CONTENTS

1 The Changing Face of Software Security and Software Development 1

2 The Significance of Security By Design 4
   2.1 The Term Security by Design 4
   2.2 The significance for Society 4
   2.3 The Significance for Software Users 6
   2.4 Significance for Software Manufacturers 7

3 Software Security through Automation and Reduction Human Factors 12
   3.1 Challenge: Security Oriented Programming Languages 13
   3.2 Challenge: Modeling Risks, Threats and Maturity Levels 14
   3.3 Challenge: Development Models for Secure Software Lifecycles 16
   3.4 Challenge: Verification and Testing 17
   3.5 Challenge: The Sustainably Secure Integration of Cryptographic Primitives and Protocols 19
   3.6 Challenge: Detecting Intentionally Introduced and Provenance Tracking 22
   3.7 Challenge: Common Language 23

4 Security by Design in Distributed Development and Integration 25
   4.1 Challenge: Standardizing Security Processes Over The Complete Supply Chain 27
   4.2 Challenge: Governance Framework in Distributed Development and Integration 30
   4.3 Challenge: Security Processes for Software Product Lines 32
   4.4 Challenge: Security when Integrating Large Systems 35
   4.5 Challenge: Assurance through Security Processes 38

5 Security by Design for Legacy Software 42
   5.1 Challenge: Statements about the Security of Legacy Software 42
   5.2 Challenge: Transfer Legacy Software into the Security Lifecycle 43
   5.3 Challenge: Increase the Security of Legacy Software 44

6 The Future with Security by Design 46

7 Appendix: Bibliography 47

Acknowledgements 57