

E DIN EN ISO 25119-2:2022-02 (D/E)

Erscheinungsdatum: 2022-01-07

Traktoren und Maschinen für die Land- und Forstwirtschaft - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Konzeptphase (ISO 25119-2:2019); Deutsche und Englische Fassung prEN ISO 25119-2:2021

Tractors and machinery for agriculture and forestry - Safety-related parts of control systems - Part 2: Concept phase (ISO 25119-2:2019); German and English version prEN ISO 25119-2:2021

Inhalt	Seite
Europäisches Vorwort.....	5
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2006/42/EG.....	6
Vorwort	7
Einleitung	8
1 Anwendungsbereich.....	10
2 Normative Verweisungen	11
3 Begriffe	11
4 Abkürzungen	11
5 Konzept — UoO	12
5.1 Ziele	12
5.2 Voraussetzungen	12
5.3 Anforderungen.....	12
5.3.1 Grundlegende Anforderungen und Umgebungsbedingungen.....	12
5.3.2 Grenzen der UoO und ihrer Schnittstellen zu anderen UoO.....	13
5.3.3 Abbildung und Zuordnung relevanter Funktionen zu beteiligten UoO, Gefährdungsquellen	13
5.3.4 Weitere Festlegungen	13
5.4 Arbeitsprodukte	14
6 HARA — Bestimmung des AgPL _r	14
6.1 Ziele	14
6.2 Voraussetzungen	14
6.3 Anforderungen.....	14
6.3.1 Verfahren zur Erstellung einer HARA.....	14
6.3.2 Aufgaben im Rahmen der HARA	14
6.3.3 Teilnehmer der HARA.....	15
6.3.4 Klassifizierung eines potenziellen Schadens	15
6.3.5 Beurteilung der Aufenthaltshäufigkeiten oder -dauer in der beobachteten Situation	15
6.3.6 Klassifizierung einer möglichen Schadensvermeidung.....	16
6.3.7 Auswahl des AgPL _r	17
6.4 Arbeitsprodukte	19
7 Funktionales Sicherheitskonzept	19
7.1 Ziele	19
7.2 Voraussetzungen	19
7.3 Anforderungen.....	19
7.3.1 Sicherheitsziele.....	19

7.3.2	Funktionale Sicherheitsanforderungen.....	19
7.3.3	Wert von $MTTF_D$	20
7.3.4	Wert für DC.....	20
7.3.5	Auswahl von Kategorien, $MTTF_{DC}$, DC und SRL.....	21
7.3.6	Erreichen des $AgPL_r$	22
7.3.7	Kompatibilität mit anderen funktionalen Sicherheitsnormen	22
7.3.8	Verbindung von E/E/PES.....	22
7.3.9	Alternative Kombinationen von SRP/CS zur Erreichung des Gesamt- $AgPL$	22
7.4	Arbeitsprodukte	23
Anhang A (normativ) Vorgesehene Architekturen für SRP/CS.....		24
A.1	Allgemeines.....	24
A.2	Kategorie B (elementar)	25
A.2.1	Allgemeines.....	25
A.2.2	Eigenschaften	25
A.3	Kategorie 1	25
A.3.1	Allgemeines.....	25
A.3.2	Eigenschaften	25
A.4	Kategorie 2	26
A.4.1	Allgemeines.....	26
A.4.2	Eigenschaften	27
A.5	Kategorie 3	28
A.5.1	Allgemeines.....	28
A.5.2	Eigenschaften	28
A.6	Kategorie 4	30
A.6.1	Allgemeines.....	30
A.6.2	Eigenschaften	30
Anhang B (informativ) Vereinfachtes Verfahren zur Abschätzung der Kanal- $MTTF_{DC}$		32
B.1	Allgemeines.....	32
B.2	$MTTF_D$ -Werte von Bauteilen.....	32
B.2.1	Bestimmung der $MTTF_D$ -Werte von Bauteilen aus Normen/Datenbanken	32
B.2.2	Bestimmung der $MTTF_D$ -Werte von Bauteilen anhand von im Einsatz bewährten Bauteilen	33
B.2.3	$MTTF_D$ für Bauteile aus B_{10}	34
B.3	„Parts Count“-Verfahren	35
B.4	Berechnung der symmetrischen $MTTF_{DC}$ für Zweikanal-Architekturen.....	36
Anhang C (informativ) Bestimmung des Diagnosedeckungsgrads (DC).....		37
C.1	Allgemeines.....	37
C.2	Schätzung des geforderten DC	37
C.3	Schätzung des Kanal-DC.....	42
C.4	Berechnung des Kanal-DC	42
C.5	Beispielberechnung des Kanal-DC.....	43
Anhang D (informativ) Schätzung von Ausfällen infolge gemeinsamer Ursache (CCF)		44
Anhang E (informativ) Systematischer Ausfall		46
E.1	Allgemeines.....	46
E.2	Anforderungen an die Beherrschung systematischer Ausfälle.....	46
E.3	Anforderungen an das Vermeiden systematischer Ausfälle	47
Anhang F (informativ) Merkmale von Sicherheitsfunktionen, die oftmals grundlegend für die Risikoreduzierung sind.....		49
F.1	Allgemeines.....	49
F.2	Anlaufsperrung	49
F.3	Stoppfunktion.....	49
F.4	Manuelle Rückstellung	49
F.5	Anlauf und Wiederanlauf.....	50

F.6	Schließzeit	50
F.7	Sicherheitsbezogene Parameter.....	50
F.8	Externe Steuerfunktion	51
F.9	Muting (Aussetzung von Sicherheitsfunktionen von Hand).....	51
F.10	Warnung der Bedienperson.....	51
Anhang G (informativ) Beispiel einer Risikoanalyse		52
G.1	Arbeitsablauf	52
G.2	Beispiel einer Risikoanalyse eines Elektro-Hydraulikgetriebes für eine selbstfahrende Arbeitsmaschine (Feldhäcksler) — Auszug aus einer vollständigen Risikoanalyse.....	52
G.2.1	Systembeschreibung	52
G.2.2	Umgebungsbedingungen	53
G.2.3	Systemzustände und Übergänge	53
G.2.4	Systemfehler	54
G.3	Beurteilung.....	55
G.3.1	Systemfehler — Unbeabsichtigtes Anhalten	55
G.3.2	Systemfehler — Trotz Anweisung keine Bewegung.....	56
G.4	Ergebnisse.....	56
Anhang H (normativ) Kompatibilität mit anderen funktionalen Sicherheitsnormen		57
H.1	Übersicht.....	57
H.2	Allgemeines.....	57
H.3	Mit IEC 61508 (alle Teile) konforme Systeme oder SRP/CS	57
H.4	Mit ISO 13849 (alle Teile) konforme Systeme oder SRP/CS.....	58
H.5	Mit ISO 26262 (alle Teile) konforme Systeme oder SRP/CS.....	59
Anhang I (informativ) Alternatives Konformitätsverfahren für verbundene Systeme		60
Anhang J (normativ) Alternative Kombinationen von SRP/CS zur Erreichung des Gesamt-AgPL		61
J.1	SRP/CS in Reihe.....	61
J.1.1	Allgemeines	61
J.1.2	Reihenabschätzung.....	61
J.1.3	Datenkommunikationen.....	62
J.2	Komplexe Kombinationen von SRP/CS zur Erreichung des Gesamt-AgPL	62
Literaturhinweise		63