

E DIN EN ISO 19014-4:2019-07 (D/E)

Erscheinungsdatum: 2019-06-07

Erdbaumaschinen - Funktionale Sicherheit - Teil 4: Gestaltung und Beurteilung von Software und Datenübertragung für sicherheitsrelevante Steuerungssysteme (ISO/DIS 19014-4:2019); Deutsche und Englische Fassung prEN ISO 19014-4:2019

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 19014-4:2019); German and English version prEN ISO 19014-4:2019

Inhalt	Seite
Europäisches Vorwort.....	4
Vorwort.....	5
Einleitung.....	6
1 Anwendungsbereich.....	7
2 Normative Verweisungen.....	7
3 Begriffe.....	7
4 Software-Entwicklung.....	10
4.1 Planung.....	10
4.2 Artefakte.....	12
4.3 Spezifikation der Sicherheitsanforderungen an die Software.....	13
4.4 Gestaltung der Software-Architektur.....	14
4.5 Software-Modulgestaltung und Codierung.....	15
4.6 Sprache, Bibliothek und Tool-Auswahl.....	17
4.7 Prüfen von Software-Modulen.....	17
4.8 Software-Modulintegration und -prüfung.....	19
4.9 Software-Validierung.....	20
5 Softwarebasierte Parametrierung.....	20
5.1 Allgemeines.....	20
5.2 Datenintegrität.....	21
5.3 Verifizierung softwarebasierter Parametrierung.....	21
6 Schutz der Übertragung sicherheitsbezogener Nachrichten in Bussystemen.....	21
7 Unabhängigkeit durch Software-Partitionierung.....	23
7.1 Mehrere Partitionen in einem einzelnen Mikrocontroller.....	24
7.2 Mehrere Partitionen im Rahmen eines ECU-Netzwerks.....	25
Anhang A (informativ) Beschreibung der Software-Methoden/Maßnahmen.....	26
A.1 Spezifikation der Anforderungen in natürlicher Sprache.....	26
A.2 Rechnergestützte Spezifikationstools.....	26
A.3 Informelle Methoden.....	26
A.4 Halbformelle Methoden.....	26
A.5 Formelle Methoden.....	26
A.6 Nachverfolgbarkeit der Sicherheitssoftware.....	27
A.7 Walkthrough.....	28
A.8 Inspektion.....	28
A.9 Rechnergestützte Gestaltungstools.....	29
A.10 Sicherheitsleistung in Echtzeit.....	29
A.11 Gestaltungsregeln.....	29
A.12 Keine dynamischen Variablen oder Objekte.....	30

A.13	Online-Prüfung der Erstellung dynamischer Variablen oder Objekte.....	31
A.14	Modularisierung.....	31
A.15	Strukturierte Programmierung.....	32
A.16	Defensive Programmierung.....	32
A.17	Verwendung vertrauenswürdiger/verifizierter Software-Elemente	33
A.18	Geeignete Programmiersprache	34
A.19	Unterstützung für Sprachteilmenge.....	34
A.20	Tools mit zunehmender Bewährtheit im Betrieb oder in der Validierung.....	34
A.21	Zertifizierte Tools und Übersetzungsprogramme.....	35
A.22	Grenzwertanalyse	35
A.23	Kontrollflussanalyse	36
A.24	Datenflussanalyse	36
A.25	Prüffallausführung anhand der Grenzwertanalyse	36
A.26	Funktions-/Black-Box-Prüfung	36
A.27	Strukturabhängige Prüfungen	37
A.28	Äquivalenzklassen und Eingabe-Partitionsprüfungen	37
A.29	Prüffallausführung aus modellbasierter Prüffallgenerierung.....	37
A.30	Leistungsprüfungen	38
A.31	Software-Modulschnittstellenprüfung.....	39
A.32	Direkte Vergleichsprüfung.....	40
Anhang B (normativ) Prüfumgebung für Softwarevalidierung.....		41
B.1	Maschinennetzwerkprüfung	41
B.2	Hardware-in-the-Loop-Prüfung	41
B.3	Prüfung der Maschinenebene	42
Anhang C (informativ) Datenintegritätssicherung.....		44
C.1	Berechnung der Datenintegritätssicherung.....	44
Anhang D (informativ) Methoden und Maßnahmen zum Übertragungsschutz		45
D.1	Keep-Alive-Nachrichten	45
D.2	Alive Counter	45
D.3	CRC	45
D.4	Sequenznummer.....	45
D.5	Nachrichtenwiederholung	45
D.6	Watchdog.....	46
D.7	Zeitgesteuerter Datenbus.....	46
D.8	Buswächter.....	46
D.9	Minislotting	46
Anhang E (informativ) Methoden und Maßnahmen für Mikrocontroller-internen Datenschutz		47
E.1	Eindeutiges bidirektionales Kommunikationsobjekt.....	47
E.2	Ausschließlich zwei unidirektionale Kommunikationsobjekte	47
E.3	IDs zur Identifizierung und Quittierung.....	47
E.4	Asynchrone Datenkommunikation	47
E.5	Streng prioritätsbasierte Planung.....	47
E.6	Zeitscheibenmethode	47
E.7	Speicherschutzmechanismen.....	47
E.8	Verifizierung sicherheitskritischer Daten	48
E.9	Statische Analyse.....	48
E.10	Statische Zuweisung.....	48