

E DIN EN ISO 19014-4:2025-10 (D/E)

Erscheinungsdatum: 2025-09-05

Erdbaumaschinen - Funktionale Sicherheit - Teil 4: Gestaltung und Beurteilung von Software und Datenübertragung für sicherheitsrelevante Steuerungssysteme (ISO/DIS 19014-4.2:2025); Deutsche und Englische Fassung prEN ISO 19014-4:2025

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 19014-4.2:2025); German and English version prEN ISO 19014-4:2025

Inhalt

Seite

Europäisches Vorwort.....	7
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden Verordnung (EU) 2023/1230.....	8
Vorwort.....	9
Einleitung.....	10
1 Anwendungsbereich.....	12
2 Normative Verweisungen.....	12
3 Begriffe.....	12
4 Software-Entwicklung.....	16
4.1 Allgemeines.....	16
4.2 Planung.....	16
4.3 Artefakte.....	18
4.4 Spezifikation der Sicherheitsanforderungen an die Software.....	19
4.5 Gestaltung der Software-Architektur.....	20
4.6 Software-Modulgestaltung und Codierung.....	21
4.7 Sprache und Tool-Auswahl.....	22
4.8 Prüfen von Software-Modulen.....	23
4.9 Software-Modulintegration und -prüfung.....	24
4.10 Verifizierung der Sicherheitsanforderungen und/oder Schutz-/ Risikominderungsmaßnahmen.....	25
5 Softwarebasierte Parametrierung.....	26
5.1 Allgemeines.....	26
5.2 Datenintegrität.....	27
5.3 Verifizierung softwarebasierter Parametrierung.....	27
6 Schutz der Übertragung sicherheitsbezogener Nachrichten in Bussystemen.....	27
7 Unabhängigkeit durch Software-Partitionierung.....	30
7.1 Allgemeines.....	30
7.2 Mehrere Partitionen in einem einzelnen Mikrocontroller.....	30
7.3 Mehrere Partitionen im Rahmen eines ECU-Netzwerks.....	33
8 Benutzerinformationen.....	33
8.1 Allgemeines.....	33
8.2 Betriebsanleitung.....	33
Anhang A (informativ) Beschreibung der Software-Methoden/Maßnahmen.....	34
A.1 Spezifikation der Anforderungen in natürlicher Sprache.....	34
A.2 Rechnergestützte Spezifikationstools.....	34
A.3 Informelle Methoden.....	34

A.4	Halbformelle Methoden	34
A.5	Formelle Methoden	34
A.6	Nachverfolgbarkeit der Sicherheitssoftware	35
A.7	Walkthrough	36
A.8	Inspektion	36
A.9	Rechnergestützte Gestaltungstools	37
A.10	Sicherheitsleistung in Echtzeit	37
A.11	Gestaltungsregeln	38
A.12	Dynamische Variablen oder Objekte ohne Online-Prüfung	38
A.13	Dynamische Variablen oder Objekte mit Online-Prüfung	39
A.14	Modularisierung	39
A.15	Strukturierte Programmierung	40
A.16	Defensive Programmierung	40
A.17	Verwendung vertrauenswürdiger/verifizierter Software-Elemente	41
A.18	Geeignete Programmiersprache	42
A.19	Unterstützung der Sprachteilmenge	42
A.20	Tools mit zunehmender Bewährtheit im Betrieb oder in der Validierung	42
A.21	Zertifizierte Tools und zertifizierte Übersetzungsprogramme	43
A.22	Grenzwertanalyse	43
A.23	Kontrollflussanalyse	43
A.24	Datenflussanalyse	44
A.25	Prüffallausführung anhand der Grenzwertanalyse	44
A.26	Funktions-/Black-Box-Prüfung	44
A.27	Strukturabhängige Prüfungen	45
A.28	Äquivalenzklassen und Eingabe-Partitionsprüfungen	45
A.29	Prüffallausführung aus modellbasierter Prüffallgenerierung	45
A.30	Leistungsnachweis	46
A.31	SW-Modulschnittstellenprüfung	47
A.32	Direkte Vergleichsprüfung	48
Anhang B (normativ) Prüfungsumgebungen für Softwarevalidierung		49
B.1	Maschinennetzwerkprüfung	49
B.2	Hardware-in-the-Loop-Prüfung	49
B.3	Prüfung der Maschinenebene	50
Anhang C (informativ) Berechnung der Datenintegritätssicherung		52
Anhang D (informativ) Methoden und Maßnahmen zum Übertragungsschutz		54
D.1	Keep-Alive-Nachrichten	54
D.2	Alive Counter	54
D.3	CRC	54
D.4	Sequenznummer	54
D.5	Nachrichtenederholung	54
D.6	Watchdog	55
D.7	Zeitgesteuerter Datenbus	55
D.8	Buswächter	55
D.9	Minislotting	55
Anhang E (informativ) Methoden und Maßnahmen für Mikrocontroller-internen Datenschutz		56
E.1	Eindeutiges bidirektionales Kommunikationsobjekt	56
E.2	Ausschließlich zwei unidirektionale Kommunikationsobjekte	56
E.3	IDs zur Identifizierung und Quittierung	56
E.4	Asynchrone Datenkommunikation	56
E.5	Streng prioritätsbasierte Planung	56
E.6	Zeitscheibenmethode	56
E.7	Speicherschutzmechanismen	56
E.8	Verifizierung sicherheitskritischer Daten	57
E.9	Statische Analyse	57
E.10	Statische Zuweisung	57

Literaturhinweise	58
Bilder	
Bild 1 — V-Modell der Software-Entwicklung	17
Bild 2 — Mikrocontroller-Netzwerk aus elektronischen Steuereinheiten auf einem Datenbus	28
Bild 3 — Mehrere Partitionen in einem einzelnen Mikrocontroller	31
Bild B.1 — Maschinennetzwerkprüfung.....	49
Bild B.2 — Hardware-in-the-Loop-Prüfung.....	50
Bild B.3 —Prüfung der Maschinenebene.....	51
Tabellen	
Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und Anhang III der Verordnung (EU) 2023/1230	8
Tabelle 1 — Spezifikation der Sicherheitsanforderungen an die Software.....	17
Tabelle 2 — Beispielspezifikation der Sicherheitsanforderungen an die Software	17
Tabelle 3 — Spezifikation der Sicherheitsanforderungen an die Software.....	19
Tabelle 4 — Gestaltung der Software-Architektur.....	20
Tabelle 5 — Software-Modulgestaltung und Codierung.....	21
Tabelle 6 — Sprache und Tool-Auswahl.....	22
Tabelle 7 — Prüfen von Software-Modulen.....	24
Tabelle 8 — Software-Modulintegration und -prüfung.....	25
Tabelle 9 — Software-Validierung	26
Tabelle 10 — Steuerung von Übertragungsfehlern und Performance Leveln	28
Tabelle 11 — Steuerung von Übertragungsfehlern und Performance Level.....	29
Tabelle 12 — Methoden und Maßnahmen innerhalb des Mikrocontrollers	32
Tabelle C.1 — Definition der Datenintegritätsparameter	52
Tabelle C.2 — Datenintegrität in Abhängigkeit vom MPL.....	53