

E DIN EN ISO 24882:2026-01 (D/E)

Erscheinungsdatum: 2025-11-28

Landwirtschaftliche Maschinen, Traktoren und Erdbewegungsmaschinen -
Cybersicherheit von Produkten (ISO/DIS 24882:2025); Deutsche und Englische
Fassung prEN ISO 24882:2025

Agricultural machinery, tractors, and earth-moving machinery - Product
cybersecurity (ISO/DIS 24882:2025); German and English version prEN ISO
24882:2025

Inhalt/Contents

Seite

Europäisches Vorwort	8
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden Verordnung (EU) 2023/1230	9
Vorwort	15
Einführung	16
1 Anwendungsbereich	17
2 Normative Verweisungen	17
3 Begriffe und Abkürzungen	17
3.1 Begriffe	17
3.2 Abkürzungen	20
4 Allgemeine Betrachtungen	21
5 Beurteilung des Risikos für das betrachtete System	24
5.1 Einführung in die Risikobeurteilung	24
5.2 Feststellung des betrachteten Systems	25
5.2.1 Allgemeines	25
5.2.2 Voraussetzungen	25
5.2.3 Anforderungen	25
5.2.4 Arbeitsprodukte	26
5.3 Identifizierung von Vermögenswerten und Schadensszenarien	26
5.3.1 Allgemeines	26
5.3.2 Voraussetzungen	26
5.3.3 Anforderungen	26
5.3.4 Arbeitsprodukte	27
5.4 Identifizierung von Bedrohungen	27
5.4.1 Allgemeines	27
5.4.2 Voraussetzungen	27
5.4.3 Anforderungen	27
5.4.4 Arbeitsprodukte	28
5.5 Bestimmung der Auswirkungseinstufung	28
5.5.1 Allgemeines	28
5.5.2 Voraussetzungen	28
5.5.3 Anforderungen	28
5.5.4 Arbeitsprodukte	30
5.6 Bestimmung der Wahrscheinlichkeitseinstufung	31
5.6.1 Allgemeines	31
5.6.2 Voraussetzungen	31
5.6.3 Anforderungen	31
5.6.4 Arbeitsprodukte	35
5.7 Bestimmung der Risikoeinstufung	35
5.7.1 Allgemeines	35
5.7.2 Voraussetzungen	35
5.7.3 Anforderungen	35
5.7.4 Arbeitsprodukte	35
5.8 Entscheidung über die Risikobehandlung	35
5.8.1 Allgemeines	35
5.8.2 Voraussetzungen	36
5.8.3 Anforderungen	36
5.8.4 Arbeitsprodukte	36
5.9 Bestimmung der Cybersicherheitsanforderungen	36
5.9.1 Allgemeines	36
5.9.2 Voraussetzungen	37

5.9.3	Anforderungen	37
5.9.4	Arbeitsprodukte	37
6	Technische Cybersicherheitsanforderungen für die Risikominderung	37
6.1	Einführung in die technischen Anforderungen	37
6.2	Sichere Softwareaktualisierung	38
6.2.1	Anwendbarkeit	38
6.2.2	Anforderungen	38
6.2.3	Hintergründe	38
6.2.4	Leitfaden	38
6.2.5	Verifizierungskriterien	39
6.3	Benachrichtigung über eine sichere Softwareaktualisierung	39
6.3.1	Anwendbarkeit	39
6.3.2	Anforderungen	39
6.3.3	Hintergründe	39
6.3.4	Leitfaden	39
6.3.5	Verifizierungskriterien	39
6.4	Integritäts- und Authentizitätsprüfung von sicheren Softwareaktualisierungen	40
6.4.1	Anwendbarkeit	40
6.4.2	Anforderungen	40
6.4.3	Hintergründe	40
6.4.4	Leitfaden	40
6.4.5	Verifizierungskriterien	40
6.5	Absicherung – sichere Konfiguration	40
6.5.1	Anwendbarkeit	40
6.5.2	Anforderungen	40
6.5.3	Hintergründe	41
6.5.4	Leitfaden	41
6.5.5	Verifizierungskriterien	41
6.6	Absicherung – Produktionsbetrieb	41
6.6.1	Anwendbarkeit	41
6.6.2	Anforderungen	41
6.6.3	Hintergründe	41
6.6.4	Leitfaden	41
6.6.5	Verifizierungskriterien	42
6.7	Sichere Protokollierung und Berichterstellung – Überwachung berechtigter und unberechtigter Zugänge	42
6.7.1	Anwendbarkeit	42
6.7.2	Anforderungen	42
6.7.3	Hintergründe	42
6.7.4	Leitfaden	42
6.7.5	Verifizierungskriterien	43
6.8	Sichere Protokollierung und Berichterstellung – Anomalieerkennung	43
6.8.1	Anwendbarkeit	43
6.8.2	Anforderungen	43
6.8.3	Hintergründe	43
6.8.4	Leitfaden	43
6.8.5	Verifizierungskriterien	43
6.9	Sichere Protokollierung und Berichterstellung – Erkennung von Integritätsverletzungen	44
6.9.1	Anwendbarkeit	44
6.9.2	Anforderungen	44
6.9.3	Hintergründe	44
6.9.4	Leitfaden	44
6.9.5	Verifizierungskriterien	44
6.10	Sichere Protokollierung und Berichterstellung – sichere Protokollierung	44
6.10.1	Anwendbarkeit	44
6.10.2	Anforderungen	44
6.10.3	Hintergründe	44

6.10.4	Leitfaden	44
6.10.5	Verifizierungskriterien	45
6.11	Sichere Protokollierung und Berichterstellung – Berichtsprotokolle und Ereignisse	45
6.11.1	Anwendbarkeit	45
6.11.2	Anforderungen	45
6.11.3	Hintergründe	45
6.11.4	Leitfaden	45
6.11.5	Verifizierungskriterien	45
6.12	Anwenderzugriffsverwaltung – Authentifizierung und Autorisierung	46
6.12.1	Verwendung	46
6.12.2	Anforderungen	46
6.12.3	Hintergründe	46
6.12.4	Leitfaden	46
6.12.5	Verifizierungskriterien	46
6.13	Anwenderzugriffsverwaltung – rollenbasierte Zugriffskontrolle (RBAC)	46
6.13.1	Anwendbarkeit	46
6.13.2	Anforderungen	47
6.13.3	Hintergründe	47
6.13.4	Leitfaden	47
6.13.5	Verifizierungskriterien	47
6.14	Diagnosezugriffsverwaltung – Authentifizierung und Autorisierung	47
6.14.1	Anwendbarkeit	47
6.14.2	Anforderungen	48
6.14.3	Hintergründe	48
6.14.4	Leitfaden	48
6.14.5	Verifizierungskriterien	48
6.15	Diagnosezugriffsverwaltung – rollenbasierte Zugriffskontrolle (RBAC)	48
6.15.1	Anwendbarkeit	48
6.15.2	Anforderungen	48
6.15.3	Hintergründe	49
6.15.4	Leitfaden	49
6.15.5	Verifizierungskriterien	49
6.16	Vertraulichkeit der Daten – Sicherheit ruhender Daten	49
6.16.1	Anwendbarkeit	49
6.16.2	Anforderungen	49
6.16.3	Hintergründe	50
6.16.4	Leitfaden	50
6.16.5	Verifizierungskriterien	50
6.17	Vertraulichkeit der Daten – Sicherheit gesendeter Daten	50
6.17.1	Anwendbarkeit	50
6.17.2	Anforderungen	50
6.17.3	Hintergründe	50
6.17.4	Leitfaden	50
6.17.5	Verifizierungskriterien	51
6.18	Integrität der Daten – Sicherheit ruhender Daten	51
6.18.1	Anwendbarkeit	51
6.18.2	Anforderungen	51
6.18.3	Hintergründe	51
6.18.4	Leitfaden	51
6.18.5	Verifizierungskriterien	51
6.19	Integrität der Daten – Sicherheit gesendeter Daten	51
6.19.1	Anwendbarkeit	51
6.19.2	Anforderungen	52
6.19.3	Hintergründe	52
6.19.4	Leitfaden	52
6.19.5	Verifizierungskriterien	52
6.20	Datenminimierung	52

6.20.1	Anwendbarkeit	52
6.20.2	Anforderungen	52
6.20.3	Hintergründe	52
6.20.4	Leitfaden	53
6.20.5	Verifizierungskriterien	53
6.21	Cybersicherheitsresilienz – Verfügbarkeit	53
6.21.1	Anwendbarkeit	53
6.21.2	Anforderungen	53
6.21.3	Hintergründe	53
6.21.4	Leitfaden	53
6.21.5	Verifizierungskriterien	54
6.22	Cybersicherheitsresilienz – Schutz vor DoS-Angriffen	54
6.22.1	Anwendbarkeit	54
6.22.2	Anforderungen	54
6.22.3	Hintergründe	54
6.22.4	Leitfaden	54
6.22.5	Verifizierungskriterien	54
6.23	Netzwerkschutz	54
6.23.1	Anwendbarkeit	54
6.23.2	Anforderungen	54
6.23.3	Hintergründe	55
6.23.4	Leitfaden	55
6.23.5	Verifizierungskriterien	55
6.24	Sicherheit durch Auslegung („Secure by Design“)	55
6.24.1	Anwendbarkeit	55
6.24.2	Anforderungen	55
6.24.3	Hintergründe	55
6.24.4	Leitfaden	55
6.24.5	Verifizierungskriterien	56
6.25	Mehrschichtiger Sicherheitsansatz („Defence in depth“)	56
6.25.1	Anwendbarkeit	56
6.25.2	Anforderungen	56
6.25.3	Hintergründe	56
6.25.4	Leitfaden	56
6.25.5	Verifizierungskriterien	57
6.26	Kryptographie	57
6.26.1	Anwendbarkeit	57
6.26.2	Anforderungen	57
6.26.3	Hintergründe	57
6.26.4	Leitfaden	57
6.26.5	Verifizierungskriterien	57
7	Produktlebenszyklus	58
7.1	Hintergründe	58
7.2	Entwicklungsphase	58
7.2.1	Auslegung	58
7.2.2	Implementierung	58
7.2.3	Verifizierung	58
7.2.4	Verifizierung	59
7.2.5	Konformitätsbeurteilung	59
7.3	Produktion	59
7.4	Betrieb	60
7.5	Außerbetriebnahme	60
7.6	Arbeitsprodukte	60
8	Anforderungen an den Umgang mit Sicherheitslücken	61
8.1	Ziele	61
8.2	Voraussetzungen	61
8.3	Anforderungen an die Überwachung von Sicherheitslücken	62

8.4	Anforderungen an die Analyse von Sicherheitslücken	62
8.5	Anforderungen an den Umgang mit Sicherheitslücken	63
8.6	Anforderungen an die Offenlegung von Sicherheitslücken	63
8.7	Arbeitsprodukte	64
9	Umgang mit Komponenten oder Entwicklungen von Dritten	64
9.1	Ziele	64
9.2	Voraussetzungen	64
9.3	Anforderungen an die Integration von handelsüblichen Komponenten	64
9.4	Anforderungen an die Integration von Open-Source-Komponenten	65
9.5	Anforderungen an vom Lieferanten entwickelte Komponenten	65
9.6	Arbeitsprodukte	66
10	Dokumentation	67
10.1	Allgemeines	67
10.2	Dokumentation der Produktauslegung	67
10.3	Dokumentation des Produkts	67
10.4	Dokumentation des Umgangs mit Sicherheitslücken	67
10.5	Dokumentation der Freigabe	68
Anhang A (informativ) Festlegung von Rollen		69
Anhang B (informativ) Beispiel für Schadensszenarien und Minderungsmaßnahmen mit Einstufungstypen		71
Anhang C (informativ) Beispiel für Cybersicherheitsziele und -anforderungen		76
Anhang D (informativ) Zuordnung der Arbeitsergebnisse nach ISO/SAE 21434 zu den Arbeitsergebnissen nach ISO 24882		78
Literaturhinweise		81

Bilder

Bild 1	— Produkt mit OEM-Kennung des betrachteten Systems	21
Bild 2	— Produkt mit Lieferantenkennung des betrachteten Systems	22
Bild 3	— Entscheidung zur Cybersicherheit	23
Bild 4	— Beziehungen zwischen verwendeten Begriffen	24
Bild 5	— Ablaufdiagramm einer Risikobeurteilung	25

Tabellen

Tabelle ZA.1	— Zusammenhang zwischen dieser Europäischen Norm und Anhang III, Teil B der Verordnung (EU) 2023/1230	9
Tabelle 1	— Kriterien für die Auswirkungseinstufung bei Sicherheit	29
Tabelle 2	— Kriterien für die Auswirkungseinstufung bei Finanzen	29
Tabelle 3	— Kriterien für die Auswirkungseinstufung beim Datenschutz	30
Tabelle 4	— Kriterien für die Auswirkungseinstufung bei der Verfügbarkeit	30
Tabelle 5	— Unterkategorien zur Bestimmung der Wahrscheinlichkeitswerte für jedes Bedrohungsszenario	31
Tabelle 6	— Fachwissen	32
Tabelle 7	— Spezifische Kenntnis über das betrachtete System	32
Tabelle 8	— Zeitfenster	33
Tabelle 9	— Geräte	34
Tabelle 10	— Bestimmung der Wahrscheinlichkeitseinstufung	34
Tabelle 11	— Bestimmung der Risikoeinstufung	35
Tabelle B.1	— Arten von Auswirkungseinstufungen für die Sicherheit	71
Tabelle B.2	— Arten von Auswirkungseinstufungen für die Finanzen	72
Tabelle B.3	— Arten von Auswirkungseinstufungen für den Datenschutz	74
Tabelle B.4	— Arten von Auswirkungseinstufungen für die Verfügbarkeit	75
Tabelle D.1	— Zuordnung von ISO/SAE 21434 zu ISO 24882	78