

Technische Universität München
Lehrstuhl für Integrierte Systeme

Safe and Secure I/O Sharing for Mixed-Criticality Embedded Real-Time Systems for Avionics

Dipl.-Ing. (BA) Daniel J. Münch, M.Sc.

Vollständiger Abdruck der von der Fakultät Elektrotechnik und Informationstechnik
der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktor-Ingenieurs (Dr.-Ing.)

genehmigten Dissertation.

Vorsitzender: Univ.-Prof. Dr.-Ing. habil. Gerhard Rigoll
Prüfer der Dissertation: 1. Univ.-Prof. Dr. sc.techn. Andreas Herkersdorf
2. Univ.-Prof. Dr.-Ing. Georg Sigl

Die Dissertation wurde am 29.10.2015 bei der Technischen Universität München
eingereicht und durch die Fakultät für Elektrotechnik und Informationstechnik am
21.04.2016 angenommen.

Contents

1. Introduction	1
1.1. Motivation and Challenge	1
1.2. Contributions	2
2. Related Work and Problem Statement	7
2.1. Constraints and Architectures of Avionic Systems	7
2.2. System Architectures in Connecting I/O	13
2.3. Comparing System Architectures in Connecting I/O	17
2.4. Approaches to Hardware-Based I/O Virtualization	20
2.5. Non-Transparent Bridge(ing) (NTB)	23
2.6. Temporal Separation	25
2.7. Easing Safety Certification	27
2.8. Spatial Separation	31
2.9. Scaling	35
2.9.1. Multi Processor I/O Virtualization (MPIOV)	35
2.9.2. Safeguarding Interrupts (SgInt)	39
2.10. Problem Statement	43
3. Conceptual Solutions	45
3.1. Temporal Separation	45
3.1.1. Deliberation of Approaches	45
3.1.2. Concept	47
3.1.3. Implementation Considerations	51
3.1.4. Discussion of the Concept	54
3.2. Easing Safety Certification	54
3.2.1. Deliberation of Approaches	55
3.2.2. Concept	56
3.2.3. Implementation Considerations	62
3.2.4. Discussion of the Concept	63
3.3. Spatial Separation	65
3.3.1. Deliberation of Approaches	65
3.3.2. I/O Memory Management Unit Handshake Protocol (IOM- MUHP)	67
3.3.2.1. Concept	67
3.3.2.2. Implementation Considerations	70
3.3.2.3. Discussion of the Concept	72
3.3.3. I/O Memory Protection Unit (IOMPU)	72
3.3.3.1. Concept	72

3.3.3.2.	Implementation Considerations	75
3.3.3.3.	Discussion of the Concept	78
3.4.	Scaling	79
3.4.1.	Multi Processor I/O Virtualization (MPIOV)	79
3.4.1.1.	Deliberation of Approaches	80
3.4.1.2.	Concept	81
3.4.1.3.	Implementation Considerations	84
3.4.1.4.	Discussion of the Concept	86
3.4.2.	Safeguarding Interrupts (SgInt)	86
3.4.2.1.	Deliberation of Approaches	87
3.4.2.2.	Concept	88
3.4.2.3.	Implementation Considerations	89
3.4.2.4.	Discussion of the Concept	92
4.	Experimental Evaluation	95
4.1.	Temporal Separation	95
4.1.1.	Evaluation Setup	95
4.1.2.	Evaluation Results	97
4.1.3.	Discussion of the Evaluation	101
4.2.	Easing Safety Certification	102
4.2.1.	Evaluation Setup	102
4.2.2.	Evaluation Results	104
4.2.3.	Discussion of the Evaluation	107
4.3.	Spatial Separation	109
4.3.1.	I/O Memory Management Unit Handshake Protocol (IOM- MUHP)	109
4.3.1.1.	Evaluation Setup	109
4.3.1.2.	Evaluation Results	111
4.3.1.3.	Discussion of the Evaluation	111
4.3.2.	I/O Memory Protection Unit (IOMPU)	111
4.3.2.1.	Evaluation Setup	115
4.3.2.2.	Evaluation Results	117
4.3.2.3.	Discussion of the Evaluation	118
4.3.3.	Comparison IOMMUHP vs. IOMPU	120
4.4.	Scaling	123
4.4.1.	Multi Processor I/O Virtualization (MPIOV)	124
4.4.1.1.	Evaluation Setup	124
4.4.1.2.	Evaluation Results	125
4.4.1.3.	Discussion of the Evaluation	129
4.4.2.	Safeguarding Interrupts (SgInt)	129
4.4.2.1.	Evaluation Setup	129
4.4.2.2.	Evaluation Results	131
4.4.2.3.	Discussion of the Evaluation	133
5.	Conclusion & Outlook	137

A. Appendix	143
A.1. Issue Xilinx Virtex 7 PCIe SR-IOV ARI	143
List of Abbreviations	145
List of Figures	147
List of Tables	151
Bibliography	153