

# Obsah

---

<b>INTRODUCTION .....</b>	<b>4</b>
<b>1 RELATED WORKS .....</b>	<b>5</b>
1.1 FINDINGS AND OBSERVATIONS.....	6
1.2 COST EFFECTIVENESS.....	7
<b>2 SOFTWARE ENGINEERING AND FORMAL METHODS.....</b>	<b>9</b>
2.1 FORMAL LOGIC .....	14
2.2 FORMAL METHODS.....	15
2.2.1 <i>What Formal Methods are widely used?</i> .....	18
2.2.2 <i>Formal Methods Tool and Notations</i> .....	18
2.2.3 <i>Who uses Formal Methods for real systems?</i> .....	19
2.3 WHY TO USE FM TECHNIQUES? .....	20
2.3.1 <i>Data Collected [VSR 2009] [146].</i> .....	21
2.3.2 <i>Outcomes the Effects on time, cost and quality,</i> .....	25
<b>3 HIGHLIGHTED PROJECTS .....</b>	<b>27</b>
3.1 THE TRANSPUTER PROJECT .....	28
3.2 RAIL'S BIGGEST PROJECT .....	29
3.3 MONDEX SMART CARD.....	30
3.4 AAMP MICROPROCESSOR .....	31
3.5 AIRBUS .....	32
3.6 THE MAESLANT KERING STORM SURGE BARRIER .....	33
3.7 THE TOKENEER SECURE ENTRY SYSTEMS .....	34
3.8 THE „MOBILE FELICA“ IC CHIP FIRMWARE .....	36
<b>4 OBSERVATION .....</b>	<b>37</b>
4.1 LIGHTWEIGHT AND HEAVYWEIGHT FORMAL METHODS .....	37
4.2 TOOL SUPPORT .....	38
4.3 INCREASING AUTOMATION .....	39
4.4 COST EFFECTIVENES .....	40
4.5 THE VERIFIED SOFTWARE REPOSITORY .....	41
4.5.1 <i>Verified File Store</i> .....	42
4.5.2 <i>FreeRTOS</i> .....	43
4.5.3 <i>Radio Spectrum Auctions</i> .....	44
4.5.4 <i>Cardiac Pacemaker</i> .....	44
4.5.5 <i>Hypervisor</i> .....	44
<b>5 VITALITY OF FORMAL METHODS.....</b>	<b>45</b>
5.1 MATURITY OF TOOLS AND ADVANCES IN THEORY .....	47
5.2 EXPERIMENTATION .....	48
5.3 THE FUTURE.....	48
<b>6 TESTING: STATIC VS DYNAMIC ANALYSIS.....</b>	<b>50</b>
<b>7 FORMAL METHODS CONCEPTS .....</b>	<b>52</b>
<b>8 THE B-METHOD.....</b>	<b>56</b>
8.1 INTRODUCTION .....	56

8.2	TOOLS FOR B-METHOD.....	63
8.2.1	<i>Atelier B (ClearSy)</i> .....	63
8.2.2	<i>B4free (www.b4free.com)</i> .....	63
8.2.3	<i>The new version 4.4.2 of the atelierB</i> .....	63
8.2.4	<i>A Public Issues Tracker for AtelierB</i> .....	63
8.3	PROOF OBLIGATION MANAGEMENT FROM THE MODEL EDITORS.....	64
8.3.1	<i>Proof Mechanism Improvement</i> .....	64
8.3.2	<i>New features of the proof rules management tool (only in the maintenance edition)</i> .....	64
8.4	CASE STUDY – RAILWAY SIGNALLING AND TRAIN CONTROL PROJECT .....	65
<b>9</b>	<b>EVENT-B.....</b>	<b>68</b>
9.1.1	<i>Refinement</i> .....	69
9.1.2	<i>Decomposition</i> .....	69
9.1.3	<i>Modelling in Event-B</i> .....	70
9.1.4	<i>Event-B Proof Obligation</i> .....	71
9.2	MODELLING ELEMENTS .....	71
9.3	MODEL STATE.....	72
9.4	EVENT-B CONTEXT.....	73
9.5	EVENT-B MACHINE .....	74
9.6	BEHAVIOR MACHINE – EVENT-B.....	74
9.7	REFINEMENT MACHINE – EVENT-B .....	74
<b>10</b>	<b>CASE STUDY 1 – PROJECT TRANSMIT, USING THE FORMAL METHOD EVENT-B [170].....</b>	<b>76</b>
10.1	DIGITAL BROADCASTING .....	76
10.1.1	<i>Antenna parameters</i> .....	76
10.1.2	<i>Frequency spectrum</i> .....	76
10.1.3	<i>Transport stream</i> .....	77
10.2	MULTIPLEXES.....	77
10.3	TRANSMITTERS.....	78
10.4	SYSTEM BEHAVIOR USING EVENT-B .....	79
<b>11</b>	<b>CASE STUDY 2 – IMPROVED ADAPTIVE FAULT TOLERANCE MODEL FOR INCREASING RELIABILITY IN CLOUD COMPUTING USING EVENT-B [174].....</b>	<b>81</b>
11.1	PROPOSED MODEL .....	81
11.2	VIRTUAL MACHINES .....	83
11.3	ADJUDICATION NODE.....	83
11.4	FAULT TOLERANCE MECHANISM .....	84
11.5	RESULT AND EVALUATION .....	86
11.6	MODELING AND REFINEMENT EVENT-B.....	87
11.6.1	<i>Abstract Model</i> .....	88
11.6.2	<i>First refinement</i> .....	88
11.6.3	<i>Second refinement</i> .....	91
11.6.4	<i>Proof Statistics</i> .....	92
11.7	APPENDIX .....	92
11.7.1	<i>Abstract Model</i> .....	92
11.7.2	<i>First refinement</i> .....	94
11.7.3	<i>Second refinement</i> .....	98
<b>12</b>	<b>CONCLUSION .....</b>	<b>103</b>
<b>13</b>	<b>REFERENCES.....</b>	<b>105</b>