

1	Introduction	1
1.1	Context & Motivation	1
1.2	Design Challenges & Contributions	3
1.3	General Design Approach for Real-Time Critical Industrial Distributed Control Systems	8
1.4	Outline	9
2	Fundamentals on Industrial Distributed Control Systems	11
2.1	Running Example: Process Control for Pet Food Production	11
2.2	Components & Network Communication	12
2.3	Real-Time Execution Behaviour & Scheduling	15
2.4	Time Synchronisation & the Precision Time Protocol	20
2.4.1	Time Synchronisation Approaches	20
2.4.2	A Detailed View on the Precision Time Protocol	20
2.5	Real-Time Ethernet Classification & Time-Sensitive Networking	21
2.5.1	The Real-Time Ethernet Classification	21
2.5.2	Time-Sensitive Networking	22
2.6	Modelling Industrial Distributed Control Systems	25
2.6.1	Hardware Description Languages	25
2.6.2	Software Programming Languages	25
2.6.3	Heterogeneous Models	26
2.6.4	General-Purpose Modelling Languages	26
2.6.5	Domain-Specific Modelling Languages	27
2.6.6	A Detailed View on IEC 61499	28
2.7	Formal Verification & Validation Techniques	33
2.7.1	Verification & Validation Approaches in IEC 61499	34

2.7.2	Overview & Benefits of Contract-Based Design	35
2.7.3	A Detailed View on Assume-Guarantee Specifications	36
2.7.4	The MULTIC Timing Specification Language	38
2.8	Summary & Assumptions	39
3	Systematic Correct-by-Construction Design for Industrial Real-Time Commu- nication	43
3.1	Contract-Based Design Approach for IEC 61499 Control Systems	43
3.2	IEC 61499 Modelling Extension for Time-Critical Network Communication	46
3.2.1	Modelling Element on System Level: Channel	47
3.2.2	Modelling Element on Application Level: Message Function Block	49
3.2.3	Mapping Model	51
3.2.4	Proof-of-Concept Implementation of IEC 61499 Extension	53
3.2.5	Summary	55
3.3	IEC 61499 Specification with Timing Properties	57
3.3.1	Integration of Timing Specification for IEC 61499 Applications . .	59
3.3.2	Defining Contracts	60
3.3.3	Evaluating Contracts	60
3.3.4	Maintaining Contracts	62
3.3.5	Applying Contracts to the Valve Control Application	63
3.3.6	Summary	63
3.4	Automated Network Configuration & Deployment	64
3.4.1	Specification of the Time-Sensitive Networking Schedule	65
3.4.2	Mapping Traffic into a Dedicated Time Slot	65
3.4.3	Automating the Overall Configuration Process	66
3.4.4	Summary	68
3.5	Target Hardware	69
3.6	Measurement Infrastructure	71
3.7	Summary	72
4	Evaluation	75
4.1	Evaluation Goals & Methodology	76
4.2	Evaluation Hardware Configuration	78
4.2.1	General Platform Configuration	78
4.2.2	Timing Assessment	80
4.2.3	Automated Network Configuration	81
4.3	Evaluation Software	84
4.3.1	General Modelling Approach	85

4.3.2	Valve Control	86
4.3.3	Joint Control	87
4.3.4	Joint Control Extended	89
4.3.5	Joint Control with Feedback Loop	91
4.4	Feasibility Analysis	91
4.4.1	Evaluation Setup	92
4.4.2	Communication Delay Analysis	92
4.4.3	Summary	97
4.5	Automated Deployment	98
4.5.1	Evaluation Setup	98
4.5.2	Functional Analysis	99
4.5.3	Summary	102
4.6	Demonstration Examples	103
4.6.1	Joint Control Application	105
4.6.2	Joint Control Extended	108
4.6.3	Joint Control with Feedback Loop	114
4.6.4	Summary	115
5	Conclusions and Future Work	119
5.1	Conclusions	119
5.2	Future Work	121
	List of Figures	123
	List of Tables	125
	Bibliography	127