

DIN EN ISO 25119-3:2024-07 (D)

Traktoren und Maschinen für die Land- und Forstwirtschaft - Sicherheitsbezogene Teile von Steuerungen - Teil 3: Serienentwicklung, Hardware und Software (ISO 25119-3:2018 + Amd 1:2020); Deutsche Fassung EN ISO 25119-3:2023 + A1:2023

Inhalt

Seite

Europäisches Vorwort.....	10
A1 Europäisches Vorwort der Änderung 1 A1	11
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2006/42/EG.....	12
Vorwort.....	18
A1 Vorwort der Änderung 1 A1	20
Einleitung.....	21
1 Anwendungsbereich.....	23
2 Normative Verweisungen.....	24
3 Begriffe.....	24
4 Abkürzungen.....	24
5 Systementwurf.....	25
5.1 Ziele.....	25
5.2 Allgemeines.....	25
5.3 Voraussetzungen.....	26
5.4 Anforderungen.....	26
5.4.1 Gliederung der Sicherheitsanforderungen.....	26
5.4.2 Technisches Sicherheitskonzept.....	27
5.5 Arbeitsprodukte.....	29
6 Hardware.....	29
6.1 Ziele.....	29
6.2 Allgemeines.....	29
6.3 Voraussetzungen.....	29
6.4 Anforderungen.....	30
6.5 Hardwarekategorien.....	31
6.6 Arbeitsprodukte.....	32
7 Software.....	33
7.1 Software-Entwicklungsplanung.....	33
7.1.1 Ziele.....	33
7.1.2 Allgemeines.....	33
7.1.3 Voraussetzungen.....	33
7.1.4 Anforderungen.....	33
7.1.5 Arbeitsprodukte.....	36
7.2 Festlegung der Sicherheitsanforderungen an die Software.....	36
7.2.1 Ziele.....	36
7.2.2 Allgemeines.....	36
7.2.3 Voraussetzungen.....	36
7.2.4 Anforderungen.....	37
7.2.5 Arbeitsprodukte.....	40
7.3 Gestaltung der Software-Architektur.....	40

7.3.1	Ziele	40
7.3.2	Allgemeines.....	41
7.3.3	Voraussetzungen	41
7.3.4	Anforderungen.....	41
7.3.5	Arbeitsprodukte	42
7.4	Gestaltung und Implementierung von Softwarekomponenten.....	43
7.4.1	Ziele	43
7.4.2	Allgemeines.....	43
7.4.3	Voraussetzungen	43
7.4.4	Anforderungen.....	43
7.4.5	Arbeitsprodukte	54
7.5	Softwarekomponentenprüfung.....	54
7.5.1	Ziele	54
7.5.2	Allgemeines.....	55
7.5.3	Voraussetzungen	55
7.5.4	Anforderungen.....	55
7.5.5	Arbeitsprodukte	64
7.6	Software-Integration und -Prüfung.....	64
7.6.1	Ziele	64
7.6.2	Allgemeines.....	64
7.6.3	Voraussetzungen	65
7.6.4	Anforderungen.....	65
7.6.5	Arbeitsprodukte	67
7.7	Software-Sicherheitsprüfung	67
7.7.1	Ziele	67
7.7.2	Allgemeines.....	67
7.7.3	Voraussetzungen	67
7.7.4	Anforderungen.....	67
7.7.5	Arbeitsprodukte	71
7.8	Softwarebasierte Parametrierung.....	71
7.8.1	Ziel.....	71
7.8.2	Allgemeines.....	71
7.8.3	Voraussetzungen	71
7.8.4	Anforderungen.....	72
7.8.5	Arbeitsprodukte	73
Anhang A (informativ) Beispiel einer Agenda für die Beurteilung der funktionalen Sicherheit		
	bei AgPL = e	74
A.1	Funktionen des Systems.....	74
A.2	Hardware	74
A.3	Sicherheitskonzept.....	74
A.4	Sicherheitsanalyse und Sicherheitsdaten	74
A.5	Sicherheitsentwurfsprozess für die Phasen des Lebenszyklus.....	75
A.6	Software-Entwicklung	75
A.7	Verifizierung und Prüfung	75
A.8	Dokumentation und Sicherheitsdokumentation	75
A.9	Zusammenfassung und Beurteilung	75
Anhang B (normativ) Unabhängigkeit durch Softwarepartitionierung.....		
B.1	Übersicht.....	76
B.2	Begriffe und Abkürzungen	76
B.2.1	Begriffe	76
B.2.2	Abkürzungen	79
B.3	Ziele	80
B.4	Allgemeines.....	80
B.5	Anforderungen.....	80
B.5.1	Allgemeine Anforderungen.....	80
B.5.2	Mehrere Partitionen in einem einzelnen Mikrocontroller.....	81
B.5.3	Mehrere Partitionen im Rahmen eines Mikrocontroller-Netzwerks.....	83

Literaturhinweise	86
Bilder	
Bild 1 — Gliederung der Sicherheitsanforderungen	26
Bild 2 — V-Modell der Hardwareentwicklung.....	31
Bild 3 — Beispiel eines integrierten Systems für die Hardwarekategorie 2	32
Bild 4 — V-Modell der Software-Entwicklung	35
Bild 5 — Prüfschnittstelle einer ECU eines E/E/PES-Systems	68
Bild 6 — Prüfung innerhalb des Netzwerks der elektronischen Steuereinheit eines E/E/PES-Systems	69
Bild 7 — Hardware-in-the-Loop-Prüfung einer ECU eines E/E/PES-Systems	70
Bild 8 — Prüfung in der Maschine eines E/E/PES-Systems.....	70
Bild B.1 — Mehrere Partitionen in einem einzelnen Mikrocontroller	81
Bild B.2 — Mehrere Partitionen innerhalb eines Mikrocontroller-Netzwerks	83
Bild B.3 — Mehrere Partitionen innerhalb einer ECU mit mehreren Prozessoren.....	84
Tabellen	
Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und Anhang I der Richtlinie 2006/42/EG.....	12
Tabelle ZA.2 — Anwendbare Normen, die die Konformitätsvermutung gemäß diesem Anhang ZA begründen.....	16
Tabelle 1 — Festlegung der Sicherheitsanforderungen an die Software	37
Tabelle 2 — Gestaltung der Software-Architektur.....	41
Tabelle 3 — Software-Entwurf und -Entwicklung — Unterstützungswerkzeuge und Programmiersprache	43
Tabelle 4 — Softwarekomponentenprüfung.....	55
Tabelle 5 — Software-Integrationsprüfung (Komponente).....	66
Tabelle 6 — Software-Sicherheitsprüfung.....	68
Tabelle B.1 — Verfahren und Maßnahmen innerhalb des Mikrocontrollers.....	82
Tabelle B.2 — Verfahren und Maßnahmen innerhalb eines Mikrocontroller-Netzwerks.....	85