

Contents

Introduction

Introduction	
B. RANDELL	1

Chapter 1. System Reliability

Introduction	
S. K. SHRIVASTAVA	5
Software Fault Tolerance Terminology Proposals	
T. ANDERSON and P. A. LEE	6
System Structure for Software Fault Tolerance	
B. RANDELL	14
Operating Systems: The Problems of Performance and Reliability	
B. RANDELL	37

Chapter 2. Recovery Blocks

Introduction	
S. K. SHRIVASTAVA	51
A Program Structure for Error Detection and Recovery	
J. J. HORNING, H. C. LAUER, P. M. MELLIAR-SMITH and B. RANDELL	53
A Reconsideration of the Recovery Block Scheme	
P. A. LEE	69
Recovery Blocks in Action: A System Supporting High Reliability	
T. ANDERSON and R. KERR	80
Sequential Pascal with Recovery Blocks	
S. K. SHRIVASTAVA	102
Fault Tolerant Sequential Programming Using Recovery Blocks	
S. K. SHRIVASTAVA and A. A. AKINPELU	112
A Recovery Cache for the PDP-11	
P. A. LEE, N. GHANI, and K. HERON	115

Recovery and Crash Resistance in a Filing System	
J. S. M. VERHOFSTAD	126

Chapter 3. Exception Handling

Introduction	
S. K. SHRIVASTAVA	141
Software Reliability: The Role of Programmed Exception Handling	
P. M. MELLIAR-SMITH and B. RANDELL	143
Exception Handling and Software Fault Tolerance	
F. CRISTIAN	154
Robust Data Types	
F. CRISTIAN	173
Systematic Detection of Exception Occurrences	
E. BEST and F. CRISTIAN	208
Safe Programming	
T. ANDERSON and R. W. WITTY	238

Chapter 4. Concurrent Systems

Introduction	
S. K. SHRIVASTAVA	247
Process Structuring, Synchronisation and Recovery Using Atomic Actions	
D. B. LOMET	249
A Formal Model of Atomicity in Asynchronous Systems	
E. BEST and B. RANDELL	266
Reliable Resource Allocation Between Unreliable Processes	
S. K. SHRIVASTAVA and J.-P. BANÂTRE	298
Concurrent Pascal with Backward Error Recovery: Language Features and Examples	
S. K. SHRIVASTAVA	322
Concurrent Pascal with Backward Error Recovery: Implementation	
S. K. SHRIVASTAVA	344
A Framework for Software Fault Tolerance in Real-Time Systems	
T. ANDERSON and J. C. KNIGHT	358

Chapter 5. Multilevel Systems

Introduction
S. K. SHRIVASTAVA 379

A Model of Recoverability in Multilevel Systems
T. ANDERSON, P. A. LEE and S. K. SHRIVASTAVA 381

The Provision of Recoverable Interfaces
T. ANDERSON and P. A. LEE 396

Structuring Distributed Systems for Recoverability and Crash Resistance
S. K. SHRIVASTAVA 410

Chapter 6. Distributed Systems

Introduction
S. K. SHRIVASTAVA 433

Consistent State Restoration in Distributed Systems
P. M. MERLIN and B. RANDELL 435

Recovery Control of Communicating Processes in a Distributed System
W. G. WOOD 448

A Dependency Commitment and Recovery Model for Atomic Actions
S. K. SHRIVASTAVA 485

Fail-Safe Extrema-Finding in a Circular Distributed System
E. BEST and F. PANZIERI 498

The Design of a Reliable Remote Procedure Call Mechanism
S. K. SHRIVASTAVA and F. PANZIERI 504

Reliable Remote Calls for Distributed Unix: An Implementation Study
F. PANZIERI and S. K. SHRIVASTAVA 518

The Newcastle Connection or UNIXes of the World Unite
D. R. BROWNBRIDGE, L. F. MARSHALL and B. RANDELL 532

Recoverability Aspects of a Distributed File System
M. JEGADO 550

Chapter 7. Fault Tolerance and System Structuring

Fault Tolerance and System Structuring
B. RANDELL 563