

Table of Contents

1	Introduction	1
1.1	Context and Motivation	1
1.2	Problem Statement and Contribution	4
1.3	Structure	6
2	Related Work	7
2.1	Open Integrated Architectures	7
2.1.1	Platform-based Design	10
2.1.2	Example Platform 1: AUTOSAR	14
2.1.3	Example Platform 2: IMA – ARINC 653	17
2.1.4	Platform Service Types	19
2.2	Deployment Evaluation	22
2.2.1	Match	26
2.2.2	Replication and Reliability	27
2.2.3	Delay and Flow	29
2.2.4	Fixed and Diverse Assignment	30
2.2.5	Mixed Criticality	31
2.3	Modular Certification	32
2.3.1	Process-focused Approaches	37
2.3.2	Modular GSN	40
2.3.3	Rich Component Model	41
2.3.4	Safety Analysis of CRMS	41
2.3.5	Conditional Safety Certificates	43
3	Solution Overview	45
3.1	Interface Specification and Mediation	48
3.2	Deployment Evaluation	50
4	Interface Specification	53
4.1	Running Example	55
4.2	Language Design	58
4.3	Common Language – General Features	61
4.3.1	Demands and Guarantees	62
4.3.2	Conditions	63
4.3.3	Architecture Relations	65
4.3.4	Parameters	69
4.4	Common Language – Failures and Failure Reactions	77
4.4.1	Failure Analysis and Classification	78
4.4.2	Platform Service Failures	81
4.4.3	Application Failures	109
4.4.4	Platform Failure Reactions	113
4.5	Application Language	116

4.5.1	Platform Service Demands.....	118
4.5.2	Health Monitoring Demands.....	123
4.5.3	Resource Protection Demands.....	128
4.5.4	Service Diversity Demands.....	131
4.6	Platform Language.....	134
4.6.1	Platform Service Guarantees	136
4.6.2	Health Monitoring Guarantees.....	141
4.6.3	Resource Protection Guarantees	147
4.6.4	Service Diversity Guarantees.....	149
5	Interface Mediation.....	153
5.1	Configuration.....	155
5.1.1	Platform Object Instantiation.....	156
5.1.2	Evaluation of Configuration-Dependent Conditions	157
5.2	System Integration	158
5.2.1	Evaluation of Deployment-Dependent Conditions	159
5.3	Manual Condition Evaluation	160
5.4	Interface Mediation.....	160
5.4.1	Mediation of Platform Service Demands.....	162
5.4.2	Mediation of Application Monitoring Demands.....	169
5.4.3	Mediation of Failure Reaction Demands.....	173
5.4.4	Mediation of Resource Protection Demands.....	178
5.4.5	Mediation of Service Diversity Demands.....	183
5.4.6	Mediation of Specific Parameters	185
5.5	Post Mediation	188
5.5.1	Visualizing Mediation Results	188
6	Deployment Evaluation	191
6.1	Problem Statement	192
6.1.1	Safety-Related Properties	194
6.1.2	Running Example	195
6.2	Objective Function.....	196
6.2.1	Cohesion Metric	196
6.2.2	Coupling Metric.....	198
6.2.3	Constraints	200
6.2.4	Objective Function Assembly.....	201
6.2.5	Parameterization	201
6.3	Deployment Optimization	203
7	Implementation and Evaluation	207
7.1	VerSal Evaluation.....	207
7.2	Deployment Evaluation	214
7.3	VerSal Implementation	217
7.4	Deployment Implementation	220
8	Conclusion.....	223
8.1	Contributions and Limitations	223
8.2	Future Work.....	225

8.3 Final Comment	226
9 References.....	227
Appendix A Architectural Meta-Model	237
A.1 System Meta-Model	238
A.2 Application Meta-Model	240
A.3 Platform Meta-Model.....	247
A.4 Deployment Meta.Model	252
Appendix B List of Common Failure Modes and Reactions	254
Appendix C NLR using EBNFs	258