



Interpretationspapier zur **Verordnung (EU) 2023 / 1230 über Maschinen**

Kapitel	III
Artikel	-
Anhang	-
Abschnitt	1.1.9. Schutz gegen Korrumpierung 1.2.1. Sicherheit und Zuverlässigkeit von Steuerungen a) 1.2.6. Störung der Energieversorgung oder der Kommunikationsnetzverbindung b) 3.3. Steuerung (Fernzugriff)
Dokument	IntPa-07.01
Datum	29. Oktober 2025
Version	1.0

1.1.9. Schutz gegen Korrumpierung

*Die Maschine bzw. das dazugehörige Produkt muss so konstruiert und gebaut sein, dass der **Anschluss von einer anderen Einrichtung an die Maschine** oder das dazugehörige Produkt durch jede Funktion der angeschlossenen Einrichtung selbst oder über eine mit der Maschine bzw. dem dazugehörigen Produkt kommunizierende entfernte **Fernzugriffseinrichtung nicht zu einer gefährlichen Situation führt.***

*Ein Hardware-Bauteil, das Signale oder Daten überträgt, die für den Anschluss oder den Zugriff auf die Software relevant sind, die für die Übereinstimmung einer Maschine oder eines dazugehörigen Produkts mit **den einschlägigen Sicherheits- und Gesundheitsschutzanforderungen** von entscheidender Bedeutung ist, muss so konstruiert sein, dass es angemessen **gegen unbeabsichtigte oder vorsätzliche Korrumpierung geschützt ist.***



Weitere Interpretationspapiere auf
www.nsbiv.ch/IntPa



Accreditation SCESp 0046
Notified Body 1247





Maschinen bzw. dazugehörige Produkte müssen **Beweise für ein rechtmässiges oder unrechtmässiges Eingreifen** in das genannte Hardware-Bauteil **sammeln**, soweit es für den Anschluss oder den Zugriff auf die Software relevant ist, die für die Konformität der Maschinen bzw. dazugehörigen Produkte von entscheidender Bedeutung ist.

Software und Daten, die für die Übereinstimmung der Maschine oder des dazugehörigen Produkts mit den einschlägigen **Sicherheits- und Gesundheitsschutzanforderungen** von entscheidender Bedeutung sind, sind als solche zu benennen und angemessen **gegen unbeabsichtigte oder vorsätzliche Korruption zu schützen**.

Die Maschine bzw. das dazugehörige Produkt muss die **installierte Software**, die für den sicheren Betrieb erforderlich ist, **kenntlich** machen und diese Informationen jederzeit in leicht zugänglicher Form bereitstellen können.

Maschinen bzw. dazugehörige Produkte müssen **Nachweise für ein rechtmässiges oder unrechtmässiges Eingreifen** in die Software oder eine **Veränderung** der in Maschinen bzw. dazugehörigen Produkten installierten Software oder ihrer **Konfiguration sammeln**.

1.2.1. Sicherheit und Zuverlässigkeit von Steuerungen

Steuerungen sind so zu konzipieren und zu bauen, dass es nicht zu **Gefährdungssituationen** kommt. Steuerungen müssen so ausgelegt und beschaffen sein, dass

a) sie, wenn den Umständen und Risiken angemessen, den zu erwartenden Betriebsbeanspruchungen sowie beabsichtigten und **unbeabsichtigten Fremdeinflüssen**, einschliesslich **vernünftigerweise vorhersehbare böswillige Versuche Dritter**, die zu einer Gefährdungssituation führen, standhalten können;

1.2.6. Störung der Energieversorgung oder der Kommunikationsnetzverbindung

b) die **Parameter** der Maschine dürfen sich nicht unkontrolliert ändern können, wenn eine derartige unkontrollierte Änderung zu **Gefährdungssituationen** führen kann;

3.3. Steuerung

Erforderlichenfalls sind Massnahmen zu treffen, die eine **unerlaubte Benutzung der Steuerung verhindern**. [...] Die Fernsteuerung muss so konstruiert und gebaut sein, dass sie

- a) **ausschliesslich die betreffende Maschine** bzw. das dazugehörige Produkt und
- b) **ausschliesslich die betreffenden Funktionen** steuert.

Ferngesteuerte Maschinen bzw. dazugehörige Produkte müssen so konstruiert und gebaut sein, dass sie **nur auf Steuerbefehle von dem für sie vorgesehenen Bedienungsgerät** reagieren.

Bei autonomen mobilen Maschinen und dazugehörigen Produkten muss die Steuerung so konzipiert sein, dass sie **die Sicherheitsfunktionen** gemäss diesem Abschnitt eigenständig erfüllt, **auch wenn Funktionen mittels einer Fernüberwachungsfunktion befohlen werden**.



1 Ziel und Zweck

In der Verordnung (EU) 2023/1230 über Maschinen (EU-MaschV) werden einige neue Anforderungen an die Wirtschaftsakteure gestellt. Derzeit besteht weder ein Leitfaden zur Anwendung der neuen EU-MaschV noch sind zu allen Anforderungen harmonisierte Normen (Stand der Technik) verfügbar.

Deshalb stellt die NSBIV AG, Zertifizierungsstelle *SIBE Schweiz* den Wirtschaftsakteuren Interpretationspapiere zur Verfügung, die nach heutigem Stand von Wissen und Technik erstellt, laufend an die technische Entwicklung und die Erfahrungen aus dem Feld angepasst werden.

Die Interpretationspapiere haben keinen gesetzlichen Charakter, können aber als Stand der Technik Papiere verwendet werden, bis harmonisierte Normen oder ein Leitfaden die Anforderungen konkretisieren.

2 Erläuterung der Anforderung

2.1 Definition Korruption

Korruption (engl. corruption) beschreibt in der Software den ungewollten oder böswilligen Verlust der Daten- oder Code-Integrität.

Dabei werden Dateien, Parameter oder Programmcode durch unter anderem durch Software-Bugs oder gezielte Manipulation so verändert, dass sie nicht mehr dem ursprünglichen Zustand entsprechen und Programme Fehlfunktionen zeigen.

2.2 Begriffe und Abkürzungen

Cyber: Dient vor allem als Präfix zur Kennzeichnung von Fachgebieten und Phänomenen wie Cyber-Security, Cyberkriminalität, Cyberspace oder digitaler Kommunikation. Es steht stellvertretend für die virtuelle Umgebungen, vernetzte Infrastrukturen, etc.

Cyber-Security: Fokussiert auf Prävention und Schutzmassnahmen gegen bekannte und erwartete Risiken.

Cyber-Resilience: Die Cyber-Resilience bezeichnet die Fähigkeit von Organisationen, IT-Systemen, Netzwerken und Daten so zu gestalten und zu betreiben, dass diese trotz fortwährender Cyberangriffe, technischen Störungen oder menschlicher Fehler

- a.) betriebsfähig bleiben (Mitigation);
- b.) schnell wiederhergestellt werden (Recovery);
- c.) und kontinuierlich aus Vorfällen lernen, um zukünftige Bedrohungen besser zu bewältigen.

Security: Maschine vor unbefugtem Zugriff schützen. IT- oder Cyber-Sicherheit (Schutz gegen Angriffe von aussen wie z.B. Cyberangriffe)

Safety: Menschen, Tiere, Sachen und, wo anwendbar, Umwelt vor Gefährdungen der Maschine schützen - Technische und Funktionale Sicherheit (Safety-SPS, Sicherheitsfunktionen wie NOT-Halt, etc.)

Im deutschen Sprachgebrauch wird nur der Begriff «Sicherheit» verwendet. Sicherheitsmängel oder -lücken in der Security können die Gewährleistung der funktionalen Sicherheit (Safety) gefährden.

FMEA: Die Fehlermöglichkeits- und Einflussanalyse, kurz Auswirkungsanalyse genannt, ist eine analytische Methode, um Fehler in System, welche die Zuverlässigkeit beeinträchtigen können, in der Entwurfsphase zu entdecken.

Englisch: Failure Mode and Effects Analysis



2.3 Erläuterung der Verordnung

Die Verordnung (EU) 2023/1230 über Maschinen (EU-MaschV) stellt Anforderungen an die Massnahmen zum Schutz gegen Korruption beziehungsweise Cyberangriffe.

Die Massnahmen müssen sicherstellen, dass von der Maschine keine Gefahrensituationen durch Korruption entstehen können.

- Die Maschine muss so konstruiert sein, dass der Anschluss externer Einrichtungen – sei es direkt oder über Fernzugriff – keine gefährlichen Situationen verursacht.
- Ein Hardware-Bauteil, das für den Zugriff auf sicherheitsrelevante Software einer Maschine entscheidend ist, muss so konstruiert sein, dass es wirksam gegen unbeabsichtigte oder absichtliche Manipulation geschützt ist.
- Maschinen müssen Eingriffe in sicherheitsrelevante Hardware erfassen und dokumentieren, wenn diese den Zugriff auf sicherheitskritische Software betreffen.
- Maschinen müssen rechtmässige oder unrechtmässige Eingriffe in sicherheitsrelevante Hardware erkennen und dokumentieren.
- Software und Daten, die für die Sicherheit und Konformität einer Maschine entscheidend sind, müssen klar gekennzeichnet, vor Manipulation geschützt und jederzeit leicht zugänglich sein.

Im Speziellen ist bezüglich der (Sicherheits-) Steuerungen zu beachten;

- Steuerungen von Maschinen müssen so gestaltet sein, dass sie keine Gefährdungssituationen verursachen und gegen vorhersehbare Störungen und Manipulationen geschützt sind.
- Sie dürfen nicht unbeabsichtigt Parameter ändern, wenn dies gefährlich sein kann, und müssen gegebenenfalls vor unbefugter Nutzung gesichert sein.
- Fernsteuerungen dürfen nur die vorgesehenen Maschinen und Funktionen steuern und nur auf autorisierte Bediengeräte reagieren.
- Bei autonomen mobilen Maschinen muss die Steuerung Sicherheitsfunktionen auch bei Fernüberwachung zuverlässig erfüllen.

Die Verordnung (EU) 2023/1230 über Maschinen richtet sich mit ausdrücklichen Anforderungen an den Hersteller respektive den Inverkehrbringer.

3 Stand der Technik

3.1 Übersicht Verordnungen und Normen

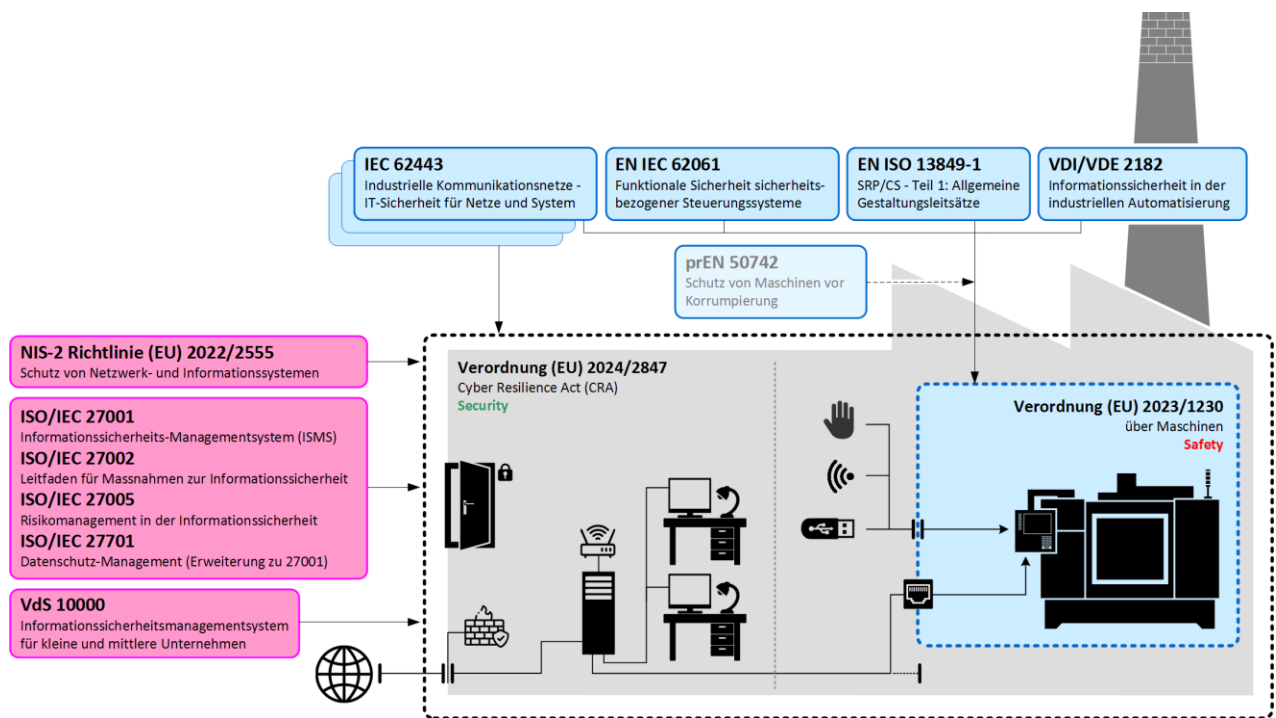
Die **Verordnung (EU) 2024/2847** über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen, auch Cyber Resilience Act (CRA) genannt, wurde am 20. November 2024 im Amtsblatt der Europäischen Union veröffentlicht. Diese Verordnung tritt zwanzig Tage nach der Veröffentlichung im EU-Amtsblatt in Kraft (10. Dezember 2024) und gilt 36 Monate nach diesem Inkrafttreten unmittelbar in jedem EU-Mitgliedstaat, nämlich ab dem 11. Dezember 2027.

DerCRA legt grundsätzliche Sicherheitsanforderungen für vernetzte digitale Produkte und deren Software fest, während die neue EU-MaschV speziell für Maschinen zusätzliche Anforderungen zum Schutz gegen Korruption aufnimmt.

Daraus folgt, dass Hersteller sowohl CRA-konforme Sicherheitsmassnahmen für eingesetzte Softwarekomponenten als auch maschinenspezifische Massnahmen zur Verhinderung von Korruption implementieren müssen, wobei beide Regelwerke sich ergänzen, und überschneidende Pflichten erzeugen können.

Die **NIS-2-Richtlinie** (EU) 2022/2555 (NIS-2) zielt darauf ab, ein hohes gemeinsames Cybersicherheitsniveau in der Europäischen Union zu gewährleisten und die Resilienz von Netz- und Informationssystemen zu stärken.

Die NIS-2 wurde am 14. Dezember 2022 verabschiedet und ersetzt die vorherige NIS-Richtlinie (EU) 2016/1148. Sie wurde eingeführt, um den Herausforderungen der zunehmenden Cyberbedrohungen und der Abhängigkeit von digitalen Technologien gerecht zu werden. Die Richtlinie verpflichtet die Mitgliedstaaten, nationale Cybersicherheitsstrategien zu entwickeln und nationale Computer Security Incident Response Teams (CSIRTs) zu benennen, die für die Reaktion auf Sicherheitsvorfälle zuständig sind.



3.2 Harmonisierten Normen

IEC 62443 IT-Sicherheit für industrielle Automatisierungssysteme

Diese Normenreihe richtet sich an Betreiber, Hersteller und Dienstleister von Maschinen mit Teil 2 und 3 für den Maschinenbau.

EN ISO 13849-1 Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen Teil 1: Allgemeine Gestaltungsleitsätze

Die heute schon unter der Maschinenrichtlinie 2006/42/EG angewendete Norm bezüglich sicherheitsbezogener Steuerung beinhaltet Anforderungen bezüglich dem Fernzugriff zur Steuerung.

5.2.4 Fernzugriff

[...] Der Entwurf des SRP/CS darf den Fernzugriff auf eine Maschine nur dann erlauben, wenn besondere Massnahmen vorhanden sind, die gefährliche Situationen verhindern, die durch die unbemerkte Anwesenheit von Personen im Inneren oder in der Nähe der Maschine entstehen können (z. B. siehe 5.2.2.2).

Sicherheitsbezogene Software des SRP/CS darf nicht durch Fernzugriff geändert werden können, es sei denn die lokale Validierung der Sicherheitsfunktionen wird durchgeführt.



EN IEC 62061 Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener Steuerungssysteme (6.8 Sicherheitsaspekte)

Die harmonisierte Norm enthält keine spezifischen Anforderungen, verweist auf Hinweise in den Technischen Regeln (TR) und Normen (IEC TR 63074, ISA TR84.00.09, ISO/IEC 27001:2013, ISO TR 22100-4 und IEC 62443)

prEN 50742 «Protection against corruption»

Für Hersteller und Inverkehrbringer von Maschinen wird in Zukunft eine Norm zur Verfügung stehen, abgeleitet aus der EU-MaschV, Anhang III, Abschnitt 1.1.9 und 1.2.1. Aktuell liegt die prEN 50742 in Entwurfsform vor. Die Verabschiedung gemäss dem Standardisierungsantrag der EU-MaschV Normen soll bis zum 20. Januar 2026 erfolgen.

3.3 Weitere Rechtsakten und Regeln zum Thema IT-Sicherheit

IEC 62443-x IT-Sicherheit für industrielle Automatisierungssysteme

Die Teile 2 und 3 dienen speziell für den Maschinenbau. Die Normenreihe richtet sich an Hersteller, wie auch an Betreiber und Dienstleister von Maschinen.

ISO/TR22100-4 Safety of machinery - Relationship with ISO 12100 Teil 4: Leitlinien für Maschinenhersteller zur Berücksichtigung von IT-Sicherheits- (Cybersicherheits-) Aspekten
Leitlinien zur Risikobeurteilung für Maschinenhersteller

IEC TR 63074 Aspekte zur Cybersicherheit in Verbindung mit der funktionalen Sicherheit von sicherheitsrelevanten Steuerungssystemen. Diese wurde im Jahr 2023 in eine technische Spezifikation überführt **IEC TS 63074**

TRBS 1115-1 Technische Regel für Betriebssicherheit - Teil 1: Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen

Richtet sich an Betreiber von Maschinen.

4 Interpretation nach SIBE Schweiz

4.1 Anforderung an die Wirtschaftsakteure

Der Schutz vor Korruption (Security) umfasst sowohl absichtliche Angriffe auf die Hardware, Anwendungsprogramme und zugehörige Software als auch unbeabsichtigte Ereignisse, die auf menschliches Versagen zurückzuführen sind (siehe auch EN62061:2021).

Somit darf es nicht möglich sein, dass Software oder Daten an der Maschine geändert werden und diese Änderung zur einer Gefährdungssituation führen können.

Die EU-MaschV verlangt bezüglich **Sicherheits- und Gesundheitsschutzanforderungen**, dass...

- **Konstruktion** der Maschine ein **angemessener Schutz gegen** unbeabsichtigte oder vorsätzliche **Korruption** vorgesehen wird.
- **Beweise** für rechtmässiges oder unrechtmässiges **Eingreifen** erfasst werden.

4.2 Mögliche Umsetzung

4.2.1 Abgrenzung

Die EU-MaschV verlangt **keine exakt definierten Massnahmen** im Zusammenhang mit dem Schutz vor Korruption, welche die Zuverlässigkeit oder Sicherheit der Maschine beeinträchtigen kann. Diese Cybersicherheitsanforderungen sind in der CRA beschrieben und gelten ab dem 11. Dezember 2027 in jedem EU-Mitgliedstaat. In diesem Dokument wird nicht auf diese Anforderungen eingegangen.

Im CRA werden generische Themen wie Erreichbarkeit Notfallkontakt, Kritikalität von Sicherheitslücken und Meldung von Sicherheitslücken behandelt.



Die zukünftigen Anforderungen werden in der Norm prEN 50742 «Protection against corruption» unter Bezugnahme auf die EU-MaschV verankert sein.

Eine Hilfestellung bietet heute die Normenreihe **IEC 62443 IT-Sicherheit für industrielle Automatisierungssysteme**, welche sich an Hersteller und Betreiber richtet.

4.2.2 Umsetzung für Hersteller von Sicherheitsbauteilen

Für Hersteller von Sicherheitsbauteilen oder Maschinen mit eigener entwickelter Sicherheitssteuerung müssen Massnahmen für Schutz gegen Korrumpierung umgesetzt werden.

In einer Risikobeurteilung resp. Fehlermöglichkeits- und -Einfluss Analyse (FMEA) sind die potenziellen Fehlerquellen zu identifizieren und entsprechende Massnahmen zu definieren. Massnahmen können dem Hersteller oder Betreiber der Maschine übertragen werden, wenn die Massnahmen gegen eine vorhersehbare Fehlanwendung berücksichtigt wurde.

Diese Massnahmen müssen in der Betriebsanleitung detailliert beschrieben werden.

4.2.3 Umsetzung für Hersteller von Maschinen

In einem grossen Teil der Maschinen werden Sicherheitsbauteile verbaut, welche gesondert in Verkehr gebracht sind. Diese Sicherheitsbauteile müssen die Anforderungen der EU-MaschV vollständig erfüllen, auch im Hinblick auf den Schutz vor Manipulation und Korrumpierung.

Beim Einbau von diesen Sicherheitsbauteilen, mit der Berücksichtigung der Anforderungen aus deren Betriebsanleitung, kann daher davon ausgegangen werden, dass der Schutz gegen Korruption gemäss EU-MaschV zu einem grossen Teil erfüllt ist.

Eine Risikobeurteilung (und Security Konzept) bezüglich des Schutzes vor Korrumpierung ist in Anbetracht von möglichen Restrisiken, wie auch Fehlanwendungen anzuwenden.

5 Beispiele und Erläuterungen

5.1 Computernetzwerke im Vergleich

Der Schutz von Rechnern im Büro und privaten Bereich ist unter Anwendung von restriktiven Massnahmen gut beherrschbar (Firewalls, Virenprogramme, regelmässige Updates und Backups).

Im Bereich der Industrie gibt es oft Lücken in den Sicherheitsstandards, insbesondere bei bestehenden Anlagen oder Maschinen mit hoher Auslastung. Die Maschinenverfügbarkeit hat häufig höhere Priorität und Eingriffe in laufende Systeme werden vermieden (Produktionsunterbrüche durch z.B. Updates, Hardwareaustausch etc.).

Stetige Weiterentwicklung mit verkettenden Maschinen bis hin zu kompletten Fertigungsstrassen mit oder ohne Fernzugriff erfordern laufend höhere Security Standards. Dadurch fehlen oft grundlegende Schutzmechanismen wie Zugriffskontrollen, Netzwerksegmentierung oder Monitoring.

5.2 Gefährdungen der Cybersicherheit

Die Gefährdungen reichen von der Manipulation von Steuerungsprozessen bis hin zum Diebstahl sensibler Daten. Cyberangriffe können auf zwei Arten erfolgen:

Aussen (Remote) über das Internet, beispielsweise durch Hacker, die Schwachstellen in der Netzwerkinfrastruktur ausnutzen.

Innen (Lokal) durch externes Wartungs- oder Instandhaltungspersonal, das über mobile Geräte wie Notebooks oder USB-Sticks Zugang zu Steuerungssystemen erhält.

Typische Angriffsformen sind das Einschleusen von Schadsoftware, das unbefugte Verändern oder Löschen von Daten sowie die gezielte Manipulation von Steuerungsabläufen.

Mutwilliges Verhalten durch Mitarbeiter. Damit können Sicherheitseinrichtungen zum Schutz von Personen manipuliert werden, wie beispielsweise Verändern von Geschwindigkeiten oder unerwarteter Anlauf der Maschine



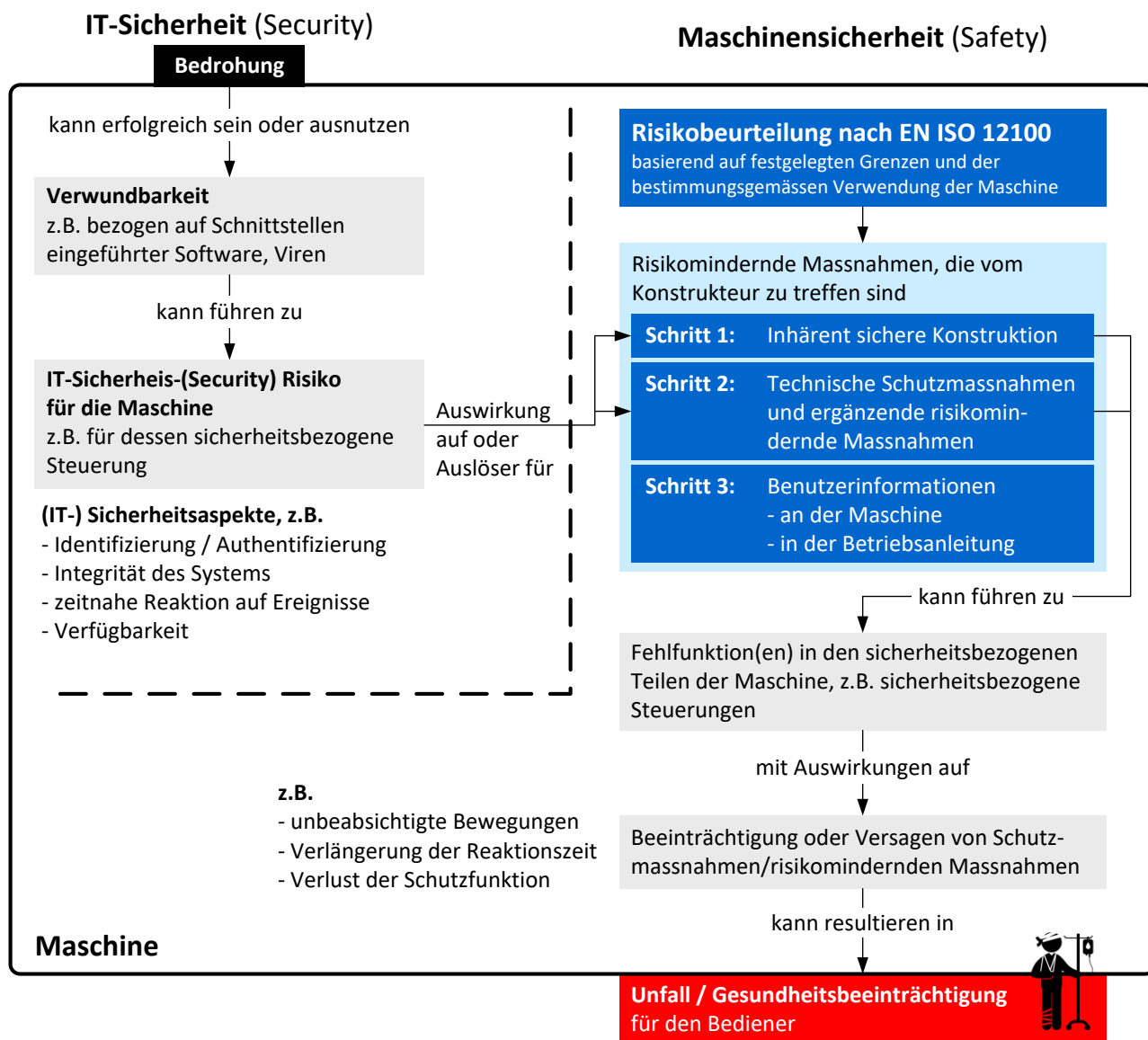
5.3 Risikobeurteilung und Schutzmassnahmen

Bei der Risikobeurteilung ist ein gesamtheitlicher Ansatz mit folgenden möglichen Fragestellungen zu verfolgen. Wurden...

- Wurden die Schnittstellen zur Maschinensicherheit analysiert? Zu anderen Maschinen?
- Sind lokale Zugriffe wie z.B. USB, Notebook, Wireless z.B. Funk betrachtet worden?
- Sind remote Zugriffsmöglichkeiten (Internet) betrachtet worden?
- Ist eine sichere Datenübertragung gewährleistet?
- Sind die Herstellerangaben von Sicherheitsbauteilen eingehalten worden?
- Ist der Zugriff eingeschränkt? Ist die Freigabe nur für autorisierte Personen möglich?
- Wurde die Verfügbarkeit eingeschränkt (Zugriff nur eine gewisse Zeit)
- Können Daten unwissentlich geändert werden? Sind Änderungen nachvollziehbar?

Eine regelmässige Beurteilung der getroffenen Massnahmen ist unabdingbar, um mit dem Stand der Technik im Bereich der IT-Security mitzuhalten.

5.3.1 Gegenüberstellung der Risikobeurteilung von Security und Safety



5.4 Security Massnahmen

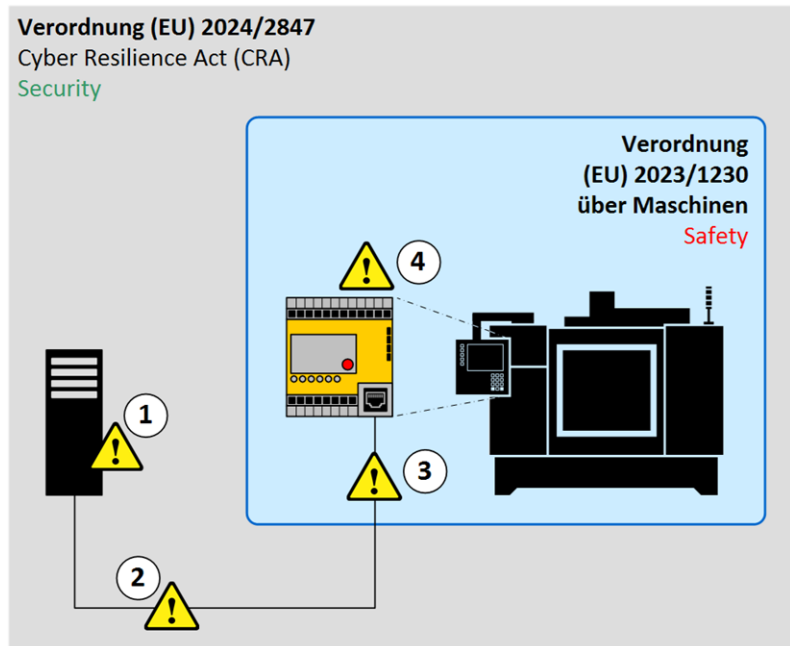
Es gibt viele mögliche Massnahmen, welche anhand der Security Risikobeurteilung oder auch nach Hersteller Angaben (z.B. Sicherheitsbauteilen) zu bewerten und zu prüfen sind.

5.4.1 Fernzugriff von Aussen (Remote)

Beispiel: schlechte Lösung (ohne Security)

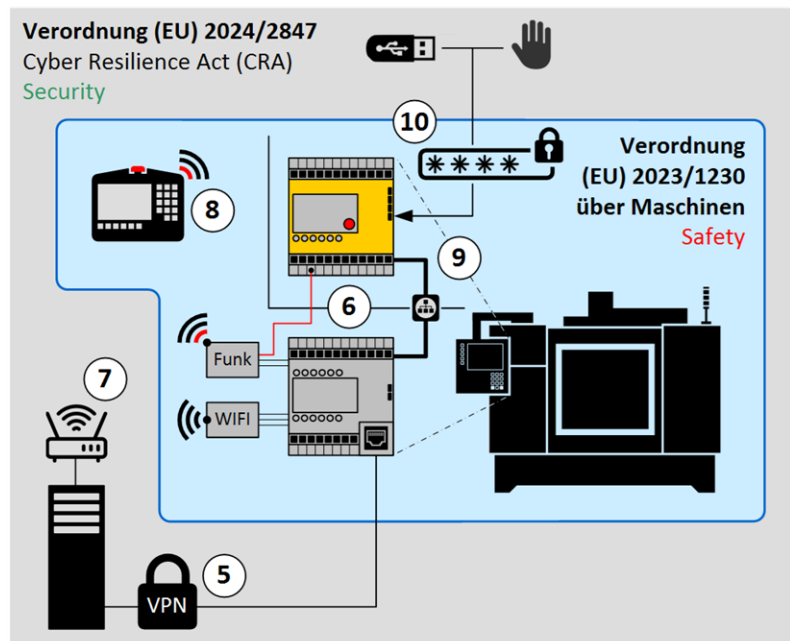
- (1) Rechner zur Fernwartung kompromittiert («gehackt»)
- (2) Sichere Verbindung («Tunnel») fehlt
- (3) Zugang nur mit einfachem Passwort z.B. «123» geschützt
- (4) Sicherheits-SPS ist vernetzt, dauern mit dem Netzwerk verbunden

Bemerkung: Ein offener LAN-Anschluss der Sicherheits-SPS ist wie eine «offene Tür»



Beispiel: gute Lösung (mit Security)

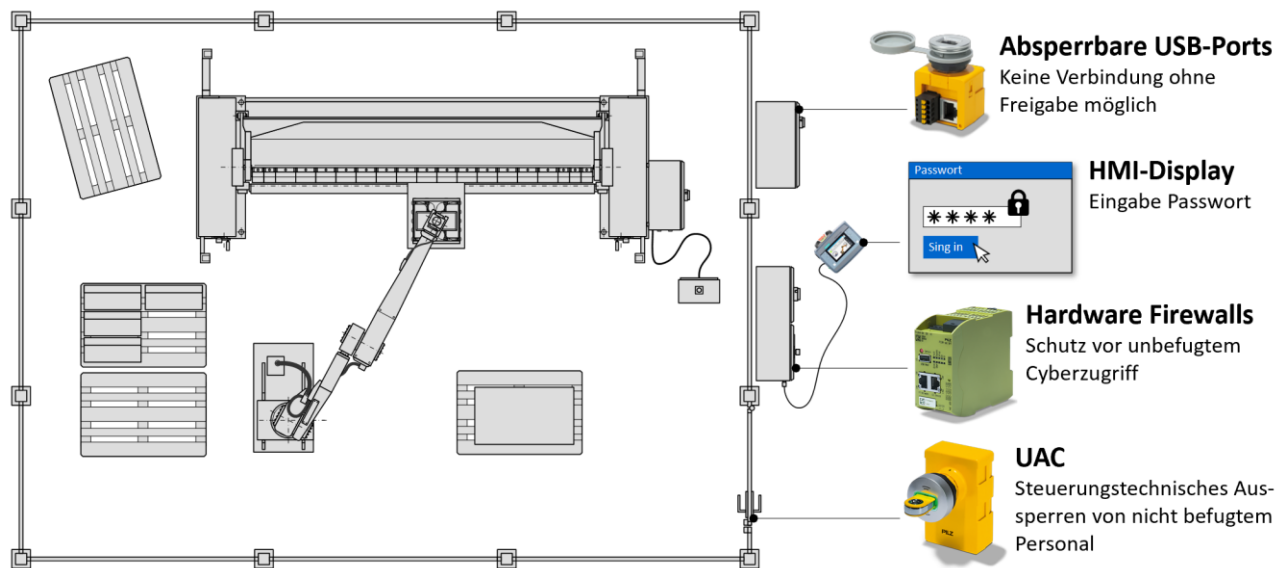
- (5) Sichere Verbindung «Sicherer Tunnel» z.B. mit VPN (Virtual Private Network)
- (6) Sicherheits-SPS ist von öffentlichem Netzwerk isoliert (Trennung)
- (7) Sichere Funk oder WiFi Verbindungen vom Hersteller (Zertifiziert)
- (8) Sicherheitsbauteile mit Zugriffsschutz (Login, deaktivieren mittel Timeout)
- (9) Lokale Verbindung zur Sicherheits-SPS über sicheres Bussystem z.B. Profisave
- (10) Zugriffsschutz auf Ports wie LAN, USB, ...



Massnahmen gegen Korrumpierung (Remote)

- Aufteilung des Netzwerks in Zonen, Firewall-Konfiguration (Segmentierung)
- Die Sicherheits-SPS ist nicht permanent am Netzwerk (Verfügbarkeit minimiert)
- Prozess-SPS mit «sicherer Tunnel» Lösung (Zugriff gegen aussen gesichert)
- Zugriff mit Passwort und zusätzlicher Authentifizierung geschützt (2-fach Authentifizierung)
- Minimal-Rechte Prinzip anwenden (Anzahl Person mit Zugriff reduziert)

5.4.2 Zugriff von Innen (Lokal)



Massnahmen gegen Korruption (lokal)

- Zutritt zum Werksareal respektive Maschine sicher (Batch Eintritt, Registrierung)
- Absperrbare USB-Ports (Zugriff intern gesichert)
- Gesperrte HMI-Display – Zugriff mit verschiedenen User-Levels (Login Schutz)
- Zugriff mit Passwort und zusätzlicher Authentifizierung geschützt (2-fach Authentifizierung)
- Instandhaltungspersonal nimmt nur Instruktionen von autorisierten Fachpersonal entgegen z.B. per Telefon und identifiziert dieses als solches (Erkennen Falschanweisungen, Sorgfaltspflicht)

5.4.3 Zugriff auf sicherheitsrelevante Bauteile

Maschinen können mit verschiedenen Arten von sicheren Steuerungen ausgerüstet werden. Der Schutz gegen Korruption ist bei der Wahl der Komponente entsprechend zu berücksichtigen.

Kontaktbehaftete Steuerungen (Sicherheitsrelais)

Diese Baugruppen sind unkritisch gegen Angriffe von innen oder aussen, da diese über keine externe digitale Schnittstelle verfügen (kein Zugriff). Verstellbare Sicherheitseinstellungen müssen mechanisch gegen Manipulation geschützt sein (Schutzdeckel mit Plombierung).

Bild Quelle: Pilz GmbH & Co. KG



Elektronische Steuerungen (nicht programmierbare Bauteile)

Diese Baugruppen sind unkritisch gegen Angriffe von innen oder aussen, da diese über keine externe digitale Schnittstelle verfügen (kein Zugriff).

Bild Quelle: ACD Antriebstechnik GmbH



Elektronische programmierbare Steuerungen

Hingegen kritisch sind, Baugruppen mit externer digitaler Schnittstelle, sei es drahtgebunden (z.B. USB, Notebook) oder kontaktlos (Wireless) wie Programmierbare Steuerungen (wie SPS- oder Mikroprozessor-Systeme). Bei Maschinensteuerungen gibt es mehrere Arten von externen Schnittstellen, welche in Form von Netzwerkverbindungen und/ oder Verbindungen zu übergeordneten Leitsystemen ausgeführt sein können.

Bild Quelle: Pilz GmbH & Co. KG



5.5 Quellenangaben / Referenzen

- DGUV FBHM-102 Safety und Security in der vernetzten Produktion
- DGUV FBHM-133 Sichere Fernwartung von Maschinen
- KAN Brief 2/25 Kommission Arbeitsschutz und Normung (DE)