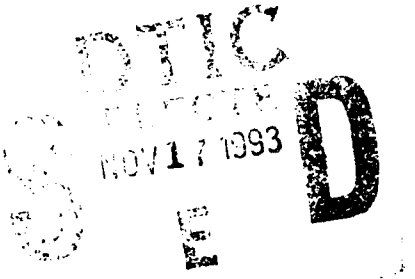
REAL-TIME FAULT TOLERANT COMPUTER SYSTEMS

SFRC. N00014-92-J-1524

YEARLY REPORT

1 October 1992 - 30 September 1993

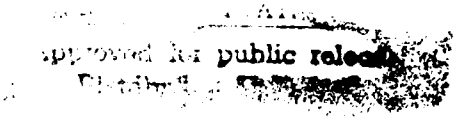


Prepared for:

Department of the Navy
Office of Naval Research
800 North Quincy Street
Ballston Tower One
Arlington, Virginia 22217-5660

Prepared By:

John P. Lehoczky, Principal Investigator
Lui Sha, Principal Investigator
Marc Bodson, Principal Investigator
Ragunathan Rajkumar, Principal Investigator
Carnegie Mellon University
Pittsburgh, PA 15213



Principal Investigator Names:

J. Lehoczky	(412) 268-8725	jpl@k.cs.cmu.edu
L. Sha	(412) 268-5875	lrs@sei.cmu.edu
M. Bodson	(412) 268-3898	bodson@galley.ece.cmu.edu
R. Rajkumar	(412) 268-8707	rr@sei.cmu.edu

PI Institution: Carnegie Mellon University
Contract title: Real-Time Fault Tolerant Computer Systems
Contract Number: N00014-92-J-1524
Reporting Period: 1 Oct 92 - 30 Sep 93

1 Productivity Measures

This project was funded to investigate the use of *analytic redundancy* as an approach to software fault tolerance. This research project is a part of a larger project at Carnegie Mellon University (the ART Project) which is also funded in part by the Office of Naval Research. The productivity measures and publications listed in this report are those which are associated exclusively with the use of analytic redundancy. A more complete report of the activities of the ART Project is contained in the yearly report for ONR Contract N00014-92-J-1771 and in the 1992 and 1993 *ART Project Briefing*.

- Papers submitted but not yet accepted: 0
- Refereed papers accepted and in press: 2
- Refereed papers published: 1
- Books submitted or published: 0
- Other reports: 0
- Ph.D. dissertations: 0
- Patents filed or granted: 0
- Invited presentations: 1
- Contributed presentations: 2
- Honors, Prizes, Awards and other Professional Activities:
  - **John Lehoczky**:
    - Associate Editor, Journal of *Real-Time Systems*,
    - Member of the program committee of the 1993 IEEE Real-Time Systems Symposium, the 1993 ICDCS and the 1993 Rate Monotonic Users Forum.
    - Member, NIH Special Study Section on Statistics (Chair, July, 1993).
  - **Lui Sha**
    - Member NASA Space Station Advisory Committee,
    - Chairman of the Board of Visitors of RICIS, an R&D center established by NASA and NASA JSC at University of Houston at Clearlake.
    - General chair, 13th IEEE Real-Time Systems Symposium,
    - Program Committee, 2nd International Workshop on Responsive Systems,
    - Associate Editor, *Real-Time Systems*
    - Associate Editor, *IEEE Computer*

- The paper Sha, L. and Sathaye, S. "Distributed system design using generalized rate monotonic theory," *Proceedings of the Second International Conference on Automation, Robotics and Computer Vision*, 1992 was selected as one of the most innovative papers presented at the conference.

- **Marc Bodson**
  - Program Committee, 1993 Automatic Control Conference
  - Member National Science Foundation Review Panel on robust, adaptive and nonlinear control.
  - Board of Directors, IEEE Pittsburgh Chapter, 1992-1993
  - Promoted to Associate Professor Electrical and Computer Engineering, Carnegie Mellon University.
- **Ragunathan Rajkumar**
  - Session chair, IEEE Workshop on Real-Time Operating Systems and Software, May, 1993.
  - Panel Participant, Sixth ISCA International Conference on Parallel and Distributed Systems, 1993
  - Publicity chair, 14th IEEE Real-Time Systems Symposium

- Graduate students supported: 1, Jennifer M. Stephan
- Undergraduate students supported: 4, W. Mark Smith, Deborah Soh, Patrick Duroseau and Ronald Russell.
- Post-docs supported: 0
- Minorities supported: 2 undergraduates (African American)
- Women supported: 1 graduate student, 1 undergraduate

Principal Investigator Names:

J. Lehoczky	(412) 268-8725	jpl@k.cs.cmu.edu
L. Sha	(412) 268-5875	lrs@sei.cmu.edu
M. Bodson	(412) 268-3898	bodson@galley.ece.cmu.edu
R. Rajkumar	(412) 268-8707	rr@sei.cmu.edu

PI Institution: Carnegie Mellon University
Contract title: Real-Time Fault Tolerant Computer Systems
Contract Number: N00014-92-J-1524
Reporting Period: 1 Oct 92 - 30 Sep 93

2 Summary of Technical Progress

2.1 Overview of Technical Approach

This project is designed to study a new approach to software fault tolerance called analytic redundancy. It has been widely acknowledged that software failures are the most important issue in large computer system reliability. The failure rate of software has risen to 9.4 times the failure rate of hardware, and software failures have captured substantial media attention in recent years. The problem of software reliability is especially difficult, because the major recognized approaches (recovery blocks and n-version programming) are known to have serious drawbacks, and do not protect against whole classes of errors such as specification or design errors.

Analytic redundancy is an approach which uses simplicity (in the form of software which is relatively simple, well understood and well tested but whose performance is merely adequate) to control complexity (in the form of software which has high performance but is not reliable). Rather than trying to combine the two algorithms (which would create an even less reliable system), we allow the complex software to control the system as long as the system is safe and the software is behaving properly (as judged by the simple software). If it is determined that the system is in an unsafe state (meaning that it is near to a state for which no action can recover) or the complex software is behaving incorrectly, then the simple software takes over. The simple software will guarantee a baseline, if not optimal, performance.

We are considering two classes of examples: (1) control systems and (2) tracking systems and are addressing both by developing an appropriate theory and experimental prototypes. In each case, we are developing a set of algorithms which span the range of complexity and functionality. The major research challenges are (1) to create a software structure which will support the analytic redundancy approach to software fault tolerance, (2) to determine conditions under which the complex algorithm is behaving erroneously and (3) to develop methods which allow the system to smoothly switch control from complex to simple and back to complex when conditions warrant. The ultimate project goal is to develop an engineering methodology in which quantitative tradeoffs between system performance and dependability can be made. Finally, we also intend to better understand the range of software faults encountered in practice, and to determine the coverage of these fault types that is provided by analytic redundancy. These two classes of problems are discussed below.

2.2 Control System Experimentation

Substantial progress was made on a number of aspects of the project including (1) completion of a thorough literature search to identify and classify software faults that have been reported, (2) decomposition of the simple controller into two distinct controllers, a safety controller to recover from

unsafe states and a pure simple controller which is highly reliable and will achieve adequate but not optimal performance, (3) creation of a software structure that incorporates schedulability analysis to support the simplex architecture, and (4) demonstration of the concepts of analytic redundancy through the use of two experimental platforms, one at the SEI Real-Time Systems Laboratory and another in the CMU ECE LASIP laboratory. Public demonstrations of both were given and are described in the hardware and software prototype section of this report.

The approach to analytic redundancy has been broadened over the year and has passed its initial demonstration tests. The architecture has been improved by dividing the simple controller, which had previously functioned both as a controller under ordinary operating conditions and as a recovery controller under unsafe operating conditions. In the experimentation, the decision logic was shown to be very sensitive to noise. Certain state variables, such as the ball velocity in the ball and beam experiment, affect the recoverability in a nonlinear manner, thus noise has an especially important impact. To cope with this problem, an observer was designed and tuned for the critical variables. The results permitted the system to operate optimally over a much larger state space. A software architecture was designed and implemented at the SEI by L. Sha and R. Rajkumar. This architecture prevents the complex software from crashing the system. The architecture also is developed according to sound scheduling principles, so priorities are assigned appropriately to ensure that the simple controller can takeover system operation when necessary, even if the complex controller crashes or enters an infinite loop. Moreover, a schedulability analysis ensures that the complex controller has short enough latency to achieve good control of the system. This architecture has successfully survived extensive testing. During the next year, we plan to extend it to a distributed system which will permit control in the face of processor failures. Finally, more sophisticated complex control algorithms are being implemented on the CMU experimental platform. Thus far, a fuzzy-logic-based controller was developed and implemented. This controller is based on one of the vaunted control algorithms which are claimed to offer high performance, but which have heretofore never been used in critical, unstable applications, because their behavior is not predictable over a wide range of operating conditions. We also intend to implement a neural-network-based controller. This illustrates one of the most important features of the analytic redundancy approach to software fault tolerance. One can, in principle, use a very sophisticated control algorithm whose performance is not fully understood over the full range of possible operating conditions, but be able to recover from an unsafe condition and use a good, if lesser performance, control algorithm until the sophisticated controller can take over. Finally, we will also develop an experimental plan which will systematically permit us to determine the coverage that analytic redundancy will afford with respect to the wide variety of software errors that can be encountered in practice.

2.3 Airborne Radar Systems

There are several distinct algorithmic approaches that can be used by airborne radar tracking systems. These include nearest neighbor algorithms, joint probabilistic data association and multiple hypothesis testing. Each approach has its strengths and weaknesses in terms of its performance, computational complexity and failure characteristics. While there is a large literature on the optimality of certain tracking algorithms, only nearest-neighbor-based algorithms have been fielded. The unsophisticated technology is well understood, and there is great hesitancy to introduce higher performance approaches because of the potential for faulty software. Thus, this application is well suited to using analytic redundancy.

We continue to explore the application of these ideas with MITRE Corporation. We are considering using different algorithms in different circumstances, and when sophisticated algorithms are used, we will

allow the simple algorithms to determine if the complex software is failing. The problem is challenging, but the approach is promising. Moreover, because of the involvement of MITRE, we will be able to implement and test our ideas in a sophisticated tracking simulation testbed. Eventually these ideas will be integrated into the rate monotonic theory to handle the real-time aspects of the problem. Limited progress has been made during the last year. The SEI/CMU team is generalizing rate monotonic scheduling to support its use for analytic redundancy on MITRE's parallel computing architecture. The MITRE team has reported that the time required to modify the AWACS tracking code for purposes of experimentation has been far larger than was originally expected. MITRE is now planning to switch to a simulated system for further experimentation.

Principal Investigator Names:

J. Lehoczky	(412) 268-8725	jpl@k.cs.cmu.edu
L. Sha	(412) 268-5875	lrs@sei.cmu.edu
M. Bodson	(412) 268-3898	bodson@galley.ece.cmu.edu
R. Rajkumar	(412) 268-8707	rr@sei.cmu.edu

PI Institution: Carnegie Mellon University
Contract title: Real-Time Fault Tolerant Computer Systems
Contract Number: N00014-92-J-1524
Reporting Period: 1 Oct 92 - 30 Sep 93

3 Publications and Presentations

3.1 Published or In Press

- Bodson, M., Lehoczky, J., Rajkumar, R., Sha, L, Soh, D., Smith, M. and Stephan, J., "Control reconfiguration in the presence of software errors," to appear *Proceedings of the IEEE Conference on Decision and Control*, December, 1993, San Antonio, Texas.
- Bodson, M., Lehoczky, J., Rajkumar, R., Sha, L., Smith, M. and Stephan, J., "Software fault-tolerance for control of responsive systems, *Proceedings of the Third International Workshop on Responsive Systems*, September, 1993.
- Sha, L., Lehoczky, J., Bodson, M., Krupp, P. and Nowacki, C., "Responsive airborne radar systems," *Proceedings of the Second International Workshop on Responsive Systems*, 1992.

Principal Investigator Names:

J. Lehoczky	(412) 268-8725	jpl@k.cs.cmu.edu
L. Sha	(412) 268-5875	lrs@sei.cmu.edu
M. Bodson	(412) 268-3898	bodson@galley.ece.cmu.edu
R. Rajkumar	(412) 268-8707	rr@sei.cmu.edu

PI Institution: Carnegie Mellon University
Contract title: Real-Time Fault Tolerant Computer Systems
Contract Number: N00014-92-J-1524
Reporting Period: 1 Oct 92 - 30 Sep 93

4 Transitions and DoD Interactions

ART project personnel frequently interact with DoD representatives, especially Lui Sha in his dual role as a member of the ART project and the SEI. Dr. Sha is deeply involved with transitioning rate monotonic scheduling theory to industry and government. His efforts include:

- Working with MITRE Corporation on the use of analytic redundancy in airborne radar systems,
- Chairmanship of the real-time task working group of the IEEE Futurebus+ standards committee,
- Interaction with the Navy NGCR,
- Named Chairman of the Board of Visitors of RICIS, an R&D center established by NASA and NASA JSC at University of Houston at Clearlake
- Coordinated the real-time version of POSIX,
- Worked with IEEE 802.6 standards group to develop a real-time capability,

Principal Investigator Names:

J. Lehoczky	(412) 268-8725	jpl@k.cs.cmu.edu
L. Sha	(412) 268-5875	lrs@sei.cmu.edu
M. Bodson	(412) 268-3898	bodson@galley.ece.cmu.edu
R. Rajkumar	(412) 268-8707	rr@sei.cmu.edu

PI Institution: Carnegie Mellon University
Contract title: Real-Time Fault Tolerant Computer Systems
Contract Number: N00014-92-J-1524
Reporting Period: 1 Oct 92 - 30 Sep 93

5 Software and Hardware Prototypes

An important part of this project is laboratory experimentation to empirically test the analytic redundancy approach to fault tolerance. Two distinct experimental systems are being developed, one in the CMU ECE LASIP laboratory and the other in the Real-Time Systems Laboratory. The former includes a ball and beam control experiment, that emphasizes the development and implementation of complex control algorithms and the development of the optimal control performance over the widest possible system state space. The latter experimental system emphasizes the development of a software architecture to support the simplex architecture, the real-time control of multiple devices, the integration of scheduling theory into the architecture and eventually the creation of a distributed control testbed. The SEI hardware and software prototypes have been demonstrated at the August 1993 SEI Symposium and at the Third Workshop on Responsive Systems. The CMU ECE LASIP prototype was demonstrated at the May 1993 Carnegie Institute of Technology (CIT) Research Review.