

Inhaltsverzeichnis

Danksagung i

Zusammenfassung iii

Abstract..... iv

TEIL I EINLEITUNG..... 1

1 Motivation und Ziel..... 3

1.1 Bedeutung eingebetteter Software..... 3

1.2 Einführung in die Entwicklung eingebetteter Software..... 4

1.3 Motivation für die Betrachtung sicherheitskritischer Fehler 6

1.4 Problemstellung..... 8

1.5 Ziel der Arbeit 9

1.6 Aufbau der Arbeit..... 10

2 Grundlagen 11

2.1 Software in eingebetteten Systemen..... 11

2.1.1 Sicherheit eingebetteter Software 12

2.1.2 Sicherheitskritische Fehler in eingebetteter Software 13

2.2 Softwaretest 14

2.2.1 Modellbasierter Softwaretest 15

2.2.2 Test eingebetteter Software..... 16

2.3 Sicherheitsanalyse 17

3 Stand der Wissenschaft 19

3.1 Bewertungsrahmen 19

3.2 Arbeiten zur codebasierten Testfallpriorisierung 21

3.2.1 Elbaum et al. und Rothermel et al. 1999 bis 2003 21

3.2.2 Elbaum et al. 2001 22

3.2.3 Kim und Porter 2002..... 23

3.2.4 Jones und Harrold 2003 23

3.2.5 Srivastava und Thiagarajan 2002 und Czerwonka et al. 2011 23

3.2.6 Walcott et al. 2006 und Zhang et al. 2009 24

3.2.7 Yoo et al. 2009..... 25

3.3 Arbeiten zur anforderungsbasierten Testfallpriorisierung 25

3.3.1 Chen et al. 2002 und 2003 26

3.3.2 Srikanth et al. 2005 und 2006 26

3.3.3 Ramasamy und Mary 2008 27

3.3.4 Srivastava et al. 2008 28

3.3.5 Le et al. 2009..... 28

| | | |
|---|---|-----------|
| 3.3.6 | Kumar et al. 2010..... | 29 |
| 3.4 | Arbeiten zur modellbasierten Testfallpriorisierung | 29 |
| 3.4.1 | Yu und Lau 2002..... | 29 |
| 3.4.2 | Korel et al. 2005 und 2007 | 30 |
| 3.4.3 | Fraser und Wotawa 2007..... | 31 |
| 3.4.4 | Malz et al. 2011..... | 31 |
| 3.5 | Sonstige Arbeiten zur Testfallpriorisierung..... | 32 |
| 3.5.1 | Srivastava 2008 und Kavitha und Sureshkumar 2010..... | 32 |
| 3.6 | Arbeiten von allgemeiner thematischer Relevanz..... | 33 |
| 3.6.1 | Risikobasierte Testfallableitung | 33 |
| 3.6.2 | Integration von Sicherheitsanalysen und Softwaretests | 35 |
| 3.6.3 | Integration von Sicherheitsanalysen und modellbasierter Softwareentwicklung | 36 |
| 3.7 | Zusammenfassende Bewertung und Fazit..... | 37 |
| TEIL II SICHERHEITSBASIERTE TESTFALLPRIORISIERUNG..... | | 41 |
| 4 | Lösungsansatz | 43 |
| 4.1 | Idee | 43 |
| 4.2 | Ausgestaltung | 43 |
| 4.2.1 | Priorisierung logischer Testfälle | 44 |
| 4.2.2 | Modellbasierte Testfallpriorisierung | 45 |
| 4.3 | Bestandteile | 45 |
| 5 | Dokumentation von Sicherheitsanalyseergebnissen | 49 |
| 5.1 | Verwendung von Sicherheitsanalyseergebnissen | 49 |
| 5.1.1 | Sicherheitsanalyse durch FMECA | 50 |
| 5.2 | Erstellung sicherheitsgerichteter Testmodelle | 51 |
| 5.2.1 | Verwendung von Aktivitätsdiagrammen..... | 52 |
| 5.2.2 | Abbildung von Kritizitätswerten auf Aktionen | 52 |
| 5.2.3 | Attributierung von Aktionen | 54 |
| 6 | Bewertung von Testfällen..... | 57 |
| 6.1 | Bewertungskriterien..... | 57 |
| 6.2 | Bewertung nach Modell- und Sicherheitsüberdeckung | 58 |
| 7 | Festlegung von Testfallfolgen | 61 |
| 7.1 | Priorisierungsansätze für Testfallmengen | 61 |
| 7.2 | Priorisierung nach Modellüberdeckung | 62 |
| 7.2.1 | Priorisierung nach totaler Aktionsüberdeckung | 62 |
| 7.2.2 | Priorisierung nach additionaler Aktionsüberdeckung | 62 |
| 7.3 | Priorisierung nach Sicherheitsüberdeckung..... | 63 |
| 7.3.1 | Priorisierung nach totaler Kritizitätsüberdeckung..... | 63 |
| 7.3.2 | Priorisierung nach additionaler Kritizitätsüberdeckung | 64 |
| 7.4 | Priorisierung nach kombinierter Modell- und Sicherheitsüberdeckung..... | 64 |

| | | |
|---|---|-----------|
| 7.4.1 | Priorisierung nach totaler Aktions- und Kritizitätsüberdeckung | 64 |
| 7.4.2 | Priorisierung nach additionaler Aktions- und Kritizitätsüberdeckung | 67 |
| 7.5 | Überblick und Anwendung | 69 |
| TEIL III EXPERIMENTELLE VALIDIERUNG..... | | 73 |
| 8 | Planung | 75 |
| 8.1 | Ziel | 75 |
| 8.2 | Forschungsfragestellungen | 76 |
| 8.3 | Metrik | 76 |
| 8.4 | Software | 78 |
| 8.4.1 | Autopiloten-Software | 79 |
| 8.4.2 | Avioniktypischer Softwareentwicklungsprozess | 79 |
| 8.5 | Fehler | 80 |
| 8.5.1 | Manuelle Fehlereinstreuung | 80 |
| 8.5.2 | Automatische Mutation | 81 |
| 8.5.3 | Erzeugung sicherheitskritischer Fehler | 82 |
| 8.5.4 | Manuelle Einstreuung sicherheitskritischer Fehler | 82 |
| 8.6 | Testfälle | 85 |
| 8.6.1 | Avioniktypisches Testziel | 85 |
| 8.6.2 | Modellbasierte Testfallentwicklung | 86 |
| 8.7 | Sicherheitsanalyseergebnisse | 89 |
| 9 | Durchführung | 91 |
| 9.1 | Testumgebung | 91 |
| 9.1.1 | Flugsimulatoren-Software | 91 |
| 9.1.2 | Integration der Autopiloten-Software | 92 |
| 9.2 | Pretest | 92 |
| 9.3 | Test | 93 |
| 9.4 | Priorisierungs-Software | 96 |
| 9.5 | Testfallpriorisierung | 97 |
| 9.5.1 | Sicherheitsbasierte Testfallpriorisierung | 98 |
| 9.5.2 | Nicht-sicherheitsbasierte Testfallpriorisierung | 99 |
| 9.5.3 | Kontrolltechniken | 101 |
| 9.5.4 | Überblick | 103 |
| 10 | Auswertung | 105 |
| 10.1 | Mess-Software | 105 |
| 10.2 | Statistik-Software | 106 |
| 10.3 | Deskriptive Statistik | 106 |
| 10.4 | Statistische Signifikanz | 109 |
| 10.5 | Effektstärke | 112 |
| 11 | Diskussion | 117 |

| | | |
|--|--|------------|
| 11.1 | Interpretation der Ergebnisse | 117 |
| 11.1.1 | Beantwortung der Forschungsfragestellungen | 117 |
| 11.1.2 | Untersuchung der Vorhersagbarkeit | 120 |
| 11.1.3 | Untersuchung des Verbesserungspotentials | 122 |
| 11.2 | Validität der Ergebnisse | 122 |
| 11.2.1 | Externe Validität | 122 |
| 11.2.2 | Interne Validität | 125 |
| 11.2.3 | Konstruktvalidität | 127 |
| TEIL IV ZUSAMMENFASSUNG UND AUSBLICK..... | | 129 |
| 12 | Beitrag der Arbeit | 131 |
| 13 | Kritische Betrachtung | 133 |
| 14 | Ausblick | 135 |
| 14.1 | Verbesserungspotential | 135 |
| 14.2 | Nutzenpotential | 136 |
| ANHANG | | 139 |
| A | Anforderungen | 141 |
| B | Testfälle | 143 |
| C | Testfallmengen | 161 |
| D | Sicherheitsanalyseergebnisse | 163 |
| E | Abbildungsverzeichnis | 167 |
| F | Tabellenverzeichnis | 169 |
| G | Definitionsverzeichnis | 171 |
| H | Beispielverzeichnis | 173 |
| I | Algorithmenverzeichnis | 175 |
| J | Literaturverzeichnis | 177 |