# The Design and Construction of Deadlock-Free Concurrent Systems

Jeremy Malcolm Randolph Martin

Thesis submitted for the degree of D. Phil to the School of Sciences in the University of Buckingham 1996

**Abstract**
**The Design and Construction of Deadlock-Free Concurrent Systems**
**Jeremy Martin**

It is a difficult task to produce software which is guaranteed never to fail, but it is a vital goal for which to strive in many real-life situations. The problem is especially complex in the field of parallel programming, where there are extra things that can go wrong. A particularly serious problem is deadlock. Here we consider how to construct systems which are guaranteed deadlock-free by design.

Design rules, old and new, which eliminate deadlock are catalogued, and their theoretical foundation illuminated. Then the development of a software engineering tool is described which proves deadlock-freedom by verifying adherence to these methods. Use of this tool is illustrated with several case studies.

The thesis concludes with a discussion of related issues of parallel program reliability.

# Acknowledgements

I am indebted to my supervisors Ian East and Sabah Jassim for their guidance, encouragement and enthusiasm for science. I have also benefited greatly from discussions with their former colleague John Rowe. My thesis is based largely on previous work and ideas of Bill Roscoe and Peter Welch, both of whom have been very helpful.

I am very grateful to my sister, Clare, who originally suggested to me the idea of studying for a doctorate and put me in touch with my supervisors. She also provided me with much useful background material. The University of Buckingham has proved a very pleasant environment where to work, with excellent facilities. I must also thank my employers, Oxford University Computing Services, for giving me time off to study.

Many thanks are due to my wife, Nathalie, who often found that although my body was present my mind was elsewhere. Thanks also to my children Adrian, Alex (who popped up half way through) and Clarisse (who popped up right at the end) for all the fun that we have had.

This thesis is dedicated, with love, to the memory of Phyllis Amy Martin, 1906 – 1994.

# Contents

# List of Figures

# List of Tables

# Declaration

I would like to draw attention to the following material contained within this thesis which I believe to be original.

**Chapter 2:** Theorems 7 and 9 are new results which generalise a theorem of A. W. Roscoe and N. Dathi and several theorems of P. H. Welch. Theorem 7 forms part of a joint publication:

J. Martin, I.East and S. Jassim *Design Rules for Deadlock-Freedom*, Transputer Communications, September 1994.

The definition of the Client-Server Protocol, and the results which follow, are a new formal adaptation of informal ideas due to Welch, G. R. R. Justo and C. J. Willcock. The Extended Resource Allocation Protocol (rule 11) is also new.

**Chapter 3:** Apart from the section which describes the normalisation of transition systems, this chapter is based entirely on original work.

**Chapter 4:** The first two case studies considered are original implementations of existing algorithms. The third is an original analysis of a published algorithm which reveals a deficiency and proposes a solution to this problem.

To the best of my knowledge, none of this material has ever previously been submitted for a degree in this or any other university.