

Part I Foundation

1	Introduction	3
1.1	Cyber-Physical Systems	3
1.2	Risk in Cyber-Physical Systems	5
	References	7
2	Cyber-Physical Systems	9
2.1	Cyber-Physical Systems	9
2.2	Cyber-Physical Systems-of-Systems	12
2.3	Emergence	14
2.4	Infrastructure	17
	2.4.1 Introduction	17
	2.4.2 ICS Architecture	18
2.5	Autonomous Cyber-Physical Systems	21
2.6	Internet of Things	22
2.7	Cloud-Based Cyber-Physical Systems	23
	2.7.1 Conceptual Architecture	23
	2.7.2 Cloud Safety, Security, and Real Time	27
2.8	Token Economy	29
2.9	Cyber-crime and Cyber-war	31
	2.9.1 Cyber-crime	32
	2.9.2 Cyber-war	35
2.10	Diffuse Computer Crime	39
	2.10.1 Supply Chain Dangers	39
	2.10.2 Insider Crime	41
2.11	Cyber-Physical Systems Engineering	42
	2.11.1 Safety- and Security-Aware Development Process	42
	2.11.2 Governance	45
	2.11.3 Competence Center	46

2.11.4	Contract-Based Engineering	47
2.11.5	Agile Methods in Safety and Security	51
	References	56
3	Three Devils of Safety and Security	77
3.1	Vulnerabilities	78
3.2	Threats	80
3.3	Failures	81
3.4	Risk Introduction	82
3.5	Cyber-Physical System Tension Field	84
	References	85
4	Safety, Security, and Risk	89
4.1	Context	89
4.2	General Resilience	91
4.3	Safety	93
4.3.1	Introduction	93
4.3.2	Composite Systems	94
4.3.3	Safety Taxonomy	96
4.3.4	Safety Metrics	97
4.3.5	Elements of Safety	99
4.3.6	Safety Culture	99
4.3.7	Safety Standards and Policies	100
4.3.8	Governance	105
4.3.9	Safety Management System	105
4.3.10	Safety Principles	107
4.3.11	Safety Implementation	108
4.3.12	Safety Assessment and Safety Audit	109
4.3.13	Safety Runtime Monitoring	111
4.3.14	How Much Safety is Enough?	114
4.4	Security	115
4.4.1	Introduction	115
4.4.2	Security Taxonomy	116
4.4.3	Security Metrics	117
4.4.4	Elements of Security	118
4.4.5	Security Culture	120
4.4.6	Security Standards and Policies	122
4.4.7	Governance	125
4.4.8	Security Management System	125
4.4.9	Security Principles	130
4.4.10	Security Implementation	130
4.4.11	Security Perimeter Protection	131
4.4.12	Zero Trust Architecture	135

4.4.13	Security Chaos Engineering	137
4.4.14	Weakest Link	138
4.4.15	Security Assessment and Security Audit	140
4.4.16	Security Runtime Monitoring	142
4.4.17	How Much Security is Enough?	144
4.5	Convergence of Safety and Security Engineering	145
4.6	Risk	146
4.6.1	Risk in Safety and Security	147
4.6.2	Risk Management Process	148
4.6.3	Risk Analysis and Assessment	151
4.6.4	Safety Risk Management	151
4.6.5	Security Risk Management	154
4.6.6	Cyber-Crisis Management	159
4.6.7	Agile Risk Management	163
4.7	Forensic Engineering	164
4.7.1	Safety Accident Forensic Engineering of Software	165
4.7.2	Cyber-Incident Forensic Engineering of Software	167
4.8	Ethics	168
	References	169
5	Safe Software and Secure Software	187
5.1	Introduction	187
5.2	Software Architecture	190
5.3	Architecture Framework	190
5.4	Trustworthy Development Process	193
5.4.1	Introduction	193
5.4.2	Defect Avoidance and Defect Elimination	197
5.4.3	Coding Standards	199
5.4.4	Good Programming Practices for Safety and Security	201
5.4.5	Modeling and Formal Languages	202
5.5	Safe Software	212
5.5.1	Time	214
5.5.2	Software Categories	216
5.5.3	In-House Software	216
5.5.4	Third-Party Software	217
5.5.5	Execution Platform	218
5.6	Secure Software	220
5.6.1	Secure by Design	222
5.6.2	In-House Software	222
5.6.3	Third-Party Software	225
5.6.4	Execution Platform	227
5.7	Correct-by-Construction	228

5.8	Importance of People	231
5.9	Drift into Vulnerabilities	234
5.9.1	The Law of Unintended Consequences	235
	References.	239
6	The Future	263
6.1	The Rise of the Three Devils	263
6.2	Safety: Autonomy	265
6.3	Security: Cryptography Apocalypse	267
6.3.1	Cryptographic Algorithms	267
6.3.2	Cryptographic Attacks	268
6.3.3	Cryptography Apocalypse	268
6.3.4	Post-Quantum Cryptography	270
6.4	Artificial Intelligence in Safety and Security.	272
6.4.1	AI in Safety	272
6.4.2	AI in Security.	287
6.5	AI Conclusions.	299
	References.	300
 Part II Principles		
7	Principle-Based Engineering	323
7.1	Risk-Based Engineering.	323
7.2	Principle-Based Engineering	325
7.2.1	Principles in Science	325
7.3	Safety and Security Principles	326
7.4	Principle-Based Engineering Process	326
7.5	Safety and Security Patterns	327
	References.	329
8	Principles for Business and Organization.	333
8.1	Principle B1: Risk Culture.	333
8.2	Principle B2: Policies.	334
8.3	Principle B3: Competence Center	336
8.4	Principle B4: Governance	337
8.5	Principle B5: Record Keeping and Trustworthy Archive.	338
8.6	Principle B6: Product Liability	339
8.7	Principle B7: Code of Ethics	341
8.8	Principle B8: People's Work Environment	341
	References.	343
9	General Principles.	347
9.1	Principle G1: Precise Safety and Security Requirements	347
9.2	Principle G2: Adequate System Architecture	348

9.3	Principle G3: Technical Debt	352
9.3.1	Technical Debt	352
9.4	Principle G4: Architecture Erosion	356
9.5	Principle G5: Separation of Concerns	358
9.6	Principle G6: General Resilience Principles	359
9.6.1	G6_1: Software Integrity	359
9.6.2	G6_2: Timing Integrity	362
9.6.3	G6_3: Fault Containment Regions.	362
9.6.4	G6_4: Single Points of Failure.	364
9.6.5	G6_5: Multiple Lines of Defense.	365
9.7	G6_6: Fail-Safe System	367
9.7.1	G6_7: Graceful Degradation	369
9.7.2	G6_8: Fault Tolerance	370
9.7.3	G6_9: Dependable Foundation (Dependable Execution Infrastructure)	379
9.7.4	G6_10: Error, Exception, and Failure Management	384
9.7.5	G6_11: Monitoring	386
9.8	G7: Code Quality	387
9.9	G8: Modeling	389
9.10	G9: Cloud-Based Cyber-Physical Systems	390
9.11	G10: Supply Chain Confidence	392
9.11.1	Black-Box Risk Analysis	394
9.11.2	Protective Shell	395
9.11.3	Black-Box testing.	398
9.11.4	Supplier Risk Management Review/Audit.	399
9.12	G10a: Supply Chain Risk Management.	399
9.13	G10b: Supply Chain Confidence: Products	401
9.14	G10c: Supply Chain Confidence: Services (Outsourcing).	403
9.15	G10d: Supply Chain Confidence: Open-Source Software.	405
9.16	Principle G11: Trustworthy Development Process	407
9.17	G12: IoT Systems	409
9.18	G13: Impact of Artificial Intelligence	412
	References.	414
10	Principles for Safety	433
10.1	Principle S1: Safety Culture.	433
10.2	Principle S2: Safety Standards and Policies	434
10.3	Principle S3: Safety Governance	435
10.4	Principle S4: Safety Management System.	435
10.5	Principle S5: Safety Principles.	436
10.6	Principle S6: Safety Implementation	437
10.7	Principle S7: Safety Assessment and Audit.	439

10.8	Principle S8: Safety Runtime Monitoring	441
10.9	Principle S9: Safe Software	442
10.10	Principle S11: Artificial Intelligence in Safety-Critical CPS	444
	References	445
11	Principles for Security	449
11.1	Principle E1: Security Culture	449
11.2	Principle E2: Security Standards and Policies	450
11.3	Principle E3: Security Governance	452
11.4	Principle E4: Information Security Management System	453
11.5	Principle E5: Security Principles	457
11.6	Principle E6: Cyber-Crisis Management	458
11.7	Principle E7: Security Implementation	459
11.8	Principle E8: Personal Data	464
11.9	Principle E9: Security Perimeter Protection	466
11.10	Principle E10: Zero Trust Architecture	467
11.11	Principle E11: Cryptography	468
	11.11.1 Lightweight Cryptography	468
11.12	Principle E12: Transition to Post-Quantum Cryptography	471
11.13	Principle E13: Security Assessment and Security Audit	472
11.14	Principle E14: Security Runtime Monitoring	474
11.15	Principle E15: Secure Software	476
11.16	Principle E16: Insider Crime	478
	11.16.1 Technical Controls	479
	11.16.2 Human Resource Management Controls	480
11.17	Principle E17: Microservices Security	484
	11.17.1 Microservices	484
	11.17.2 Microservices Security	485
	11.17.3 Microservices Governance	486
	11.17.4 Migration to Microservices	487
11.18	Principle E18: Artificial Intelligence in Security	489
	11.18.1 ICT Defense Mandate	489
	11.18.2 Artificial Intelligence Defense for Security	490
	11.18.3 Attacks against Defense AI Machine Learning	491
	References	492
12	Principles for Risk	507
12.1	Risk Handling	507
12.2	Principle R1: Risk	508
12.3	Principle R2: Risk Management Process	511
12.4	Principle R3: Risk Metrics	512
12.5	Principle R4: Forensic Engineering	513
	References	514

13 Final Words 517

13.1 Uncertainty. 517

13.2 Disciplined Engineering. 518

13.3 Why? 518

13.4 Final Words 519

Reference 520

References 521

Index. 527