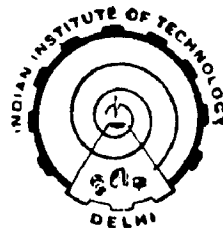


**FAIL SAFE SIGNAL PROCESSING TECHNIQUES
USING MICROPROCESSORS AND APPLICATION TO
DESIGN AND DEVELOPMENT OF
ROUTE INTERLOCKING SYSTEM FOR RAILWAYS**

by
M. R. VERMA

A Thesis submitted to the
Indian Institute of Technology, Delhi
for the award of the degree of
DOCTOR OF PHILOSOPHY



Department of Electrical Engineering
INDIAN INSTITUTE OF TECHNOLOGY, DELHI
NEW DELHI-110016
April 1987

to Rita, my wife

CERTIFICATE

This is to certify that the thesis entitled "Fail safe signal processing techniques using microprocessors and application to design and development of route interlocking system for railways", being submitted by M.R.Verma to the Indian Institute of Technology, Delhi, for the award of the degree of Doctor of Philosophy, is a record of bonafide research work carried out under my supervision. The results contained in this thesis have not been submitted for the award of any degree or diploma.

Vinod Chandra

(Vinod Chandra)

14.4.1987

Assistant Professor,
Department of Electrical Engineering,
Indian Institute of Technology,
New Delhi 110016

ACKNOWLEDGEMENT

I am extremely grateful to my supervisor, Dr. Vinod Chandra for his guidance and constant encouragement during the work.

My thanks are due to Prof. N. K. Nanda, Electronics and Communication Engineering Department, University of Roorkee for his valuable suggestions from time to time.

I am thankful to Prof. A. B. Bhattacharya, Head, Centre for Applied Research in Electronics for allowing me to use the facilities of the Centre.

The project was supported financially by the Information Planning and Analysis Group, Electronics Commission, Department of Electronics, Govt. of India.

I am also thankful to Shri V. Ramasamy, Executive Director (S & T), Railway Board for his support and encouragement. My thanks are also due to Shri M. K. Bapat, Ex Director (S & T), R.D.S.O., Lucknow for his useful suggestions.

My thanks are due to Shri M. Subramanian and Shri M. R. Muralidhar for their valuable help.

My thanks to Shri K. R. Bobal, Shri R. P. Kapoor and Mrs. R. K. Mansukhani for bringing out the thesis in this form.

My special thanks are due to my wife Rita for giving me the moral support during the work.

MR Verma
(M. R. VERMA)

ABSTRACT

The thesis deals with design and development of a real time control system FIRM (Fail safe Interlocking system for Railways using Microprocessors) for control of trains in a station yard. Route interlocking is a critical application involving the safety of human lives. The design is based on fail safe principles where a fault in the system causes a safe reaction.

A new approach has been proposed for the design of fail safe systems. The approach is based on need based safety levels where different subsystems are implemented to the safety levels required by them. This reduces the system complexity and provides an increased standard of safety compared to the systems which are implemented to a uniform standard of safety. A simulator for the design validation of route interlocking systems has been described. The interlocking system for any given yard and its control environment can be simulated and fault can be injected at various levels.

The FIRM architecture employing dual hardware and software diversity of processors, and a number of hardware functional modules has been described. Development of an engineering prototype of FIRM, its laboratory testing, reliability and safety analysis, and experimental installation have also been discussed.

CONTENTS

| | |
|---|----|
| INTRODUCTION | xi |
| CHAPTER 1 FAULT TOLERANCE AND FAIL SAFE DESIGN TECHNIQUES | |
| 1.1 Introduction | 1 |
| 1.2 Definitions | 3 |
| 1.2.1 Basic Definitions | 3 |
| 1.2.2 Definitions pertaining to System Safety | 4 |
| 1.3 Redundancy Techniques | 7 |
| 1.3.1 Information Redundancy | 7 |
| 1.3.2 Hardware Redundancy | 7 |
| 1.3.3 Time Redundancy | 9 |
| 1.3.4 Software Redundancy | 9 |
| 1.4 Examples of some Fault Tolerant systems for Real Time Applications | 10 |
| 1.4.1 The STAR (Self Test And Repair) Computer | 10 |
| 1.4.2 SIFT (Software Implemented Fault Tolerance) | 11 |
| 1.4.3 FTMP (Fault Tolerant Multiprocessor Architecture) | 13 |
| 1.4.4 Agusta 129 | 14 |
| 1.4.5 C.vmp (Computer Voted Multiprocessor System) | 15 |
| 1.4.6 ESS (The Electronic Switching System) | 16 |
| 1.4.7 Pluribus | 17 |
| CHAPTER 2 ROUTE INTERLOCKING PRINCIPLES AND EXAMPLES OF ELECTRONIC INTERLOCKING SYSTEMS | |
| 2.1 Principles of Route Interlocking | 20 |
| 2.2 Advantages of Electronic Interlocking | 27 |

| | | |
|-----------|--|----|
| 2.3 | Dual Hardware Redundancy | 28 |
| 2.3.1 | The SIMIS System of Siemens | 29 |
| 2.4 | Triple Modular Redundancy | 31 |
| 2.4.1 | The Japan National Railway System | 31 |
| 2.4.2 | The British Railways System | 32 |
| 2.5 | Software Redundancy | 34 |
| 2.5.1 | The Ericsson System JZS 750 | 34 |
| 2.5.2 | The US & S System Microlock | 35 |
| 2.5.3 | The Vital Processor Interlocking System of GRS | 36 |
| 2.6 | Critical comparison of the various Techniques | 36 |
| | | |
| CHAPTER 3 | A SIMULATOR FOR DESIGN VALIDATION OF ROUTE INTERLOCKING SYSTEM | |
| 3.1 | Introduction | 42 |
| 3.2 | The Route Interlocking Simulator | 45 |
| 3.3 | The SPRINT Software | 47 |
| 3.3.1 | The SPRINT Data Structures | 47 |
| 3.3.2 | The SPRINT Program Structure | 52 |
| 3.3.3 | The SPRINT Program Description | 55 |
| 3.4 | SPRINT Application | 61 |
| 3.4.1 | Input Data Coding | 61 |
| 3.4.2 | Output Data generated by the Program | 63 |
| 3.4.3 | Other Applications of SPRINT | 65 |
| 3.5 | Macro Simulation of FIRM | 66 |
| | | |
| CHAPTER 4 | A NEW APPROACH TO THE DESIGN OF FAIL SAFE SYSTEMS | |
| 4.1 | Introduction | 69 |
| 4.2 | Levels of Safety | 71 |

| | | |
|--|--|-----|
| 4.3 | Hierarchical Transaction | 79 |
| 4.4 | The Security Kernel | 82 |
| 4.5 | Development of a Model for FIRM | 84 |
| 4.6 | Conclusion | 86 |
| CHAPTER 5 THE FIRM ARCHITECTURE AND ITS HARDWARE IMPLEMENTATION | | |
| 5.1 | Introduction | 88 |
| 5.2 | The FIRM Architecture | 92 |
| 5.2.1 | The Sequence Controller and the Processor Modules | 92 |
| 5.2.2 | The See-Saw Mode | 94 |
| 5.2.3 | A Typical Functional Module | 98 |
| 5.3 | Micro Specifications and their Validation | 101 |
| 5.4 | Conclusion | 108 |
| CHAPTER 6 THE FIRM SOFTWARE | | |
| 6.1 | Introduction | 111 |
| 6.2 | The FIRM Program Structure | 112 |
| 6.3 | The FIRM Data Structure | 114 |
| 6.4 | The Software Routines | 116 |
| 6.4.1 | The Control Task | 118 |
| 6.4.2 | The Input / Output Routines | 125 |
| 6.4.3 | The Supervisory Program | 126 |
| 6.5 | Conclusion | 128 |
| CHAPTER 7 DEVELOPMENT AND EXPERIMENTAL INSTALLATION OF AN ENGINEERING PROTOTYPE OF FIRM | | |
| 7.1 | Introduction | 130 |
| 7.2 | The FIRM Engineering Prototype | 132 |

| | | |
|-----------|--|-----|
| 7.3 | Reliability and Safety Analysis of the FIRM Prototype | 135 |
| 7.3.1 | Reliability Analysis | 138 |
| 7.3.2 | Safety Analysis | 140 |
| 7.4 | Conclusion | 142 |
| CHAPTER 8 | CONCLUSION AND SCOPE FOR FUTURE WORK | 144 |