

# DIN EN 16590-3:2015-04 (D)

Traktoren und Maschinen für die Land- und Forstwirtschaft - Sicherheitsbezogene Teile von Steuerungen - Teil 3: Serienentwicklung, Hardware, Software (ISO 25119-3:2010 modifiziert); Deutsche Fassung EN 16590-3:2014

---

Inhalt	Seite
Vorwort .....	4
Einleitung .....	5
1 Anwendungsbereich .....	7
2 Normative Verweisungen .....	7
3 Begriffe .....	7
4 Abkürzungen .....	7
5 Systementwurf .....	8
5.1 Ziele .....	8
5.2 Allgemeines .....	8
5.3 Voraussetzungen .....	9
5.4 Anforderungen .....	9
5.4.1 Gliederung der Sicherheitsanforderungen .....	9
5.4.2 Funktionales Sicherheitskonzept .....	10
5.4.3 Technisches Sicherheitskonzept .....	11
6 Hardware .....	13
6.1 Ziele .....	13
6.2 Allgemeines .....	13
6.3 Voraussetzungen .....	14
6.4 Anforderungen .....	14
6.5 Hardware-Kategorien .....	15
6.6 Arbeitsprodukte .....	16
7 Software .....	16
7.1 Software-Entwicklungsplanung .....	16
7.1.1 Ziele .....	16
7.1.2 Allgemeines .....	16
7.1.3 Voraussetzungen .....	16
7.1.4 Anforderungen .....	17
7.1.5 Arbeitsprodukte .....	19
7.2 Spezifikation der Sicherheitsanforderungen an die Software .....	19
7.2.1 Ziele .....	19
7.2.2 Allgemeines .....	19
7.2.3 Voraussetzungen .....	20
7.2.4 Anforderungen .....	20
7.2.5 Arbeitsprodukte .....	23
7.3 Software-Architektur und -entwurf .....	23
7.3.1 Ziele .....	23
7.3.2 Allgemeines .....	23
7.3.3 Voraussetzungen .....	23
7.3.4 Anforderungen .....	24
7.3.5 Arbeitsprodukte .....	26
7.4 Entwurf und Implementierung von Softwaremodulen .....	26

7.4.1	Ziele .....	26
7.4.2	Allgemeines .....	26
7.4.3	Voraussetzungen .....	26
7.4.4	Anforderungen .....	26
7.4.5	Arbeitsprodukte .....	35
7.5	Testen von Softwaremodulen .....	35
7.5.1	Ziele .....	35
7.5.2	Allgemeines .....	35
7.5.3	Voraussetzungen .....	36
7.5.4	Anforderungen .....	36
7.5.5	Arbeitsprodukte .....	44
7.6	Software Integrationstest .....	44
7.6.1	Ziele .....	44
7.6.2	Allgemeines .....	44
7.6.3	Voraussetzungen .....	44
7.6.4	Anforderungen .....	45
7.6.5	Arbeitsprodukte .....	47
7.7	Software-Sicherheitsvalidierung .....	47
7.7.1	Ziele .....	47
7.7.2	Allgemeines .....	47
7.7.3	Voraussetzungen .....	47
7.7.4	Anforderungen .....	48
7.7.5	Arbeitsprodukte .....	49
7.8	Softwarebasierte Parametrierung .....	49
7.8.1	Ziel .....	49
7.8.2	Allgemeines .....	50
7.8.3	Voraussetzungen .....	50
7.8.4	Anforderungen .....	50
7.8.5	Arbeitsprodukte .....	51
<b>Anhang A (informativ) Beispiel einer Agenda für die Beurteilung der funktionalen Sicherheit bei AgPL = e .....</b>		<b>52</b>
A.1	Funktionen des Systems .....	52
A.2	Hardware .....	52
A.3	Sicherheitskonzept .....	52
A.4	Sicherheitsanalyse und Sicherheitsdaten .....	52
A.5	Sicherheitsentwurfsprozess für die Phasen des Lebenszyklus .....	53
A.6	Softwareentwicklung .....	53
A.7	Verifizierung und Tests .....	53
A.8	Dokumentation und Sicherheitsdokumentation .....	53
A.9	Zusammenfassung und Beurteilung .....	53
<b>Anhang B (informativ) Unabhängigkeit durch Softwarepartitionierung .....</b>		<b>54</b>
B.1	Allgemeines .....	54
B.2	Begriffe und Abkürzungen .....	54
B.3	Ziele .....	58
B.4	Allgemeines .....	58
B.5	Anforderungen .....	58
B.5.1	Allgemeine Anforderungen .....	58
B.5.2	Mehrere Partitionen in einem einzelnen Mikrocontroller .....	59
B.5.3	Mehrere Partitionen im Rahmen eines Mikrocontroller-Netzwerks .....	61
<b>Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2006/42/EG .....</b>		<b>64</b>
<b>Literaturhinweise .....</b>		<b>65</b>