Wiley Series in Systems Engineering and Management • Andrew P. Sage, Series Editor

Verification, Validation, and Testing of Engineered Systems

Avner Engel

WILEY

VERIFICATION, VALIDATION, AND TESTING OF ENGINEERED SYSTEMS

WILEY SERIES IN SYSTEMS ENGINEERING AND MANAGEMENT

Andrew P. Sage, Editor

A complete list of the titles in this series appears at the end of this volume.

VERIFICATION, VALIDATION, AND TESTING OF ENGINEERED SYSTEMS

AVNER ENGEL

WILEY
A JOHN WILEY & SONS, INC., PUBLICATION

Published by John Wiley & Sons, Inc., Hoboken, New Jersey
Published simultaneously in Canada

Editorial contribution—Dr. Peter Hahn

Library of Congress Cataloging-in-Publication Data:

Engel, Avner.
Verification, validation, and testing of engineered systems/Avner Engel.
p. cm.—(Wiley series in systems engineering and management)
Includes bibliographical references and index.
ISBN 978-0-470-52751-1 (cloth)
1. Quality assurance. 2. Quality control. 3. Systems engineering. 4. System failures (Engineering)–Prevention. 5. Testing. I. Title.
TS156.6.E53 2010
658.5′62—dc22
2009045885

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

To my parents:
Josef Engel, Lea Engel and Tova Engel

and my revered teachers:
Dr. Itzhak Frank, Professor Jerry Weinberg and Professor Miryam Barad

Contents

Preface

Systems testing is carried out one way or another in all development and manufacturing projects, but seldom is this done in a truly organized manner and no book currently available describes the process in a comprehensive and implementable form. Along the same line of thinking, virtually no systems Verification, Validation, and Testing (VVT) research is conducted throughout the academic world. This is especially odd, since some 50–60 percent of a systems development cost is expended on either performing VVT activities or correcting system defects during the development process or during the life of the developed product.

This book attempts to put together a comprehensive compendium of VVT activities and corresponding VVT methods for implementation throughout the entire lifecycle of systems (i.e. Definition, Design, Implementation, Integration, Qualification, Production, Use/Maintenance and Disposal). In addition, the book strives to alleviate the fundamental testing conundrum, namely: What should be tested? How should one test? When should one test? And, when should one stop testing? In other words, how should one select a VVT strategy and how should it be optimized? Although early quality pioneers (e.g., Juran in the 1950s) proposed a conceptual quality cost model, no one proposed a quantitative and credible model which can be used to answer the above questions. This book provides such a model, together with data from a real-life project, which show significant potential savings in either cost, time or both. The book is organized in three parts:

The first part (Chapter 1) provides introductory material about systems and VVT concepts. This part presents a comprehensive explanation of the role of VVT in the process of engineered systems throughout their lifetime and explains the essence of systems VVT and the linkage between VVT and systems development, manufacturing, use/maintenance and retirement.

The second part (Chapters 2–5) is essentially a reference guide, describing typical systems VVT activities which may be conducted during an engineered systems lifetime. A reciprocal and comprehensive set of methods for carrying out these VVT activities is also provided. More specifically, the second part describes 40 systems development VVT activities (Chapter 2) and 27 systems post-development activities (Chapter 3). Corresponding to these activities, this part also describes 17 non-testing systems VVT methods (Chapter 4) and 33 testing systems methods (Chapter-5). In-text citations are provided wherever needed, usually within theoretical sections of the book. In addition, subchapters contain a set of citations for further reading. Readers will undoubtedly be able to absorb and implement some or all of this information in their daily work-life as systems or test engineers.

The third part of the book (Chapters 6–8) describes ways to model systems quality cost, time and risk (Chapter 6), as well as ways to acquire quality data and optimize the VVT strategy in the face of funding, time and other resource limitations and in accordance with different business objectives (Chapter 7). Finally, this part describes the methodology used to validate the quality model along with examples describing a system's quality improvements (Chapter 8). Readers will be able to learn how to collect and aggregate quality data within their organizations. In addition to becoming familiar with this significant information, readers will be introduced to four Cost, Time and Risk Models. Systems engineers are encouraged to use these models in order to optimize their VVT strategies, thereby realizing as much as ten percent reduction in engineering manpower or schedule in the development of engineered systems. The software is freely available to readers via an Internet site (**http://www.adisw.com**) in binary form under Beta release conditions.

Fundamentally, this book is written with two categories of audience in mind. The first category is composed of VVT practitioners, including Systems, Test, Production and Maintenance engineers as well as first and second line managers. These people may be employed by development and manufacturing industries (e.g., Aerospace, Automobile, Communication, Healthcare equipment, etc.), by various civilian agencies (e.g. NASA, ESA, etc.) or with the military (e.g., Air force, Navy, Army, etc.). This book may also be used as a supplemental graduate level textbook in courses related to systems VVT. Typical academic readers may be graduate school students or members of Systems, Electrical, Aerospace, Mechanical, and Industrial Engineering faculties. This book may be fully covered in two to three semesters (although parts of the book may be covered in one semester). University instructors will most likely use the book to provide engineering students with knowledge about VVT, as well as to give students an introduction to formal modeling and optimization of VVT strategy.

ACKNOWLEDGMENTS

Many friends and colleagues have contributed generously to the writing of this book. To all of them, I would like to express my sincere gratitude and appreciation. In particular, I wish to thank Dr. Peter Hahn, who has been a tireless and devoted companion in the book-writing project from its inception. He edited the original manuscript and contributed numerous and valuable suggestions to improve the book.

The SysTest project, partially funded by the European Commission (see Appendix A), focused my attention onto systems verification, validation and testing. My appreciation goes to all the consortium members and in particular to professor Eduard Igenbergs of the Technical University of Munich, who provided both a philosophical foundation and ample encouragement, and to Professor Tyson Browning of the Texas Christian University, part of whose scientific writings and words of wisdom are embedded in this book. The Advanced System and Software Engineering Technology (ASSET) group at Israel Aerospace Industries (IAI) was a significant milieu for learning and expanding. My special gratitude goes to ASSET group leader, Dr. Michael Winokur. I am also grateful to Shalom Shachar of the IAI/Lahav Division, who conducted the SysTest pilot project at IAI, helped in collecting field data and became a sounding board and advisor regarding many aspects of the VVT quantitative model. In addition, I am beholden to Michael Garber of Adi Mainly Software (AMS), who developed the VVT-Tool software package which embodies the VVT model.

Several close friends were involved in creating this book. In particular, I would like to mention Avi Egozi and Arie Rokach, who suggested the book project in the first place and provided advice throughout the writing process. Also my sincere appreciation goes to Menachem Cahani (Pampam), who volunteered to illustrate several caricatures in the book. I also am genuinely indebted to Professor Miryam Barad of the Tel-Aviv University, an esteemed teacher who taught me how to conduct scientific research and write about it.

Most of all, my deepest thanks go to my wife, Rachel, and my children, Ofer, Amir, Jonathan and Michael, who encouraged my book efforts with advice, patience and love,

Avner Engel
Tel-Aviv, Israel

Part I

Introduction

Chapter **1**

Introduction

1.1 OPENING

This chapter serves as motivation for learning about systems Verification, Validation and Testing (VVT) as well as a map for using the book as a reference source on this complex and multifaceted process. We emphasize here the multitude of reasons for applying VVT. It sets the tone for the subject matter we hope to cover. It gives the reader insight into the attitudes of the author and the care with which the book was prepared. A clear statement is made of the purpose for which the book has been written.

The book is a compendium of facts about systems VVT. In fact, we think little has yet been published that is as comprehensive on this subject. By listing the potential audience for the book, we hope to encourage its wide distribution and to increase among engineers, managers, academicians and students an appreciation of the benefits of rigorously applying VVT to almost every endeavor involving a product or service, be it for purposes commercial, private or public. This chapter contains the following elements:

Opening. This part provides a background, purpose and the intended audience of the book. In addition, it describes its structure and contents as well as the scope of application and some terminology descriptions.

VVT systems and process. This part introduces VVT systems and processes as components of engineered systems. In addition, it describes basic VVT definitions and elaborates on the fundamental VVT dilemmas. Also, this part describes modeling of systems and VVT lifecycle as well as modeling of VVT processes and risks as cost and time drivers.

Verification, Validation, and Testing of Engineered Systems, Avner Engel

Canonical systems VVT paradigm. This part introduces the concept of canonical systems VVT paradigm which includes phases of systems' lifecycle, views of systems and VVT aspects of systems.

Methodology application. This part introduces methodology application including VVT methodology overview, VVT tailoring and typical VVT documentation.

1.1.1 Background

The manufacturing industry used to be concerned with the design, development, production and maintenance of stand-alone products, whether simple or complex. Today, however, manufacturing has broadened its scope to include products, services or solutions that include a variety of components, integrate a large mix of technologies and involve both people and machines. It is this broad range of complex entities that we address in this book. The basic term we use for these complex entities is *engineered systems*. However, throughout this book, when appropriate, we will freely use terms such as *products* or *services*. The term engineered systems is distinguished from *systems* in the sense that the former is created by engineers who apply science and mathematics to find suitable solutions to problems.

Traditional and high-technology manufacturing industries are responding to the challenge to satisfy consumer needs and ensure competitive and sustainable growth by reducing time to market and customizing products (or expanding product ranges) while producing the required goods in the quantities demanded with the appropriate quality at reduced costs. For instance, in the automobile sector, the lead time for manufacturing a car at the beginning of the 1990s was five to six years, whereas today it is about two to three years and is estimated to be only 18 months in the near future. Therefore, controlling schedules, costs and quality in product development, manufacturing and maintenance remains a major challenge for today's industries. Increases in complexity, decreases in development budgets and shortened time to market for new products, services and solutions are leading developers to search for new ways of improving the quality of what they deliver by improving their technologies, processes, methodologies and tools.

The overall development process is only as strong as its weakest link. A critical and largely ignored link in this process is system VVT, which comprise vital activities and involve processes. A tool of systems engineering, VVT focuses on ensuring that engineered systems are delivered as error free as possible, are functionally sound and meet or exceed the user's needs. Often VVT is carried out as merely a vehicle for finding and eliminating errors. It can do much more than that. Today, many system developers perform VVT only in the test phase of the project, a late and highly constrained period in the product development cycle. As a result, increases in overall development time and costs associated with product rework often exceed 20% of expanded engineering efforts (Capers, 1996). Admittedly, balancing testing cost and schedule with quality is difficult. However, quality problems discovered later by the user can

necessitate expensive repairs and are likely to damage the reputation of the system or, worse, damage the reputation of the system's developer.

Given the fundamental role of VVT in achieving product quality and reducing waste, this book aims at rectifying two critical current VVT problems, namely, lack of comprehensive system VVT methodology and lack of a practical, quantitative VVT process model for selecting a VVT strategy to optimize testing cost, schedule and economic risk. This book, which to a large measure is based on the European Commission–supported SysTest project, was written in order to rectify these problems.

1.1.2 Purpose

One of the central objectives of this book is the creation of generic VVT methodology. This *VVT methodology* consists of a selection of VVT activities and methods which can be applied throughout the system lifecycle in different industrial application fields and can be tailored according to the individual project needs.

The VVT methodology delivers generic means for comprehensive cost-effective VVT in the industry. In addition, the objectives of this methodology are as follows:

- To cover the entire product lifecycles from the definition to the disposal of the system
- To supply tailoring rules for different industry domains (e. g. electronics/avionics, control systems, automobile, food packaging systems, steel production), development cycles and project types
- To specify activities and methods for VVT on the system level together with their interrelationship
- To define VVT strategies that can be used in a broad variety of industrial applications

1.1.3 Intended Audience

The VVT methodology described in this book is applicable to all regional and industrial sectors. Although system VVT is performed throughout industry, it has not become a topic for research within the international community either in industry or in academia. Therefore, the definition of a generic VVT methodology will provide comprehensive knowledge for many students and practitioners. This book was written for the reader who has a background knowledge of project management, systems engineering and quality assurance. Those who participate in system development will benefit from the material covered in this book. These include:

1. *Project Managers and VVT Managers.* This book can guide project and VVT managers in the methods they select, adapt and tailor for planning, control and tracking of projects.

2. *Quality Assurance (QA)/Quality Control (QC) Staff.* For QA and, QC staff, this book offers an overview of the system QA activities and methods available and their principal advantages and disadvantages. Quality assurance staff can apply the VVT methodology guidelines for the selection of VVT procedures and the estimation of process and product risks.
3. *Members of a VVT Team.* This book serves as an aid for test teams by providing them with an overview of useful procedures for conducting a VVT process within the context of system development projects and beyond. Thus, the VVT methodology guidelines of this book become a useful tool for categorizing VVT activities within the system lifecycle overall context and by referencing further information.
4. *System Developers and Maintainers.* This book is relevant for system developers in that they deliver insight into the measures of error avoidance and error detection. Developers can draw important conclusions about the functional domains of the system developed that are critical where VVT are concerned.
5. *Mechanical, Electronics and Software Designers.* Other specialists need this book in order to take VVT aspects into account when they determine structures and select the technologies for system development, production and maintenance. This book can be an important basis for this, as it shows not only the possibilities but also the limitations of VVT procedures.
6. *Component and Subsystem Suppliers.* A clear definition and a specification with respect to VVT measures are essential, especially for system development projects that involve supplier companies. This book forms a convenient basis for those projects since it provides a mutual definition, nomenclature and techniques as well as a body of VVT methods.
7. *Auditors.* To evaluate the maturity of a development project, auditors and auditing agencies can also apply the VVT methodology. Adherence to standards, deployment of established procedures, as well as the maturity of the processes' implementation can be evaluated in this way.
8. *Regulatory and Standardization Agencies.* Material presented in this book may be helpful in forming and updating national or international standards and regulations of standardization committees in which certain procedures for defined system classes are classified as binding or just recommended. Of course, it is not the aim of this book to define or force standardization. However, it could provide important suggestions with regard to such an endeavor.

1.1.4 Book Structure and Contents

This book is divided into three parts and a set of appendices as described below.

Part I: Introduction Part I of this book contains basic introductory material organized in one chapter. It starts by describing the purpose, the intended audience, the structure and the content of the book, the scope of the applications and the terminology and notation used throughout this book. It continues by providing basic introduction to systems theory, relevant background on systems and software VVT as well as risk and uncertainty theory. In addition, this chapter introduces VVT concepts and discusses the modeling of systems and the VVT lifecycles. It then defines generic phases, views and aspects of the system lifecycle that are used in this book. Finally, the chapter provides a VVT methodology overview, typical VVT documents and a methodology for VVT tailoring.

Part II: VVT Activities and Methods Part II of this book describes the VVT activities typically associated with each phase of the system lifecycle. For each VVT activity, the book describes one or more methods for carrying out those activities:

- *Chapter 2, System VVT Activities: Development,* describes typical VVT activities which may be conducted during system development, that is, during the Definition, Design, Implementation, Integration and Qualification phases of the system's lifecycle.
- *Chapter 3, System VVT Activities: Postdevelopment,* describes typical VVT activities which may be conducted during system postdevelopment, that is, during Production, Use/Maintenance and Disposal phases of the system's lifecycle.
- *Chapter 4, System VVT Methods: Nontesting,* describes a set of VVT nontesting methods, complementing the VVT activities described in the VVT activities chapters. In particular this chapter describes the following nontesting system VVT methods: preparing VVT products, performing VVT activities and participating in reviews.
- *Chapter 5, System VVT Methods: Testing,* describes a set of VVT testing methods, complementing the VVT activities described in the VVT activities chapters. Specifically, this chapter describes a collection of system testing methods grouped into the following categories: white-box testing and black-box testing; the latter is further divided into basic testing, high-volume testing, special testing, environment testing and phase testing.

Part III: Modeling and Optimizing VVT Process Part III of this book describes ways to model system quality cost, time and risk as well as ways to acquire quality data and optimize the VVT strategy in accordance with different business objectives. In addition, Part III describes the methodology used to validate the quality models along with examples describing a system's quality improvements.

- *Chapter 6, Modeling Quality Cost, Time and Risk,* describes system quality modeling—in particular, VVT cost and risk modeling, VVT time and risk modeling and fuzzy VVT cost modeling.
- *Chapter 7, Obtaining Quality Data and Optimizing VVT Strategy,* presents typical quality data of engineered systems from various industries as well as practical ways and means to elicit and aggregate quality data (i.e., cost, time and risks of VVT activities). The chapter continues by describing various techniques to optimize VVT strategies in order to reduce cost, time and system risks.
- *Chapter 8, Methodology Validation and Examples,* describes a validation process which compares actual measurements of system quality cost and time with model prediction. Finally, this chapter provides several examples of the entire system quality improvement process.

Appendices This portion of this book contains a collection of appendices as follows:

- *Appendix A—SysTest Project*
- *Appendix B—VVT Master Plan (VVT-MP)*
- *Appendix C—Acronyms*
- *Index*

Figure 1.1 will help the reader to navigate this book.

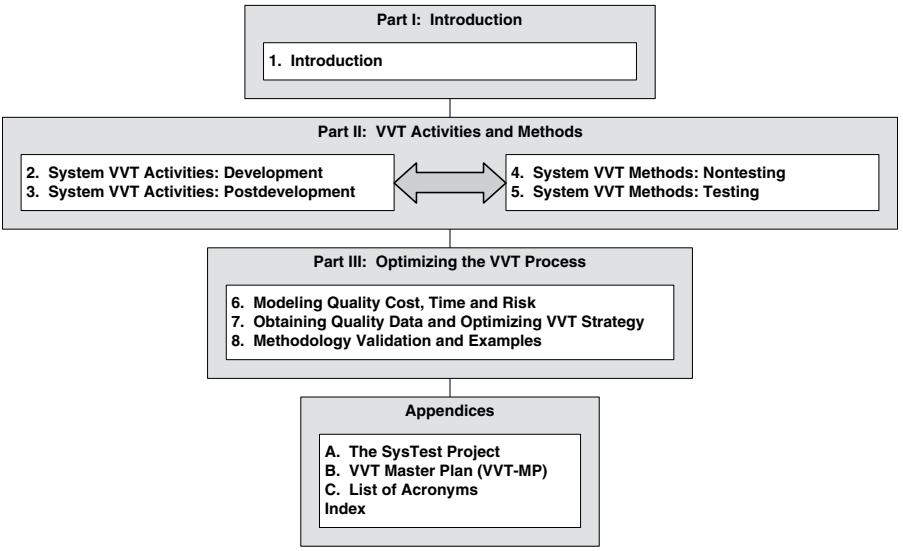

Figure 1.1 Book structure and navigation.

1.1.5 Scope of Application

This book covers system VVT, hopefully, without bias toward a specific application. The VVT methods described are applicable to a broad spectrum