DIN EN 16590-3:2015-04 (E)

Tractors and machinery for agriculture and forestry - Safety-related parts of control systems - Part 3: Series development, hardware and software (ISO 25119-3:2010 modified)

Contents

Page

Foreword 4

Introduction 5

1 Scope 7

2 Normative references 7

3 Terms and definitions 7

4 Abbreviated terms 7

5 System design 8
5.1 Objectives 8
5.2 General 8
5.3 Prerequisites 9
5.4 Requirements 9
5.4.1 Structuring safety requirements 9
5.4.2 Functional safety concept 10
5.4.3 Technical safety concept 11

6 Hardware 13
6.1 Objectives 13
6.2 General 13
6.3 Prerequisites 14
6.4 Requirements 14
6.5 Hardware categories 15
6.6 Work products 16

7 Software 16
7.1 Software development planning 16
7.1.1 Objectives 16
7.1.2 General 17
7.1.3 Prerequisites 17
7.1.4 Requirements 17
7.1.5 Work products 20
7.2 Software safety requirements specification 20
7.2.1 Objectives 20
7.2.2 General 20
7.2.3 Prerequisites 20
7.2.4 Requirements 21
7.2.5 Work products 24
7.3 Software architecture and design 24
7.3.1 Objectives 24
7.3.2 General 24
7.3.3 Prerequisites 24
7.3.4 Requirements 24
7.3.5 Work products 27
7.4 Software module design and implementation 27

7.4.1 Objectives ... 27
7.4.2 General ... 27
7.4.3 Prerequisites ... 27
7.4.4 Requirements ... 27
7.4.5 Work products ... 36
7.5 Software module testing ... 36
7.5.1 Objectives ... 36
7.5.2 General ... 36
7.5.3 Prerequisites ... 36
7.5.4 Requirements ... 36
7.5.5 Work products ... 44
7.6 Software integration and testing ... 44
7.6.1 Objectives ... 44
7.6.2 General ... 44
7.6.3 Prerequisites ... 45
7.6.4 Requirements ... 45
7.6.5 Work products ... 46
7.7 Software safety validation ... 47
7.7.1 Objectives ... 47
7.7.2 General ... 47
7.7.3 Prerequisites ... 47
7.7.4 Requirements ... 47
7.7.5 Work products ... 49
7.8 Software-based parameterisation ... 49
7.8.1 Objective ... 49
7.8.2 General ... 49
7.8.3 Prerequisites ... 49
7.8.4 Requirements ... 50
7.8.5 Work products ... 50

Annex A (informative) Example of agenda for assessment of functional safety at AgPL = e ... 52

A.1 Functions of system ... 52
A.2 Hardware ... 52
A.3 Safety concept ... 52
A.4 Safety analysis and safety data ... 52
A.5 Safety design process for phases of life cycle ... 52
A.6 Software development ... 53
A.7 Verification and testing ... 53
A.8 Documentation and safety documentation ... 53
A.9 Summary and assessment ... 53

Annex B (informative) Independence by software partitioning ... 54

B.1 General ... 54
B.2 Terms, definitions and abbreviated terms ... 54
B.3 Objectives ... 56
B.4 General ... 57
B.5 Requirements ... 57
B.5.1 General requirements ... 57
B.5.2 Several partitions within a single microcontroller ... 57
B.5.3 Several partitions within the scope of a micro-controller network ... 60

Annex ZA (informative) Relationship between this European Standard and the Essential Requirements of EU Machinery Directive 2006/42/EC ... 63

Bibliography ... 64