

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

Traktoren und Maschinen für die Land- und Forstwirtschaft - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Konzeptphase (ISO 25119-2:2010 modifiziert);
Deutsche Fassung EN 16590-2:2014

Inhalt	Seite
Vorwort	4
Einleitung	5
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Abkürzungen.....	7
5 Konzept — Definition der Betrachtungseinheit	8
5.1 Ziele.....	8
5.2 Voraussetzungen.....	8
5.3 Anforderungen.....	9
5.3.1 Betrachtungseinheit und Umgebungsbedingungen	9
5.3.2 Grenzen der Betrachtungseinheit und ihre Schnittstellen zu anderen Betrachtungseinheiten.....	9
5.3.3 Gefährdungsquellen.....	9
5.3.4 Weitere Festlegungen	10
5.3.5 Arbeitsprodukte.....	10
6 Risikoanalyse und Methodenbeschreibung	10
6.1 Ziele.....	10
6.2 Voraussetzungen.....	10
6.3 Anforderungen.....	11
6.3.1 Verfahren zur Erstellung einer Risikoanalyse	11
6.3.2 Aufgaben bei der Risikoanalyse	11
6.3.3 Teilnehmer an der Risikoanalyse	11
6.3.4 Beurteilung und Klassifizierung eines potentiellen Schadens.....	11
6.3.5 Beurteilung der Aufenthaltsdauer in der beobachteten Situation	12
6.3.6 Beurteilung einer möglichen Schadensvermeidung	12
6.3.7 Herleitung des geforderten Performance Levels AgPL _r	13
6.4 Arbeitsprodukte.....	14
7 Systementwurf.....	14
7.1 Ziele.....	14
7.2 Voraussetzungen.....	14
7.3 Anforderungen.....	14
7.3.1 Zuweisung des AgPL	14
7.3.2 Erreichen des geforderten landwirtschaftlichen Performance Levels AgPL _r	15
7.3.3 Erreichen des Performance Levels	16
7.4 Arbeitsprodukte.....	16
Anhang A (normativ) Vorgesehene Architekturen für sicherheitsbezogene Teile von Steuerungen.....	17
A.1 Allgemeines	17
A.2 Kategorie B (elementar).....	17
A.3 Kategorie 1	18
A.4 Kategorie 2	18
A.5 Kategorie 3	19
A.6 Kategorie 4.....	21

Anhang B (informativ) Vereinfachtes Verfahren zur Abschätzung der Kanal-MTTF_{dC}	24
B.1 Allgemeines	24
B.2 MTTF _d -Werte für Bauteile	24
B.2.1 Bestimmung der MTTF _d -Werte für Bauteile	24
B.2.2 MTTF _d für Bauteile von B ₁₀	25
B.3 „Parts Count“-Verfahren	25
B.4 Berechnung der symmetrischen MTTF _{dC} für Zweikanalarchitekturen	26
Anhang C (informativ) Bestimmung des Diagnosedeckungsgrads (DC)	27
C.1 Allgemeines	27
C.2 Schätzung des geforderten DC	27
C.3 Schätzung des Kanal-DC	30
C.4 Berechnung des Kanal-DC	30
C.5 Berechnung des DC	31
Anhang D (informativ) Schätzung von Ausfällen gemeinsamer Ursache (CCF)	32
Anhang E (informativ) Systematischer Ausfall	34
E.1 Allgemeines	34
E.2 Anforderungen an die Beherrschung systematischer Ausfälle	34
E.3 Anforderungen an das Vermeiden systematischer Ausfälle	35
Anhang F (informativ) Merkmale von Sicherheitsfunktionen	37
F.1 Allgemeines	37
F.2 Anlaufverriegelung	37
F.3 Stoppfunktion	37
F.4 Manuelle Rückstellung	37
F.5 Anlauf und Wiederanlauf	38
F.6 Ansprechzeit	38
F.7 Sicherheitsbezogene Parameter	38
F.8 Externe Steuerfunktion	38
F.9 Muting (Aussetzung von Sicherheitsfunktionen von Hand)	39
F.10 Warnung des Maschinenführers	39
Anhang G (informativ) Beispiel einer Risikoanalyse	40
G.1 Arbeitsablauf	40
G.2 Beispiel einer Risikoanalyse eines Elektro-Hydraulikgetriebes für eine selbstfahrende Arbeitsmaschine (Futtererntemaschine) — Auszug aus einer vollständigen Risikoanalyse	40
G.2.1 Systembeschreibung	40
G.2.2 Umgebungsbedingungen	41
G.2.3 Systemzustände und Übergänge	41
G.2.4 Systemfehler	42
G.3 Beurteilung	43
G.3.1 Systemfehler — Unbeabsichtigtes Anhalten	43
G.3.2 Systemfehler — Trotz Anweisung keine Bewegung	44
G.4 Ergebnisse	44
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2006/42/EG	45
Literaturhinweise	46