

Contents

1	Introduction	1
1.1	European Regulation	2
1.1.1	Overview of Current Regulation and its Objectives	2
1.1.2	UN Regulation No. 155	3
1.1.3	UN Regulation No. 156	3
1.1.4	EU NIS-2	3
1.1.5	EU Cyber Resilience Act (CRA)	4
1.1.6	EU General Safety Regulation	6
1.1.7	EU Machinery Regulation	6
1.1.8	EU General Data Protection Regulation	7
1.2	UN Regulation No. 155 and International Standard ISO/SAE 21434	7
1.3	Structure of This Book	10
1.4	Naming Convention	11
	References	12
2	Standards for the Manufacturing and Automotive Industries	13
2.1	ISO/SAE 21434	14
2.2	IEC 62443	14
2.3	ISO/IEC 27001	15
2.4	ISO 26262	16
2.5	ISO/SAE PAS 8475	17
2.6	ISO PAS 5112	17
2.7	ISO/SAE TR 8477	17
2.8	ENX and TISAX®	18
2.9	VDA Information Security Assessment	19
2.10	ENX VCS	19

2.11	Other Standards Related to Safety and Cybersecurity	19
2.11.1	ISO/IEC 5888	19
2.11.2	ISO/TR 4804	20
2.11.3	ISO PAS 8800	20
2.11.4	ISO/IEC TR 5469	20
2.11.5	IEC 61508	20
	References.	21
3	Integrated Management Systems and Integrated Risk Management	23
3.1	Overview of Risk Management Methods and Systems	24
3.1.1	ISO/IEC 27001	24
3.1.2	BSI-Standard 200-1	25
3.1.3	ISO/IEC 27005	25
3.1.4	ISO 31000	25
3.1.5	ISO 22301	25
3.1.6	TISAX®	26
3.1.7	IEC 62443	26
3.1.8	ISO/SAE 21434	27
3.2	Harmonization and Integration of Management Systems	32
3.3	An ISO/SAE 21434 TARA for IT/OT Systems	34
	References.	35
4	Threat Analysis and Risk Assessment	37
4.1	Why is It Necessary?	38
4.2	When Does It Take Place in the Vehicle Life Cycle?	39
4.2.1	Initial TARA	41
4.2.2	TARA During Development	41
4.2.3	TARA for Production.	42
4.2.4	TARA After SW Change or Vulnerability	42
4.3	Detail Level According to Available Information	43
4.3.1	“The 3-Days TARA”—Initial TARA.	43
4.3.2	“The 30-Days TARA”—TARA During Development and Reuse	44
4.3.3	“The 300-Days TARA”—The Inefficient or Overblown TARA	45
4.4	Overview of the TARA Process	46
4.5	Tooling	50
	References.	51
5	Defining the Scope of a TARA Project	53
5.1	How to Define the Scope	55
5.2	Assumptions.	59
5.2.1	Important Assumption: Shall Existing or Planned Controls for the Item Be Considered for the TARA?	59

5.3	Scope for Automotive Embedded Devices	60
5.3.1	TARA for Standalone ECUs or Functional Systems	61
5.3.2	TARA at the Vehicle Level (E/E Architecture)	62
5.4	Scope for IT/OT Systems for Vehicle-Backend Architectures. . . .	63
5.5	Scope for Manufacturing Plants.	64
5.6	Defining the Attacker Model	64
5.6.1	Who is the Attacker?	65
5.6.2	Attacker Modeling Approach Following ETSI TVRA	67
5.6.3	Relationship Between Attacker Model and Threats	70
5.7	Practical Case Studies	70
5.7.1	Case Study 1: Automotive Embedded Device	74
5.7.2	Case Study 2: Vehicle-Backend Architecture	76
5.7.3	Case Study 3: Automotive Manufacturing Plant	78
	References.	81
6	Identifying the Assets of the Item	83
6.1	Definition of Asset	85
6.2	Asset Identification	85
6.2.1	Typical Assets for Automotive Embedded Devices	88
6.2.2	Typical Assets for IT/OT Systems	96
6.2.3	Safety-Relevant Assets.	99
6.3	Cybersecurity Properties	100
6.3.1	CIA Triad: Confidentiality, Integrity, Availability	100
6.3.2	Other Cybersecurity Properties	102
6.4	Damage Scenarios	103
6.4.1	Identification of Damage Scenarios.	104
6.4.2	Impact Rating.	105
6.4.3	Additional Stakeholders.	108
6.4.4	Scalability	111
6.5	Practical Case Studies	113
6.5.1	Case Study 1: Automotive Embedded Device	113
6.5.2	Case Study 2: Vehicle-Backend Architecture	118
6.5.3	Case Study 3: Automotive Manufacturing Plant	125
	References.	132
7	Modeling and Evaluating Threat Scenarios	135
7.1	Identifying Threats.	136
7.1.1	Brainstorming	137
7.1.2	Threat Catalogs	139
7.1.3	STRIDE	143
7.1.4	EVITA	144
7.1.5	HEAVENS	145
7.1.6	ETSI TVRA	146
7.1.7	PASTA	146

- 7.2 Attack Paths 147
 - 7.2.1 How to Identify the Attack Paths? 147
 - 7.2.2 Description of Attack Paths 148
 - 7.2.3 Attack Trees 149
- 7.3 Feasibility Evaluation 151
 - 7.3.1 Attack Potential-Based Approach 152
 - 7.3.2 CVSS-Based Approach 157
 - 7.3.3 Attack Vector-Based Approach 160
 - 7.3.4 Determining the Attack Feasibility Rating
by Attack Paths with Several Steps 161
 - 7.3.5 Relation to the Attacker Model 164
- 7.4 Practical Case Studies 164
 - 7.4.1 Case Study 1: Automotive Embedded Device 165
 - 7.4.2 Case Study 2: Vehicle-Backend Architecture 168
 - 7.4.3 Case Study 3: Automotive Manufacturing Plant 171
- References 175
- 8 Performing the Risk Evaluation 179**
 - 8.1 Risk Evaluation 180
 - 8.1.1 Risk Matrix 180
 - 8.1.2 Risk Formula 183
 - 8.2 Understanding Data and Working with Statistics 184
 - 8.2.1 Threat Scenarios 184
 - 8.2.2 Damage Scenarios 185
 - 8.2.3 Assets 185
 - 8.3 Practical Case Studies 186
 - 8.3.1 Case Study 1: Automotive Embedded Device 186
 - 8.3.2 Case Study 2: Vehicle-Backend Architecture 187
 - 8.3.3 Case Study 3: Automotive Manufacturing Plant 187
 - Reference 193
- 9 Risk Treatment Decision. 195**
 - 9.1 Risk Treatment Decision and Risk Tolerance 196
 - 9.2 Risk Avoidance 196
 - 9.3 Risk Reduction 196
 - 9.3.1 Cybersecurity Goals 197
 - 9.3.2 Cybersecurity Controls 198
 - 9.4 Risk Sharing and Risk Acceptance 201
 - 9.4.1 Cybersecurity Claims 201
 - 9.5 After TARA is Before TARA—Risk Re-Evaluation 202
 - 9.5.1 Statistics 202

Contents	xv
9.6 Practical Case Studies	203
9.6.1 Case Study 1: Automotive Embedded Device	204
9.6.2 Case Study 2: Vehicle-Backend Architecture	205
9.6.3 Case Study 3: Automotive Manufacturing Plant	207
References.	208
Appendix	211
Index.	253