ISO 19014-4:2026-10 (E)

Earth-moving machinery - Functional safety - Part 4: Design and evaluation of software and data transmission 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 1

4 Software development 4
4.1 General 4
4.2 Planning 4
4.3 Artefacts 6
4.4 Software safety requirements specification 7
4.5 Software architecture design 8
4.6 Software module design and coding 8
4.7 Language and tool selection 9
4.8 Software module testing 10
4.9 Software module integration and testing 11
4.10 Safety requirements and protective or risk reduction measures 12

5 Software-based parameterization 13
5.1 General 13
5.2 Data integrity 13
5.3 Software-based parameterization verification 13

6 Transmission protection of safety-related messages on bus systems 13

7 Independence by software partitioning 15
7.1 General 15
7.2 Several partitions within a single microcontroller 16
7.3 Several partitions within the scope of an electronic control unit (ECU) network 18

8 Information for use 18
8.1 General 18
8.2 Instruction handbook 18

Annex A (informative) Description of software methods or measures 20

Annex B (normative) Software validation test environments 32

Annex C (informative) Data integrity assurance calculation 35

Annex D (informative) Methods and measures for transmission protection 37

Annex E (informative) Methods and measures for data protection internal to microcontroller 39

Bibliography 41