Preface

The accelerated development of digital technologies has led to the widespread use of software in all aspects of our life. Nowadays, the control over critical infrastructures such as power plants, transportation, telecommunications, health, and banking systems leans significantly on digital systems. Hence, we are constantly increasing our reliance on computers. The degree of reliance that can be justifiably placed on computer-based systems is expressed by the notion of dependability.

Dependability encompasses such vital characteristics of the system as safety - the non-occurrence of catastrophic consequences for the system operational environment, security - the non-occurrence of unauthorized disclosure of information, integrity - the non-occurrence of inadequate information alteration, availability - the readiness for correct service of the system, and reliability - the property of the system to continuously provide service.

The complexity of modern software-intensive systems poses the greatest threat to dependability. Furthermore, software - the most complex system component - is recognized to be the most error-prone part of the system. Indeed, cost and time pressure as well as immature development methods often lead to poor software quality, and consequently, to a low degree of dependability on software-intensive systems. Therefore, it is important to understand how dependability is manifested in software-intensive systems, how it is developed, and how it can be enhanced at various levels in systems and organizations. With this study, dependability can be associated to increasing the strategic capabilities of systems and organizations as well as their performance.

OBJECTIVE

The main purpose of this book is to offer a selective overview of the dependability research, from engineering various software-intensive systems to validating existing IT-frameworks and solving generic and particular problems related to the dependable use of IT in our society. We seek to uncover the existing research on the topic as well as the key challenges associated with the engineering of dependable IT systems in the future.

ORIGINS

This book has sprung from the initiative of the NODES (Network On DEependable Systems) network – a Nordic and Baltic education network in dependability, financed by Nordforsk during 2007-2011. The network consists of researchers from the Technical University of Denmark, the Tallinn University of...
Technology, Estonia, the SINTEF ICT Research Centre and the University of Oslo, Norway, the Linköping University, Sweden, and the Åbo Akademi University, Finland. One of the objectives of NODES is to promote cooperation as well as ensure a wide dissemination of the Nordic and Baltic research results in the dependability topic. Part of the material of this book seeks to address this objective and is thus based on research results initially presented at the yearly NODES workshops during 2007-2010. Complementing the work of the NODES researchers, we have invited submissions from well-known researchers in the dependability area. Each chapter was peer-reviewed by two reviewers, thus ensuring the scholarly value of the book. The result consists of 11 chapters detailing the NODES research and 8 chapters from other researchers working in the dependability field.

TARGET AUDIENCE

This book is intended for individuals interested in the designing, operation, maintenance, and management of dependable software-intensive systems at all levels. The target audience thus includes engineers, researchers, scientists, practitioners, managers, developers, educators, and students who are looking for the state-of-the-art information about engineering dependability. In particular, IT-systems developers and technology innovators can take advantage of the leading-edge research ideas, results, and case studies described in the book. The combination of theoretical and practical content will enable, at the same time, a broader audience to take advantage of the book. It will also enable readers to draw parallels with their own work or research and apply or advance the research efforts of others in their own projects. Readers will gain by having access to an original, timely, comprehensive reference work on research and applications in the area of dependability.

POTENTIAL

Another objective of the NODES network is to establish a Dependability Curriculum to be employed in postgraduate studies. The scholar and timely content of this book can thus contribute to establishing the field of dependability as an engineering discipline in the Nordic region, as well as globally. It can stimulate the interest of prospect engineers and acting practitioners to the subject as well as supplement various courses in dependability curricula. Hence, the potential use of the book is envisioned as both a scholarly library reference as well as a post-graduate textbook.

OVERVIEW

The aim of the book is to offer a selected view on dependability. The chapters focus on novel results and applications that have a potential impact on the analysis, design, and maintenance of dependable software-intensive systems. The order of the chapters in the book is topical, as we have organized them in five sections as follows: “Modeling for Dependability,” “Ensuring Dependability,” “Security Fundamentals,” “Applied Security,” and “Analysis of Risks and Dependability.” In the following, we introduce each section and chapter in some detail.
In Section 1, “Modeling for Dependability,” we collect several approaches for modeling dependability aspects. The modeled aspects concern fault management systems, exception handling, and (network) availability. The modeling approaches are very different, from a case-study based one, to a theoretical approach, and to an example-based description.

Fault management systems typically consist of a loop involving multiple steps. The authors of Chapter 1 argue via six case studies that it is inefficient and ineffective to only improve individual steps of fault management systems. Instead, they propose a holistic approach that addresses the interdependencies and communication among all the phases involved in the fault management systems.

Exception handling is an important mechanism in the design of dependable systems as it allows preserving the original design in the presence of possibly faulty components, allows the treatment of rare and undesired cases, as well as can be used to address imperfections in software. In Chapter 2, the author develops a theory of exception handling. This is modeled with the so-called “try-catch” statements, whose semantics is based on weakest exceptional preconditions.

Availability is one of the attributes describing dependability as “readiness for correct service”. In Chapter 3, the authors present a formal method-based model for network availability targeted at distributed applications. The modeling approach is constructive and is based on the refinement concept.

The chapters grouped in Section 2, “Ensuring Dependability,” study several dependability aspects and their satisfiability in different lifecycle stages, from capturing dependability requirements, to ensuring them throughout the stepwise development, to testing existing systems for dependability. The methods and frameworks employed and extended vary from formal ones such as Event-B and contract-based development, to semiformal ones such as Simulink, to theoretical ones such as extended finite state machines. The applicability area addressed is also rich, from multi-agent systems, to control systems, to integrated circuits.

In Chapter 4, the authors address the dependability of large-scale, dynamically-reconfigurable multi-agent systems, in which agents cooperate to achieve a common goal. In particular, they study the scalability and reliability of these systems. The Event-B method is employed to formally validate the design as well as to ensure these properties.

The focus of Chapter 5 is on studying the safety and fault tolerance requirements for software-intensive control systems. The authors propose the integration of the Failure Modes and Effect Analysis (FMEA) method with the Event-B formal development tools. Their approach is also illustrated with a case study of a heating control system.

FPGA (Field Programmable Gate Array)-based systems offer an attractive technology for implementing systems-on-chip (SoC), at the core of our IT-based society. In Chapter 6, the authors propose a design method for FPGA-based systems with the support of a formal method. Their design is based on stepwise development and is applied to an aircraft anti-icing case study.

An alternative way of studying the dependability of systems is via testing. In Chapter 7, the authors propose a reactive planning tester that aims to fill the gap among various other more extreme planning strategies for testing. The systems under study are non-deterministic and the proposed tester is applied to a case study of the city lighting controller.

In Chapter 8, the authors address the dependability of a digital hydraulic controller. They propose the application of contract-based design in Simulink (a graphical language for the model-based design of control systems) for this, with a semi-formal approach where contracts influence the system structure and the interface specifications. An analysis of the impact of the contracts on the development process and on the system quality is also provided.
Section 3, "Security Fundamentals," addresses the modeling of security requirements for contemporary software-intensive systems from different points of view. Namely, we first learn about two different, graphically-aided, thorough technical approaches addressing security and then follow the investigation of analyzing security both from a classical context and a dependability-based context. One approach is aimed at automated analysis, another approach is theoretically defined, while the third is of a survey type.

Security is among the topics addressed by numerous researchers, resulting in various security-enhancing techniques. In Chapter 9, the authors propose a graphical language that can be used in place of four existing modeling languages for security. The proposed language has a number of advantages, such as allowing models to be used in automated analysis and allowing models to be transformed to and from the four earlier languages.

In Chapter 10, the authors present a method for software development that considers security requirements throughout the entire software development lifecycle. Security properties of earlier abstract models are preserved during transformations to more concrete models. The method proposes a rigorously defined language based on UML state machines and is illustrated via a running example.

Although security is an attribute of dependability, the authors of Chapter 11 argue that a common framework for specifying both security and dependability is missing. Several challenges for this are identified and analyzed. Based on these challenges, the authors propose a definition to the notion of system security that extends the classical notion of dependability.

In Section 4, "Applied Security," we group several approaches dealing with the practical usage of this dependability attribute. One approach is a survey, another approach extends an existing methodology, and the other approach introduces a novel-IT framework. The addressed applicability area is that of mobile devices, smart cards, as well as general software-intensive systems.

As mobile devices are nowadays widespread, their security guarantees are of an utmost interest. In Chapter 12, the authors survey the state-of-the-art regarding the security of mobile devices and compare their various features. This study is highly relevant as the mobile devices are becoming more and more the digital image of their owners, and hence, are likely to be used instead the desktops and laptops in the near future.

Smart cards are a very widespread platform nowadays and they seem not to be exploited to their full potential. In Chapter 13, the authors study the security requirements for open, multi-application smart cards. They employ the Security-by Contract paradigm, initially devised for mobile devices, to address the security requirements of smart cards.

While the security of software intensive systems is important, it is also often costly. In Chapter 14, the authors present SecInvest, a security investment support framework based on Bayesian Belief Networks. This framework proposes to explore alternative solutions and decide based on the investigation whether to invest in security or take the associated risk. SecInvest can thus help to transform security from a cost to an asset.

In Section 5, "Analysis of Risks and Dependability," we gather five chapters dealing with the modeling and especially with the assessment of risks and other aspects of dependability. The approaches in these chapters are quite different, so that they extend or integrate various methodologies, they survey the literature of interest, or they address a certain application area. The chapters employ and extend a wide range of frameworks and methods such as STAIRS, CORAS, weighted dependability trees, general refinement patterns, stochastic activity networks, Event-B, and the PRISM model checker.

In Chapter 15, the authors address the modular system development process, where the upgrade of any system component may pose risks for the safety and security of the entire system. A model-based risk
analysis method is first adjusted to be applied component-wise. Then, the authors propose a stepwise-integration of the component-based risk analysis method into a component-based development process.

The uncertainty due to the lack or inaccuracy of the input data is another risk to be taken into account. In Chapter 16, the authors address the uncertainty occurrence in the input data for approaches that employ weighted dependency trees for system analysis. A systematic literature review is provided on handling uncertainty; while useful in itself, this survey can also serve as a resource for identifying the adequate approach for various developers.

Developing software-intensive systems is a challenging and resource-consuming activity, hence, it helps having a control strategy over it. In Chapter 17, the authors propose the application of general refinement patterns to assist the design decisions. Moreover, they propose measures for the evaluation of the design progress of the system.

The congestion of traffic is a well-known problem in the big cities and on various highways. However, the agglomeration of so many vehicles containing numerous wireless network devices enables the development of innovative applications, for instance aimed at improving the traffic safety. In Chapter 18, the authors address the dependability modeling and evaluation of two such applications.

While refinement-based approaches are powerful in ensuring the stepwise correctness of models, they lack the tools for verifying other properties, such as that of achieving a sufficient level of dependability. The authors of Chapter 19 take this challenge and propose probabilistic model checking methods for addressing it. Combining probabilistic model checking with probabilistic refinement thus combines logical reasoning about functional correctness with probabilistic reasoning about dependability.

It is our hope that this book will reach its aim and will be of benefit both to the NODES researchers and to the wider community of researchers and practitioners in the dependability field.

Luigia Petre  
Åbo Akademi University, Finland

Kaisa Sere  
Åbo Akademi University, Finland

Elena Troubitsyna  
Åbo Akademi University, Finland

Turku, December 2010

ENDNOTES

1  http://crest.abo.fi/NODES/index.htm
2  http://www.nordforsk.org/en?set_language=en
3  http://crest.abo.fi/NODES/index_files/Page338.htm