

Contents

1	Introduction	1
1.1	Cyber-Physical Systems	1
1.2	QoS of Cyber-Physical Systems	2
1.2.1	Safety Integrity Levels	3
1.2.2	Security Capability Levels	3
1.3	Engineering Cyber-Physical Systems	9
1.4	Specification PEARL Approach	10
	References	12
2	Specification PEARL Language	15
2.1	Extending PEARL for Distributed Systems	15
2.2	Specification PEARL Notation	16
2.2.1	Hardware Configuration	17
2.2.2	Software Configuration	19
2.3	Specification PEARL CASE Environment and its Program Libraries	19
2.3.1	Configuration Manager	20
2.3.2	Operating System	21
2.4	Specification PEARL Behavioural Model	22
2.4.1	Task-Forming Rules	24
2.4.2	Translation from Timed State Transition Diagrams to Program Tasks	25
2.5	Case Study—Railroad Crossing	25
	References	32
3	Specification PEARL Methodology	33
3.1	System Life-Cycle	33
3.2	System Model	33
3.3	Virtual Machine	34
3.4	Simulation Model	35

3.5	Configuration Manager and Operating System Model	36
3.6	System Verification and Validation	37
3.6.1	Verification and Validation of Temporal Feasibility	38
4	UML 2 Profile for Specification PEARL	41
4.1	Mapping Specification PEARL Architecture Constructs to UML	42
4.1.1	Station Layer	43
4.1.2	Collection Layer	44
4.1.3	Binding the Specification PEARL TSTD to UML's State Chart Concept	49
4.2	UML Application Architecture with Specification PEARL Stereotypes	52
	References	52
5	UML Safety Pattern for Specification PEARL	53
5.1	Design for Safety.	54
5.2	Safety Shell	56
5.3	Safety Shell Functionality	57
5.3.1	Protected Input/Output	58
5.3.2	State Guard	60
5.3.3	Timing Guard	62
5.3.4	Exception Handler	63
	References	64
6	Specification PEARL Security	65
6.1	Design for Security	65
6.1.1	Sensing and Communication Security	66
6.1.2	Actuation Control and Feedback Security	66
6.1.3	Storage Security	66
6.2	Securing Identification and Communication.	67
6.2.1	RFID Security.	67
6.2.2	Secure Identification	69
6.2.3	Secure Communication	70
6.3	Securing Operation	71
6.3.1	Biometric Security.	71
6.3.2	One-Time Pad.	74
6.4	Securing Storage	75
6.5	Security Shell	76
6.6	Security Level Specification	78
	References	79
7	Evaluation of the Methodology	81
7.1	Design for Correctness and Timeliness	81
7.2	Design for Safety.	82

7.3 Design for Security	85
7.4 Design for Licenseability	87
References	87
8 Conclusion.	89
Appendix A: Textual Architecture Description	91
Appendix B: Graphical Architecture Description	99
Appendix C: CM API	103
Appendix D: RTOS API	105
Appendix E: Project Layout	113
Index	127

Engineering Safe and Secure Cyber-Physical Systems

The Specification PEARL Approach

Gumzej, R.

2016, XIII, 128 p. 28 illus., Hardcover

ISBN: 978-3-319-28903-8