DGUV Test
Prüf- und Zertifizierungssystem der
Deutschen Gesetzlichen Unfallversicherung

Institut für Arbeitsschutz der DGUV
Prüf- und Zertifizierungsstelle

Grundsätze für die Prüfung und Zertifizierung des Schutzes vor Korrumpierung

Stand 07-2026

Prüfgrundsätze GS-IFA-M25

Inhaltsverzeichnis

0. Vorbemerkung

Die vorliegenden Prüfgrundsätze sind eine Gemeinschaftsarbeit der folgenden Prüf- und Zertifizierungsstellen im DGUV Test:

- Prüf- und Zertifizierungsstelle Druck und Papierverarbeitung
  Fachbereich Energie Textil Elektro Medienerzeugnisse
- Prüf- und Zertifizierungsstelle Elektrotechnik
  Fachbereich Energie Textil Elektro Medienerzeugnisse
- Prüf- und Zertifizierungsstelle Fachbereich Holz und Metall
- Institut für Arbeitsschutz der DGUV, Prüf- und Zertifizierungsstelle im DGUV Test
- Prüf- und Zertifizierungsstelle Nahrungsmittel und Verpackung
  Fachbereich Nahrungsmittel
- Prüf- und Zertifizierungsstelle Fachbereich Rohstoffe und chemische Industrie
- Prüf- und Zertifizierungsstelle Fachbereich Verkehr und Landschaft

Aktuelle Kontaktdaten der Prüf- und Zertifizierungsstellen sind auf der Internetseite https://www.dguv.de/dguv-test hinterlegt.

Änderungshistorie

Datum (Stand)	Änderung	Verantwortlicher Bearbeiter	Freigabe am	Freigabe durch
2026-07-06 (07-2026)	Ersterstellung	Jonas Stein	2026-07-07	Dr. Michel Bergs
2026-07-13 (07-2026)	Editorielle Korrekturen	Jonas Stein	2026-07-13	Dr. Michel Bergs

1 Allgemeines

1.1 Anwendungsbereich

Diese Prüfgrundsätze finden Anwendung auf die Teilprüfung von Maschinen und Sicherheitsbauteilen nach Anhang II und Anhang III der Verordnung (EU) 2023/1230 im Folgenden Maschinenverordnung (MVO).
Die Prüfgrundsätze gelten in Zusammenhang mit der DGUV Test Prüf- und Zertifizierungsordnung, Teil 1: Zertifizierung von Produkten, Prozessen und Dienstleistungen (DGUV Grundsatz 300-003) in der jeweils gültigen Fassung. Sie finden Anwendung als Teilprüfung bei einer EU-Baumusterprüfung und freiwilligen Baumusterprüfung nach MVO.
Eine Zeichenvergabe für Teilaspekte ist nicht vorgesehen, da diese Prüfgrundsätze nur die Minimalanforderungen der MVO zum Schutz vor Korrumpierung enthalten.

1.2 Prüfgrundlagen

Die Prüfung basiert auf folgenden Grundlagen:

Harmonisierte Normen gemäß (EU) 2023/1230
Harmonisierte Normen sind noch in Vorbereitung

Sonstige Grundlagen

- prEN 50742:2025
  Anmerkung: prEN 50742 wird nach Erscheinen von DIN EN 50742 durch diese ersetzt.
- CVSS 4.0 Metrik zur Einstufung von Schwachstellen
- IETF RFC 9116
- Zur Kommunikation von Schwachstellen werden die Begriffe nach CWE (Common Weakness Enumeration) verwendet
- BSI TR-02102-1 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen" Version: 2026-01

1.3 Gültigkeit

Diese Prüfgrundsätze gelten ab dem Tag der Freigabe und bis zu ihrem Ersatz durch eine überarbeitete Ausgabe oder ihre Zurückziehung.

1.4 Begriffsbestimmungen

Grundbegriffe werden gemäß der prEN 50742 verwendet.

2 Benötigte Unterlagen und Prüfgegenstände

Folgende Prüfgegenstände (z. B. Maschinen oder Sicherheitsbauteile), Software und Dokumente werden zur Prüfung bereitgestellt:

1. Funktionsbereiter Prüfgegenstand mit Spannungsversorgung
2. ggf. Software zum Auslesen der Logdaten und Konfigurationssoftware
3. Technische Dokumentation einschließlich:
    a. Risikobeurteilung z. B. nach EN ISO 12100 einschließlich aller risikominimierenden Maßnahmen
    b. Dokumentation der sicherheitsrelevanten Funktionen und zu den jeweiligen technischen Schutzmaßnahmen
    c. Auflistung aller physikalischen (z. B. eine Steckverbindung) und logischen (z. B. ein Protokoll) Schnittstellen sowohl intern als auch extern
    d. Auflistung aller Softwarekomponenten mit Versionsständen als SBOM
    e. Dokumentation, auf welche Weise die Anforderungen der prEN 50742 erfüllt wurden (Weg A oder Weg B).
4. Risikoanalyse zum Schutz vor Korrumpierung (Threat Assessment) nach prEN 50742
5. Die Originalbetriebsanleitung, in der folgende Informationen für den Betrieb dokumentiert sind
    a. Den Security Kontext (Bestimmungsgemäße Verwendung mit Blick auf Security) des Produktes
    b. Angaben zu Softwareversionen und Konfiguration, die für die Sicherheit relevant sind
    c. Dokumentation, wie die die eindeutige Software-Version und Konfiguration für sicherheitsrelevante Teile ermittelt werden kann
    d. Informationen über verbleibende Security-Risiken, die nicht durch andere Maßnahmen eliminiert werden konnten
    e. Dokumentation zum Auslesen und Interpretieren der Logdaten
6. Ggf. Herstellererklärung über die serienmäßige Fertigung
7. Ein Verweis auf den Notfallkontakt auf der Unternehmenswebseite zur Meldung von kritischen Schwachstellen mit Bezug auf die Korrumpierbarkeit des Produktes. Der Notfallkontakt wird entsprechend der BSI und DGUV-Empfehlung nach RFC 9116 erstellt.
   Über den Notfallkontakt ist der Hersteller für Prüfstellen, Behörden und Dritte, die Schwachstellen melden, erreichbar.
8. Konformitätserklärung (ggf. im Entwurf)

3 Internes Ermittlungsprotokoll über die Eigenschaften der Prüfgegenstände

Test ID	Testkriterium	E = entfällt, J = ja, N = nein	E	J	N	Bemerkung oder Quelle
Prüfling						
T01	Liegen Hardware, Software und Dokumente aus *notwendige Prüfgegenstände* vor?		☐	☐	☐	
T02	Ist es plausibel, dass die Dokumentation vollständig ist? (per Stichprobe)		☐	☐	☐	
T03	Ist der Prüfgegenstand eindeutig und dauerhaft gekennzeichnet? (Software wird über einen Hash eindeutig und dauerhaft gekennzeichnet registriert)		☐	☐	☐	
T04	Ist die eingereichte Dokumentation eindeutig gekennzeichnet?		☐	☐	☐	
Allgemeine Anforderungen						
T05	Ist dokumentiert, auf welchem Weg die Konformität erreicht wurde (z. B. Weg A oder B nach prEN 50742)?		☐	☐	☐	
T06	Liegt eine Risikobeurteilung nach ISO 12100 vor?		☐	☐	☐	
T07	Wurden die Gefährdungen in einer Risikobeurteilung ermittelt und die risikominimierenden Maßnahmen definiert?		☐	☐	☐	
T08	Wurden die sicherheitsrelevanten Funktionen zu den technischen Schutzmaßnahmen dokumentiert?		☐	☐	☐	
T09	Wurde ein threat assessment durchgeführt und dokumentiert?		☐	☐	☐	
T10	Wurde ein Security-Kontext definiert?		☐	☐	☐	
T11	Ist der dokumentierte Security-Kontext plausibel?		☐	☐	☐	
T12	Hat der Hersteller in nachfolgender Reihenfolge Maßnahmen angewandt und dokumentiert, um die Maschine vor gefahrbringenden Bedrohungen zu schützen: • Schwachstellen eliminieren • Schwachstellen mitigieren • Für verbleibende Schwachstellen in der Betriebsanleitung alle notwendigen Informationen überkompensierende Gegenmaßnahmen durch den Benutzer bereitstellen		☐	☐	☐	

Test ID	Testkriterium	E = entfällt, J = ja, N = nein	E	J	N	Bemerkung oder Quelle
T13	Interpretation von T12: Sind die Maßnahmen aus T12 angemessen?		☐	☐	☐	
T14	Wurde überprüft und dokumentiert, dass Maßnahmen aus T12 keine negativen Auswirkungen auf die Sicherheit der Maschine haben?		☐	☐	☐	
Betriebsanleitung						
T15	Enthält die Betriebsanleitung Informationen zum Security-Kontext?		☐	☐	☐	
T16	Enthält die Betriebsanleitung Angaben zur Softwareversion und Konfiguration, die für die sicherheitsrelevanten Funktionen erforderlich sind?		☐	☐	☐	
T17	Beschreibt die Betriebsanleitung, wie man auf die Informationen zur Softwareversion und Konfiguration für sicherheitsrelevante Funktionen sowie zu Änderungen daran zugreift und sie ausliest?		☐	☐	☐	
T18	Beschreibt die Betriebsanleitung, wie die Informationen zur Softwareversion und Konfiguration für sicherheitsrelevante Funktionen sowie Änderungen daran zu interpretieren sind?		☐	☐	☐	
T19	Enthält die Betriebsanleitung alle notwendigen Informationen über kompensierende Gegenmaßnahmen und verbleibende Security-Restrisiken (z. B. im Security Kontext)?		☐	☐	☐	
T20	Enthält die Betriebsanleitung Informationen darüber, unter welchen Rollen Änderungen durchgeführt werden dürfen?		☐	☐	☐	
T21	Beschreibt die Betriebsanleitung, wie man auf die gesammelten Nachweise zugreift und sie ausliest?		☐	☐	☐	
T22	Beschreibt die Betriebsanleitung, wie man die gesammelten Nachweise interpretiert?		☐	☐	☐	
Schnittstellen und Verbindungen der Maschine						
T23	Verfügt das Produkt über externe oder Interne Schnittstellen oder Verbindungen und hat der Hersteller dies vollständig dokumentiert? z. B.: Netzwerkverbindungen, Wifi-Verbindungen, Single-Wire, Kabel zur Stromversorgung, optische Verbindungen, Kartenlesegerät oder Verbindungen zu externen Systemen wie Cloud-Services, Industrienetzwerke oder Service-Tools, Anwendungsprotokolle (industrielle Kommunikationsprotokolle), kabelgebunden		☐	☐	☐	

Test ID	Testkriterium	E = entfällt, J = ja, N = nein	E	J	N	Bemerkung oder Quelle
	und kabellose Schnittstellen, physikalische Ports, Embedded HMI					
T24	Hat der Hersteller alle zugänglichen Schnittstellen und Verbindungen, die die Sicherheit der Maschine beeinflussen können, vollständig identifiziert und dokumentiert?		☐	☐	☐	
Prozessanforderungen						
T25	Liegt eine Liste des Herstellers der möglichen Bedrohungen (threats), die gefahrbringende Situationen auslösen können, vor?		☐	☐	☐	
T26	Ist eine Einflussanalyse des Herstellers zu den Schwachstellen vorhanden, in der die Safety Risk (Schadensschwere) und Wahrscheinlichkeit (für ein erfolgreiches Ausnutzen der Schwachstelle) berücksichtigt wird? Die Wahrscheinlichkeit, das Ziel/Opfer eines Angriffs zu werden, darf nicht berücksichtigt werden.		☐	☐	☐	
T27	Wurden Schwachstellen dokumentiert, die nicht eliminiert werden konnten?		☐	☐	☐	
T28	Wurde dokumentiert, warum die Schwachstellen aus T27 nicht eliminiert werden konnten?		☐	☐	☐	
T29	Sind implementierte Security-Maßnahmen für die Schwachstellen aus T27 dokumentiert?		☐	☐	☐	
T30	Wurden verbleibende Restrisiken für Schwachstellen, die nicht eliminiert und ausreichend mitigiert werden konnten, und kompensierende Gegenmaßnahmen dokumentiert?		☐	☐	☐	
Protokollierung *nachfolgend genannte Eingriffe sind bei der Protokollierung zu berücksichtigen:* • *sicherheitsrelevante Parametrierung / Konfiguration (Identifikation über CRC, etc.)* • *Update/Modifikation von SRESW (Identifikation nur über CRC, Versionsnummer, etc.)* • *Update/Modifikation von SRASW (Identifikation nur über CRC, Versionsnummer, etc.)* • *Parametrierung von HMIs, falls daraus Gefährdungen entstehen können* • *Update/Modifikation von Software zur Darstellung von sicherheitsrelevanten Anweisungen*						
T31	Hat das Produkt digitale oder physische Mittel (z. B. Siegel) zur Nachverfolgbarkeit von Eingriffen?		☐	☐	☐	
T32	Sind die Maßnahmen aus T31 geeignet? (Stichprobe und ggf. Bemerkung)		☐	☐	☐	
T33	Sind die digitalen Nachweise lesbar und zugänglich? (Zugriffsversuch)		☐	☐	☐	
T34	Hat der Hersteller für alle physischen Maßnahmen hinreichend begründet, warum		☐	☐	☐	

Test ID	Testkriterium	E = entfällt, J = ja, N = nein	E	J	N	Bemerkung oder Quelle
	digitale Nachweise nicht vernünftigerweise implementierbar sind?					
T35	Erfolgt die Sammlung der Nachweise von Eingriffen automatisch, ohne Mitwirkung durch Benutzer? (Eingriffsversuch)		☐	☐	☐	
T36	Ist das Sammeln von Nachweisen vor Deaktivierung geschützt?		☐	☐	☐	
T37	Ist dokumentiert, wo die Logeinträge gespeichert werden? In der Steuerung, in den Komponenten, in einem Speichermedium außerhalb der Maschine		☐	☐	☐	
T38	Enthält das Log für jede Art von Eingriff mindestens den letzten Eintrag (Nachweis)?		☐	☐	☐	
T39	Hat der Hersteller dokumentiert, ob und wie die Daten des Rückverfolgungsprotokolls für jeden Eingriff mindestens für 5 Jahre gespeichert werden?		☐	☐	☐	
T40	Wird das Rückverfolgungsprotokoll spätestens nach Inbetriebnahme der Maschine aktiviert?		☐	☐	☐	
T41	Hat der Hersteller ein Verfahren/Prozess beschrieben, wie T40 gewährleistet wird oder werden bereits Nachweise über Eingriffe gesammelt?		☐	☐	☐	
T42	Werden die Logs vor zufälliger und gezielter Manipulation geschützt? (Zugriffsrechte, Versuch der Manipulation)		☐	☐	☐	
T43	Hat der Hersteller in der Betriebsanleitung einen Prozess zur Löschung (Reset) des Logs beschrieben und kann dieser ausschließlich auf diese Art durchgeführt werden?		☐	☐	☐	
T44	Wird bei einem Reset der Logdaten ein Eintrag über das Löschen im Log angelegt?		☐	☐	☐	
T45	Enthalten digitale Nachweise für jeden Eintrag mindestens: • Art des Eingriffs, • Mittel, die eine Korrelation der geloggten Ereignisse ermöglichen, z. B. Zeitstempel mit Bezug zu Systemzeit, laufende Nummer, Systemzeit, Boot-Zähler, etc. • Das Löschen der Logdatei?		☐	☐	☐	
Identifikation der Softwareversion und Konfiguration						
T46	Stellt das Produkt Informationen zur Softwareversion und Konfiguration auf Anfrage bereit? (Durch das Produkt selbst oder ein externes Hilfsmittel)		☐	☐	☐	
T47	Sind die Informationen für Menschen lesbar?		☐	☐	☐	
Kryptographie						

Test ID	Testkriterium	E = entfällt, J = ja, N = nein	E	J	N	Bemerkung oder Quelle
T48	Entsprechen genutzte kryptographische Algorithmen dem Stand der Technik (vgl. BSI TR-02102-1)?		☐	☐	☐	
T49	Hat der Hersteller für alle Algorithmen, die nicht dem Stand der Technik entsprechen, die Ausnahme begründet?		☐	☐	☐	
Schutzmaßnahmen gegen Korrumpierung						
T50	Wurde eine risikobasierter Ansatz genutzt, um erforderliche Security-Maßnahmen zu ermitteln?		☐	☐	☐	
T51	Berücksichtigt der risikobasierte Ansatz das Safety Risk (Schadensschwere) und die Risiken der Bedrohungen (Wahrscheinlichkeit des Ausnutzens einer Schwachstelle) unter Berücksichtigung der bestimmungsgemäßen Verwendung der Maschine und des Security Kontext?		☐	☐	☐	
T52	Wurde für jede sicherheitsrelevante Funktion auf Basis der Ergebnisse des Threat Assessments ein SRSL bestimmt und dokumentiert?		☐	☐	☐	
T53	Zu T52: Liegt für jeden SRSL eine Korrelation mit der Wahrscheinlichkeit des Ausnutzens (z. B. Angriffspotential) der Schwachstelle vor?		☐	☐	☐	
T54	Zu T53: Wurden alle relevanten Verbindungen und Schnittstellen berücksichtigt?		☐	☐	☐	
T55	Zu T53: Wurden alle Schwachstellen für die relevanten Verbindungen und Schnittstellen mit einbezogen?		☐	☐	☐	
T56	Zu T53: Wurden entsprechende Wahrscheinlichkeiten bzw. Angriffspotentiale für die Schwachstellen berechnet (z. B. nach prEN 50742 Anhang B)?		☐	☐	☐	
T57	Zu T52: Liegt für jeden SRSL eine Korrelation mit dem Maß der Risikominimierung (Schadensschwere) durch die Schutzmaßnahme (sicherheitsrelevante Funktion) vor?		☐	☐	☐	
T58	Zu T52: Wurde die höchste Wahrscheinlichkeit / das höchste Angriffspotential zur Bestimmung jedes SRSL verwendet (z. B. nach prEN 50742 Tabelle B.6 oder Tabelle 2)?		☐	☐	☐	
T59	Werden nachfolgende Security-Anforderungen auf die sicherheitsrelevanten Funktionen und zugehörigen Schnittstellen und Verbindungen angewandt? (separate Erfassung)		☐	☐	☐	
T60	Wurden mindestens die Security-Anforderungen nach EN50742 zum jeweiligen SRSL erfüllt? (separate Erfassung)		☐	☐	☐	

Test ID	Testkriterium	E = entfällt, J = ja, N = nein	E	J	N	Bemerkung oder Quelle
T61	Wurden alle Threats durch die implementierten Security-Maßnahmen ausreichend mitigiert?		☐	☐	☐	
T62	Zu T61: Falls nein, konnten alle verbleibenden Schwachstellen eliminiert werden?		☐	☐	☐	
T63	Zu T62: Falls nein, hat der Hersteller begründet, warum dies nicht möglich war?		☐	☐	☐	
T64	Zu T62: falls nein, konnten alle Schwachstellen, die nicht eliminiert werden konnten, durch die Implementierung zusätzlicher Maßnahmen ausreichend mitigiert werden?		☐	☐	☐	
T65	Zu T64: Falls nein, hat der Hersteller begründet, warum dies nicht möglich war?		☐	☐	☐	
T66	Zu T64: Falls nein, wurde das verbleibende Risiko durch Schwachstellen, die weder eliminiert noch mitigiert werden konnten, identifiziert sowie kompensierende Gegenmaßnahmen definiert?		☐	☐	☐	

Impressum

Institut für Arbeitsschutz der DGUV
Prüf- und Zertifizierungsstelle
Alte Heerstraße 111
53757 Sankt Augustin
Telefon: +493013001-3601
E-Mail: sekretariat-ifa-z@dguv.de
Internet: https://dguv.de/dguv-test