BGHM
Berufsgenossenschaft
Holz und Metall

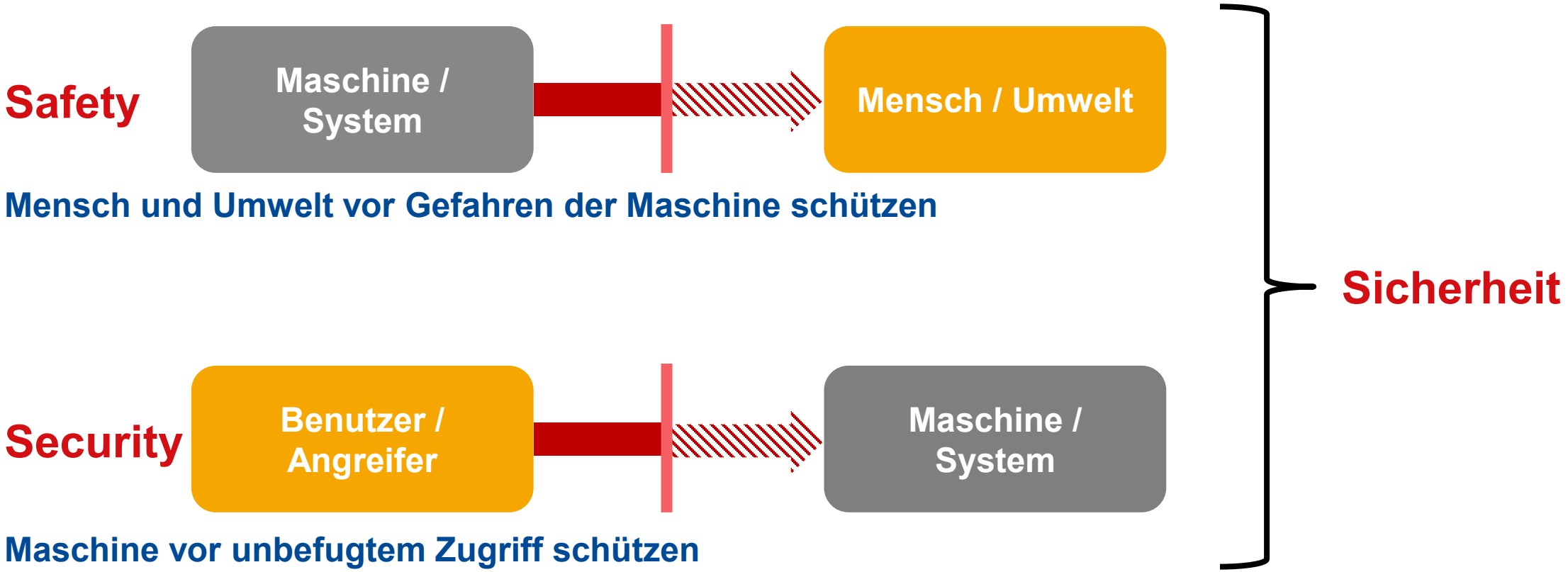
Ihre gesetzliche Unfallversicherung

Industrial Security – Sichere Fernwartung

Neue Verordnungen, neue Normen

Fachveranstaltung Maschinen,
M. Eberle, 30.06.2026

Safety, Security und Sicherheit



Industrial Security

- Information Technology (IT) und Operational Technology (OT)
- „Office IT“ „Shopfloor IT“

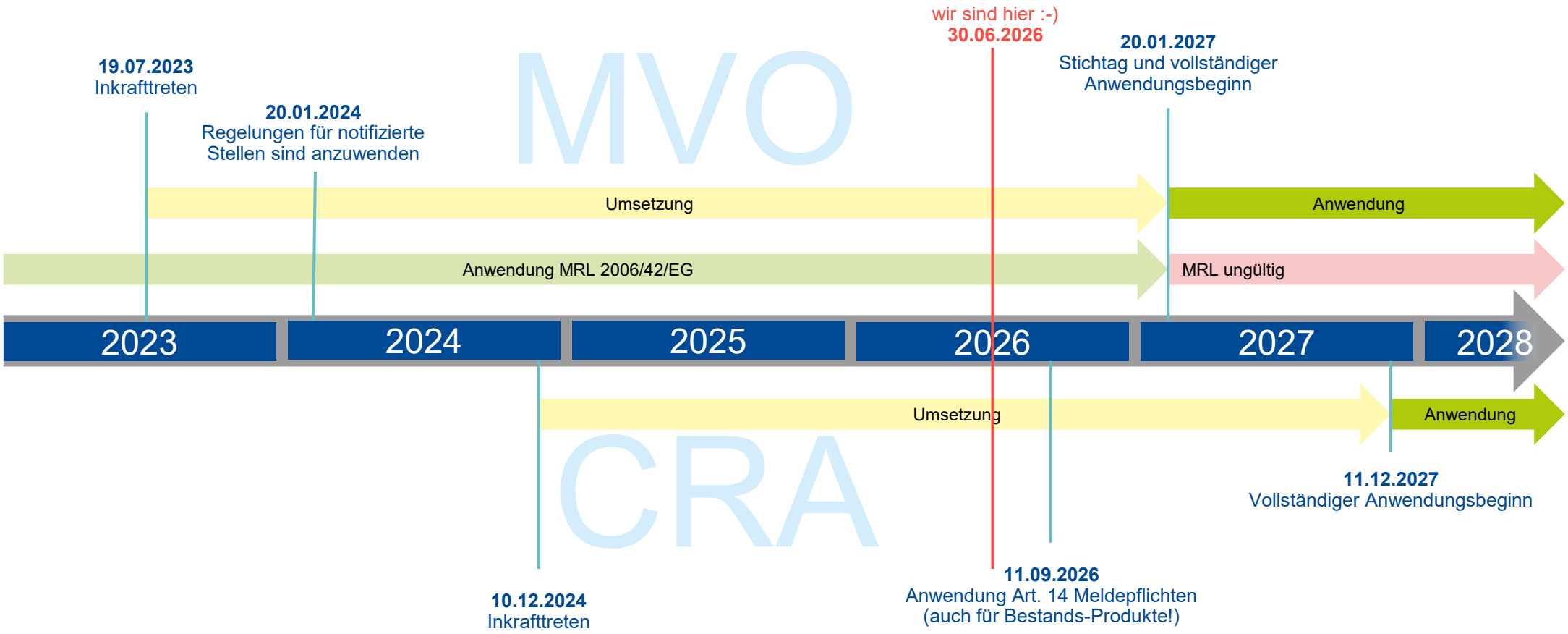
- Unterschiedliche Priorität der Schutzziele:

IT	OT
1. Vertraulichkeit	1. Verfügbarkeit
2. Integrität	2. Integrität
3. Verfügbarkeit	3. Vertraulichkeit

Aber:

- Keine strikte Trennung, fließender Übergang → keine genaue Definition
- Ähnliche / gleiche Lösungen zum effektiven Schutz → Unterscheidung nicht essenziell

Neue EU-Verordnungen



Maschinenrichtlinie und Maschinenverordnung

Aktuelle MRL 2006/42/EG fordert **nicht explizit** Security-Maßnahmen

- Anhang I Abschnitt 1.2.1 Sicherheit und Zuverlässigkeit von Steuerungen

→ **Implizite Forderung**?

Neue MVO (EU) 2023/1230 fordert **explizit** Security-Maßnahmen

(ab dem **20.01.2027 vollumfänglich anzuwenden**, Stichtagsregelung)

Anhang III „ Grundlegende Sicherheits- und Gesundheitsschutzanforderungen“

- Abschnitt 1.1.9 „Schutz gegen Korrumpierung“ neu
- Abschnitt 1.2.1 „Sicherheit und Zuverlässigkeit von Steuerungen“ erweitert
- Fokus auf die Security **sicherheitsrelevanter** (Safety) Elemente

→ **Ziel: Maschine ohne Gefährdungen**

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****. […]“*

→ (digitale) Schnittstellen sind zu betrachten

→ Ggf. Funk (RFID, W-LAN, Funkfernsteuerungen, …) nicht vergessen!

1.1.9. Schutz gegen Korrumpierung

*„[…] 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. […]“*

- → Sicherheitsrelevante Hardware-Bauteile sind zu schützen
- → Was ist „angemessen“? Von welcher Bedrohungssituation geht man aus und von welchen Folgen? (→ „Security Risk Assessment“)
- → Eine zugeschraubte (ggf. werkzeuglos) Klappe vor einer Schnittstelle kann ein angemessener Schutz sein
- → Perimeter-Betrachtung: In welchem Umfeld steht die Maschine bestimmungsgemäß?

1.1.9. Schutz gegen Korrumpierung

„[…] 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. […]“

→ Maschinen(-steuerung) selbst muss in der Lage sein, Veränderungen („Manipulationen“) zu erkennen bzw. erkenntlich zu machen

→ Log-Datei, gebrochenes physikalisches Siegel, …

1.1.9. Schutz gegen Korrumpierung

„[…] 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 Korrumpierung zu schützen****. […]“*

→ Wie für Hardware, so für sicherheitsrelevante Software und Daten

1.1.9. Schutz gegen Korrumpierung

„[…] 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 Produkte installierten Software oder ihrer Konfiguration sammeln.“

→ „kenntlich machen“ z. B. auf dem HMI

→ „Nachweise“ = „Beweise“

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;“*

→ gegen beabsichtigte Angriffe schützen!

1.2.1. Sicherheit und Zuverlässigkeit von Steuerungen

„Steuerungen müssen so ausgelegt und beschaffen sein, dass

[…]

f) das Rückverfolgungsprotokoll der Daten, das im Zusammenhang mit einem Eingreifen generiert wurden, und der Versionen der Sicherheitssoftware, die nach dem Inverkehrbringen oder der Inbetriebnahme der Maschine oder des dazugehörigen Produkts hochgeladen wurden, bis zu fünf Jahre nach dem Hochladen ausschließlich für den Nachweis der Konformität der Maschine oder des dazugehörigen Produkts mit diesem Anhang auf begründete Anforderung einer zuständigen nationalen Behörde zugänglich ist.“

→ Rückverfolgungsprotokoll im Unterschied zu Beweisen (Rückverfolgung ist weitergehend)

→ Eingreifen = jede Veränderung der sicherheitsrelevanten Software / Hardware

„Cyber Resilience Act“ (CRA)

Verordnung (EU) 2024/2847 […] über horizontale **Cybersicherheitsanforderungen für Produkte mit digitalen Elementen** […]

- am 20. November 2024 im Amtsblatt der EU veröffentlicht
- ab dem **11. Dezember 2027** vollumfänglich anzuwenden
- erfasst grundsätzlich alle Produkte mit „digitalen Elementen“
- an Hersteller (und Bevollmächtigte, Einführer, Händler) gerichtet
- parallel zur MVO anzuwenden und für die Konformitätserklärung zu beachten
- **keine Safety-Anforderungen**
- Fokus auf **Security über den gesamten Lebenszyklus**

→ Ziel: Schwachstellenmanagement

Anwendungsbereich

Artikel 2 (1):

„Diese Verordnung gilt für auf dem Markt bereitgestellte **Produkte mit digitalen Elementen**, deren **bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung** eine **direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz** einschließt.“

→ Betrachtet ebenfalls (digitale) Schnittstellen mit Verbindung nach „außen

„Digitale Elemente“

Artikel 3:

1. „Produkt mit digitalen Elementen“: ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden;

4. „Software“ den Teil eines elektronischen Informationssystems, der aus Computercode besteht;

5. „Hardware“ ein physisches elektronisches Informationssystem, das digitale Daten verarbeiten, speichern oder übertragen kann, oder Teile eines solchen Systems;

Kategorien von Produkten

Der CRA teilt Produkte in **verschiedene Kategorien gemäß ihrer Risikoklasse** ein, wobei sich das Konformitätsbewertungsverfahren entsprechend ändert:

- **Standardkategorie**
  - → i. d. R. zutreffend für Maschinen
  - → Selbsterklärung der Konformität nach Modul A (interne Fertigungskontrolle) ausreichend
- **Wichtige Produkte** (Anhang III)
  - Klasse I → erweitertes Bewertungsverfahren (Modul B+C oder H)
  - Klasse II → erweitertes Bewertungsverfahren (Modul B+C oder H) oder Zertifizierung
- **Kritische Produkte** (Anhang IV)
  - → Zertifizierung, oder unter bestimmten Voraussetzungen Modul B+C oder H

Kategorien und Klassen von Produkten

Standard	Wichtig (Kl. I)	Wichtig (Kl. II)	Kritisch
Art. 6, Art. 32 (1)	Art. 7, Art. 32 (2) / Anhang III	Art. 7, Art. 32 (3) / Anhang III	Art. 8, Art. 32 (4) / Anhang IV
• PCs • Unterhaltungselektronik • Software • Spielzeug • **Maschinen** • SPS • …	• Router, Modems, Switches • Betriebssysteme • VPN • Passwortmanager • Browser • PKI • Mikroprozessoren • **Ggf. Sicherheits-steuerungen** • …	• Hypervisor • Firewalls • IDS und IPS • Manipulationssichere Mikroprozessoren • …	• Smart-Meter-Gateways • Security-Chips • Smartcards • …

Meldepflichten – auch für Bestandsprodukte

- Aus Artikel 69 (3) und Artikel 71 (2) ergibt sich, dass die in Artikel 14 geregelten Meldepflichten für Hersteller bereits ab dem **11. September 2026** anzuwenden ist und auch für alle **vor dem 11. Dezember 2027** in den Verkehr gebrachten Produkte gilt.

Ab 11. September 2026 Meldepflicht für Hersteller für
→ Neue Produkte
→ und Bestandsprodukte!

Übersicht der Pflichten und Anforderungen aus CRA

1. **Cybersicherheit mitdenken**
   - Durchführen einer Security-Risikobeurteilung (Artikel 13 (2))
   - „secure by design“: gespeicherte und übertragene Daten werden grundsätzlich verschlüsselt, Angriffsfläche möglichst gering halten, …
   - „secure by default“: Standardeinstellungen haben ein hohes Maß an Sicherheit, automatische Sicherheitsupdates, …
   - Software Bill of Materials (→ „SBOM“)
2. **Anforderungen nachweisen**
   - Konformitätserklärung, je nach Kategorie und Klasse mit Prüfung und Zertifizierung
3. **Schwachstellen offenlegen**
   - Schwachstellenmeldungen über zentrale Meldeplattform (→ „CSAF“)
4. **Sicher im gesamten Supportzeitraum**
   - Pflicht zum Monitoring und zur Behandlung von Schwachstellen und Bereitstellung von Security Updates über den gesamten Lebenszyklus (min. 5 Jahre), Notfallkontakt (→ „security.txt“)

vgl. BSI https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html

Konformitätserklärung – MVO und CRA

Ab 11.12.2027 muss in einer EU-Konformitätserklärung einer Maschine (mit digitalen Elementen) sowohl die

- Maschinenverordnung (EU 2023/1230) als auch der
- Cyber Resilience Act (EU 2024/2847)

referenziert werden.

Außerdem wie gehabt ggf. harmonisierte Normen

Konformitätsbewertungsverfahren bei Maschinen:

- nach **MVO** gemäß Modul A, H, B, C oder G (je nach Maschine)
- nach **CRA** gemäß Modul A (interne Fertigungskontrolle, Selbsterklärung des Herstellers, da Maschinen i. d. R. kein „wichtiges“ oder „kritisches“ Produkt im Sinne des CRA sind)

Harmonisierte Normen

Für die Anforderungen aus der Maschinenverordnung (EU 2023/1230):

- EN 50742 - Safety of machinery - Protection against corruption
- Ende 2026 fertig? → Harmonisierung erwartet

Für die Anforderungen aus dem Cyber Resilience Act (EU 2024/2847):

- EN 40000-X Normenreihe auf Basis der bzw. in Referenz zur IEC 62443 Reihe
- zunächst Fokus auf wichtige und kritische Produkte (Anhang III und IV)
- 2027 fertig? → Harmonisierung erwartet

Normungsvorhaben prEN 50742 „Safety of Machinery - Protection against corruption“

- Schaffung einer Norm zur gezielten Abdeckung der neuen Anforderungen aus MVO Anhang III Abschnitt 1.1.9. und 1.2.1
- Wird bearbeitet in IEC TC 44X / WG 02
- Normungsprojekt 03/2024 gestartet
- Fertigstellung Ende 2026 angestrebt

→ Ziel: harmonisierte Typ B1 Norm

Gedanke der EN 50742

1. Risikobeurteilung hinsichtlich Security, aufbauend auf Risikobeurteilung aus EN ISO 12100 durchführen
   → Durch Korrumpierung entstehen keine originär neuen Gefährdungen an einer Maschine
   → Die Korrumpierung (Manipulation) einer (steuerungs-)technische Schutzmaßnahme kann zur „Wiederbelebung“ einer abgemilderten / behandelten Gefährdung führen
2. Allgemeine Prozessanforderungen
3. **Zwei Wege:**
   a) **Vorgehen nach EN 50742-„homegrown“-Ansatz**
   b) **Vorgehen nach IEC 62443-4-1 (Komponenten) bzw. IEC 62443-3-3 (Maschinen)**
4. Benutzerhinweise

Sichere Fernwartung

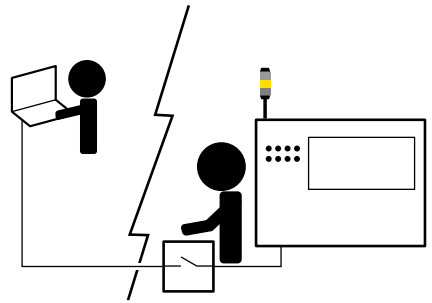
Fachbereich AKTUELL FBHM-133

Warum Fernwartung?

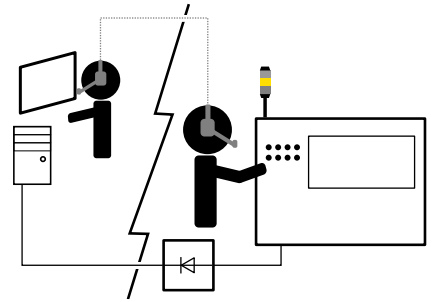
- Minimierung von Ausfallzeiten
- Zeit- und Kostenersparnis durch ersparte Wege

- Änderungen an Konfiguration und Parametrierung
- Diagnose, Fehlerbehebung
- Aktualisierung von Software
- Ergänzen von Softwarefunktionen

- Maschinen sind ohnehin zunehmend vernetzt → geringe Hürde für Zugriff aus der Ferne



Bildquelle: Jonas Stein, Institut für Arbeitsschutz der DGUV (IFA)

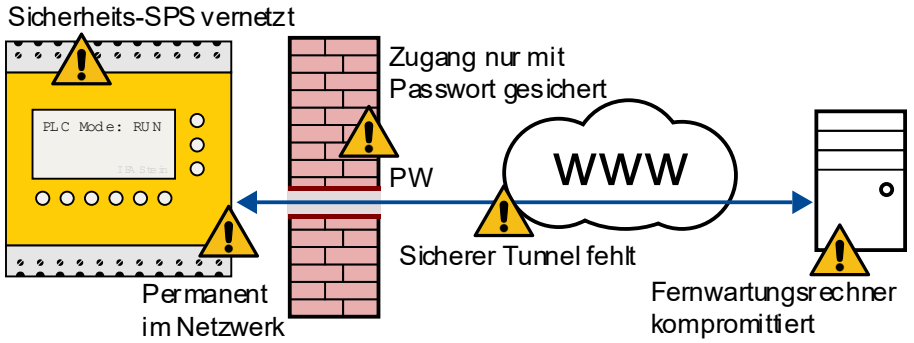


Bildquelle: Jonas Stein, Institut für Arbeitsschutz der DGUV (IFA)

Gefahren? Korrumpierung aufgrund mangelnder Security

- Jede unzureichend abgesicherte Schnittstelle kann ein Einfallstor in das Unternehmensnetzwerk darstellen
- Übertragene Daten können mitgelesen und / oder manipuliert werden

→ wirtschaftliche Konsequenzen



Bildquelle: Jonas Stein, Institut für Arbeitsschutz der DGUV (IFA)

Mögliche Folgen an der Maschine

- Unerwarteter Anlauf
- Betrieb außerhalb sicherer Grenzwerte (Leistung, Geschwindigkeit, Temperatur, …)
- verlangsamte oder deaktivierte Sicherheitsfunktionen
- …

→ Gefährdung der Beschäftigten vor Ort

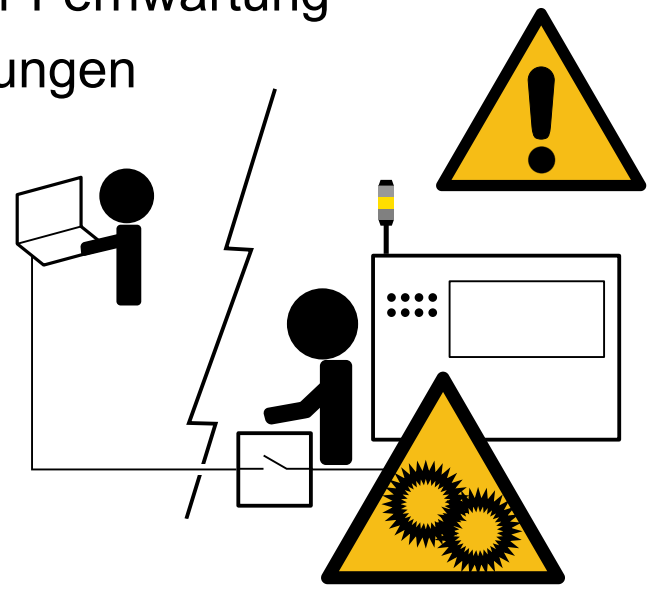
Gefahren? Ähnlich wie bei der klassischen Instandhaltung

- unzureichend Koordination der Arbeiten und fehlende Absprachen
- fehlende Sicherungsmaßnahmen an der Maschine während der Fernwartung
- Ungeprüfte, undokumentierte oder nicht abgesprochene Änderungen
- Änderungen an der falschen Maschine
- fehlende Gefährdungsbeurteilung

Mögliche Folgen an der Maschine

- Unerwarteter Anlauf
- Betrieb außerhalb sicherer Grenzwerte (Leistung, Geschwindigkeit, Temperatur, …)
- verlangsamte oder deaktivierte Sicherheitsfunktionen
- …

→ Gefährdung der Beschäftigten vor Ort



Bildquelle: Jonas Stein, Institut für Arbeitsschutz der DGUV (IFA), bearbeitet

Definition und Abgrenzung Fernwartung

- Zugriff auf lokale Mess-, Steuer- und Regelungstechnik (MSR) einer Maschine oder Anlage über Netzwerkschnittstellen aus der Ferne zu temporären Wartungszwecken

- „Electropedia“ der IEC: „Wartung mit ferngesteuerten Geräten; Über ein Kommunikationsnetz durchgeführte **Softwarewartung**“ (übersetzt aus dem engl. Original)

Fernwartung ist:

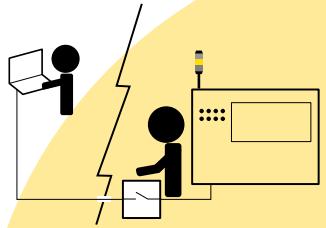
- keine vorausschauende Wartung (Predictive Maintenance)
- keine permanente Fernsteuerung

Synonyme: „Remote Service“, „Remote Access“, „Teleservice“, „ferngesteuerte Instandhaltung“, „Remote-Instandhaltung“ oder „Remote Maintenance“, teilweise auch „Fernzugriff” und „Ferndiagnose”

Neue Maschinenverordnung EU 2023/1230

- Anhang III, Abschnitt 1.1.9. Schutz gegen Korrumpierung:
  „Die Maschine bzw. das dazugehörige Produkt muss so konstruiert und gebaut sein, dass […] eine mit der Maschine bzw. dem dazugehörigen Produkt kommunizierende entfernte ***Fernzugriffseinrichtung*** *nicht zu einer gefährlichen Situation führt.“*

Formen der Fernwartung

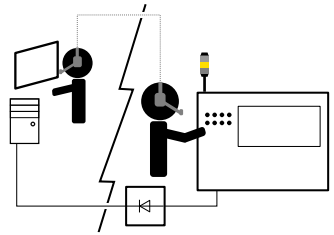


Aktive Fernwartung

- aktiver Zugriff auf Konfiguration von Steuerungskomponenten aus der Ferne
- lesender und schreibender Zugriff
- Person vor Ort überwacht nur

Hybride Fernwartung

Passive Fernwartung



- Person vor Ort bekommt Anweisungen aus der Ferne (z. B. Telefon) und setzt diese aktiv um
- Person in der Ferne hat nur lesenden Zugriff (z.B. Bildschirmübertragung, Datenbrille)

Grundsätzlich: Auswahl geeigneter Personen gemäß „Zusammenarbeit mehrerer Unternehmer“ (§ 6 DGUV Vorschrift 1) beachten

Bildquelle: Jonas Stein, Institut für Arbeitsschutz der DGUV (IFA)

Technische Maßnahmen

- Sichere Segmentierung von Netzwerken.
- Auswahl einer geeigneten Soft- und Hardware-Architektur für den Fernwartungszugang.
- Einsatz einer kryptografisch abgesicherten Verbindung auf dem Stand der Technik (VPN).
- Einsatz anerkannter Verfahren zur Authentifizierung und Autorisierung auf dem Stand der Technik, möglichst mit zweitem Faktor.
- Vorgehen nach dem Minimale-Rechte-Prinzip.
- Die Fernwartung darf nur von Betreibenden aus initiiert werden können, im Idealfall direkt an der konkreten Maschine oder zumindest von einem Rechner in örtlicher Nähe zur Maschine und muss an der Maschine durch eine aktive Handlung bestätigt („von innen nach außen“) werden.

Technische Maßnahmen

- Zeitliche Limitierung der Fernwartungszugänge; sie dürfen nicht permanent bestehen bleiben und sind durch ein initial-definiertes Timeout zeitlich begrenzt.
- Zugangsberechtigungen müssen dokumentiert werden, sodass die Betreibenden einen Überblick über alle bestehenden Zugänge haben.
- Fernwartungssitzungen müssen dokumentiert werden (Zeitstempel An- und Abmeldung, Benutzende, Maschine, …).
- Durchgeführte Änderungen müssen nachvollziehbar sein (z. B. automatisierte Aufzeichnung).
- An der Maschine muss zwangläufig signalisiert werden, wenn eine Fernwartung aktiv ist.
- Die betreffende Maschine muss eindeutig zur Fernwartung ausgewählt werden.

Technische Maßnahmen

- Not-Halt und Sicherheitsfunktionen haben stets Vorrang vor Fernwartungs-Befehlen bzw. dürfen durch die Fernwartung nicht beeinflusst werden.
- Das Aussetzen oder Rücksetzen von Sicherheitsfunktionen und Schutzeinrichtungen darf nicht aus der Ferne möglich sein.
- Steuerbefehle, die mittel- oder unmittelbar zu einer unerwarteten Gefährdung vor Ort führen können, sollten technisch unterbunden werden (z. B. „ANTRIEB EIN“).
- Sind Steuerbefehle oder Betriebsartenwahl aus der Ferne möglich, sind vor Ort geeignete Maßnahmen zu treffen, um den daraus entstehenden Gefährdungen zu begegnen.

Organisatorische Maßnahmen

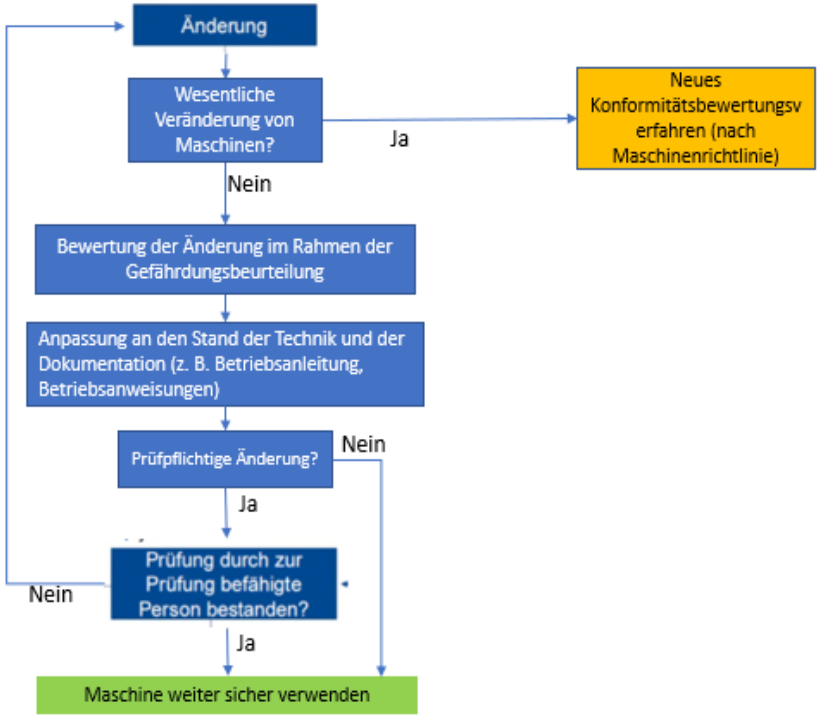
- Die Fernwartung ist im Rahmen der Gefährdungsbeurteilung zu berücksichtigen.
- Eine Fernwartung findet nicht im regulären, produktiven Betrieb statt. Die Maschine muss zuvor in einen zur Fernwartung geeigneten, jedoch sicheren Zustand (Schutzeinrichtungen aktiv, Zugangsschutz, …) versetzt werden.
- Die Maschine muss entsprechend gekennzeichnet sein, damit es auch für Dritte leicht zu erkennen ist, dass sie sich „in Fernwartung“ befindet. Ein Betreten der Gefahrenbereiche ist durch eine entsprechende Absicherung zu verhindern.
- Es muss während des Fernwartungsvorgangs permanent fachkundiges Personal vor Ort sein, das im Notfall eingreifen kann.
- Bei Beendigung der Fernwartung und Trennung der Verbindung erscheint eine entsprechende Meldung an der Maschine, die quittiert werden muss.

Organisatorische Maßnahmen

- Die Auswahl geeigneter Personen für die Durchführung von Instandhaltungstätigkeiten gemäß „Zusammenarbeit mehrerer Unternehmer“ (§ 6 DGUV Vorschrift 1) muss beachtet und die Verantwortung der beteiligten Stellen geklärt werden.
- Es muss eine Betriebsanweisung für die Fernwartung (basierend auf der Betriebsanleitung der Herstellfirma) erstellt werden. Anhand dieser müssen Beschäftigte in die für sie geltenden Schutzmaßnahmen und das richtige Verhalten im Notfall unterwiesen werden.

Wesentliche Veränderung durch Fernwartung?

- Änderung an Software kann zu einer wesentlichen Veränderung der Maschine führen:
- → Bewertungsverfahren gemäß Interpretationspapier des BMAS bzw. **Maschinenverordnung EU 2023/1230** durchführen.
- Speziell zu Software den „Blue Guide“ („Leitfaden für die Umsetzung der Produktvorschriften der EU 2022“) der Europäischen Kommission beachten.
- ISO 13849-1:2023-04: Änderungen an „safety-related Software“ dürfen per Fernwartung nicht möglich sein, wenn eine Validierung vor Ort nicht sichergestellt werden kann.



Grafik: Sebastian Gatzmanga, BG RCI

Fachbereich AKTUELL FBHM-133 „Sichere Fernwartung“

- Informationen zu sicherer Fernwartung (T-O Prinzip) kompakt zusammengefasst auf 10 Seiten
- Verfügbar seit 08/2023
- https://publikationen.dguv.de/DguvWebcode?query=p022417

Fachbereich AKTUELL FBHM-102 „Safety und Security in der vernetzten Produktion“

- Informationen zur Analyse und Beurteilung vernetzter Produktionsanlagen hinsichtlich Security inkl. Checkliste auf 18 Seiten
- Verfügbar seit 01/2025
- https://publikationen.dguv.de/DguvWebcode?query=p012761

Zusammenfassung

Gesetzliche Anforderungen, Normen und Regelwerk

Gesetzliche Anforderungen für Maschinen

An Hersteller gerichtet:

- **MRL 2006/42/EG** bis 19.01.2027 und **MVO (EU) 2023/1230** ab 20.01.2027

Wenn „digitale Elemente“ / „vernetzt“:

- **CRA (Cyber Resilience Act)** – Verordnung **(EU) 2024/2847** des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen ab 11.12.2027 (aber Meldepflichten ab 11.09.2026!)

Außerdem (wie bisher):

- Niederspannungsrichtlinie (2014/35/EU)
- EMV-Richtlinie 2014/30/EU
- …

Gesetzliche Anforderungen für Maschinen

An Betreiber gerichtet:

- **BetrSichV**
  - **TRBS 1115** Sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen
  - **TRBS 1115-1** Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen

- **NIS2-Richtlinie (EU) 2022/2555** des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (→ Betroffenheitsprüfung)
  - Wesentliche Einrichtungen und Wichtige Einrichtungen (Kritis)
  - Meldepflichten
  - Risikomanagement- und Kontrollmaßnahmen

Nützliche Links

- Fachveranstaltung "Maschinensicherheit Steuerungen„
- → nächste Fachveranstaltung zu „Safety und Security“ am 21.09.2027 in Nümbrecht (Teilnahme für BGHM-Mitgliedsbetriebe kostenfrei, Anmeldung ab ca. Mai 2027 über „meineBGHM“)

- Home – Herstellerseminar Industrial Security: Praxisnahe Umsetzung europäischer Security Anforderungen mit Vorträgen Praxisübungen und Demonstrationen

- BGHM: FAQs Maschinenverordnung

- BGHM: FAQs Cyber-Resilience-Act

Vielen Dank für Ihre Aufmerksamkeit!

Martin Eberle – FR Safety und Security
Berufsgenossenschaft Holz und Metall

martin.eberle@bghm.de

Foto: Martin Eberle