Foreword

Despite means of fault prevention such as extensive testing or formal verification, errors inevitably occur during system operation. To avoid subsequent system failures, critical distributed systems, therefore, require engineering of means for fault tolerance. Achieving fault tolerance requires some redundancy, which, unfortunately, is bound to limitations. Appropriate fault models are needed to describe which types of faults and how many faults are tolerable in a certain context. Previous research on distributed systems has often introduced fault models that abstract too many relevant system properties such as dependent and propagating component failures. In this research work, Timo Warns introduces new structural failure models that are both accurate (to cover relevant properties) and tractable (to be analyzable). These new failure models cover dependent failures (for instance, failure correlation by geographic proximity) and propagating failures (for instance, propagation by service utilization). To evaluate the new failure models, Timo Warns shows how some seminal problems in distributed systems can be solved with improved resilience and efficiency, as compared to existing solutions.

Particularly, the textbook-style introduction to distributed systems and the rigorous presentation of the new failure models and their evaluation may serve as an example for other software engineering research projects – which is why this book is a valuable addition to both a researcher's and a student's library.

Wilhelm Hasselbring