

E DIN EN ISO 19014-4:2024-04 (D/E)

Erscheinungsdatum: 2024-02-23

Erdbaumaschinen - Funktionale Sicherheit - Teil 4: Gestaltung und Beurteilung von Software und Datenübertragung für sicherheitsrelevante Steuerungssysteme (ISO/DIS 19014-4:2024); Deutsche und Englische Fassung prEN ISO 19014-4:2024

Earth-moving machinery - Functional safety - Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system (ISO/DIS 19014-4:2024); German and English version prEN ISO 19014-4:2024

| Inhalt | Seite |
|--|--------------|
| Europäisches Vorwort..... | 9 |
| Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden Richtlinie 2006/42/EG..... | 10 |
| Vorwort..... | 11 |
| Einleitung..... | 12 |
| 1 Anwendungsbereich..... | 14 |
| 2 Normative Verweisungen..... | 14 |
| 3 Begriffe..... | 14 |
| 4 Software-Entwicklung..... | 18 |
| 4.1 Allgemeines..... | 18 |
| 4.2 Planung..... | 18 |
| 4.3 Artefakte..... | 20 |
| 4.4 Spezifikation der Sicherheitsanforderungen an die Software..... | 21 |
| 4.5 Gestaltung der Software-Architektur..... | 22 |
| 4.6 Software-Modulgestaltung und Codierung..... | 23 |
| 4.7 Sprache und Tool-Auswahl..... | 25 |
| 4.8 Prüfen von Software-Modulen..... | 25 |
| 4.9 Software-Modulintegration und -prüfung..... | 27 |
| 4.10 Software-Validierung..... | 28 |
| 5 Softwarebasierte Parametrierung..... | 28 |
| 5.1 Allgemeines..... | 28 |
| 5.2 Datenintegrität..... | 29 |
| 5.3 Verifizierung softwarebasierter Parametrierung..... | 29 |
| 6 Schutz der Übertragung sicherheitsbezogener Nachrichten in Bussystemen..... | 29 |
| 7 Unabhängigkeit durch Software-Partitionierung..... | 31 |
| 7.1 Allgemeines..... | 31 |
| 7.2 Mehrere Partitionen in einem einzelnen Mikrocontroller..... | 32 |
| 7.3 Mehrere Partitionen im Rahmen eines ECU-Netzwerks..... | 34 |
| 8 Benutzerinformationen..... | 34 |
| 8.1 Allgemeines..... | 34 |
| 8.2 Betriebsanleitung..... | 34 |
| Anhang A (informativ) Beschreibung der Software-Methoden/Maßnahmen..... | 36 |
| A.1 Spezifikation der Anforderungen in natürlicher Sprache..... | 36 |
| A.2 Rechnergestützte Spezifikationstools..... | 36 |
| A.3 Informelle Methoden..... | 36 |
| A.4 Halbformelle Methoden..... | 36 |

| | | |
|--|--|-----------|
| A.5 | Formelle Methoden | 36 |
| A.6 | Nachverfolgbarkeit der Sicherheitssoftware | 37 |
| A.7 | Walkthrough | 38 |
| A.8 | Inspektion | 38 |
| A.9 | Rechnergestützte Gestaltungstools | 39 |
| A.10 | Sicherheitsleistung in Echtzeit | 39 |
| A.11 | Gestaltungsregeln | 40 |
| A.12 | Dynamische Variablen oder Objekte ohne Online-Prüfung | 40 |
| A.13 | Dynamische Variablen oder Objekte mit Online-Prüfung | 41 |
| A.14 | Modularisierung | 41 |
| A.15 | Strukturierte Programmierung | 42 |
| A.16 | Defensive Programmierung | 42 |
| A.17 | Verwendung vertrauenswürdiger/verifizierter Software-Elemente | 43 |
| A.18 | Geeignete Programmiersprache | 44 |
| A.19 | Unterstützung der Sprachteilmenge | 44 |
| A.20 | Tools mit zunehmender Bewährtheit im Betrieb oder in der Validierung | 44 |
| A.21 | Zertifizierte Tools und zertifizierte Übersetzungsprogramme | 45 |
| A.22 | Grenzwertanalyse | 45 |
| A.23 | Kontrollflussanalyse | 45 |
| A.24 | Datenflussanalyse | 46 |
| A.25 | Prüffallausführung anhand der Grenzwertanalyse | 46 |
| A.26 | Funktions-/Black-Box-Prüfung | 46 |
| A.27 | Strukturabhängige Prüfungen | 47 |
| A.28 | Äquivalenzklassen und Eingabe-Partitionsprüfungen | 47 |
| A.29 | Prüffallausführung aus modellbasierter Prüffallgenerierung | 47 |
| A.30 | Leistungsnachweis | 48 |
| A.31 | SW-Modulschnittstellenprüfung | 49 |
| A.32 | Direkte Vergleichsprüfung | 50 |
| Anhang B (normativ) Prüfungsumgebungen für Softwarevalidierung | | 51 |
| B.1 | Maschinennetzwerkprüfung | 51 |
| B.2 | Hardware-in-the-Loop-Prüfung | 51 |
| B.3 | Prüfung der Maschinenebene | 52 |
| Anhang C (informativ) Berechnung der Datenintegritätssicherung | | 54 |
| Anhang D (informativ) Methoden und Maßnahmen zum Übertragungsschutz | | 56 |
| D.1 | Keep-Alive-Nachrichten | 56 |
| D.2 | Alive Counter | 56 |
| D.3 | CRC | 56 |
| D.4 | Sequenznummer | 56 |
| D.5 | Nachrichtenwiederholung | 56 |
| D.6 | Watchdog | 57 |
| D.7 | Zeitgesteuerter Datenbus | 57 |
| D.8 | Buswächter | 57 |
| D.9 | Minislotting | 57 |
| Anhang E (informativ) Methoden und Maßnahmen für Mikrocontroller-internen Datenschutz | | 58 |
| E.1 | Eindeutiges bidirektionales Kommunikationsobjekt | 58 |
| E.2 | Ausschließlich zwei unidirektionale Kommunikationsobjekte | 58 |
| E.3 | IDs zur Identifizierung und Quittierung | 58 |
| E.4 | Asynchrone Datenkommunikation | 58 |
| E.5 | Streng prioritätsbasierte Planung | 58 |
| E.6 | Zeitscheibenmethode | 58 |
| E.7 | Speicherschutzmechanismen | 58 |
| E.8 | Verifizierung sicherheitskritischer Daten | 59 |
| E.9 | Statische Analyse | 59 |
| E.10 | Statische Zuweisung | 59 |
| Literaturhinweise | | 60 |

Bilder

| | |
|--|-----------|
| Bild 1 — V-Modell der Software-Entwicklung | 19 |
| Bild 2 — Mikrocontroller-Netzwerk aus elektronischen Steuereinheiten auf einem Datenbus | 30 |
| Bild 3 — Mehrere Partitionen in einem einzelnen Mikrocontroller | 33 |
| Bild B.1 — Maschinennetzwerkprüfung..... | 51 |
| Bild B.2 — Hardware-in-the-Loop-Prüfung..... | 52 |
| Bild B.3 — Prüfung der Maschinenebene..... | 53 |

Tabellen

| | |
|---|-----------|
| Tabelle ZA.1 — Übereinstimmung zwischen dieser Europäischen Norm und Anhang I der Richtlinie 2006/42/EG..... | 10 |
| Tabelle 1 — Spezifikation der Sicherheitsanforderungen an die Software..... | 19 |
| Tabelle 2 — Beispielspezifikation der Sicherheitsanforderungen an die Software | 20 |
| Tabelle 3 — Spezifikation der Sicherheitsanforderungen an die Software..... | 22 |
| Tabelle 4 — Gestaltung der Software-Architektur..... | 23 |
| Tabelle 5 — Software-Modulgestaltung und Codierung..... | 24 |
| Tabelle 6 — Sprache und Tool-Auswahl..... | 25 |
| Tabelle 7 — Prüfen von Software-Modulen..... | 26 |
| Tabelle 8 — Software-Modulintegration und -prüfung..... | 27 |
| Tabelle 9 — Software-Validierung | 28 |
| Tabelle 10 — Steuerung von Übertragungsfehlern und Performance Level..... | 30 |
| Tabelle 11 — Steuerung von Übertragungsfehlern und Performance Level..... | 31 |
| Tabelle 12 — Methoden und Maßnahmen innerhalb des Mikrocontrollers | 34 |
| Tabelle C.1 — Definition der Datenintegritätsparameter | 54 |
| Tabelle C.2 — Datenintegrität in Abhängigkeit vom MPL..... | 55 |