

Contents

Glossary	xxvii
1 Introduction	1
1.1 Problem statement	1
1.1.1 UAS operations and the need for contingency management	3
1.1.2 RPAS flight planning and replanning	5
1.2 Objectives and methodology	7
1.3 Thesis outline	9
2 Background	11
2.1 Introduction	11
2.2 UAS regulation	11
2.3 UAS contingency management	15
2.4 Automation levels	16
2.5 Software architectures for mission control	18
2.6 Flight plans and Mission plans	19

3	Contingency management in UAS	21
3.1	Introduction to risk assessment in UAS	21
3.1.1	System description	23
3.1.2	Identification of threats and hazards	24
3.1.3	Identification of harms	24
3.1.4	Determination of risk	25
3.1.5	Determination of the acceptable level of risk	27
3.1.6	Identification of the means for risk mitigation	28
3.2	Contingency Management approach	32
3.2.1	System description	37
3.2.2	Identification of threats and hazards	39
3.2.3	Identification of harms	53
3.2.4	Determination of risk	53
3.2.5	Determination of the acceptable level of risk	53
3.2.6	Identification of the means for risk mitigation	53
3.3	Automated Contingency Management	55
4	On-board Mission Management System software architecture	57
4.1	Introduction	57
4.2	Initial Mission Manager architecture design	62
4.2.1	Path Planner	62
4.2.2	Guidance System	63
4.2.3	Flight Director	64
4.3	Safe Mission Manager architecture design	64
4.3.1	Safety Monitor	68
4.3.2	Contingency Manager	70
4.3.3	Mission Manager	73
4.3.4	Flight Termination	75
4.4	Safety aspects relating to the software development	76
4.4.1	Preliminary software level determination	77
4.4.2	Architectural strategies for fault contention	78
4.4.3	Prototyping and deployment to XtratuM	80
4.4.4	Formal methods for software verification	82

5	Reconfigurable Mission Plans	85
5.1	Definition	85
5.1.1	Waypoints.	87
5.1.2	Mission goals	87
5.1.3	Legs	88
5.1.4	Segments	90
5.1.5	Routes	94
5.1.6	Mission boundaries	98
5.2	Specification	99
5.2.1	Waypoints.	100
5.2.2	Mission goals	101
5.2.3	Legs	102
5.2.4	Segments	103
5.2.5	Routes	104
5.2.6	Mission boundaries	105
5.3	Dynamic, risk-based route configuration.	105
6	Probabilistic Risk Assessment Framework	109
6.1	Probabilistic Risk Model	109
6.2	Ground risk model	111
6.2.1	Impact model.	112
6.2.2	Strike model	115
6.2.3	Harm model	116
6.2.4	Data source.	117
6.2.5	Model limitations	120
6.3	Air risk model	121
6.3.1	Impact model.	121
6.3.2	Strike model	126
6.3.3	Harm model	126
6.3.4	Data source.	127
6.3.5	Model limitations	130
6.4	Probabilistic Risk Model for nondeterministic paths.	131
6.5	Risk-based, cost estimation of Reconfigurable Mission Plan routes	131

7	Validation results	133
7.1	Introduction	133
7.2	Mission definition and risk assessment	134
7.2.1	Mission specification	134
7.2.2	Mission risk assessment	142
7.2.3	Static route configuration analysis	156
7.2.4	Dynamic route configuration analysis	157
7.3	Flight simulation results	177
7.3.1	Nominal operation	177
7.3.2	Contingency scenario CS1	185
7.3.3	Contingency scenario CS2	190
8	Conclusions and future work	197
8.1	Conclusions	197
8.2	Future work	199
	Bibliography	201
A	Formal design and verification of the contingency management policy: a case study	221
A.1	Introduction	221
A.2	Specification of the Safety Monitor model	222
A.3	Specification of the Contingency Plan model	224
A.4	Specification of the Mission Plan model	228
A.5	Formal specification and verification of the policy	229
B	On-board Mission Management System software architecture implementation	235
B.1	Introduction	235
B.2	Top-level SMMS model	237
B.3	Flight simulator interface	239
B.4	Remote Pilot interface	239

B.5 Safety Monitor System model	241
B.6 Contingency Manager System model.	243
B.7 Mission Manager System model.	246
B.7.1 Path Planner.	246
B.7.2 Guidance System	249
B.7.3 Flight Director.	251
B.8 Flight Termination System model.	252
C Reconfigurable Mission Plan implementation and tools	253
C.1 Introduction	253
C.2 Mission Graph construction.	254
C.3 Dynamic route configuration tools	255
C.3.1 Route search tools	256
C.3.2 Specification of the Route object	259
D Automatic deployment to XtratuM	261
D.1 Introduction	261
D.1.1 XtratuM run-time environment	261
D.2 Automatic deployment tools	262
D.2.1 Identification of the application partitioning scheme.	263
D.2.2 Code generation.	264
D.2.3 Configuration of the XtratuM project directory	265
D.3 Safe Mission Management System deployment issues.	266
E Bayesian Belief Network impact model parameters	267
E.1 Ground impact model CPTs	267
E.2 Mid-air collision model in controlled airspace CPTs.	268
E.3 Mid-air collision model in uncontrolled airspace CPTs	268