

Contents

1	Safety the Basis for Future Mobility	1
1.1	Safety is Much More Than Safety Engineering	2
1.2	Safety as a Social Right	4
1.3	Legal Basis for “Auto-Mobility”	6
1.3.1	The German Road Traffic Act (StVG)	8
1.3.2	Origin of the German Road Traffic Act	10
1.3.3	Adaptation of the Traffic Right for the Globalisation Trend	10
1.3.4	Activities in Germany for Future Mobility Solutions	13
1.3.5	Genevan and Viennese Convention	14
1.4	European Union (EU) and Legislation	16
1.4.1	EU Directives Related to Road Traffic	18
1.4.2	European Vehicle Class	22
1.4.3	EU Directive for Future Mobility	24
1.5	Licensing Act	25
1.6	US Road Traffic Regulations	26
1.7	UNECE	28
1.8	Legal View on Future Mobility	31
1.8.1	New Licensing Approach for Automated Vehicles	36
1.8.2	ITS Law	40
1.8.3	ETSI—European Telecommunications Standards Institute	44
1.8.4	OECD, Organisation for Economic Co-operation and Development	47
1.8.5	ETSC European Transport Safety Council	49
1.8.6	IT Security Act	50
1.9	Product Liability	51
1.10	Common Law and Civil Law	56

1.11	Legal Regulation in China	56	3.6.4	Control System Architecture in Comparison with the Human Control System	136
1.12	Insurance	59			
2	Risk Management	61	3.7	Cyclic Data Processing Versus Distributed Event-Driven Data Processing	139
2.1	Risk Management Cycle	63	3.7.1	Distributed Control	143
2.1.1	Development of the Context	64	3.7.2	Configuration of Human Control System	145
2.1.2	Identification of Risk	64	3.8	Cybernetics and Control	146
2.1.3	Assessment of the Risk in the Target Context	65	3.8.1	Digital Twin	149
2.1.4	Development of a Strategy and Treatment of Potential Risk	66	3.8.2	Cybernetics About Behaviour and Control	152
2.1.5	Development and Defining of Activities and Their Objectives	67	3.8.3	Cybernetics and Sufficiently Perceiving the Environment	154
2.1.6	Development of an Implementation and Realisation Strategy	67	4	System Safety Engineering	159
2.1.7	Review and Evaluation of the Plan	68	4.1	Observer of a System	159
2.2	Technical Risk	68	4.1.1	Viewpoints and Perspective	160
2.3	Risk in Road Traffic	72	4.1.2	ISO 26262 in an Architecture Matrix	172
2.3.1	Causes of Technical Risk	74	4.2	Road Traffic Perspective	177
2.3.2	Control of Technical Risk	76	4.2.1	Road Traffic Environment	180
2.4	Standardisation of Safety for Road Vehicles	79	4.2.2	The Context of Automated Road Vehicles	184
2.4.1	Risk and Integrity Definition from the IEC 61508	82	4.2.3	Breakdown from Stakeholders View to an Operational View	186
2.4.2	Risk According to ISO 26262	91	4.3	Operational Design Domain as per SAE J3016	187
2.5	Critical Infrastructure	101	4.4	Layered Approach for Automated Driving	189
2.5.1	Organisation for Critical Infrastructure	102	4.4.1	Phases of an Hierarchical Engineering Approach	195
2.5.2	Cloud Computing	103	4.4.2	Context Layer	199
2.5.3	Transport and Traffic and Critical Infrastructure	105	4.4.3	Development of the Operational Safety Concept	200
3	Automation in Mobility	109	4.4.4	Development of the Vehicle Safety Concept	202
3.1	Human Driving: a Closed-Loop Control System	109	4.4.5	Process Sequence for the Engineering Model	203
3.2	Human Driving	110	4.5	Software Development	204
3.2.1	Driver's HMI	111	4.5.1	Software Development Based on ISO 26262	205
3.2.2	Driver in the Loop	112	4.5.2	Safety Mechanism in Basic Software	207
3.2.3	Human Driving Journey	113	4.5.3	Safety for POSIX-Based Architecture	210
3.3	Human Control Mechanism	114	4.5.4	Failure and Errors in POSIX-Systems	216
3.4	Human Behaviour and Context	117	4.5.5	Hypervisor Approach	217
3.4.1	Observer of the Observer	118	4.6	Real-Time Embedded Systems	218
3.4.2	Industry Automation	120	4.6.1	Timing and Determinism	220
3.4.3	Multiple Contexts for Different Layers of Abstraction	122	4.6.2	Scheduling in Real-Time Systems	222
3.5	Communication and Interfaces	124	4.6.3	Mix-Criticality Application in Hard Real-Time Systems	229
3.6	Human Driver as a Control System	126	4.6.4	Control and Data Flow Monitoring	231
3.6.1	Human Communication	130	4.7	Operating Systems in Vehicles	234
3.6.2	Human Perception	131	4.7.1	AUTOSAR	237
3.6.3	Technical Control System Comparison	134	4.7.2	ARINC 653	240
			4.7.3	Comparison of AUTOSAR with ARINC 653 Framework	243

4.7.4	Safe Processing Environment	245
4.7.5	Predictive Health Monitoring	249
4.7.6	Safety and Security Error Propagation	252
4.8	Development of Software-Intensive Tools	253
4.9	Verification and Validation	256
4.9.1	Verification of Diverse Objectives Such as Safety and Security	258
4.9.2	Validation	259
4.9.3	Validation According VMAD	260
4.9.4	Safety Validation in ISO 26262	263
4.9.5	Validation Phase	264
5	Organisational Viewpoint	267
5.1	Accident Research	268
5.2	Quality Management	273
5.3	Software Quality	277
5.4	Process Models	280
5.4.1	Cyclic Process Models	284
5.4.2	PDCA and CIP	285
5.5	Complexity Due to Organisation	288
5.6	Vehicle Structure and Organisation	289
5.7	Dimensions of a Capable Organisation	292
5.8	Structure of Organisations	293
5.9	Organisational Aspects for Future Mobility	296
5.10	Organisational Structure in Product Development	303
5.10.1	Classical Organisation Until the Last Millennium	304
5.10.2	Future Driver of a Development Organisation	305
6	Automated Driving and Control	307
6.1	Vehicle Behaviour	307
6.1.1	Degree of Freedom of Road Vehicles	309
6.1.2	Framework for Inertial System of Space and Time	312
6.1.3	Road Vehicle in "Real World"	315
6.1.4	Criticality Depending on Distance	319
6.2	Driver-Vehicle Interface	322
6.2.1	Controllability by the Driver	323
6.2.2	Accidents and Measures Against Their Root Causes	330
6.3	Control and Communication	331
6.3.1	Event-Driven Control	332
6.3.2	Publish-Subscribe Networks	336
6.3.3	Data Distribution Service (DDS)	341
6.3.4	Communication Networks and Energy Transport	342
6.4	Hazard and Risk in Road Traffic	344

6.5	Horizontal and Vertical Engineering	347
6.5.1	Closed-Loop Control and Signal Chains	350
6.5.2	Closed-Loop Control on Various Layers of Abstraction	354
6.5.3	Analyse Methodology	360
6.5.4	Layered System Analysis	361
6.5.5	Quantitative Aspects of Layer of Protection Analysis	365
6.6	Methods for Risk Management	370
6.6.1	Failure Mode and Effect Analysis (FMEA)	372
6.6.2	Fault Tree Analysis (FTA)	374
6.6.3	Markov Analysis	375
6.6.4	HazOp (Hazard and Operability Studies or Analysis)	376
6.6.5	Preliminary Hazard and Risk Analysis (PHA, PRA)	378
6.6.6	Operational Safety Assessment (OSA)	381
6.7	Application from Avionics	383
6.7.1	Flight Envelope	386
6.7.2	Adaption to Automated Driving	387
6.8	Outlook on Future Automated Mobility	390
	Outlook	391