DGUV
Fachbereich Holz und Metall
Berufsgenossenschaft
Holz und Metall

# Fachbereich AKTUELL

FBHM-102

## Safety und Security in der vernetzten Produktion

Sachgebiet Maschinen, Robotik und Fertigungsautomation

Entwurf Überarbeitung Stand: 19.09.2024

**Die Sicherheit von Produktionssystemen ist eine zentrale Voraussetzung für den Erfolg der mittlerweile etablierten vernetzten Produktion. Es betrifft zum einen das Gebiet der Arbeitssicherheit beziehungsweise der technischen Sicherheit (Safety), zum anderen aber auch das Gebiet der IT- oder Cyber-Sicherheit (Security). In dieser Schrift wird beschrieben, wie die beiden Arbeitsgebiete zusammenhängen und weshalb in vernetzten Produktionssystemen beide berücksichtigt werden müssen. Zu den weiteren Themen gehören Methoden zur Analyse bestehender Produktionssysteme und Schutzmaßnahmen.**

## Inhaltsverzeichnis




Abbildung 1 – Der Begriff Sicherheit

Im Gegensatz zum englischen wird im deutschen Sprachgebrauch der Begriff „Sicherheit“ für zwei verschiedene technische Arbeitsgebiete verwendet. Eine klare Unterscheidung der beiden Begriffe „Safety“ und „Security“, wie im Englischen, sieht der deutsche Wortschatz nicht vor. In der Vergangenheit wurden diese beiden Bereiche getrennt bearbeitet, eine gemeinsame, interdisziplinäre oder abgestimmte Vorgehensweise existierte nicht. Diese Fachbereich AKTUELL stellt die beiden Begriffe „Safety“ und „Security“ einander gegenüber, erläutert sie und beschreibt Auswirkungen von IT-Sicherheitsbedrohungen für Maschinen und Anlagen sowie daraus folgende Gefährdungen mit hohem Verletzungsrisiko für Beschäftigte. Es werden grundlegende Vorgehensweisen und Maßnahmen formuliert, um das Bewusstsein für die rechtzeitige Berücksichtigung von negativen

Auswirkungen in Bezug auf die Arbeitssicherheit in Produktionsanlagen hervorzuheben.

Eine umfassende Beschreibung von Schutzmechanismen gegen ungewollte oder unerlaubte Zugriffe auf technische Anlagen ist für jede Anlage oder Maschine spezifisch und daher nicht Gegenstand dieser Schrift.

# 1 Einführung und Zielgruppe

In den letzten Jahrzehnten stieg der Automatisierungsgrad von Maschinen und Anlagen immer schneller und umfassender. Speziell die Anwendung von programmierbaren elektronischen Steuerungen und Rechnersystemen mit immer höherer Verarbeitungsgeschwindigkeit, Komplexität und erweiterten Schnittstellen zur Sensorik und Aktorik nimmt zu. Das ermöglicht permanent neue Einsatzgebiete, zusätzlich getrieben durch die stetige Miniaturisierung und fallende Hardwarekosten.

Unter dem Aspekt der Sicherheit war das in der Vergangenheit wenig problematisch, da zwar der Automatisierungsgrad von Maschinen und Anlagen zunahm, diese jedoch überwiegend im

„Stand-alone-Betrieb“ eingesetzt wurden. Eine übergeordnete Verknüpfung mit Anlagen und Maschinen in anderen Fertigungsstraßen oder -stätten fand in der Regel nicht statt. Somit konzentrierte sich die Betrachtung sicherheitstechnischer Aspekte bisher nur auf den störungsfreien und anwendungssicheren Betrieb von Maschinen und Anlagen. Diese betrachten Gefahren durch Ausfälle, die ohne Fremdeinwirkung auftreten. Hierzu zählen insbesondere Hardware- oder Softwarefehler sowie Bedienungsfehler. Die Anforderungen wurden in der Europäischen Maschinenrichtlinie 2006/42/EG sowie im einschlägigen technischen Regelwerk unter der Überschrift „Funktionale Sicherheit“ spezifiziert und werden allgemein dem Begriff „Safety“ zugeordnet.

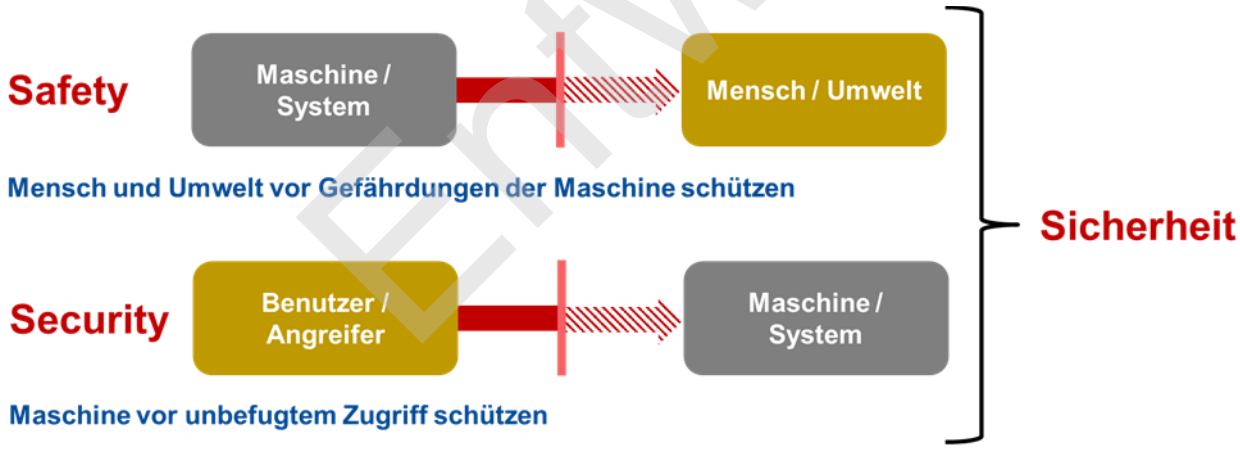


Abbildung 2 – Definition "Safety and Security"

Die funktionale Sicherheit (Safety) einer Maschine, die meist durch eine sicherheitsgerichtete Steuerung umgesetzt wird, verfolgt das Ziel, Mensch und Umwelt vor den von der Maschine ausgehenden Gefährdungen zu schützen. Die IT-Sicherheit (Security) verfolgt das Ziel, ein technisches System oder eine Maschine vor einem unbefugten Zugriff und damit zum Beispiel vor Manipulation zu schützen. Ist die Security unzureichend, kann dies dazu führen, dass auch die Safety nicht mehr sichergestellt ist und somit eine Gefahr für Mensch und Umwelt besteht. Das Zusammenwirken von Safety und Security ist somit essenziell für den sicheren Betrieb.

Unter Berücksichtigung technischer Weiterentwicklungen werden die Verbindungen von einzelnen Maschinen und kompletten Fertigungsstraßen nicht mehr nur auf die Vernetzung innerhalb einer Produktionsstätte, sondern auch regional und global übergreifend auf Produktionsstätten an weit auseinanderliegenden Fertigungsstandorten erfolgen.

Das bedeutet jedoch auch, dass man nicht mehr von sogenannten gekapselten Produktionssystemen sprechen kann. Vielmehr ist zu berücksichtigen, dass der Datenaustausch von Maschineninformationen über Datenwege erfolgt, die auch einen **ungewollten** Zugriff auf Sicherheitsparameter und andere produktions-, aber auch sicherheitsrelevante Daten ermöglichen. Ein Schutz der über Datennetzwerke ausgetauschten Daten ist demnach unabdingbar. Der Schutz gegen vorsätzliche Angriffe durch nicht autorisierte Personen wird als Informationssicherheit bezeichnet. Informationssicherheit hat die Schutzziele, die Vertraulichkeit, Verfügbarkeit und Integrität (also Unveränderlichkeit und Vollständigkeit) von Informationen sicherzustellen und wird allgemein auch als Security, IT-Security oder Cyber-Security/ Cybersicherheit bezeichnet.

Derzeit sind Security-Aspekte in der bis Januar 2027 noch anzuwendenden Europäischen Maschinenrichtlinie 2006/42/EG noch nicht explizit erfasst. Die neue, ab dem 20. Januar 2027 vollständig anzuwendende EU-Maschinenverordnung 2023/1230 (MVO) stellt dann erstmals ausdrücklich Anforderungen in Bezug auf die Security an alle, die Maschinen herstellen beziehungsweise in Verkehr bringen. An Betreiber (Arbeitgeber) richtet sich die 2023 neu erschienene Technische Regel für Betriebssicherheit (TRBS) 1115 Teil 1 „Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen“.

Für Hersteller und Inverkehrbringer von Maschinen wird künftig die EN 50742 „Protection against corruption“ konkrete Anforderungen enthalten, die sich aus der EU-Maschinenverordnung 2023/1230, Anhang III, Abschnitt 1.1.9 und 1.2.1 ableiten. An diese durch die Hersteller ergriffenen Maßnahmen anknüpfend, sollten Betreiber nahtlos mit eigenen Maßnahmen zur Erfüllung der Anforderungen aus der TRBS 1115-1 anschließen. Die Einhaltung der Anforderungen aus der EU-Maschinenverordnung 2023/1230 hinsichtlich Security kann bereits jetzt von Herstellern vertraglich gefordert werden, da diese nicht im Widerspruch zur derzeit noch (bis 19.01.2027) anzuwendenden Maschinenrichtlinie 2006/42/EG stehen. Ab dem 20.01.2027 sind diese zwingend zu erfüllen.

Für Betreiber von Kritischen Infrastrukturen (KRITIS) existieren mit dem europäischen Rechtsakt zur Cybersicherheit 2019/881 („Cybersecurity Act“, CSA) und der EU-Richtlinie zur Netzwerk- und Informationssicherheit 2016/1148 (NIS-2-Richtlinie) weitere Anforderungen hinsichtlich Security. Für Hersteller von Produkten mit digitalen Elementen wird der in Arbeit befindliche, kommende europäische Rechtsakt zur Cyberresilienz („Cyber Resilience Act“, CRA) weitere Anforderungen enthalten.

Früher bestand im Bereich der Maschinensicherheit nur ein geringer Bedarf, Security-Aspekte zu berücksichtigen. Die Angriffsszenarien aus dem Bereich der IT-Security zeigten in den letzten Jahren, dass diese Thematik auch für die Maschinensicherheit relevant ist und beachtet werden muss. Die Bedrohungslage hat sich deutlich verschärft. Es gibt mittlerweile neben unzähligen Angriffen auf Büro-Netzwerke (z. B. Verschlüsselungstrojaner, Diebstahl geistigen Eigentums) auch viele Beispiele von erfolgreichen Angriffen auf industrielle Steuerungen.

Öffentlich bekannt sind beispielsweise ein Angriff auf den Hochofen eines Stahlwerkes in

Deutschland, ein Angriff auf die Wasserversorgung einer Region in den USA und der TRISIS-Angriff. Solche Angriffe können direkte Auswirkungen auf die Sicherheit und Gesundheit von Menschen haben.

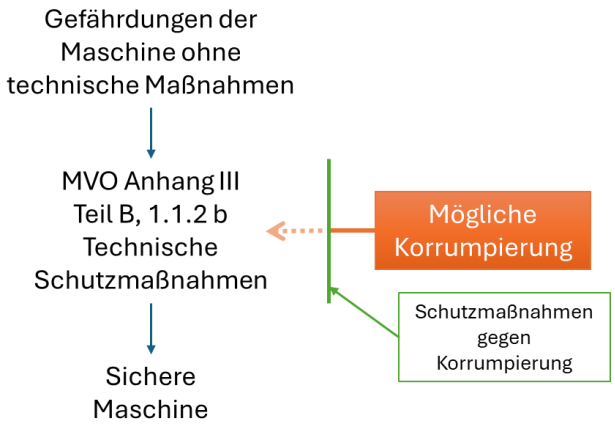


Abbildung 3 – Auswirkungen der Security auf die Maschinensicherheit

Diese Schrift soll den Zusammenhang von Safety und Security aufzeigen und die Notwendigkeit von umfassender Security in der vernetzten Produktion für die Arbeitssicherheit verdeutlichen. Es werden Anforderungen an Betreiber aus der BetrSichV beziehungsweise TRBS und an Hersteller aus der Maschinenverordnung dargestellt und Verweise auf Normen zur Erfüllung der Anforderungen durch entsprechende Maßnahmen gegeben. In den Anlagen 1 und 2 finden Betreiber Hilfsmittel zur Bewertung ihrer industriellen Steuerungssysteme in Maschinen.

## 2 Mögliche Gefahren und deren Folgen

Manipulationen von industriellen Steuerungssystemen stehen inzwischen im Fokus von Angreifern und Angreiferinnen. Ziel der Angreifenden ist es in solchen Fällen die Kontrolle über komplexe Industrieanlagen zu erhalten. Angriffe und Manipulationen können einerseits zu einem kompletten Produktionsausfall oder zu Diebstählen von Produktions-, Prozessdaten sowie von Know-how führen. Andererseits können sie auch massive Auswirkungen auf die Maschinensicherheit und damit auf die Arbeitssicherheit haben. Veränderungen in Maschinenparametern können beispielsweise Sicherheitseinrichtungen des Personenschutzes betreffen. Sicherheitsfunktionen könnten dahingehend manipuliert werden, dass diese passiviert werden, dass Geschwindigkeiten verändert werden oder dass ein ungewollter Maschinenanlauf erfolgt. Hierbei kann es zu großen Gefährdungen mit schweren bis hin zu tödlichen Verletzungen von Beschäftigten kommen. Dies gilt es durch den Arbeitsschutz dauerhaft zu verhindern.

Der Schutz von Bürocomputernetzen ist aufgrund verschiedener Faktoren und der restriktiven Anwendung bewährter und vor allem verfügbarer Werkzeuge, wie z. B. Antivirenprogrammen, Firewalls, Updates, Patches und Backuplösungen, mittlerweile sehr gut beherrschbar. Die Systeme in Produktionsnetzwerken sind dahingehend meist noch nicht auf dem gleichen Sicherheitsstandard, obwohl die Erfahrungen aus der Absicherung von Bürocomputernetzen bestehen.

Gründe für dieses Ungleichgewicht sind vielfältig. Die Verfügbarkeit von Maschinen wird in der Regel höher priorisiert als die Absicherung, wie durch notwendige Updates und Patches der Maschinensteuerungen. Aufgrund der Heterogenität von Maschinen, Steuerungen und Betriebssystemen und damit auch der Einbindung oft zahlreicher verschiedener Maschinenhersteller ist die Situation komplexer als in gewöhnlichen Bürocomputernetzen. Es ist einerseits riskanter, Updates einzuspielen, da es zu einem unerwarteten Anlagenstillstand führen könnte, andererseits ist die Angriffsoberfläche durch die Heterogenität größer. Außerdem sind

die Produktionsnetzwerke im Allgemeinen nicht sinnvoll ausreichend fein segmentiert. Der Einsatz von Gateways mit Firewalls ist zudem in Produktionsnetzen oft noch nicht ausreichend umgesetzt.

Diese bewährten Geräte prüfen den Datenverkehr zwischen unterschiedlichen Netzwerken und blockieren Datenpakete nach zuvor definierten Regeln.

| Mögliche Auswirkungen von Angriffen | |
|---|---|
| **Wirtschaftliche Auswirkungen** | **Auswirkungen auf die Arbeitssicherheit** |
| Produktionsausfall | Veränderung von sicherheitsrelevanten Parametern |
| Diebstahl von Produktionsdaten | Passivierung von Sicherheitseinrichtungen |
| Verlust von „Know-how“ | Verzögerung von Sicherheitsfunktionen |
| Veränderung von Produktionsdaten → Qualitätsmängel | |
| Verlust der Verfügbarkeit durch Fremd-Aktivierung von Safety-Prozeduren | |
| Zerstörung von Maschinen | |

Abbildung 4 - Mögliche Folgen von Angriffen

Achten Sie besonders darauf, dass Gefahren in Bezug auf Manipulation und Datendiebstahl in vernetzten Industrieanlagen nicht nur durch Angriffe Dritter über das Internet bestehen. Auch direkte Tätigkeiten an der Maschine selbst, durch externes Instandhaltungs- oder Wartungspersonal, beinhalten Gefahren. Schon durch den Einsatz von zum Beispiel USB-Sticks oder Notebooks, die unmittelbar mit der Steuerung einer Maschine verbunden werden, könnten Schadsoftware übertragen oder auch Daten, wie Prozessparameter, kopiert oder verändert werden.

# 3 Analyse von bestehenden Maschinen oder Anlagen

Die bislang fehlende gemeinsame Betrachtung von Safety- und Security-Anforderungen in der Industrieumgebung sind vor dem Hintergrund der fortschreitenden Vernetzung von Maschinen und Anlagen nicht weiter akzeptabel. Die etablierten und bewährten Maßnahmen, Strategien und Vorkehrungen der IT-Sicherheit müssen auch in die Welt der industriellen Steuerungssysteme transportiert werden. Die maßgebliche Frage ist somit: Wie können Produktionssysteme gegen ungewollte Angriffe von außen und innen geschützt werden?

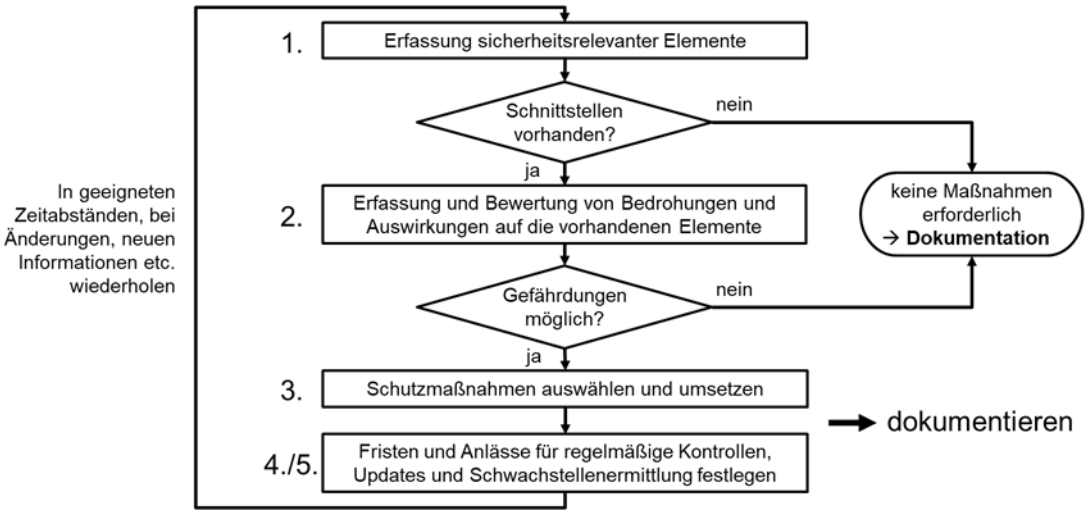


Abbildung 5 Vorgehen nach TRBS 1115-1 Abschnitt 4.4.3

Der Betreiber ist dafür verantwortlich, in einem ersten Schritt zunächst eine Analyse durchzuführen, aus der hervorgeht, welche Maschinen und Anlagen überhaupt betroffen sein können. Diese Betreiber-Pflicht wird in der BetrSichV und der TRBS 1115-1 Abschnitt 4.4.3 konkretisiert. Die Erfassung und grobe Bewertung der vorhandenen Maschinen und Anlagen können im Sinn einer „Inventarliste“ vorgenommen werden.

Dabei können grundsätzlich folgende Unterscheidungen und ersten groben Bewertungen vorgenommen werden (Risikoanalyse der Angreifbarkeit):

## 3.1 Maschinen mit kontaktbehafteten Steuerungen

Maschinen, in denen die Steuerungen über kontaktbehaftete Bauteile realisiert wurden, sind unkritisch in Bezug auf Angriffe von außen und auch von innen, da sie nicht über programmierbare Bauteile verfügen. Ein externer Zugriff ist nicht möglich.
*Security-Maßnahmen erübrigen sich.*

## 3.2 Maschinen mit elektronischen Steuerungen

Maschinen, in denen die Steuerungen über elektronische, aber nicht über programmierbare Bauteile realisiert wurden, sind unkritisch in Bezug auf Angriffe von außen und auch von innen. Der Steuerungsablauf kann nur durch Veränderung der Elektronik bewusst geändert werden. Ein externer Zugriff ist nicht möglich.
*Security-Maßnahmen erübrigen sich.*

## 3.3 Maschinen mit programmierbaren Steuerungen

Maschinen, in denen die Steuerungen über programmierbare Komponenten (in der Regel SPS- oder Mikroprozessor-Systeme) realisiert wurden, sind in Bezug auf die Ausführung weiter zu differenzieren.
Programmierbare Steuerungen haben grundsätzlich Schnittstellen, über welche die Programmierung erfolgt. Weiterhin können diverse Kommunikationsschnittstellen vorhanden sein.

### 3.3.1 Maschinensteuerungen ohne Netzwerkverbindungen

Programmierbare Steuerungen ohne eine Netzwerkverbindung zu einer anderen Steuerung oder zu einem übergeordneten Rechnersystem verfügen zumindest über eine Schnittstelle, über die ein Programm geladen oder gelesen werden kann. Durch den nachträglichen Anschluss eines Programmiersystems (z. B. Notebook, USB-Stick) besteht jederzeit die Möglichkeit, gewollt oder auch ungewollt eine Programmänderung durchzuführen. Diese Programmänderungen können auch durch das „Einschleusen“ schadhafter Software ausgelöst werden. Ein weiterer kritischer Aspekt ist das SPS- oder Mikroprozessorsystem selbst. In diesem kann bereits seit Auslieferung ein sogenannter „Schläfer“ vorhanden sein, der zeit- oder ereignisbezogen aktiviert werden und die Maschinensteuerung beeinflussen kann. Auch bei älteren Maschinen ist somit eine Analyse notwendig, mögliche Vorsichtsmaßnahmen sind zu treffen.

### 3.3.2 Maschinensteuerungen mit Netzwerkverbindungen, aber ohne Verbindungen zu übergeordneten Systemen

Programmierbare Steuerungen mit Netzwerkverbindungen zu anderen Maschinensteuerungen, aber **ohne** Verbindung zu einem übergeordneten Rechnersystem verfügen über Schnittstellen, über die Programme geladen oder gelesen werden können. Zusätzlich erfolgt die Verbindung zu anderen Steuerungssystemen über weitere Schnittstellen (z. B. Verbindung mehrerer SPS-Systeme, dezentrale I/O) für einen gewollten Datenaustausch. Durch den Anschluss eines Programmiersystems (z. B. Notebook, USB-Stick) besteht jederzeit die Möglichkeit gewollt oder auch ungewollt eine Programm- und/oder Parameteränderung im gesamten vernetzten System durchzuführen. Diese Änderungen können durch das „Einschleusen“ von schadhafter Software ausgelöst werden, die nicht nur eine einzige Steuerung, sondern das gesamte Netzwerk einschließlich des übergeordneten Systems manipulieren kann. Ein weiterer kritischer Aspekt sind die SPS- oder Mikroprozessorsysteme selbst. In ihnen kann bereits seit Auslieferung ein sogenannter „Schläfer“ vorhanden sein, der zeit- oder ereignisbezogen aktiviert werden und die Maschinensteuerungen beeinflussen kann. Bei diesen Steuerungsarchitekturen ist besonders zu beachten, dass die angeschlossenen Systeme nicht von einem Hersteller stammen müssen, sondern auch von verschiedenen Herstellern sein können. Auch bei älteren Maschinen und Anlagen ist somit eine Analyse notwendig, mögliche Vorsichtsmaßnahmen sind zu treffen.

### 3.3.3 Maschinensteuerungen mit Netzwerkverbindungen und Verbindungen zu übergeordneten Systemen

Programmierbare Steuerungen mit Netzwerkverbindungen zu anderen Maschinensteuerungen **und einer** Verbindung zu einem übergeordneten Rechnersystem verfügen über Schnittstellen, über die Programme und Daten geladen oder gelesen werden können. Zusätzlich erfolgt die Verbindung zu anderen Steuerungssystemen über weitere Schnittstellen (z. B. Verbindung mehrerer SPS-Systeme, dezentrale I/O) und zu den übergeordneten Rechnersystemen, die eine direkte Verbindung zum Internet haben können. Durch den Anschluss eines Programmiersystems (z. B. Notebook, USB-Stick) besteht jederzeit die Möglichkeit, gewollt oder auch ungewollt eine Programm- und/oder Parameteränderung im gesamten vernetzten System durchzuführen. Das kann entweder über den Anschluss an eine Schnittstelle des Steuerungssystemes oder über einen übergeordneten Rechner erfolgen. Auch eine

Kommunikation über das Internet ist demnach möglich.

Programm- oder Parameteränderungen können durch das „Einschleusen“ von schadhafter Software ausgelöst werden, die nicht nur eine einzige Steuerung, sondern das gesamte Netzwerk einschließlich des übergeordneten Systems manipulieren kann.

Außer in den SPS- oder Mikroprozessor-systemen können Gefahren somit auch in dem übergeordneten Rechnersystem selbst auftreten. Maschinensteuerungen und/oder Rechnersysteme können demnach sowohl über die „SPS-typischen Programme“ als auch über die in der Office-Welt verwendeten Programme manipuliert werden. Bei diesen Architekturen ist besonders zu beachten, dass die angeschlossenen Systeme nicht von einem Hersteller stammen müssen, sondern durchaus auch von verschiedenen Herstellern sein können. Entsprechend vielfältig können auch die verwendeten Betriebssysteme sein. In diesen Fällen darf sich die Analyse nicht nur auf die „Steuerungswelt“ beziehen, sondern sollte auch die gesamte Office-Umgebung einbeziehen. Dies gestaltet sich aufgrund der unterschiedlichen Betrachtungs- und Sprachweisen der Safety-Welt und der Security-Welt als äußerst schwierig und komplex.

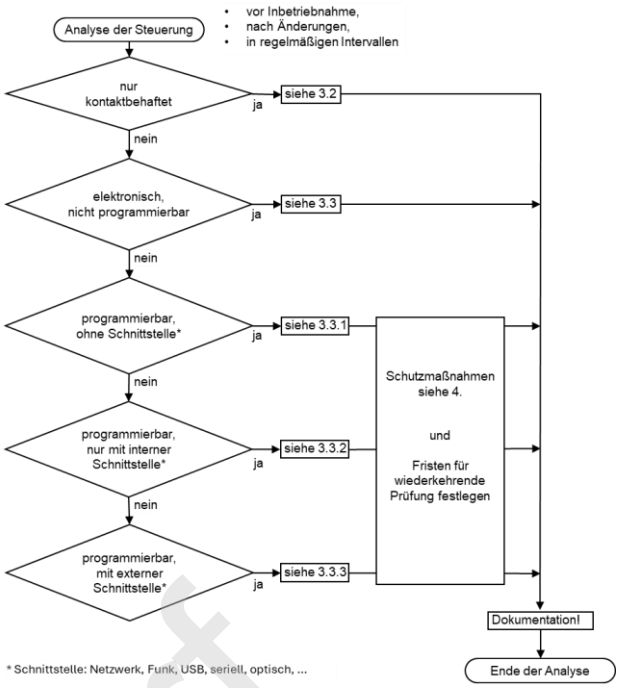


Abbildung 5 – Entscheidungsbaum zu oben genannten Kriterien und nachfolgenden Maßnahmen

# 4 Ansatzpunkte möglicher Schutzmaßnahmen

Die wichtigste Maßnahme ist, dass innerhalb eines Unternehmens das Bewusstsein für die Gefahr von Manipulationen und Industriespionage in Produktionsanlagen wächst und ein gemeinsames „Security-Safety-Management“ für Office- und Automatisierungsanwendungen umgesetzt wird. Hierbei sind intern klare **Verantwortlichkeiten** festzulegen. Die erforderliche **Fachkunde** kann sowohl intern bereitgestellt oder, wenn erforderlich, durch externe Dienstleistungen ergänzt werden. Es empfiehlt sich, das Thema „Security for Safety“ ganzheitlich im Rahmen des Informationssicherheitsmanagements des Unternehmens zu betrachten.

Um in Industrieanlagen einen möglichst hohen Schutz gegen IT-Angriffe zu erreichen, ist eine systematische Vorgehensweise erforderlich. Eine Hilfestellung bietet die Normenreihe IEC 62443 „IT-Sicherheit für industrielle Automatisierungssysteme“, die sich sowohl an Betreiber als auch Hersteller und Dienstleister richtet. Das in Abschnitt 1 dargestellte Zusammenwirken von Hersteller- und Betreibermaßnahmen ist zu beachten.

Die nachfolgenden Punkte zeigen eine beispielhafte Vorgehensweise.

## 4.1 Risikoanalyse zur Schutzbedürftigkeit

Zuerst sollte eine Risikoanalyse durchgeführt werden, um schutzbedürftige Informationen und Komponenten zu identifizieren und aufzulisten. Für die Auflistung sollte die Wichtigkeit bewertet werden und eine Kennzeichnung erfolgen, ob zum Beispiel Daten garantiert verfügbar sein müssen, jederzeit eine Rückverfolgbarkeit möglich sein muss oder sie nicht verändert werden dürfen, wie Maschinenparameter. Dabei sollte bewertet werden, was passieren kann, wenn Daten, Maschinenparameter oder Programme aufgrund des Zugriffs einer externen Bedrohung ausfallen oder verloren gehen. Sicherheitsrelevante Informationen (Software und Parameter) und Komponenten sind immer schutzbedürftig.

## 4.2 Zoneneinteilung

Als Ergebnis der Risikoanalyse kann im zweiten Schritt eine organisatorische und technische Zonenaufteilung vorgenommen werden. Dabei sollten nur Maschinen und Komponenten in Zonen zusammengefasst werden, die miteinander kommunizieren müssen. Diese Aufteilung hat viele Vorteile, wenn mit technischen Maßnahmen eine Netzsegmentierung, zum Beispiel durch Firewalls, abgeleitet wird. Fällt eine Zone beispielsweise durch einen Hackerangriff, einen Virus oder interne Manipulation aus, sind andere Zonen nicht betroffen und arbeiten unbeeinflusst weiter. Diese Netzsegmentierung sollte regelmäßig auf Aktualität und Effektivität überprüft werden. Die Zoneneinteilung sollte auch hinsichtlich organisatorischer Vorgaben, Rahmenbedingen und Verantwortlichkeitsbereichen betrachtet werden. Die Zoneneinteilung sollte technisch und organisatorisch aufeinander abgestimmt sein, um Widersprüche und Lücken in der Verantwortlichkeit zu vermeiden.

## 4.3 Minimale-Rechte-Prinzip

Zusätzlich sollte nach dem Minimale-Rechte-Prinzip („principle of least privilege“) vorgegangen werden. Das bedeutet: Nur die zur Erfüllung der konkreten Aufgabe benötigten Berechtigungen dürfen an die jeweiligen Benutzergruppen (Personal zur Maschinenbedienung, Einrichtung, Instandhaltung,

Programmierung, …) oder Systeme (Maschinenkomponenten, andere Maschinen, übergeordnete Produktionssteuerung, …) vergeben werden. Das setzt allerdings voraus, dass ein Rechte- und Rollensystem vorhanden ist, das detailliert konfiguriert werden kann.

## 4.4 Authentisierung und Autorisierung

Prinzipiell gibt es in gut strukturierten und gesicherten Netzwerken individuelle Konten für Benutzerinnen und Benutzer. Hierbei ist jeder Zugriff authentisiert und auch autorisiert. Durch individuelle Nutzerkennungen (Authentisierung) und Passwörter (Autorisierung) für alle am Netz Beteiligten können Rechte im Netz vergeben werden. Diese müssen im Vorfeld definiert werden und können auch in Gruppen zusammengefasst werden. Maschinen könnten so beispielsweise nur eine Leseberechtigung auf einen Netzwerkspeicher bekommen, wenn sie von dort ein Maschinenprogramm laden müssen. Programmierer und Programmiererinnen von NC-Steuerungen hingegen erhalten zusätzlich einen Schreibzugriff auf definierte Netzwerk-komponenten wie Maschinen und Anlagen. Generell sollte festgelegt werden, dass Passwörter personenbezogen, ausreichend komplex und auch nur autorisierten Personen zugänglich sind.  Ist herstellerseitig bereits ein Passwort vorhanden, sollte dieses unmittelbar bei Inbetriebnahme geändert werden. Die Nutzung eines zweiten Faktors (z. B. eines Security-Tokens) ist empfehlenswert. Die Authentisierung und Autorisierung von Benutzenden sind ebenso für lokale Schnittstellen erforderlich.

Beispiel 1:

Eine Maschine wird bei einer Störung durch einen externen Monteur oder eine Monteurin mit einem auf einem USB-Stick eingeschleusten Trojaner kompromittiert. Hat die „Maschine“ uneingeschränkten Zugriff auf das Firmennetzwerk, wird sich der Trojaner ungehindert ausbreiten können. Werden USB-Sticks im Vorfeld auf einem autarken Rechner auf Schadsoftware überprüft und haben Maschinen als Netzwerkkomponenten klar definierte Schreib- und Leserechte, wird der Ausbreitung von Schadsoftware Einhalt geboten und der Schaden begrenzt.

**Beispiel 2:**

Speziell präparierte USB-Geräte sind in der Lage, ein System anzugreifen, ohne dass Benutzer und Benutzerinnen davon erfahren oder Schadsoftware-Scanner dies wahrnehmen können. Ein Angreifer oder eine Angreiferin sorgt dafür, dass präparierte Hardware (geschenkte USB-Sticks auf Messen, Tastatur bei Werksführung neben Maschinensteuerung liegen lassen und abwarten, …) arglos vom Technikpersonal angeschlossen wird. Als Gegenmaßnahme ist beispielsweise eine regelmäßige Unterweisung der Beschäftigten, nur explizit vom Unternehmen freigegebene USB-Geräte zu nutzen, zielführend. Als technische Maßnahme können nicht benötigte Schnittstellen grundsätzlich deaktiviert oder die Fähigkeiten der Schnittstelle durch Software-Regeln eingeschränkt werden.

## 4.5 Drahtlose Kommunikation

Im industriellen Umfeld findet zahlreiche drahtlose Kommunikation statt. Diese erfolgt z. B. über Funkfernsteuerungen, Tablets, Laptops und dergleichen. Im Unterschied zu kabelgebundener Kommunikation hat drahtlose Kommunikation keine klar definierte Ausbreitungsgrenze. Die Kommunikation kann unauffällig mitgelesen, manipuliert und gestört werden, solange man sich in Reichweite befindet (von außerhalb des Werksgeländes, per Drohne über dem Dach, durch eine Fremdfirma im Werk, …). Dadurch können unautorisiert Maschinenbefehle gesendet werden, die zu einem Unfall führen. Bei drahtloser Kommunikation ist besonders auf einen Schutz gegen unautorisierten Fremdzugriff zu achten. Die Betriebsanleitung oder technische Dokumentation des Herstellers sollte darüber Auskunft geben, welche Schutzmaßnahmen vorhanden sind. Falls dies nicht der Fall ist, sollte der Betreiber den Hersteller kontaktieren.

## 4.6 Fernwartung

Um eine hohe Produktivität zu erreichen, ist es heutzutage oft erwünscht, dass Fernzugriffe auf Maschinen, z. B. von Herstellern, ermöglicht werden. Bei der Fernwartung von Maschinen und Anlagen werden Daten über das Internet zwischen Betreiber und Hersteller übertragen. Werden keine Vorkehrungen getroffen, ergeben sich hierbei mehrere Schwachstellen in Bezug auf die Sicherheit. Weiterführende Informationen zur Fernwartung enthält die Fachbereich AKTUELL FBHM-133 „Sichere Fernwartung von Maschinen“ [1].

## 4.7 Security-Monitoring

Wenn die oben beschriebenen Maßnahmen umgesetzt sind, ist es empfehlenswert, ein Monitoring zu implementieren. Es soll sicherheitsrelevante Informationen schreibgeschützt archivieren (Logfile). Dazu gehören erfolgreiche und fehlgeschlagene Logins mit Benutzernamen und Zeitstempel.

Manche Angriffe von intern und extern können in diesen Logfiles mit technischen Hilfsmitteln nach- vollzogen werden. Daraus können gegebenenfalls erforderliche Gegenmaßnahmen eingeleitet werden.

In der EU-Maschinenverordnung 2023/1230 gibt es in Anhang III in den Abschnitten 1.1.9 und 1.2.1 Anforderungen an **Hersteller** von Maschinen, welche Daten aufgezeichnet werden müssen. Eine Konkretisierung dieser Anforderungen ist in der kommenden EN 50742 zu erwarten.

In der TRBS 1115-1 befasst sich der Abschnitt 4.5.2, Satz (2), Punkt 5 mit der Protokollierung und Überwachung von Datenverkehr durch den **Betreiber**: *„Überwachung - Um sicherheitsrelevante Ereignisse rechtzeitig zu erkennen, sollten Überwachungen innerhalb der IT/OT-Umgebung an geeigneten Stellen installiert werden, beispielsweise an der Segmentgrenze. Die Auswertung von Meldungen kann je nach Relevanz durch die Aufschaltung auf Meldeanlagen oder durch regelmäßige Prüfung am System selbst erfolgen. Die Überwachungs- und Protokolldaten sind durch geeignete Maßnahmen vor Veränderung zu schützen.“* [2].

Dies kann z. B. durch Software zur automatisierten Anomalieerkennung im Netzwerkverkehr oder eine regelmäßige manuelle Auswertung der aufgezeichneten Logdaten erfolgen.

## 4.8 Notfallmanagement

Für Institutionen und Sicherheitsforscher, die Unternehmen eine Schwachstelle melden möchten, sollte eine zuverlässige und niederschwellige Erreichbarkeit über einen

Notfallkontakt ermöglicht werden, z. B. nach RFC 9116 mittels „security.txt“ [3].

Um im Notfall bei einem Angriff oder dem Bekanntwerden einer Schwachstelle vorbereitet zu sein, sind im Vorfeld Zuständigkeiten festzulegen.

Es sollte ein Notfallplan erstellt werden, wie eine kompromittierte Maschine in einen sicheren Zustand gebracht werden kann. Vor einer Wiederinbetriebnahme ist gegebenenfalls mit Unterstützung des Herstellers sicherzustellen, dass die Kompromittierung vollständig beseitigt und die Schwachstelle geschlossen ist.

Im Einzelfall ist zu prüfen, ob eine Meldepflicht des Sicherheitsvorfalls gegenüber Behörden besteht.

Die in Abschnitt 3 bereits angesprochene Inventarliste zur Erfassung aller sicherheitsrelevanten Elemente sollte idealerweise in einer Datenbank erfolgen, sodass regelmäßige, automatisierte Abfragen nach dem CSAF (Common Security Advisory Framework) möglich sind [4].

### 4.9 Backup

Sollte trotz aller präventiven Anstrengungen dennoch eine Schwachstelle ausgenutzt worden sein, müssen auch Vorkehrungen für diesen Fall getroffen worden sein. Regelmäßige Backups sind hierfür eine wichtige Maßnahme. Backups müssen regelmäßig auf Wiederherstellbarkeit geprüft werden. Sind einzelne Segmente betroffen, können Backups die Daten, Informationen und Prozessdaten schnell wiederherstellen.

## 5 Zusammenfassung und Anwendungsgrenzen

Die Resilienz einer vernetzten Industrie wird wesentlich davon abhängen, ob es gelingen wird, die Sicherheitsaspekte für Safety und Security anzuwenden. Hierbei spielen die technischen Anforderungen sowie das Verhalten der Maschinen- und Anlagenbetreiber eine gleichermaßen entscheidende Rolle. Schon jetzt darf sich der Begriff „Sicherheit“ nicht mehr nur allein auf den Aspekt „Safety“ beziehen, sondern sollte gleichermaßen auch immer die „Security“ beinhalten.

Diese Fachbereich AKTUELL beruht auf dem durch den Fachbereich Holz und Metall, Sachgebiet Maschinen, Robotik und Fertigungsautomation der Deutschen Gesetzlichen Unfallversicherung DGUV zusammengeführten Erfahrungswissen.

Sie soll insbesondere dazu dienen, bei der Beurteilung von Maschinen und Anlagen neben Safety-Anforderungen auch Security-Aspekte zu berücksichtigen und notwendige Sicherheitsmaßnahmen umzusetzen.

Die Bestimmungen nach einzelnen Gesetzen und Verordnungen bleiben durch diese Informationsschrift unberührt. Die Anforderungen der gesetzlichen Vorschriften gelten uneingeschränkt. Um vollständige Informationen zu erhalten, ist es erforderlich, die in Frage kommenden Vorschriftentexte einzusehen.

Diese „Fachbereich AKTUELL“ befindet sich in der Entwurfsfassung. Bitte senden Sie Ihre Kommentare bis zum 05.12.2024 unter Verwendung der Kennung „FBHM-102, Entwurf 09/2024“ oder des Titels an die Kommentaradresse.

Der Fachbereich Holz und Metall setzt sich unter anderem zusammen aus Vertretern und Vertreterinnen der Unfallversicherungsträger, staatlichen Stellen, Sozialpartnern, herstellenden und betreibenden Firmen.

Weitere Fachbereich AKTUELL beziehungsweise Informationsblätter des Fachbereichs Holz und Metall stehen im Internet zum Download bereit [5].

## Literaturverzeichnis


[1] *Fachbereich AKTUELL FBHM-133 „Sichere Fernwartung von Maschinen“,* DGUV, 07/2023.

[2] *TRBS 1115 Teil 1 „Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen“, BAuA, 11/2022.*

[3] *RFC 9116 „A File Format to Aid in Security Vulnerability Disclosure“, E. Foudil, Y. Shafranovich, 04/2022.*

[4] *Common Security Advisory Framework (CSAF), BSI, 07/2024.*

[5] *www.dguv.de/fb-holzundmetall Publikationen oder www.bghm.de Webcode: <626>.*


## Bildnachweis

Die gezeigten Bilder wurden freundlicherweise zur Verfügung gestellt von:

- Abbildung 1 – FB HM, SG MRF, Berthold Heinke
- Abbildung 2, 4, 5 – BGHM, Martin Eberle
- Abbildung 3 – DGUV IFA, Jonas Stein
- Abbildung 6 – BGN, Klaus-Dieter Pohl

## Kommentaradresse


Fachbereich Holz und Metall der DGUV
Sachgebiet Maschinen, Robotik und Fertigungsautomation
c/o Berufsgenossenschaft Holz und Metall
Isaac-Fulda-Allee 18
55124 Mainz

Email: fb-holzundmetall@bghm.de


Die Fachbereiche der DGUV werden von den Unfallkassen, den branchenbezogenen Berufsgenossenschaften sowie dem Spitzenverband DGUV selbst getragen. Für den Fachbereich Holz und Metall ist die Berufsgenossenschaft Holz und Metall der federführende Unfallversicherungsträger und damit auf Bundesebene erster Ansprechpartner in Sachen Sicherheit und Gesundheit bei der Arbeit für Fragen zu diesem Gebiet.

An der Erarbeitung dieser Fachbereich AKTUELL haben mitgewirkt:

- BG ETEM
- BGN
- BG RCI
- IFA

# Anlage 1: Checkliste für Betreiber von Maschinen

Diese Checkliste soll den Betreiber dabei unterstützen, Maschinen und Anlagen zu bewerten und sicherer zu gestalten. Sie erhebt keinen Anspruch auf Vollständigkeit.

| Fragestellung | Ja | Nein | Nicht zutreffend | Wo/Wie |
|---|---|---|---|---|
| **1. Grundsätzliches** | | | | |
| a) Werden Wechseldatenträger vor jeder (auch der ersten) Benutzung auf Schadsoftware gescannt? | | | | |
| b) Wird das Bedienpersonal regelmäßig unter Security-Aspekten unterwiesen? | | | | |
| c) Werden für die Anlagenwartung und Programmierung nur Systeme eingesetzt, die aktuell auf Schadsoftware überprüft wurden? | | | | |
| d) Werden regelmäßige Backups erstellt? | | | | |
| e) Wird vor jeder Softwareänderung ein Backup erstellt? | | | | |
| f) Werden Schutzmaßnahmen regelmäßig aktualisiert? | | | | |
| **2. Risikoanalyse** | | | | |
| a) Sind die schutzbedürftigen Informationen und Komponenten identifiziert und aufgelistet? | | | | |
| b) Ist eine Risikobewertung durchgeführt in Bezug auf Wichtigkeit und Ableitung von Schutzzielen (z. B. garantierte Verfügbarkeit der Daten; jederzeit digitale Rückverfolgbarkeit von Produktionsdaten sichergestellt)? | | | | |
| c) Sind mögliche Bedrohungen und ihre Folgen dokumentiert? | | | | |
| **3. Zoneneinteilung** | | | | |
| a) Wurden Maschinen, Komponenten und Informationen ähnlichen Schutzbedarfs in Zonen eingeteilt? | | | | |
| b) Sind einzelne Zonen untereinander durch technische Maßnahmen getrennt (Netzsegmentierung), z. B. durch Firewalls? | | | | |
| c) Sind bei Ausfall einer Zone (z. B. durch Hackerangriff, Virus, Trojaner, …) möglichst wenig andere Zonen betroffen? | | | | |
| d) Ist organisiert, dass die Netzsegmentierung auf Effektivität und Aktualität (Updates, Filterregeln, …) periodisch wiederkehrend geprüft wird? | | | | |
| **4. Ganzheitliche Organisation von Authentisierung und Autorisierung** | | | | |
| a) Gibt es für alle Nutzenden individuelle Benutzerkonten (Nutzer/Nutzerin + Passwort) und wird unternehmensweit eine Passwortrichtlinie durchgesetzt? | | | | |
| b) Ist definiert und umgesetzt, welche Nutzenden welche Rechte im Netz haben (Lesezugriff, Schreibzugriff)? | | | | |

| Fragestellung | Ja | Nein | Nicht zutreffend | Wo / Wie |
|---|---|---|---|---|
| c) Werden Standardpasswörter von Maschinen und Anlagen turnusmäßig geändert und sind nur befugten Personen zugänglich? | | | | |
| d) Werden Fernzugriffe überwacht und auch mit wechselnden Passwörtern geschützt? | | | | |
| e) Wird jeder Zugriff von Maschinen auf das Netz oder von Personen auf das Netz/auf Maschinen authentisiert? | | | | |
| f) Werden Zugriffe auf externe Schnittstellen (USB, Internet, VPN, …) auch über sichere Authentisierung abgesichert? | | | | |
| **5. Absicherung von Funktechnologien** | | | | |
| a) Erstrecken sich die Reichweiten nur auf das Nötigste (Signalstärke oder Abschirmung)? | | | | |
| b) Gibt es sichere Passwörter? | | | | |
| c) Wurden ggf. voreingestellte Passwörter durch individuelle Passwörter ersetzt? | | | | |
| d) Können Safety-relevante Parameter nur über sichere Kommunikation geändert werden? | | | | |
| e) Gibt es Regelungen zum Aufbau und Beenden einer Kommunikation? | | | | |
| **6. Fernwartung** | | | | |
| a) Gibt es Regelungen zum Aufbau und zum Beenden einer Fernwartung? | | | | |
| b) Sind Fernwartungen generell über verschlüsselte Verbindungen aufgebaut (z. B. VPN, SSH)? | | | | |
| c) Sind USB-Ports bei Monteureinsätzen vor Ort gesichert und mit organisatorischen Maßnahmen belegt (z. B. USB-Stick-Prüfung an Pforte mittels Virenscanner, Instandhaltung gibt USB-Ports danach frei)? | | | | |
| d) Sind Änderungen, die Gefährdungen hervorrufen können (z. B. Maschinenanlauf), nur möglich, wenn zuvor vor Ort an der Maschine eine Bestätigung erfolgt ist? | | | | |
| **7. Monitoring und Hackerangriffserkennung** | | | | |
| a) Werden mindestens alle externen Zugriffe auf abgesicherte Netzwerke protokolliert? | | | | |
| b) Werden verdächtige Ereignisse wie falsche Passworteingabe, Senden von Daten an unbekannte Empfänger gemeldet? | | | | |
| c) Werden dann Gegenmaßnahmen eingeleitet? | | | | |
| d) Sind Virenscanner im Netzwerk implementiert, die jeweils auf aktuellen Stand gehalten werden? | | | | |

| Fragestellung | Ja | Nein | Nicht zutreffend | Wo / Wie |
|---|---|---|---|---|
| **8. Backups** | | | | |
| a) Werden regelmäßig Backups durchgeführt? | | | | |
| b) Wird jede Zone dabei unabhängig von anderen Zonen berücksichtigt? | | | | |
| c) Sind die Backup-Datenträger abgesichert? | | | | |
| d) Wird das Backup gegen Fremdzugriff und Abhandenkommen sicher aufbewahrt? | | | | |
| e) Werden regelmäßige Prüfungen auf Wiederherstellbarkeit durchgeführt? | | | | |
| f) Sind die Backup-Systeme redundant aufgebaut, sodass ein weiteres Backup bei Nicht-Wiederherstellbarkeit zur Verfügung steht? | | | | |
| **9. Organisatorische Maßnahmen** | | | | |
| a) Wurde eine geeignete verantwortliche Person für Security bestimmt? | | | | |
| b) Wird das System regelmäßig auf Schwachstellen überprüft? | | | | |
| c) Ist das Updatemanagement organisiert? | | | | |
| d) Ist bei Initialisierung des Systems organisiert, dass alle individuellen Einstellungen wiederhergestellt werden (z. B. die Zugangsdaten bei Austausch eines Maschinenrechners)? | | | | |
| **10. Dokumentation der Sicherheitsmaßnahmen** | | | | |
| a) Sind sämtliche Schnittstellen (Ports) dokumentiert? | | | | |
| b) Sind die Ergebnisse der Risikoanalyse dokumentiert? | | | | |
| c) Wurde die Rechteverteilung dokumentiert? | | | | |
| d) Ist das Maschineninventar mit zugehörigen Nutzenden und Passwörtern (verschlüsselt) dokumentiert? | | | | |
| e) Sind Sicherheitsvorfälle und deren Gegenmaßnahmen bzw. daraus abgeleitete Strategien und Schutzmaßnahmen dokumentiert? | | | | |

# Anlage 2: Beispiel-Bewertung vorhandener Systeme

| **Bezeichnung der Maschine, Anlage, etc.** | **Steuerungen** | | | | | Bemerkungen |
|---|---|---|---|---|---|---|
| | Kontakt-behaftete | Elektronische | Program-mierbare ohne Netzwerk-verbindung | Programmierbare mit Netzwerk-verbindung, keine Verbindung zu übergeordneten Systemen | Programmier-bare mit Netzwerk-verbindung, mit Verbindung zu übergeordneten Systemen | |
| **Tischbohr-maschine** | | **X** Keine Maßnahme erforderlich | | | | |
| **Presse 12** | | | **X** Maßnahme siehe DOK … | | | Kommunikation mit Maschine 1 und 3 |
| **CNC Fräse** | | | | **X** Maßnahme siehe DOK … | | |
| **Automatik-Lagerkran** | | | | | **X** Abstimmung mit Lagerrechner Maßnahme siehe DOK… | Austausch von Lageraufträgen mit Lagerrechner Y |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |