ISO 19014-2:2026-10 (E)

Earth-moving machinery - Functional safety - Part 2: Design and evaluation of hardware and architecture requirements for safety-related parts of the control system

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Symbols and abbreviated terms 3

5 General requirements 4
5.1 Application 4
5.2 Existing safety control system (SCS) 4
5.3 Safety requirements and/or protective/risk reduction measures 4

6 System design 4
6.1 Overview 4
6.2 General requirements 5
6.3 Hardware design 5

7 System safety performance evaluation 6
7.1 Machine performance level achieved (MPLa) 6
7.2 Hardware safety evaluation 7
7.2.1 General 7
7.2.2 Fault consideration 7
7.2.3 Fault exclusion 7
7.2.4 Mean time to dangerous failure (MTTFd) 7
7.3 Diagnostic coverage (DC) 8
7.3.1 Diagnostic coverage(DC) of electronic safety control systems (ESCS) 8
7.3.2 Diagnostic coverage (DC) of non-electronic safety control systems (N/ESCS) 8
7.4 Requirements for MPLa = d for hydraulic steering and braking systems 8
7.4.1 General 8
7.5 Category classifications 9
7.5.1 General 9
7.5.2 Category B/Category 1 12
7.5.3 Category 2 13
7.5.4 Conflicting safety functions 14
7.5.5 Considerations for the SRP/CS of fail-operational systems 14
7.6 Combination of SCS to achieve an overall MPLa 14

8 Information for use and maintenance 16
8.1 General 16
8.2 Operator's manual 16

Annex A (informative) Example systems and evaluations 17

Annex B (normative) Compatibility with other functional safety standards 31

Annex C (informative) Safety function evaluation 32

Annex D (normative) Exceptions, exclusions, additions to ISO 13849-1:2023 and ISO 13849- 2:2012 34

Bibliography 37