Chapter 1
Introduction

Alexander Romanovsky and Martyn Thomas

Abstract The aims of the book are explained in the context of current demands for cost-effective and dependable software and the methods that are typically employed in the software industry. The target audiences are identified and the contribution that the book could make to each audience is described. The structure of the book is described in outline.

1.1 Deployment of Formal Methods

The commercial and industrial uses of computer-based systems are growing in complexity every year, and this is causing managers and developers to look for new ways to improve productivity and dependability. Software is already pervasive in products and services that are vital to the safe, secure and efficient working of most parts of industry, commerce, health, transport and leisure. For more and more systems, it is essential that they can be developed cost-effectively and that their users can have high confidence that they will work safely and reliably. This is an engineering task.

All engineers use mathematically formal methods. They use methods that exploit well-established scientific results, embedded in mature engineering processes, because such methods allow a rigour of expression and analysis that is essential in tackling projects of industrial scale reliably and cost-effectively, and in gaining confidence that what is being built will be fit for its intended purpose. Formal methods, in this sense, are what distinguishes engineering disciplines from less professional ways of working.

Professional engineers are rightly conservative; they do not rush to adopt new methods in place of their traditional, trusted ways of working: quite reasonably they experiment on pilot projects first, and if they can, they learn from other en-

A. Romanovsky (✉)
Newcastle University, Newcastle upon Tyne, UK
e-mail: alexander.romanovsky@ncl.ac.uk

M. Thomas
Martyn Thomas Associates, London, UK
e-mail: martyn@thomas-associates.co.uk

A. Romanovsky, M. Thomas (eds.), *Industrial Deployment of System Engineering Methods*, DOI 10.1007/978-3-642-33170-1_1,

gineers. For civil engineers this process has been going on for centuries, at least since Archimedes, and mechanical, electrical, and chemical engineers have all built science into their methods gradually and over more than a century.

The software industry worldwide is still immature compared with other engineering industries. The most widely applied methods and tools use little of the computer science of the past 40 years, and software contains many unnecessary errors as a result. Most of these errors cannot be corrected by testing the software and fixing the failures in the way that mechanical systems and structures can be tested and fixed, because digital systems are so complex that testing every state that could contain an error would take an impractical amount of time and resources. As the computer scientist Edsger Dijkstra remarked forty years ago, testing software can reveal the presence of bugs but never their absence.

For these reasons, new, science-based methods are increasingly important for engineers building computer-based systems. These methods offer high productivity *and* high dependability by reducing the opportunity for introducing errors and by automating most of the task of finding the residual errors and showing that the design is correct. The *DEPLOY* project on *Industrial Deployment of System Engineering Methods Providing High Dependability and Productivity* (http://www.deploy-project.eu/) set out to collect the experience of introducing formal methods into several very different application domains and to make that experience available as widely as possible.

This book is the result. It is a book of experience, written for

- technical leaders in industry who may be thinking about the possible introduction of formal methods;
- early and mid-career professionals who may need to assess the importance of these methods for their future careers, and
- system and software engineers developing important systems.

We hope that the book will also prove valuable to

- standards makers and regulators;
- academics who can make use of the examples and experience for teaching purposes;
- undergraduate and postgraduate students, for understanding the industrial context for the methods they are studying, and
- the developers of tools and methods who may not have experience in the practical issues that determine whether their work will be usable in a real commercial or industrial environment.

1.2 Book Structure

This is not a tutorial on any particular method, although Event-B was widely used in the DEPLOY project and we have included a description of and introduction to it in Appendix A. Inevitably, much of the experience that we report comes from the

use of Event-B and the Rodin toolset, but we have sought to make the conclusions as independent of particular methods as possible so that the lessons from DEPLOY are widely applicable. We see this as the start of a process that will continue to accumulate and disseminate experience; how the reader can contribute and where s/he can find further evidence is explained in Appendix B.

The structure of the book is as follows:

Chapter 2 describes the aims and approach of DEPLOY, to show the scale of the work on which our experience and conclusions are based and to provide the context for later chapters;

Chapters 3–9 describe the experiences of introducing or extending the use of formal methods in particular application domains (electronic commerce, satellite systems, rail transportation, automotive, microprocessor design and other safety-related domains);

Chapter 10 describes the results of a large survey of the use of formal methods in industry and compares our industrial deployment projects with experience acquired elsewhere;

Chapter 11 explores the issues that arise when increasingly formal methods are introduced into industrial companies operating within their own context of existing methods and tool chains, regulatory requirements, policies for reuse and intellectual property, and other practical considerations;

Chapter 12 shows the sorts of issues that arise when new methods are first used on real, industrial projects from the perspective of the tool developers. It describes the enhancements that have to be made to the methods and the supporting toolset so that they have the power to support teams of engineers with very particular needs and constraints;

Chapter 13 explains how we addressed training and technology transfer more generally, and explains how and why we would do things differently now;

Chapter 14 looks at the ecosystem that is required before an industrial company can adopt new methods as the basis for product development and support, possibly over decades of service lifetime, and describes what has been created to provide continuing support for the growing community of companies using Event-B and Rodin;

Chapter 15 summarises what we have learnt and draws some conclusions;

Appendix A provides a description of and a brief tutorial on Event-B to facilitate understanding of the examples that occur in several of the chapters;

Appendix B describes our online evidence repository, the way in which evidence was collected and how readers can contribute their own experiences. It provides examples of Case Studies and Frequently Asked Questions.

Acknowledgements We are grateful to Ronan Nugent from Springer for supporting the idea of this book and helping us with its publication, and to Alexei Iliasov for helping us in dealing with LaTeX formatting.