runtime monitoring for deadness errors was presented at the IEEE Ada Conference in October 1984, and an invited publication appeared in IEEE Software in March 1985. A new language, called TSL (for Task Sequencing Language) to be used for specifying Ada tasking behavior, was designed and presented at the International Ada Conference in May 1985.
Dear Captain Thomas:

Regarding: Grant AFOSR-83-0355 "Techniques for the Design and Implementation of Highly Reliable Multi-Processing Systems".

Enclosed is a short outline of our work and progress under grant AFOSR-83-0355 during the current year. Also included is a short proposal and budget for the continuation of our work in the coming year, September 30, 1985 - September 29, 1986. The budget is based on the third year budget included with the original four-year proposal approved by AFOSR in August, 1983. There are minor differences due to the changes in Stanford's personnel costs.

The following enclosed papers, reports, and implementation design study, were sponsored by AFOSR during the period September 30, 1984 through September 29, 1985 under Grant AFOSR-83-0355.

A. Papers.

These papers were published during the current year's work in refereed conference proceedings or technical journals. One of the papers was invited for publication in a special issue of IEEE Software.


B. Technical Reports.
The following technical reports were also sponsored under the AFOSR Grant. The reports include full details of prototype implementations and examples. It is generally not possible to publish the complete details of these reports in conference proceedings or technical journals because of space limitations.


C. Draft Documents of work currently in Progress under AFOSR sponsorship.

1. "Preliminary Design of a Runtime TSL Monitor" by Doug Bryan, Computer Systems Laboratory, Stanford University.

D. Related Work by this research group that is currently being used in the TSL implementation.


Yours sincerely,

David C. Luckham
Professor of Electrical Engineering (Research)
Research Progress Report and Proposal
under
AFOSR Grant-83-0355

Techniques for the Design and Implementation of
Highly Reliable Multi-Processing Systems

Principle Investigator: David C. Luckham


This is the second year of Grant AFOSR-83-0355. It has been both a consolidation year and a break-through year. Main accomplishments this year are:

- Completion of implementation of a prototype runtime monitor for detecting deadness errors in Ada tasking, and reports detailing implementation.

- Presentation of the work on runtime monitoring for deadness errors at the IEEE Ada conference, October 1984, and invited publication in IEEE Software in March 1985.

- Design of TSL, a new language for specifying Ada tasking behavior.


During this year work has been completed on runtime monitoring for deadness errors. The basic principles of detecting deadness errors in Ada tasking were applied in the implementation of a prototype runtime monitor. This was successfully demonstrated on example tasking programs. Design principles used in the Ada implementation of the monitor were defined; as a result, runtime monitors developed by this work are extensible and reusable.

This work was published in two reports and three papers. It was presented at the IEEE Ada Conference in October 1984. Subsequently this work was invited for a special issue of IEEE Software on Ada, appearing in March 1985.
One of the principle outcomes of our experiments on detecting deadness errors was the conception and design of a language for specifying a much wider class of tasking errors, called *task sequencing errors*. This language is called TSL, Task Sequencing Language. A paper on TSL has been accepted for presentation at the International Ada Conference in Paris, May 14 - 16, 1985.

Runtime monitoring tools for deadness errors can now be extended to check for sequences of task interactions specified by TSL statements. This gives them the capability to detect very subtle errors in Ada tasking programs. This kind of tool has many applications in testing and monitoring distributed systems, including for example, flight control systems, communication networks, and secure message systems.

Current work on this project is focused on the design and applications of TSL. Extension of the previous tools for runtime deadness monitoring to support use of TSL is in progress. All implementation is in Ada and is designed for possible integration into future Ada support environments.


Proposed research for the next year is on the following projects:

1. *Application of TSL as a testing and debugging tool*. This involves use of TSL to formulate critical properties of actual distributed Ada tasking systems for testing them by runtime monitoring.

2. *Application of TSL as a specification language for design of distributed systems in Ada*. This involves use of TSL as a language extension of Ada to specify tasking activity of an Ada tasking system prior to implementation.

3. *Design and implementation of a TSL runtime monitor*.

4. *Theory of connected events in distributed systems*.

Project 1 is aimed at testing the design of TSL as a practical language for specifying erroneous behavior patterns in tasking programs. Practical examples of Ada systems are to be used for these studies, including for example, a distributed message network. Some redesign of TSL is expected to result from this study.
Project 2 is aimed at developing TSL as a new task specification language, somewhat higher level than Ada itself, but having compatible scope and visibility rules. This goes beyond the use of TSL as a testing and debugging language. TSL specifications should be transformable into Ada tasking bodies. Again, changes to TSL are expected to result.

Project 3 is aimed at implementing a runtime monitor for TSL. A design document outlining our current implementation design is included with this proposal. This design builds on previous packages developed for the deadness error monitor. It is intended eventually to run efficiently on distributed hardware.

Projects 1 - 3 depend on theoretical investigation of concepts related to uncertainty of information obtained from distributed systems at runtime, for example the concept of connected events described in the accompanying publications. This work will be pursued in project 4.
### 3 Budget September 30, 1985 - September 29, 1986.

<table>
<thead>
<tr>
<th>Position</th>
<th>Salary</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professor David Luckham</td>
<td>$14,077</td>
<td>20%</td>
</tr>
<tr>
<td>Senior Research Associate</td>
<td>7,845</td>
<td>15%</td>
</tr>
<tr>
<td>1 Ph.D. student</td>
<td>13,500</td>
<td>50% Academic</td>
</tr>
<tr>
<td>Secretary</td>
<td>4,080</td>
<td>17%</td>
</tr>
<tr>
<td>Administrative Assistant</td>
<td>1,308</td>
<td>100% Summer</td>
</tr>
<tr>
<td>SEL Engineering Support</td>
<td>40,810</td>
<td>40%</td>
</tr>
<tr>
<td>Benefits</td>
<td>10,603</td>
<td>25.4% through 8/31/86</td>
</tr>
<tr>
<td></td>
<td></td>
<td>25.6% through 8/31/87</td>
</tr>
<tr>
<td>Total Salaries &amp; Benefits</td>
<td>$52,311</td>
<td>$52,311</td>
</tr>
<tr>
<td>Expendable materials and supplies</td>
<td>1,264</td>
<td></td>
</tr>
<tr>
<td>Postage, Xeroxing, telephone</td>
<td>2,107</td>
<td></td>
</tr>
<tr>
<td>Computer Charges</td>
<td>16,330</td>
<td></td>
</tr>
<tr>
<td>Travel - 2 East Coast Trips</td>
<td>3,324</td>
<td></td>
</tr>
<tr>
<td>Subtotal</td>
<td>75,336</td>
<td></td>
</tr>
<tr>
<td>University Overhead @ 60%</td>
<td>51,982</td>
<td></td>
</tr>
<tr>
<td>1 Year Total</td>
<td>127,318</td>
<td></td>
</tr>
</tbody>
</table>