

ISO 25119-2:2018 (E)

Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 2: Concept phase

Contents

	Foreword
	Introduction
1	Scope
2	Normative references
3	Terms and definitions
4	Abbreviated terms
5	Concept — UoO
5.1	Objectives
5.2	Prerequisites
5.3	Requirements
5.3.1	Basic requirements and ambient conditions
5.3.2	Limits of UoO and its interfaces with other UoO
5.3.3	Mapping and allocation of relevant functions to involved UoO, sources of stress
5.3.4	Additional determinations
5.4	Work products
6	HARA — Determination of the AgPLr
6.1	Objectives
6.2	Prerequisites
6.3	Requirements
6.3.1	Procedures for preparing a HARA
6.3.2	Tasks in the HARA
6.3.3	Participants in HARA
6.3.4	Classification of a potential harm
6.3.5	Classification of exposure in the situation observed
6.3.6	Classification of a possible avoidance of harm
6.3.7	Selecting the AgPLr
6.4	Work products
7	Functional safety concept
7.1	Objectives
7.2	Prerequisites
7.3	Requirements
7.3.1	Safety goals
7.3.2	Functional safety requirements
7.3.3	Value of MTTFD
7.3.4	Value of DC
7.3.5	Selection of categories, MTTFDC, DC and SRL
7.3.6	Achieving the AgPLr
7.3.7	Compatibility with other functional safety standards
7.3.8	Joining E/E/PES
7.3.9	Alternate combinations of SRP/CS to achieve overall AgPL
7.4	Work products
Annex A	(normative) Designated architectures for SRP/CS
A.1	General
A.2	Category B (basic)

- A.2.1 General
- A.2.2 Properties
- A.3 Category 1
- A.3.1 General
- A.3.2 Properties
- A.4 Category 2
- A.4.1 General
- A.4.2 Properties
- A.5 Category 3
- A.5.1 General
- A.5.2 Properties
- A.6 Category 4
- A.6.1 General
- A.6.2 Properties

Annex B (informative) Simplified method to estimate channel MTTFDC

- B.1 General
- B.2 Component MTTFD values
 - B.2.1 Determination of component MTTFD values from standards/databases
 - B.2.2 Determination of component MTTFD values from proven in use components
 - B.2.3 MTTFD for components from B10
- B.3 Parts count method
- B.4 Calculation of symmetric MTTFDC for two-channel architectures

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

- C.1 General
- C.2 Estimation of the required DC
- C.3 Estimation of channel DC
- C.4 Calculation of channel DC
- C.5 Example calculation of channel DC

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

Annex E (informative) Systematic failure

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

Annex F (informative) Characteristics of safety-related functions that are often fundamental to risk reduction

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

Annex G (informative) Example of a risk analysis

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

Annex H (normative) Compatibility with other functional safety standards

- H.1 Overview**
- H.2 General**
- H.3 IEC 61508 (all parts) compliant systems or SRP/CS's**
- H.4 ISO 13849 (all parts) compliant systems or SRP/CS's**
- H.5 ISO 26262 (all parts) compliant systems or SRP/CS's**

Annex I (informative) Joined systems alternative compliance method

Annex J (normative) Alternate combinations of SRP/CS to achieve overall AgPL

- J.1 SRP/CS in series**
 - J.1.1 General**
 - J.1.2 Series estimation**
 - J.1.3 Data communication**
- J.2 Complex combinations of SRP/CS to achieve overall AgPL**

Page count: 47