Inhaltsverzeichnis

Formelzeichen und Abkürzungen VIII

Kurzfassung – Abstract XII

1 Einleitung und Aufgabenstellung 1

1.1 Ausgangssituation und Problemstellung 2

1.2 Vorgehensweise und Aufbau der Arbeit 3

2 Stand der Forschung und Technik 4

2.1 Definition der mobilen Arbeitsmaschine 4

2.2 Mechatronische Systeme bei mobilen Arbeitsmaschinen 7

2.2.1 Elektronischer Eingriff in die Fahrzeugführung 10

2.2.2 Automatisierung von Arbeitsprozessen 15

2.2.3 Komponenten, Subsysteme, vernetzte Systeme 19

2.3 Entwicklungsprozesse und -modelle 23

2.3.1 Konventionelle Vorgehensweise 24

2.3.2 Verteilte Entwicklung verteilter Systeme 26

2.4 Stand der Normung 27

3 Funktionale Sicherheit als Teil der konstruktiven Sicherheit 31

3.1 Definition der funktionalen Sicherheit 31

3.2 Maßnahmen zur Gewährleistung des sicheren Zustands 33

3.3 Risikominderung bei mobilen Arbeitsmaschinen 34

4 Entwicklungsmethoden 37

4.1 Überblick über mögliche Methoden 38

4.2 Konventionelle Methoden für die Systementwicklung 38

4.2.1 Methoden zur Spezifikation und Systemauslegung 38

4.2.1.1 Systemstrukturanalyse 38

4.2.1.2 Bestimmung des Gefährdungspotenzials durch Risikoanalyse 40

4.2.1.3 System-FMEA nach VDA 4.2 43

4.2.1.4 Methoden zu Spezifikation und Design von Software 47

4.2.2 Methoden für Test und Validierung 49

4.2.2.1 Test von Funktionalität und Fehlerverhalten mechatronischer Systeme 50
4.2.2.2 Methoden zu Test und Validierung von Software 50
4.3 Modellbasierte Methoden für die Softwareentwicklung 51
4.3.1 Modellbasierte Spezifikation 55
4.3.2 Model-in-the-Loop (MIL) 56
4.3.3 Rapid-Control-Prototyping (RCP) 57
4.3.4 Software-in-the-Loop (SIL) 58
4.3.5 Automatische Generierung von Serien-Code 59
4.3.6 Hardware-in-the-Loop (HIL) 61

5 Sicherstellung der erforderlichen Systemintegrität – Entwicklungskonzept 63
5.1 Sicherheitsgerechte Systemarchitektur 64
5.2 Vorgehensmodell für System- und Softwareentwicklung 66
5.3 Entwicklungsschritte mit Zuordnung der Methoden und Maßnahmen 68
5.3.1 Analyse und Spezifikation der Systemanforderungen und -architektur 69
5.3.2 Analyse und Spezifikation der Softwareanforderungen und -architektur 69
5.3.3 Design der Softwaresubsysteme und -module 70
5.3.4 Implementierung und Codierung der Software 71
5.3.5 Test der Softwaresubsysteme und -module 72
5.3.6 Integrationstests der Software und Teilsysteme, Komponententests 73
5.3.7 Systemtest und Validierung 74
5.3.8 Universelle Maßnahmen für die gesamte Entwicklung 74

6 Anwendungsbeispiel „Gerät steuert Traktor“ mit Vorgewendeautomatik 76
6.1 Systembeschreibung und Aufbau der Automatiken 76
6.1.1 Versuchsträger und Elektronikkonzept 76
6.1.2 Messdatenerfassung 79
6.1.3 Aufbau der Automatiken 79
6.2 System- und Risikoanalyse der Automatisierungen 88
6.3 Entwicklung ausgewählter MSR-Sicherheitsfunktionen 92
6.3.1 Entwicklung einer fehlertoleranten Sensorerfassung 92
6.3.2 Entwicklung einer sicherheitsgerechten Ressourcenverteilung für den hydraulischen Durchfluss 95

6.3.3 Modellbasierte Entwicklung des Traktorrechners – Geschwindigkeitsregelung 100
6.3.4 Modellbasierte Entwicklung des Rechners der Kreiselegge – automatische Generierung von Serien-Code 102

7 Versuchsdurchführung und Verallgemeinerung der Ergebnisse 106
7.1 Überwachung sicherheitsrelevanter Prozessgrößen 106
7.1.1 Überwachung gültiger Bereiche sicherheitsrelevanter Prozessparameter 107
7.1.2 Plausibilisierung sicherheitsrelevanter Parameter 110
7.1.3 Konkurrierende Zugriffe auf Systemressourcen 112
7.1.3.1 Konflikte beim gemeinsamen Zugriff auf den hydraulischen Ölstrom 112
7.1.3.2 Konflikte beim gemeinsamen Zugriff auf die Soll-Geschwindigkeit 116
7.1.3.3 Fazit 117
7.2 Koordination von Bewegungsabläufen 118
7.3 Sicherheitsgerechtes Verhalten der Teilsysteme im Fehlerfall 120
7.4 Korrekte Interpretation und Verarbeitung des Fahrereingriffs 122

8 Zusammenfassung 124

9 Anhang 126
9.1 Bewertungskatalog System-FMEA (angepasst an mobile Arbeitsmaschinen) 126
9.2 Matrix analytisch herleitbarer Betriebs- und Schnittstellenzustände 130

10 Literatur 132