ISO 19014-4:2020 (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

Foreword

Introduction

- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Software development
 - 4.1 General
 - 4.2 Planning
 - 4.3 Artifacts
 - 4.4 Software safety requirements specification
 - 4.5 Software architecture design
 - 4.6 Software module design and coding
 - 4.7 Language and tool selection
 - 4.8 Software module testing
 - 4.9 Software module integration and testing
 - 4.10 Software validation
- 5 Software-based parameterization
 - 5.1 General
 - 5.2 Data integrity
 - 5.3 Software-based parameterization verification
- 6 Transmission protection of safety-related messages on bus systems
- 7 Independence by software partitioning
 - 7.1 General
 - 7.2 Several partitions within a single microcontroller
 - 7.3 Several partitions within the scope of an ECU network
- 8 Information for use
 - 8.1 General
 - 8.2 Instruction handbook
- Annex A (informative) Description of software methods/measures
 - A.1 Requirements specification in natural language
 - A.2 Computer-aided specification tools
 - A.3 Informal methods
 - A.4 Semi-formal methods
 - A.5 Formal methods
 - A.6 Traceability of the safety software
 - A.7 Walk-through
 - A.8 Inspection
 - A.9 Computer-aided design tools
 - A.10 Safety performance in real time
 - A.11 Design rules
 - A.12 Dynamic variables or objects without online check
 - A.13 Dynamic variables or objects with online check
 - A.14 Modular approach

- A.15 Structured programming
- A.16 Defensive programming
- A.17 Use of trusted/verified software elements
- A.18 Suitable programming language
- A.19 Language subset support
- A.20 Tools with increased confidence from use or validation
- A.21 Certified tools and certified translators
- A.22 Boundary value analysis
- A.23 Control flow analysis
- A.24 Data flow analysis
- A.25 Test case execution from boundary value analysis
- A.26 Functional/Black box testing
- A.27 Structure-based testing
- A.28 Equivalence classes and input partition testing
- A.29 Test case execution from model-based test case generation
- A.30 Performance testing
- A.31 SW module interface testing
- A.32 Back-to-back comparison testing

Annex B (normative) Software validation test environments

- B.1 Machine network testing
- B.2 Hardware-in-the-loop testing
- B.3 Machine level testing
- Annex C (informative) Data integrity assurance calculation

Annex D (informative) Methods and measures for transmission protection

- D.1 Keep alive messages
- D.2 Alive counter
- D.3 CRC
- D.4 Sequence number
- D.5 Message repetition
- D.6 Watchdog
- D.7 Time-triggered data bus
- D.8 Bus guardian
- D.9 Minislotting

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

- E.1 Unambiguous bidirectional communication object
- E.2 Strictly two unidirectional communication objects
- E.3 IDs for identification and acknowledgement
- E.4 Asynchronous data communication
- E.5 Strict priority-based scheduling
- E.6 Time slicing method
- E.7 Memory protection mechanisms
- E.8 Verification of safety critical data
- E.9 Static analysis
- E.10 Static allocation

Page count: 40