

Contents

List of Figures	XV
List of Tables	XVII
Acronyms	XIX
I. Foundation	1
1. Introduction	3
1.1. Research Questions	5
1.2. Outline and Impact	6
2. Automotive Development	9
2.1. Development Models	9
2.2. Function Oriented Development	12
2.3. Systems Engineering	13
2.4. System Security Engineering	15
2.5. Normative References	15
3. Methodology	17
3.1. Representation in the Thesis	17
3.2. Information Sources	18
II. Meta-Functional Aspects	21
4. Dependability as an Umbrella-Term	25
4.1. Related Work	26
4.2. Dependability Impairments	27
4.3. Dependability Attributes	29
4.4. Dependability Means	33
5. Security Taxonomy	35
5.1. Related Work	37
5.2. Security	37
5.3. Security Threats	38
5.4. Security Objectives	44
5.5. Security Mitigations	49
6. Terms and Definitions	51

III. Security Development Process Design	53
7. Security Relevance Evaluation	57
7.1. Process Description	57
7.2. Cluster SRE	61
7.3. Questionnaire	65
7.4. SRE Analysis	72
8. Function-oriented Security Risk Analysis	77
8.1. Process Description	77
8.2. Cluster SRA	87
8.3. Traceability of SRA	87
8.4. Template Adjustments	92
9. Security Risk Analysis on System Level	93
9.1. Process Description	93
9.2. Method Design	96
9.3. Item Definition for System SRAs	98
9.4. Threat Catalog for System SRAs	103
9.5. System SRA Analysis	107
10. Risk Treatment	111
10.1. Process Description	111
10.2. Security Defense Methods	115
10.3. Assignment of Security Requirements	121
IV. Use Cases and Evaluation	129
11. Evaluation Criteria	131
11.1. Automotive SPICE	131
11.2. Improvement Goals	132
12. Use Case: Security Relevance Evaluation	135
12.1. Light Functions	135
12.2. Improvement Evaluation	137
13. Use Case: Function-oriented Security Risk Analysis	139
13.1. Light Functions	139
13.2. Improvement Evaluation	140
14. Use Case: System Security Risk Analysis	143
14.1. Light Functions	145
14.2. Method Evaluation	146

15. Use Case: Risk Treatment	149
15.1. Light Functions	150
15.2. Method Evaluation	151
 V. Closing	 153
16. Discussion	155
16.1. Security development planning	156
16.2. Emergency	156
16.3. Safety and Security	156
16.4. Formal Methods	157
17. Conclusion	159
18. Future Work	163
18.1. Holistic View on the Development Process	164
18.2. Assumption Guarantee Contracts	164
18.3. Contract based Security Development	165
Bibliography	169
Appendices	181
Appendix A. Attacker Model Categories and Rating	183
Appendix B. Basic Threat Classes for System SRA	185
Appendix C. Categories of Defense Method Properties	187