

DIN EN ISO 25119-2:2024-07 (D)

Traktoren und Maschinen für die Land- und Forstwirtschaft - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Konzeptphase (ISO 25119-2:2019); Deutsche Fassung EN ISO 25119-2:2023

Inhalt	Seite
Europäisches Vorwort.....	10
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2006/42/EG.....	11
Vorwort.....	17
Einleitung.....	18
1 Anwendungsbereich.....	20
2 Normative Verweisungen.....	21
3 Begriffe.....	21
4 Abkürzungen.....	21
5 Konzept — UoO.....	22
5.1 Ziele.....	22
5.2 Voraussetzungen.....	22
5.3 Anforderungen.....	22
5.3.1 Grundlegende Anforderungen und Umgebungsbedingungen.....	22
5.3.2 Grenzen der UoO und ihrer Schnittstellen zu anderen UoO.....	23
5.3.3 Abbildung und Zuordnung relevanter Funktionen zu beteiligten UoO, Quellen von Beanspruchung.....	23
5.3.4 Weitere Festlegungen.....	23
5.4 Arbeitsprodukte.....	24
6 HARA — Bestimmung des AgPL _r	24
6.1 Ziele.....	24
6.2 Voraussetzungen.....	24
6.3 Anforderungen.....	24
6.3.1 Verfahren zur Erstellung einer HARA.....	24
6.3.2 Aufgaben im Rahmen der HARA.....	24
6.3.3 Teilnehmer der HARA.....	25
6.3.4 Klassifizierung eines potentiellen Schadens.....	25
6.3.5 Klassifizierung der Exposition in der beobachteten Situation.....	25
6.3.6 Klassifizierung einer möglichen Schadensvermeidung.....	26
6.3.7 Auswahl des AgPL _r	27
6.4 Arbeitsprodukte.....	29
7 Funktionales Sicherheitskonzept.....	29
7.1 Ziele.....	29
7.2 Voraussetzungen.....	29
7.3 Anforderungen.....	29
7.3.1 Sicherheitsziele.....	29
7.3.2 Funktionale Sicherheitsanforderungen.....	29
7.3.3 Wert von MTTF _D	30
7.3.4 Wert für DC.....	30
7.3.5 Auswahl von Kategorien, MTTF _{DC} , DC und SRL.....	30
7.3.6 Erreichen des AgPL _r	31

7.3.7	Kompatibilität mit anderen funktionalen Sicherheitsnormen	32
7.3.8	Verbindung von E/E/PES	32
7.3.9	Alternative Kombinationen von SRP/CS zur Erreichung des Gesamt-AgPL.....	32
7.4	Arbeitsprodukte	32
Anhang A (normativ) Vorgesehene Architekturen für SRP/CS.....		34
A.1	Allgemeines.....	34
A.2	Kategorie B (elementar)	34
A.2.1	Allgemeines.....	34
A.2.2	Eigenschaften	34
A.3	Kategorie 1	35
A.3.1	Allgemeines.....	35
A.3.2	Eigenschaften	35
A.4	Kategorie 2	36
A.4.1	Allgemeines.....	36
A.4.2	Eigenschaften	36
A.5	Kategorie 3	38
A.5.1	Allgemeines.....	38
A.5.2	Eigenschaften	38
A.6	Kategorie 4	40
A.6.1	Allgemeines.....	40
A.6.2	Eigenschaften	40
Anhang B (informativ) Vereinfachtes Verfahren zur Abschätzung der Kanal-MTTF_{DC}.....		42
B.1	Allgemeines.....	42
B.2	MTTF _D -Werte von Bauteilen.....	42
B.2.1	Bestimmung der MTTF _D -Werte von Bauteilen aus Normen/Datenbanken	42
B.2.2	Bestimmung der MTTF _D -Werte von Bauteilen anhand von im Einsatz bewährten Bauteilen	43
B.2.3	MTTF _D für Bauteile aus B ₁₀	44
B.3	„Parts Count“-Verfahren	45
B.4	Berechnung der symmetrischen MTTF _{DC} für Zweikanal-Architekturen.....	46
Anhang C (informativ) Bestimmung des Diagnosedeckungsgrads (DC).....		47
C.1	Allgemeines.....	47
C.2	Schätzung des geforderten DC	47
C.3	Schätzung des Kanal-DC	52
C.4	Berechnung des Kanal-DC	52
C.5	Beispielberechnung des Kanal-DC.....	53
Anhang D (informativ) Schätzung von Ausfällen infolge gemeinsamer Ursache (CCF)		54
Anhang E (informativ) Systematischer Ausfall		56
E.1	Allgemeines.....	56
E.2	Verfahrensweise für die Beherrschung systematischer Ausfälle.....	56
E.3	Verfahrensweise für das Vermeiden systematischer Ausfälle	57
Anhang F (informativ) Merkmale von Sicherheitsfunktionen, die oftmals grundlegend für die Risikoreduzierung sind		59
F.1	Allgemeines.....	59
F.2	Anlaufsperrung	59
F.3	Stoppfunktion.....	59
F.4	Manuelle Rückstellung	59
F.5	Anlauf und Wiederanlauf.....	60
F.6	Schließzeit	60
F.7	Sicherheitsbezogene Parameter	60
F.8	Externe Steuerfunktion	60
F.9	Muting (Aussetzung von Sicherheitsfunktionen von Hand).....	61
F.10	Warnung der Bedienperson	61
Anhang G (informativ) Beispiel einer Risikoanalyse		62

G.1	Arbeitsablauf	62
G.2	Beispiel einer Risikoanalyse eines Elektro-Hydraulikgetriebes für eine selbstfahrende Arbeitsmaschine (Feldhäcksler) — Auszug aus einer vollständigen Risikoanalyse	62
G.2.1	Systembeschreibung	62
G.2.2	Umgebungsbedingungen	63
G.2.3	Systemzustände und Übergänge	63
G.2.4	Systemfehler	64
G.3	Beurteilung.....	65
G.3.1	Systemfehler — Unbeabsichtigtes Anhalten	65
G.3.2	Systemfehler — Trotz Anweisung keine Bewegung.....	66
G.4	Ergebnisse.....	66
Anhang H (normativ) Kompatibilität mit anderen funktionalen Sicherheitsnormen		67
H.1	Übersicht.....	67
H.2	Allgemeines.....	67
H.3	Mit IEC 61508 (alle Teile) konforme Systeme oder SRP/CS.....	67
H.4	Mit ISO 13849 (alle Teile) konforme Systeme oder SRP/CS.....	68
H.5	Mit ISO 26262 (alle Teile) konforme Systeme oder SRP/CS.....	68
Anhang I (informativ) Alternatives Konformitätsverfahren für verbundene Systeme		70
Anhang J (normativ) Alternative Kombinationen von SRP/CS zur Erreichung des Gesamt-AgPL		71
J.1	SRP/CS in Reihe.....	71
J.1.1	Allgemeines.....	71
J.1.2	Reihenabschätzung.....	71
J.1.3	Datenkommunikation.....	72
J.2	Komplexe Kombinationen von SRP/CS zur Erreichung des Gesamt-AgPL	72
Literaturhinweise		73
Bilder		
Bild 1 — Bestimmung des AgPL _r		29
Bild 2 — Beziehung zwischen AgPL, Kategorien, MTTF _{DC} , DC und SRL		31
Bild 3 — Schema einer Kombination sicherheitsbezogener Teile.....		32
Bild A.1 — Vorgesehene Architektur für Kategorie 2		36
Bild A.2 — Vorgesehene Architektur für Kategorie 3		38
Bild A.3 — Vorgesehene Architektur für Kategorie 4		40
Bild G.1 — Grundaufbau des Antriebsstrangs		63
Bild G.2 — Zustandsdiagramm		64
Bild J.1 — Reihenabschätzung		71
Tabellen		
Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und Anhang I der Richtlinie 2006/42/EG.....		11

Tabelle ZA.2 — Anwendbare Normen, die die Konformitätsvermutung gemäß diesem Anhang ZA begründen.....	15
Tabelle 1 — Klassifizierung von Verletzungen	25
Tabelle 2 — Klassifizierung der Exposition gegenüber der Gefährdungssituation	26
Tabelle 3 — Klassifizierung der Schadensvermeidung.....	26
Tabelle 4 — Mittlere Zeit bis zum gefahrbringenden Ausfall.....	30
Tabelle 5 — Diagnosedeckungsgrad (DC).....	30
Tabelle B.1 — Beispiel einer $MTTF_{DC}$-Berechnung für eine Platine	45
Tabelle C.1 — Elektrische Subsysteme (ohne Mikrocontroller)	47
Tabelle C.2 — Elektronische Subsysteme (mit Mikrocontrollern).....	47
Tabelle C.3 — Prozessoren	48
Tabelle C.4 — Unveränderliche Speicherbereiche	48
Tabelle C.5 — Veränderliche Speicherbereiche	49
Tabelle C.6 — I/O-Einheiten und Schnittstelle (externe Kommunikation)	49
Tabelle C.7 — Stromversorgung (gilt für Systeme mit und ohne Mikrocontroller).....	50
Tabelle C.8 — Programmablaufüberwachung	51
Tabelle C.9 — Geschätzter DC	52
Tabelle C.10 — Berechneter DC	53
Tabelle D.1 — Prozess zur Bewertung von Maßnahmen gegen CCF	54
Tabelle D.2 — Quantifizierung von Ausfällen infolge gemeinsamer Ursache.....	55
Tabelle G.1 — Systemfehler— Unbeabsichtigtes Anhalten.....	65
Tabelle G.2 — Szenario 1	66
Tabelle G.3 — Szenario 2	66
Tabelle H.1	68
Tabelle J.1 — Berechnung des AgPL für in Reihe angeordnete SRP/CS	72