DIN EN 16590-2:2014-11 (E)

Tractors and machinery for agriculture and forestry - Safety-related parts of control systems - Part 2: Concept phase (ISO 25119-2:2010 modified)

Contents

Page

Foreword 5

Introduction 6

1 Scope 8

2 Normative references 8

3 Terms and definitions 8

4 Abbreviated terms 8

5 Concept -- Unit of observation 9
5.1 Objectives 9
5.2 Prerequisites 9
5.3 Requirements 9
5.3.1 Unit of observation and ambient conditions 9
5.3.2 Limits of unit of observation and its interfaces with other units of observation 10
5.3.3 Sources of stress 10
5.3.4 Additional determinations 10
5.4 Work products 11

6 Risk analysis and method description 11
6.1 Objectives 11
6.2 Prerequisites 11
6.3 Requirements 11
6.3.1 Procedures for preparing a risk analysis 11
6.3.2 Tasks in risk analysis 11
6.3.3 Participants in risk analysis 11
6.3.4 Assessment and classification of a potential harm 11
6.3.5 Assessment of exposure in the situation observed 12
6.3.6 Assessment of a possible avoidance of harm 12
6.3.7 Selecting the required AgPLr 13
6.4 Work products 15

7 System design 15
7.1 Objectives 15
7.2 Prerequisites 15
7.3 Requirements 15
7.3.1 Assignment of AgPL 15
7.3.2 Achieving the required AgPLr 16
7.3.3 Achievement of the performance level 17
7.4 Work products 17

Annex A (normative) Designated architectures for SRP/CS 18

A.1 General 18
A.2 Category B (basic) 18
A.3 Category 1 19
A.4 Category 2 19
A.5 Category 3 20

A.6 Category 4 22

Annex B (informative) Simplified method to estimate channel MTTFdC 24

B.1 General 24
B.2 Component MTTFd values 24
B.2.1 Determination of component MTTFd values 24
B.2.2 MTTFd for components from B10 25
B.3 Parts count method 25
B.4 Calculation of symmetric MTTFdC for two-channel architectures 26

Annex C (informative) Determination of diagnostic coverage (DC) 27

C.1 General 27
C.2 Estimation of the required DC 27
C.3 Estimation of channel DC 29
C.4 Calculation of channel DC 30
C.5 Calculation of DC 30

Annex D (informative) Estimates for common-cause failure (CCF) 31

Annex E (informative) Systematic failure 33

E.1 General 33
E.2 Procedure for the control of systematic failures 33
E.3 Procedure for the avoidance of systematic failures 33

Annex F (informative) Characteristics of safety functions 36

F.1 General 36
F.2 Start interlock 36
F.3 Stop function 36
F.4 Manual reset 36
F.5 Start and restart 37
F.6 Response time 37
F.7 Safety-related parameters 37
F.8 External control function 37
F.9 Muting (manual suspension of safety functions) 37
F.10 Operator warning 37

Annex G (informative) Example of a risk analysis 38

G.1 Workflow 38
G.2 Example risk analysis of an electro-hydraulic transmission for a self-propelled working machine (forage harvester) -- Extract from a complete risk analysis 38
G.2.1 System description 38
G.2.2 Surrounding conditions 39
G.2.3 System states and transitions 39
G.2.4 System failures 40
G.3 Assessment 41
G.3.1 System failure -- Stops unintentionally 41
G.3.2 System failure -- Does not move when commanded 42
G.4 Results 42

Annex ZA (informative) Relationship between this European Standard and the Essential Requirements of EU Machinery Directive 2006/42/EC 43

Bibliography 44