

# DIN EN ISO 19014-4:2021-01 (D)

Erdbaumaschinen - Funktionale Sicherheit - Teil 4: Gestaltung und Beurteilung von Software und Datenübertragung für sicherheitsrelevante Steuerungssysteme (ISO 19014-4:2020); Deutsche Fassung EN ISO 19014-4:2020

---

Inhalt	Seite
Europäisches Vorwort.....	4
Vorwort.....	5
Einleitung .....	6
1 Anwendungsbereich.....	7
2 Normative Verweisungen .....	7
3 Begriffe .....	7
4 Software-Entwicklung.....	11
4.1 Allgemeines.....	11
4.2 Planung.....	11
4.3 Artefakte .....	13
4.4 Spezifikation der Sicherheitsanforderungen an die Software.....	14
4.5 Gestaltung der Software-Architektur .....	15
4.6 Software-Modulgestaltung und Codierung .....	16
4.7 Sprache und Tool-Auswahl.....	18
4.8 Prüfen von Software-Modulen .....	18
4.9 Software-Modulintegration und -prüfung.....	20
4.10 Software-Validierung.....	21
5 Softwarebasierte Parametrierung.....	21
5.1 Allgemeines .....	21
5.2 Datenintegrität.....	22
5.3 Verifizierung softwarebasierter Parametrierung .....	22
6 Schutz der Übertragung sicherheitsbezogener Nachrichten in Bussystemen.....	22
7 Unabhängigkeit durch Software-Partitionierung.....	24
7.1 Allgemeines.....	24
7.2 Mehrere Partitionen in einem einzelnen Mikrocontroller.....	25
7.3 Mehrere Partitionen im Rahmen eines ECU-Netzwerks.....	27
8 Benutzerinformationen.....	27
8.1 Allgemeines.....	27
8.2 Betriebsanleitung.....	28
Anhang A (informativ) Beschreibung der Software-Methoden/Maßnahmen .....	29
A.1 Spezifikation der Anforderungen in natürlicher Sprache.....	29
A.2 Rechnergestützte Spezifikationstools .....	29
A.3 Informelle Methoden .....	29
A.4 Halbformelle Methoden .....	29
A.5 Formelle Methoden.....	29
A.6 Nachverfolgbarkeit der Sicherheitssoftware .....	30
A.7 Walkthrough .....	31
A.8 Inspektion.....	31
A.9 Rechnergestützte Gestaltungstools .....	32
A.10 Sicherheitsleistung in Echtzeit.....	32
A.11 Gestaltungsregeln .....	33

A.12	Dynamische Variablen oder Objekte ohne Online-Prüfung .....	33
A.13	Dynamische Variablen oder Objekte mit Online-Prüfung .....	34
A.14	Modularisierung .....	34
A.15	Strukturierte Programmierung.....	35
A.16	Defensive Programmierung.....	35
A.17	Verwendung vertrauenswürdiger/verifizierter Software-Elemente .....	36
A.18	Geeignete Programmiersprache .....	37
A.19	Unterstützung der Sprachteilmenge .....	37
A.20	Tools mit zunehmender Bewährtheit im Betrieb oder in der Validierung .....	38
A.21	Zertifizierte Tools und zertifizierte Übersetzungsprogramme .....	38
A.22	Grenzwertanalyse .....	39
A.23	Kontrollflussanalyse .....	39
A.24	Datenflussanalyse .....	39
A.25	Prüffallausführung anhand der Grenzwertanalyse .....	40
A.26	Funktions-/Black-Box-Prüfung .....	40
A.27	Strukturabhängige Prüfungen .....	40
A.28	Äquivalenzklassen und Eingabe-Partitionsprüfungen .....	41
A.29	Prüffallausführung aus modellbasierter Prüffallgenerierung .....	41
A.30	Leistungsnachweis.....	42
A.31	Software-Modulschnittstellenprüfung.....	43
A.32	Direkte Vergleichsprüfung.....	43
<b>Anhang B (normativ) Prüfumgebungen für Softwarevalidierung .....</b>		<b>44</b>
B.1	Maschinennetzwerkprüfung .....	44
B.2	Hardware-in-the-Loop-Prüfung .....	45
B.3	Prüfung der Maschinenebene .....	46
<b>Anhang C (informativ) Berechnung der Datenintegritätssicherung.....</b>		<b>47</b>
<b>Anhang D (informativ) Methoden und Maßnahmen zum Übertragungsschutz .....</b>		<b>49</b>
D.1	Keep-Alive-Nachrichten .....	49
D.2	Alive Counter .....	49
D.3	CRC .....	49
D.4	Sequenznummer.....	49
D.5	Nachrichtenwiederholung .....	49
D.6	Watchdog.....	49
D.7	Zeitgesteuerter Datenbus.....	50
D.8	Buswächter.....	50
D.9	Minislotting .....	50
<b>Anhang E (informativ) Methoden und Maßnahmen für Mikrocontroller-internen Datenschutz .....</b>		<b>51</b>
E.1	Eindeutiges bidirektionales Kommunikationsobjekt.....	51
E.2	Ausschließlich zwei unidirektionale Kommunikationsobjekte .....	51
E.3	IDs zur Identifizierung und Quittierung .....	51
E.4	Asynchrone Datenkommunikation .....	51
E.5	Streng prioritätsbasierte Planung.....	51
E.6	Zeitscheibenmethode .....	51
E.7	Speicherschutzmechanismen.....	51
E.8	Verifizierung sicherheitskritischer Daten .....	52
E.9	Statische Analyse.....	52
E.10	Statische Zuweisung.....	52
<b>Literaturhinweise .....</b>		<b>53</b>