Ausgabe: November 2022
GMBl 2023 S. 522 [Nr. 25]
geändert: GMBl 2025, S. xx [Nr. xx]

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

Die Technischen Regeln für Betriebssicherheit (TRBS) geben den Stand der Technik, Arbeitsmedizin und Arbeitshygiene sowie sonstige gesicherte arbeitswissenschaftliche Erkenntnisse für die Verwendung von Arbeitsmitteln wieder.

Sie werden vom **Ausschuss für Betriebssicherheit** ermittelt bzw. angepasst und vom Bundesministerium für Arbeit und Soziales (BMAS) im Gemeinsamen Ministerialblatt (GMBl) bekannt gegeben.

Die TRBS 1115 Teil 1 konkretisiert im Rahmen ihres Anwendungsbereichs Anforderungen der Betriebssicherheitsverordnung. Bei Einhaltung dieser Technischen Regeln kann der Arbeitgeber davon ausgehen, dass die entsprechenden Anforderungen der Verordnung erfüllt sind. Wählt der Arbeitgeber eine andere Lösung, muss er damit mindestens die gleiche Sicherheit und den gleichen Gesundheitsschutz für die Beschäftigten erreichen.

1 Anwendungsbereich

2 Begriffsbestimmungen

3 Anforderungen der Cybersicherheit an sicherheitsrelevante MSR-Einrichtungen

4 Planung und Realisierung der Ausrüstung eines Arbeitsmittels mit einer sicherheitsrelevanten MSR-Einrichtung im Hinblick auf Cybersicherheit durch den Arbeitgeber

5 Überprüfung der Wirksamkeit der Cybersicherheitsmaßnahmen

6 Prüfung des Arbeitsmittels vor Inbetriebnahme und Wiederinbetriebnahme nach prüfpflichtiger Änderung nach §§ 14 und 15 BetrSichV

7 Wiederkehrende Prüfung von Arbeitsmitteln mit sicherheitsrelevanten MSR-Einrichtungen nach §§ 14 und 16 BetrSichV

8 Verwendung und Instandhaltung

Anhang 1

Management der Cybersicherheit

Anhang 2

Erläuterungen und Beispiele für erforderliche Cybersicherheitsmaßnahmen

Anhang 3

Regelwerke und Normen

1 Anwendungsbereich

(1) Diese Technische Regel konkretisiert die Betriebssicherheitsverordnung (BetrSichV) im Hinblick auf die Ermittlung und Festlegung erforderlicher Cybersicherheitsmaßnahmen für die dauerhafte Sicherstellung der Funktionsfähigkeit von sicherheitsrelevanten Mess-, Steuer- und Regeleinrichtungen (MSR-Einrichtungen), die als technische Schutzmaßnahme für die sichere Verwendung eines Arbeitsmittels inklusive einer überwachungsbedürftigen Anlage eingesetzt werden.

Cyberbedrohungen können dazu führen, dass eine sicherheitsrelevante MSR-Einrichtung ihre Sicherheitsfunktion nicht mehr ausüben kann oder sogar zusätzliche Gefährdungen herbeigeführt werden.

Die in dieser TRBS dargestellte Vorgehensweise zur Festlegung, Umsetzung und Prüfung von Cybersicherheitsmaßnahmen ist auch geeignet, um über sicherheitsrelevante MSR-Einrichtungen hinausgehende Teile des Arbeitsmittels (z. B. notwendige Kommunikationsmittel) oder andere technische Infrastrukturen gegen Cyberbedrohungen zu schützen, wenn dieses als Ergebnis der Gefährdungsbeurteilung als erforderlich angesehen wird.

Für nicht verwendungsfertig beschaffte Arbeitsmittel oder solche verwendungsfertig beschaffte Arbeitsmittel, bei denen die ausreichende Cybersicherheit nicht bereits Bestandteil des Inverkehrbringens war, bietet diese Technische Regel auch Hilfestellung für die Spezifikation, Planung und Realisierung von Cybersicherheitsmaßnahmen.

(2) Diese TRBS beschreibt ergänzend zur TRBS 1201 auch die Durchführung von Prüfungen zur Cybersicherheit sowie das Vorgehen bei Änderungen von Arbeitsmitteln im Zusammenhang mit der Cybersicherheit von sicherheitsrelevanten MSR-Einrichtungen.

(3) Anhang 1 enthält Anforderungen, die der Arbeitgeber berücksichtigen muss, wenn er ein Management der Cybersicherheit (zum Begriff siehe Abschnitt 2.5) im Betrieb einführt oder die relevanten Inhalte z. B. in sein Management der funktionalen Sicherheit oder in sein allgemeines Informationssicherheitsmanagement integriert.

(4) Anhang 2 enthält Erläuterungen und Beispiele für erforderliche Cybersicherheitsmaßnahmen, die sich, anders als in TRBS 1115, nicht an Druckanlagen, Ex-Anlagen oder Aufzugsanlagen orientieren, sondern an der Art der kompromittierbaren Schnittstellen und dem Grad ihrer Vernetzung.

(5) Diese TRBS behandelt keine Arbeitsmittel oder sicherheitsrelevanten MSR-Einrichtungen, die aufgrund nicht vorhandener Schnittstellen (sowohl kabelgebunden als auch kabellos) nicht kompromittiert werden können.

(6) Diese TBRS betrachtet nicht die Abwehr von wirtschaftlichen Schäden oder von Angriffen auf den Datenschutz (z. B. von personenbezogenen Daten). Sie kann dafür gleichwohl als Erkenntnisquelle herangezogen werden.

2 Begriffsbestimmungen

2.1 Allgemeines

Folgende Begriffe sind bereits in TRBS 1201 bestimmt:

1. Kontrolle
2. Art und Umfang erforderlicher Prüfungen
3. Prüffrist

4. Notbefehlseinrichtung
5. Sicherheitseinrichtung
6. Sicherheitsrelevante MSR-Einrichtungen

Folgende Begriffe sind bereits in TRBS 1115 bestimmt:

1. Funktionale Sicherheit
2. Sicherheitslebenszyklus

2.2 Cybersicherheit

(1) Cybersicherheit im Sinne dieser TRBS bezeichnet gemäß Verordnung (EU) 2019/881 alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen.

Hinweis: Die Verordnung (EU) 2019/881 übersetzt aus dem englischen Original „activities“ in der deutschen Fassung mit „Tätigkeiten“. Im Sinne dieser TRBS sind damit alle technischen und organisatorischen Maßnahmen zu verstehen, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen.

(2) Da in der europäischen Rechtsetzung der Begriff „Cybersicherheit“ mit einem umfassenderen Verständnis verwendet wird, wird in dieser TRBS der Begriff „Cybersicherheit“ auf den Schutz sicherheitsrelevanter MSR-Einrichtungen, die als technische Schutzmaßnahme für die sichere Verwendung eines Arbeitsmittels inklusive einer überwachungsbedürftigen Anlage eingesetzt werden, eingeschränkt verwendet.

Hinweis: In vielen Quellen wird anstelle des Begriffs „Cybersicherheit“ der Begriff „Informationssicherheit“ verwendet.

2.3 Cyberbedrohung

Cyberbedrohung im Sinne dieser TRBS bezeichnet gemäß Verordnung (EU) 2019/881 einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.

Hinweis: Unter „Umständen“ können z. B. Sicherheitslücken wie unveränderte Standardpasswörter verstanden werden.

2.4 IT/OT-Umgebung

Die IT/OT-Umgebung im Sinne dieser TRBS bezeichnet die IT/OT-Systeme (Netz- und Informationssysteme im Sinne der Verordnung (EU) 2019/881), die temporär oder dauerhaft einen Informationsaustausch mit sicherheitsrelevanten MSR-Einrichtungen haben.

Hinweis 1: Die IT/OT-Umgebung kann als möglicher Angriffsweg einen Einfluss auf die Zuverlässigkeit der sicherheitsrelevanten MSR-Einrichtungen besitzen.

Hinweis 2: IT-Systeme sind die Hard- und Softwarekomponenten zur elektronischen Datenverarbeitung (IT – Information Technology). OT-Systeme sind die Hard- und Softwarekomponenten zur Steuerung, Regelung, Überwachung und Kontrolle von Maschinen, Anlagen und Prozessen (OT – Operational Technology).

2.5 Management der Cybersicherheit

Das Management der Cybersicherheit im Sinne dieser TRBS bezeichnet die Festlegung, Umsetzung und Kontrolle der Regelungen und Vorgehensweisen zur Sicherstellung des erforderlichen Schutzes von sicherheitsrelevanten MSR-Einrichtungen vor Cyberbedrohungen.

2.6 Instandhaltung

Instandhaltung im Sinne dieser TRBS umfasst die für die Aufrechterhaltung der Cybersicherheit erforderlichen Tätigkeiten an der Hard- und Software der betroffenen Komponenten. Insbesondere zählen hierzu sicherheitsrelevante Software-Updates.

3 Anforderungen der Cybersicherheit an sicherheitsrelevante MSR-Einrichtungen

3.1 Allgemeines

(1) Durch den steigenden Vernetzungsgrad können sicherheitsrelevante MSR-Einrichtungen zunehmend zum Ziel von Cyberbedrohungen werden. Dies hat der Arbeitgeber bei seiner Gefährdungsbeurteilung zu berücksichtigen.

(2) Der Arbeitgeber hat nach § 3 BetrSichV die auftretenden Gefährdungen zu beurteilen und daraus notwendige Maßnahmen für das sichere Verwenden von Arbeitsmitteln abzuleiten. Nach § 5 Absatz 1 BetrSichV dürfen nur Arbeitsmittel zur Verfügung gestellt werden, also auch zugehörige sicherheitsrelevante MSR-Einrichtungen, die für den Einsatzzweck geeignet und unter den vorgesehenen Einsatzbedingungen sicher sind. Im Rahmen der Gefährdungsbeurteilung und bei der Auswahl und Implementierung der sicherheitsrelevanten MSR-Einrichtungen sind auch Cyberbedrohungen zu berücksichtigen.

(3) Mögliche Auswirkungen von Cyberbedrohungen können sein:

1. Beeinflussung der Verfügbarkeit (z. B. Deaktivieren oder Blockieren der Funktion von sicherheitsrelevanten MSR-Einrichtungen),
2. Verletzung der Integrität (z. B. unberechtigte Änderung von Daten),
3. Verletzung der Vertraulichkeit (z. B. Abfluss von Daten einschließlich Passwörtern und Signaturen).

(4) Sicherheitsrelevante MSR-Einrichtungen, ihre Integration in das Arbeitsmittel und ihre Anwendung müssen nach dem Stand der Technik vor Cyberbedrohungen derart geschützt sein, dass Gefährdungen für Beschäftigte und bei überwachungsbedürftigen Anlagen auch andere Personen in deren Gefahrenbereich vermieden werden. Cybersicherheitsmaßnahmen dienen dazu, die Funktionsfähigkeit von sicherheitsrelevanten MSR-Einrichtungen während der gesamten Verwendungsdauer des Arbeitsmittels auch bei Cyberbedrohungen aufrechtzuerhalten.

(5) Zur Erfüllung der Vorgaben des § 3 Absatz 7 BetrSichV in Verbindung mit § 4 Absatz 6 BetrSichV sind Verfahren zu etablieren, um die Eignung und Funktionsfähigkeit der Cybersicherheitsmaßnahmen

1. regelmäßig in geeigneten Zeitabständen,
2. bei Änderungen am Arbeitsmittel (siehe hierzu Abschnitt 8.3),
3. bei neuen Erkenntnissen zu Cyberbedrohungen z. B. aus veröffentlichten oder firmeninternen Cybersicherheitsvorfällen und Schwachstellenmeldungen oder aus einschlägigen Veröffentlichungen,

4. bei Änderungen des Stands der Technik der Cybersicherheit

zu überprüfen.

3.2 Cybersicherheit im Sicherheitslebenszyklus

Cybersicherheit muss während des gesamten Sicherheitslebenszyklus der sicherheitsrelevanten MSR-Einrichtung gewährleistet sein (siehe auch Abbildung 1). Betroffen sind folgende Elemente:

1. Hardware,
2. Software,
3. Daten/Informationen,
4. Schnittstellen

sowie die mit ihrer Verwendung verbundenen

1. Prozesse,
2. Richtlinien,
3. Organisationen sowie
4. Personen,
5. IT/OT-Umgebung.

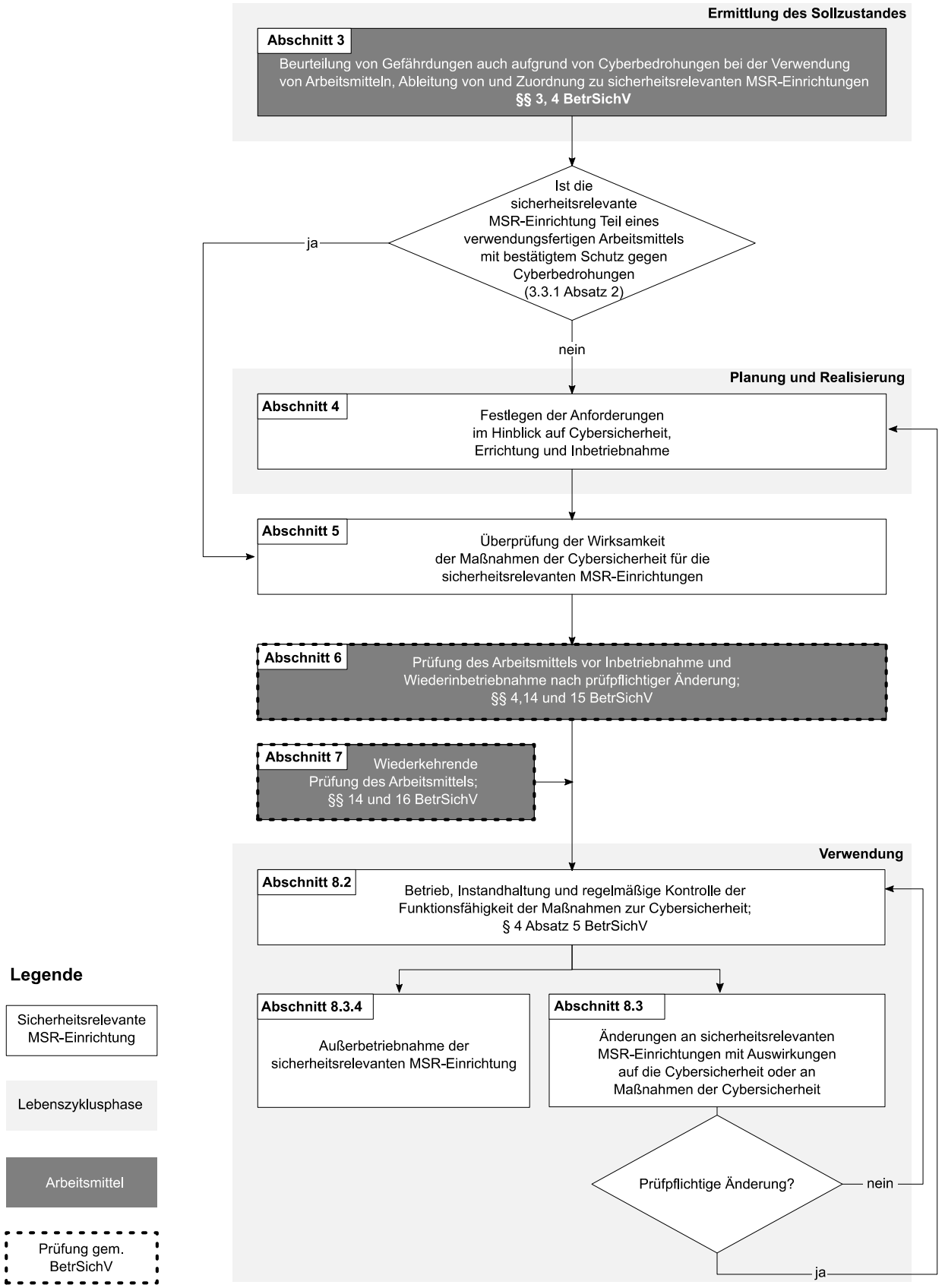

Abb. 1 Berücksichtigung der Cybersicherheitsmaßnahmen in den Abläufen bei Planung, Realisierung und Verwendung einer sicherheitsrelevanten MSR-Einrichtung

3.3 Organisatorische Maßnahmen

3.3.1 Allgemeines

(1) Die Wirksamkeit der Cybersicherheitsmaßnahmen muss dauerhaft sichergestellt werden. Dafür ist es erforderlich, Zugriffsrechte, Fachkunde (Qualifikation), Tätigkeiten, Verantwortlichkeiten, Zuständigkeiten und Aufgaben derjenigen Personen eindeutig festzulegen, die

1. für den Auswahl-, Beschaffungs- und Integrationsprozess verantwortlich sind oder
2. im Betrieb Umgang mit einer sicherheitsrelevanten MSR-Einrichtung und der IT/OT-Umgebung haben können (in der Regel auch die Verwender eines Arbeitsmittels).

Die unter Nummer 1. aufgeführten Personen müssen über eine der Aufgabe entsprechende Fachkunde verfügen. Die unter Nummer 2. aufgeführten Personen müssen mindestens über die erforderlichen Kenntnisse zu den in ihrem Zuständigkeitsbereich festgelegten Cybersicherheitsmaßnahmen verfügen.

(2) Für die Art und den Umfang der erforderlichen Festlegung von Cybersicherheitsmaßnahmen sind zwei Fälle zu unterscheiden:

1. Die sicherheitsrelevante MSR-Einrichtung wird als Teil eines verwendungsfertigen Arbeitsmittels durch den Hersteller des Arbeitsmittels auf dem Markt bereitgestellt, wobei ein anforderungsgerechter Schutz gegen Cyberbedrohungen nach dem Stand der Technik bestätigt wurde.

   In diesem Fall hat der Arbeitgeber die vom Hersteller festgelegten technischen (z. B. Firewall) und organisatorischen (z. B. Installieren von Updates) Cybersicherheitsmaßnahmen für das Arbeitsmittel aufrechtzuerhalten.

2. Die sicherheitsrelevante MSR-Einrichtung wird

   a) verwendungsfertig als Teil des Arbeitsmittels durch den Hersteller auf dem Markt ohne ausreichende Cybersicherheitsmaßnahmen bereitgestellt,

   b) nicht entsprechend den Herstellervorgaben hinsichtlich der vorgesehenen Umgebungsrandbedingungen oder Cybersicherheitsmaßnahmen betrieben oder

   c) durch den Arbeitgeber in eigener Verantwortung zur Verfügung gestellt (siehe auch TRBS 1115).

   Hierbei hat der Arbeitgeber eigene Verfahren festzulegen, um die Anwendung von geeigneten Cybersicherheitsmaßnahmen für die sicherheitsrelevanten MSR-Einrichtung über die gesamte Verwendungsdauer des Arbeitsmittels sicherzustellen. Über die Festlegungen des Absatz 1 hinaus sind hierbei die zu nutzenden Werkzeuge und Methoden festzulegen (siehe hierzu Abschnitt 4).

(3) Wenn der Arbeitgeber zur Aufrechterhaltung von Eignung und Anwendung von Cybersicherheitsmaßnahmen sicherheitsrelevanter MSR-Einrichtungen ein Management der Cybersicherheit im Betrieb einführt, sind die in Anhang 1 beschriebenen Maßnahmen zu berücksichtigen.

3.3.2 Qualifikation zur Durchführung der Gefährdungsbeurteilung

(1) Nach § 3 Absatz 3 BetrSichV darf eine Gefährdungsbeurteilung nur von fachkundigen Personen durchgeführt werden. Diese müssen in der Lage sein, Gefährdungen der Beschäftigten bei der Verwendung von sicherheitsrelevanten MSR-Einrichtungen bzw. Arbeitsmitteln mit sicherheitsrelevanten MSR-Einrichtungen systematisch zu ermitteln und zu bewerten sowie aus dem Ergebnis Schutzmaßnahmen abzuleiten. Die notwendige Qualifikation muss der Arbeitgeber unter Berücksichtigung der vorliegenden technischen Systeme festlegen und dokumentieren.

(2) Die erforderliche Fachkunde für eine Beurteilung der Cybersicherheit umfasst technische Kenntnisse, Ausbildung und Erfahrung auf mehreren Gebieten. Der Umfang hängt von den Schnittstellen und den vom Hersteller bereitgestellten Informationen über das Arbeitsmittel ab. Die nachstehend genannten Aspekte hat der Arbeitgeber bei der Festlegung von Art und Umfang der erforderlichen Fachkunde zu berücksichtigen:

1. Kenntnisse gesetzlicher Anforderungen und Vorschriften sowie Normen zur Cybersicherheit
2. Grundlegende Kenntnisse im Bereich Cybersicherheit sowie Branchenkenntnisse

   Für die Beurteilung der Cybersicherheit der sicherheitsrelevanten MSR-Einrichtungen sind im Wesentlichen Kenntnisse zu den Cyberbedrohungen der jeweiligen Schnittstellen notwendig. Daher sind grundlegende Kenntnisse und Erfahrung im Bereich der Cybersicherheit unerlässlich. Dazu gehören

   a) Arbeitsprozesse zur Bewertung und Aufrechterhaltung der Cybersicherheit (z. B. Erfahrung mit einem Informationssicherheitsmanagement oder eine IT-Risikobeurteilung),

   b) Typische Schwachstellen und Cyberbedrohungen für das Arbeitsmittel und daraus resultierende Folgen.

   Für die Behandlung der Cybersicherheit im Rahmen der Gefährdungsbeurteilung sind ergänzende branchenspezifische Kenntnisse erforderlich.

3. spezifische Kenntnis über das jeweilige Unternehmen

   Für die Festlegung von wirksamen Cybersicherheitsmaßnahmen sind die Kenntnis des Managements der Cybersicherheit des Betriebs und die verwendeten Technologien notwendig. Dies sind unter anderem Prozesse zum Umgang mit Updates, Protokollierung, Überwachung.

4. angemessene Kenntnisse über Maßnahmen zum Schutz vor Cyberbedrohungen

   Ungeeignete oder fehlerhafte Cybersicherheitsmaßnahmen können selbst zusätzliche Angriffe auf sicherheitsrelevante MSR-Einrichtungen ermöglichen oder diese negativ beeinflussen. Deshalb ist technisches Wissen und Erfahrung zur Verwendung geeigneter Maßnahmen erforderlich, insbesondere zu:

   a) grundsätzlichen Funktionen der geeigneten Cybersicherheitsmaßnahmen,

   b) möglichen Nachteilen und Auswirkungen der jeweiligen Cybersicherheitsmaßnahmen,

   c) Beurteilung der Eignung der Cybersicherheitsmaßnahmen,

   d) Methoden zur wirkungsvollen Überwachung der Maßnahmen,

e) Prinzip der minimalen Rechte.

(3) Falls der Arbeitgeber für eine sicherheitsrelevante MSR-Einrichtung eigenständig Cybersicherheitsmaßnahmen ermittelt und umsetzt, sind gegenüber den Anforderungen des Absatzes 2 tiefergehende Fachkunde und Qualifikationen erforderlich. Zusätzlich sind ausreichende Kenntnisse zu den folgenden Bereichen erforderlich:

1. Informationssicherheitsmanagement,
2. Vorgehensweisen zur Ermittlung von relevanten Cybergefährdungen auf Basis der Cyberbedrohungen und Schwachstellen,
3. Vorgehensweisen zur systemspezifischen Auswahl von geeigneten Cybersicherheitsmaßnahmen, z. B.
   a) Hardwarearchitektur und Segmentierung (siehe hierzu Abschnitt 4.5.2 Absatz 2 Nummer 1),
   b) Zugangs- und Zugriffskontrolle,
   c) sichere Installation und Änderung von Cybersicherheitsmaßnahmen,
   d) Funktionsreduktion und Härtung,
   e) Überwachung von Hardware, Software und ihrer Kommunikation,
   f) Notfallmanagement (z. B. response and recover, Disaster Recovery).

3.4 Dokumentation

Entsprechend den Anforderungen des § 3 Absatz 8 BetrSichV sind auch die Cybersicherheitsmaßnahmen für sicherheitsrelevante MSR-Einrichtungen zu dokumentieren. Dazu gehören auch Art und Umfang der diesbezüglichen Festlegungen zu Prüfungen sowie deren Fristen. Eine elektronische Form der Dokumentation ist zulässig.

4 Planung und Realisierung der Ausrüstung eines Arbeitsmittels mit einer sicherheitsrelevanten MSR-Einrichtung im Hinblick auf Cybersicherheit durch den Arbeitgeber

4.1 Allgemeines

In diesem Abschnitt werden Maßnahmen beschrieben, die der Arbeitgeber im Zuge der Planung und Realisierung sicherheitsrelevanter MSR-Einrichtungen zu treffen hat, sofern diese nicht als Bestandteil eines verwendungsfertigen Arbeitsmittels mit bestätigtem Schutz vor Cyberbedrohungen geliefert werden.

4.2 Festlegung des Schutzkonzepts für die Cybersicherheit des Arbeitsmittels durch den Arbeitgeber

(1) Für Arbeitsmittel mit sicherheitsrelevanten MSR-Einrichtungen sind die erforderlichen Cybersicherheitsmaßnahmen zu ermitteln. Es wird empfohlen, diese Maßnahmen in einem Schutzkonzept der Cybersicherheit zu dokumentieren. Dies kann auch durch eine Ergänzung des Schutzkonzepts der funktionalen Sicherheit (siehe TRBS 1115) erfolgen.

(2) Die Vorgaben der Hersteller sicherheitsrelevanter MSR-Einrichtungen zur Cybersicherheit sind bei der Einbindung in das Arbeitsmittel zu beachten.

(3) Bei der Ermittlung des Schutzkonzepts sind auch Ersatzmaßnahmen für die Zeitdauer ausgeschalteter oder eingeschränkt verfügbarer Maßnahmen der Informationssicherheit, z. B. für den Fall von Fernwartung, zu berücksichtigen.

4.3 Umsetzung des Schutzkonzepts für die Cybersicherheit bezogen auf sicherheitsrelevante MSR-Einrichtungen

(1) Entsprechend den möglichen Gefährdungen werden gemäß TRBS 1115 für jede sicherheitsrelevante MSR-Einrichtung die Anforderungen an ihre Zuverlässigkeit festgelegt. Die Cybersicherheitsmaßnahmen müssen geeignet sein, um die Funktionsfähigkeit der sicherheitsrelevanten MSR-Einrichtungen zu schützen und an deren Zuverlässigkeit angepasst sein.

(2) Bei Bildung von Segmenten mit mehreren sicherheitsrelevanten MSR-Einrichtungen (siehe hierzu Abschnitt 4.5.2) richten sich die Cybersicherheitsmaßnahmen für das gesamte Segment nach der sicherheitsrelevanten MSR-Einrichtung mit den höchsten Anforderungen an die Cybersicherheit.

4.4 Anforderungen an die Cybersicherheit sicherheitsrelevanter MSR-Einrichtungen

4.4.1 Sicherheitsrelevante MSR-Einrichtungen als Teil eines verwendungsfertigen Produktes mit bestätigtem Schutz vor Cyberbedrohungen

(1) Wird die sicherheitsrelevante MSR-Einrichtung verwendungsfertig als Teil des Arbeitsmittels mit bestätigtem Schutz gegen Cyberbedrohungen nach dem Stand der Technik durch den Hersteller auf dem Markt bereitgestellt, hat der Arbeitgeber die vom Hersteller festgelegten technischen und organisatorischen Cybersicherheitsmaßnahmen aufrechtzuerhalten.

(2) Für die sicherheitsrelevanten MSR-Einrichtungen sowie ggf. für einzelne Komponenten oder die IT/OT-Umgebung sind

1. die von den jeweiligen Herstellern erstellten Unterlagen wie z. B. Betriebsanleitung, Konfigurations-Identifikationsdokumente (KID) und IT-Sicherheitshandbücher,
2. die Festlegungen der für die Gewährleistung der Funktionsfähigkeit der Cybersicherheitsmaßnahmen einzuhaltenden Fristen oder Anlässe der notwendigen Aktualisierungen (z. B. Updates der Virensignaturen), Prüfungen und Kontrollen sowie
3. die Festlegung von Informationsquellen zu aktuellen Cyberbedrohungen und deren Nutzung

in die Dokumentation nach Abschnitt 3.4 aufzunehmen.

4.4.2 Sicherheitsrelevante MSR-Einrichtungen als Teil eines verwendungsfertigen Produktes ohne bestätigtem Schutz vor Cyberbedrohungen

Wird die sicherheitsrelevante MSR-Einrichtung als Teil eines verwendungsfertigen Produktes auf dem Markt bereitgestellt, unterliegt dieses Produkt insgesamt den Anforderungen der entsprechenden Rechtsvorschriften zum Inverkehrbringen. Zum Zeitpunkt der Erarbeitung dieser TRBS berücksichtigen die meisten gesetzlichen Rechtsvorschriften zum Inverkehrbringen die Behandlung von Cyberbedrohungen noch nicht ausreichend. Es obliegt dem Arbeitgeber zu beurteilen, ob bei der bestimmungsgemäßen Verwendung des Produktes Gefährdungen durch Cyberbedrohungen entstehen können. Ist dieses der Fall, finden die Regelungen unter Abschnitt 4.4.3 Anwendung.

4.4.3 Sicherheitsrelevante MSR-Einrichtungen, die vom Arbeitgeber in eigener Verantwortung zur Verfügung gestellt werden

(1) Im Schutzkonzept der Cybersicherheit sind die erforderlichen Cybersicherheitsmaßnahmen für die sicherheitsrelevanten MSR-Einrichtungen festgelegt. Basierend auf dem Schutzkonzept sind Anforderungen an die Komponenten der sicherheitsrelevanten MSR-Einrichtungen und falls erforderlich an die IT/OT-Umgebung in einer Spezifikation der Cybersicherheit festzulegen. Die erforderliche Dokumentation kann auch durch eine Ergänzung der Spezifikation der funktionalen Sicherheit (siehe TRBS 1115) erfolgen.

(2) Für die Festlegung der erforderlichen Cybersicherheitsmaßnahmen ist wie folgt vorzugehen:

1. Erfassung aller Elemente gemäß Abschnitt 3.2 der sicherheitsrelevanten MSR-Einrichtungen und der IT/OT-Umgebung im erforderlichen Umfang.
2. Erfassung und Bewertung von Bedrohungen der Integrität und Verfügbarkeit der sicherheitsrelevanten MSR-Einrichtungen, die durch Cyberbedrohung dieser Elemente ausgehen.
3. Auswahl und Umsetzung von Cybersicherheitsmaßnahmen, um den Cyberbedrohungen in geeigneter Weise zu begegnen und die Auswirkungen im erforderlichen Umfang zu begrenzen. Bereits bestehende Cybersicherheitsmaßnahmen können hierbei berücksichtigen werden. Auf die erforderliche Rückwirkungsfreiheit der Cybersicherheitsmaßnahmen auf die Sicherheitsfunktion ist zu achten.
4. Festlegungen der einzuhaltenden Fristen oder Anlässe für die Durchführung von Aktualisierungen (z. B. Updates der Virensignaturen) und Kontrollen.
5. Festlegung eines Vorgehens zur regelmäßigen Ermittlung von Schwachstellen in der IT/OT-Umgebung und den Cyberbedrohungen.

4.5 Cybersicherheitsmaßnahmen

4.5.1 Auslegungsgrundsätze

(1) Zum Schutz vor Cyberbedrohungen sind die Schnittstellen von sicherheitsrelevanten MSR-Einrichtungen, der Vernetzungsgrad und die Zugriffsmöglichkeiten auf das für die Verwendung des Arbeitsmittels notwendige Maß zu reduzieren.

(2) Zusätzlich ist auf die ausreichende Widerstandsfähigkeit der betroffenen technischen Systeme der sicherheitsrelevanten MSR-Einrichtung selbst und der IT/OT-Umgebung gegenüber Cyberbedrohungen zu achten.

(3) Methoden und Verfahren sind so festzulegen, dass auch ergonomische Aspekte sowie ihre Akzeptanz bei den Beschäftigten berücksichtigt werden, damit eine Maßnahme der Cybersicherheit keine unsicheren Verhaltensweisen begünstigt (z. B. längere Wechselintervalle und starke Passwörter oder Einsatz von Token anstatt häufige Passwortwechsel).

4.5.2 Anforderungen an Cybersicherheitsmaßnahmen

(1) Zur Sicherstellung der Widerstandsfähigkeit der sicherheitsrelevanten MSR-Einrichtung sind Cybersicherheitsmaßnahmen im erforderlichen Umfang zu implementieren. Die IT/OT-Umgebung ist hierbei im erforderlichen Umfang einzubeziehen. Dies betrifft

1. Verfügbarkeit

   a) von Informationen, die innerhalb einer sicherheitsrelevanten MSR-Einrichtung oder zwischen MSR-Einrichtungen oder der Umgebung ausgetauscht werden und Einfluss auf die Funktion der sicherheitsrelevanten MSR-Einrichtung besitzen, z. B. Schutz gegen Blockierung der Funktion durch DoS-Ereignisse (Denial of Service),

   b) von innerhalb einer sicherheitsrelevanten MSR-Einrichtung gespeicherten Informationen, wie z. B. die Parameter eines Sensors oder das Applikationsprogramm des Logiksystems, die unmittelbar die Integrität der sicherheitsrelevanten MSR-Einrichtung bestimmen,

   c) von Programmen, die für die Funktion der sicherheitsrelevanten MSR-Einrichtung erforderlich sind.

2. Integrität

   a) von Informationen, die innerhalb einer sicherheitsrelevanten MSR-Einrichtung oder zwischen MSR-Einrichtungen oder der Umgebung ausgetauscht werden und

   b) von innerhalb einer sicherheitsrelevanten MSR-Einrichtung gespeicherten Informationen, wie z. B. die Parameter eines Sensors oder das Applikationsprogramm des Logiksystems, die unmittelbar die Integrität der sicherheitsrelevanten MSR-Einrichtung bestimmen,

   c) von anderen gespeicherten Informationen (z. B. Material- und Anlagenspezifikationen, Betriebsanleitungen, Risikoanalysen für Prozessanlagen, Funktionspläne, Systemarchitekturdiagramme), die in einem mittelbaren Zusammenhang mit der Integrität der sicherheitsrelevanten MSR-Einrichtung oder ihrer Funktionsfähigkeit stehen.

3. Vertraulichkeit von Informationen, die kommuniziert werden oder gespeichert sind und Angreifer bei Planung und Ausführung von Angriffen unterstützen. Dies schließt Dokumentationen zu sicherheitsrelevanten Einrichtungen ein, z. B. Grenzwertlisten in Office-Dokumenten.

(2) Insbesondere die folgenden Maßnahmen sind zu berücksichtigen:

1. Segmentierung und Fernzugriffsmöglichkeit

   Segmentierung von Netzwerken ist ein Verfahren, bei dem ein Netzwerk in kleinere, separate Subnetzwerke unterteilt wird, z. B. um Bereiche mit unterschiedlichen Schutzbedarfen oder Funktionen zusammenzufassen (Zonenbildung). Die IT/OT-Umgebung als auch die sicherheitsrelevanten MSR-Einrichtungen müssen abhängig von ihrem Schutzbedarf in entsprechend geschützten Segmenten betrieben werden.

   Um eine unzulässige Beeinflussung der sicherheitsrelevanten MSR-Einrichtung zu verhindern, dürfen Netzwerkteilnehmer Verbindungen nur zu den anderen Netzwerkteilnehmern aufbauen können, zu denen eine Verbindung sicherheitstechnisch erforderlich ist. Dies kann logisch (z. B. mit einem virtuellen lokalen Netz, VLAN) oder bevorzugt physisch (z. B über eine separate Leitung) erfolgen.

   Der Zugriff auf die IT/OT-Umgebung und die sicherheitsrelevante MSR-Einrichtung aus dem Internet und umgekehrt (Fernzugriff) ist mit besonders hohen Risiken verbunden und deshalb technisch zu unterbinden oder mit besonderen Cybersicherheitsmaßnahmen (z. B. zwingende Freigabe des Zugriffs durch den Arbeitgeber) zu schützen.

Der Zugriff auf die sicherheitsrelevante MSR-Einrichtung aus der IT/OT-Umgebung durch automatisierte Dienste, z. B. Auslesen von Statusinformationen, ist rückwirkungsfrei zu initiieren und geeignet abzusichern.

2. Regelungen zu Zugang und Zugriff

   Der Schutz der Komponenten wird u. a. durch die Kontrolle und Restriktion des physischen und logischen Zugangs auf die Komponenten erreicht. Entsprechend sind

   a) den jeweiligen Tätigkeitsprofilen (Rollen) zugeordnete Rechte,

   b) wirksame Authentifizierungsverfahren (Zugangskarten, Passwörter etc.) und

   c) physische Barrieren (Räume, Schränke etc.)

   festzulegen.

3. Härtung von Komponenten

   Die Funktionalität der Hard- und Softwarekomponenten sind auf ein dem Einsatzzweck entsprechendes Mindestmaß zu reduzieren. Die Reduzierung umfasst insbesondere:

   a) Verzicht auf oder Deaktivieren oder Blockieren von nicht benötigten Hardwareschnittstellen,

   b) Verzicht auf oder Entfernen/Deaktivieren von Softwarekomponenten und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe nicht zwingend notwendig sind,

   c) Abschalten oder Unterdrücken von nicht autorisierten Kommunikationsverbindungen, Diensten oder Funktionen (z. B. durch Whitelisting).

4. Unabhängigkeit von sicherheitsrelevanten MSR-Einrichtungen

   Sicherheitsrelevante MSR-Einrichtungen müssen so ausgelegt sein, dass sie durch die IT/OT-Umgebung nicht unzulässig beeinflusst werden können. Dies schließt die teilweise oder vollständige Nichtverfügbarkeit von Systemfunktionen ein (z. B. DoS-Angriff).

   In Einzelfällen können Komponenten von verschiedenen Systemen gemeinsam genutzt werden, d. h. es erfolgt eine Kombination von sicherheitsrelevanten und betrieblichen Funktionen innerhalb einer Komponente, z. B. auf Sensor-/Aktor-Ebene, beim Logiksystem, beim Programmiergerät und bei der IT/OT-Umgebung. Dies ist in der Gefährdungsbeurteilung zu berücksichtigen.

5. Überwachung

   Um cybersicherheitsrelevante 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.

6. Notfallmanagement

   Es müssen Maßnahmen festgelegt werden, wie im Fall einer Kompromittierung der sicherheitsrelevanten MSR-Einrichtung eine Gefährdung von Beschäftigten ausgeschlossen wird. Mindestens sind folgende Szenarien zu berücksichtigen:

   a) Kompromittieren der sicherheitsrelevanten MSR-Einrichtung

b) Kompromittieren von Kommunikationspartnern der sicherheitsrelevanten MSR-Einrichtung (z. B. Verbindungsabbruch, Schadsoftware auf der Engineering Station)

Bei den möglichen Maßnahmen ist

a) die Notwendigkeit eines Notfallplans zur Abschaltung unter Verwendung vorhandener nicht-digitaler Infrastrukturen, z. B. Abschaltmöglichkeiten der Hilfsenergie von Ventilen, unabhängige Not-Aus-Systeme, gezielte Deaktivierung von Steuerausgangssignalen, zu prüfen,

b) vor der Wiederinbetriebnahme sicherzustellen, dass die Sicherheitslücke behoben ist und keine Spuren vom Angriff im System verblieben sind.

4.6 Cybersicherheit bei der Errichtung der sicherheitsrelevanten MSR-Einrichtung

(1) Bei der fachgerechten Auswahl und Installation sicherheitsrelevanter MSR-Einrichtungen einschließlich der verwendeten Komponenten müssen die gemäß Abschnitt 4.4.3 Absatz 2 erforderlichen Cybersicherheitsmaßnahmen vom Arbeitgeber berücksichtigt werden.

(2) Hinsichtlich der erforderlichen Cybersicherheit sind mindestens folgende Punkte sicherzustellen:

1. Die cybersicherheitsrelevanten Einstellparameter von sicherheitsrelevanten MSR-Einrichtungen und Cybersicherheitskomponenten sind vollständig und nach Festlegungen der Gefährdungsbeurteilung konfiguriert,
2. spezifische Herstellervorgaben hinsichtlich der Cybersicherheit für die Installation und den Betrieb der sicherheitsrelevanten MSR-Einrichtung und der Cybersicherheitskomponenten wurden berücksichtigt und
3. die Installation der Cybersicherheitsmaßnahmen weist keine Abweichungen von der Spezifikation auf, die die Cybersicherheitsmaßnahmen selbst und/oder ihre Cybersicherheit beeinträchtigen können.

5 Überprüfung der Wirksamkeit der Cybersicherheitsmaßnahmen

(1) Der Arbeitgeber hat die Wirksamkeit von Schutzmaßnahmen vor der erstmaligen Verwendung eines Arbeitsmittels zu überprüfen (siehe § 4 Absatz 5 BetrSichV und TRBS 1111 Abschnitt 5.7). Ziel der Überprüfung ist die Bestätigung, dass die erforderliche Cybersicherheit der sicherheitsrelevanten MSR-Einrichtung gegeben ist. Die Wirksamkeit von Cybersicherheitsmaßnahmen kann in Anlehnung an TRBS 1111 Abschnitt 4.2 Absatz 7 angenommen werden, wenn

1. Cybersicherheitsmaßnahmen nach der erstellten Spezifikation (vgl. Abschnitt 4.4.3 Absatz 1) geeignet sind, ggf. den Angaben in der Betriebsanleitung entsprechen und funktionsfähig sind und
2. die Beschäftigten über die in diesem Zusammenhang für sie geltenden organisatorischen Cybersicherheitsmaßnahmen (siehe hierzu Abschnitt 8.1) unterwiesen und erforderlichenfalls nach den Angaben in der Betriebsanleitung bzw. der Spezifikation eingearbeitet sind.

Eine Überprüfung der Wirksamkeit der Cybersicherheitsmaßnahmen vor erstmaliger Verwendung gemäß § 4 Absatz 5 BetrSichV ist nicht erforderlich, wenn diese im Rahmen von §§ 14 oder 15 BetrSichV geprüft werden.

(2) In Abhängigkeit der Komplexität des Arbeitsmittels sind bei der Überprüfung der Wirksamkeit der Cybersicherheitsmaßnahmen insbesondere folgende Punkte relevant:

1. Es muss sichergestellt sein, dass die Spezifikationen der Cybersicherheitsmaßnahmen den Anforderungen der Gefährdungsbeurteilung entsprechen.
2. Alle Cybersicherheitskomponenten müssen funktionsfähig sein. Dies schließt die jeweiligen Anwendungsprogramme und Ausrüstungen mit ein, die für eine Überprüfung gebraucht werden.
3. Die Beurteilungskriterien zur Bewertung der Cybersicherheitsmaßnahmen müssen eindeutig festgelegt sein.
4. Für die Überprüfung sind mindestens festzulegen:
   a) die zu den Sicherheitsfunktionen gehörenden Cybersicherheitsmaßnahmen sowie die Fristen ihrer Kontrollen,
   b) Art und Umfang der Überprüfung.

(3) Durch die Überprüfung der Cybersicherheitsmaßnahmen dürfen sich keine Gefährdungen durch unzulässige Rückwirkungen auf die sicherheitsrelevanten MSR-Einrichtungen ergeben. Nach der Überprüfung der Cybersicherheitsmaßnahmen sind die sicherheitsrelevanten MSR-Einrichtungen, ggf. vorhandene zusätzliche Cybersicherheitskomponenten und alle an der Überprüfung beteiligten Arbeitsmittel wieder in den normalen Betriebszustand zurückzuversetzen, sofern temporäre Veränderungen vorgenommen wurden, um die Überprüfung durchführen zu können.

6 Prüfung des Arbeitsmittels vor Inbetriebnahme und Wiederinbetriebnahme nach prüfpflichtiger Änderung nach §§ 14 und 15 BetrSichV

(1) Es ist zu prüfen, ob die vorgesehenen Cybersicherheitsmaßnahmen geeignet und funktionsfähig sind. Dabei sind die zugehörige Dokumentation des Herstellers bezüglich der Cybersicherheitsmaßnahmen (siehe Abschnitt 4.4.2) und die Spezifikation der Cybersicherheitsmaßnahmen (siehe Abschnitt 4.4.3) auf Plausibilität zu prüfen. Prüfinhalte, die im Rahmen eines Konformitätsbewertungsverfahrens geprüft und dokumentiert wurden, müssen nicht erneut geprüft werden (§ 14 Absatz 1 Satz 3 BetrSichV, § 15 Absatz 1 Satz 4 BetrSichV).

(2) Die Gefährdungsbeurteilung kann zu dem Ergebnis kommen, dass Cyberbedrohungen die Sicherheit des Arbeitsmittels gefährden können. In dem Fall müssen die Cybersicherheitsmaßnahmen vor Inbetriebnahme geprüft werden.

(3) Bestandteil der Prüfung ist auch die Feststellung, ob ein Verfahren vorhanden ist, das bei der Festlegung der Cybersicherheitsmaßnahmen anlassbezogen neue Erkenntnisse berücksichtigt, die z. B. aus Cybersicherheitsvorfällen oder dem fortschreitenden Stand der Cybersicherheitstechnik hervorgehen (siehe hierzu auch Abschnitt 8.1).

(4) Die mit der Prüfung des Arbeitsmittels beauftragte Person kann sich die durch die Anwendung eines Managements der Cybersicherheit nach Anhang 1 erzeugten Ergebnisse zu eigen machen.

Eine im Rahmen eines Managements der Cybersicherheit nach Anhang 1 vorhandene Dokumentation erfüllt für sicherheitsrelevante MSR-Einrichtungen die Dokumentationspflichten nach § 3 Absatz 8 BetrSichV.

(5) Wird abweichend von Absatz 3 kein Management der Cybersicherheit nach Anhang 1 angewendet, kann sich die zur Prüfung befähigte Person oder zugelassene Überwachungsstelle die Ergebnisse der Überprüfung der Wirksamkeit der Cybersicherheitsmaßnahmen zu eigen machen, wenn Durchführung und Ergebnis der Überprüfung für sie nachvollziehbar sind.

7 Wiederkehrende Prüfung von Arbeitsmitteln mit sicherheitsrelevanten MSR-Einrichtungen nach §§ 14 und 16 BetrSichV

(1) Bei der wiederkehrenden Prüfung des Arbeitsmittels ist zu prüfen, ob Vorgaben zur regelmäßigen Kontrolle der Funktionsfähigkeit der Cybersicherheitsmaßnahmen sicherheitsrelevanter MSR-Einrichtungen und ihrer IT/OT-Umgebung vorliegen (siehe hierzu § 4 Absatz 5 Satz 3 BetrSichV).

(2) Bei der wiederkehrenden Prüfung des Arbeitsmittels ist zu prüfen, ob die vorgesehenen Cybersicherheitsmaßnahmen weiterhin geeignet und funktionsfähig sind. Die mit der Prüfung des Arbeitsmittels beauftragte Person muss nachvollziehen, wie die geforderte Eignung und Funktionsfähigkeit der Cybersicherheitsmaßnahmen weiterhin erreicht wird. Dabei sind die zugehörige Dokumentation des Herstellers bezüglich der Cybersicherheitsmaßnahmen (siehe Abschnitt 4.4.2) und die Spezifikation der Cybersicherheitsmaßnahmen (siehe Abschnitt 4.4.3) zu berücksichtigen, soweit dies für die wiederkehrende Prüfung erforderlich ist.

(3) Die mit der Prüfung des Arbeitsmittels beauftragte Person kann sich die durch die Anwendung eines Managements der Cybersicherheit nach Anhang 1 erzeugten Ergebnisse zu eigen machen.

(4) Bestandteil der wiederkehrenden Prüfung sind auch die Feststellungen, ob

1. prüfpflichtige Änderungen an sicherheitsrelevanten MSR-Einrichtungen des Arbeitsmittels hinsichtlich der Auswirkungen auf die erforderlichen Cybersicherheitsmaßnahmen bewertet wurden,
2. prüfpflichtige Änderungen an den Cybersicherheitsmaßnahmen hinsichtlich möglicher Auswirkungen auf die sicherheitsrelevanten MSR-Einrichtungen bewertet wurden und
3. anlassbezogene neue Erkenntnisse zu Cyberbedrohungen, z. B. nach bekanntgewordenen Sicherheitslücken oder aus dem fortschreitenden Stand der Cybersicherheitstechnik berücksichtigt, und falls erforderlich Anpassungen an den Cybersicherheitsmaßnahmen vorgenommen wurden.

8 Verwendung und Instandhaltung

8.1 Unterweisung von Beschäftigten

(1) Die Beschäftigten müssen über die für sie geltenden organisatorischen Cybersicherheitsmaßnahmen für sicherheitsrelevante MSR-Einrichtungen und deren Umsetzung unterwiesen werden. Abhängig vom Zuständigkeitsbereich muss dabei Folgendes vermittelt werden:

1. gegen welche Cyberbedrohung die für sie relevanten Cybersicherheitsmaßnahmen schützen
2. die korrekte Reaktion auf Cyberbedrohungen
3. das erforderliche Verhalten im Falle einer Cyberbedrohung mit möglichen Auswirkungen auf sicherheitsrelevante MSR-Einrichtungen (Notfallmanagement)

(2) Beschäftigten, die gemäß § 10 Absatz 2 Satz 2 BetrSichV für Instandhaltungsmaßnahmen unterwiesen werden, muss der richtige Umgang mit und unter welchen Umständen welche Instandhaltungsmaßnahmen durchzuführen sind, z. B. manuelles Herstellen oder Trennen von Verbindungen, Freigeben von Ports, Scans, Updates, vermittelt werden.

8.2 Betrieb, Instandhaltung und regelmäßige Kontrolle der Funktionsfähigkeit der Cybersicherheitsmaßnahmen

(1) Die vorgesehenen Cybersicherheitsmaßnahmen müssen während der gesamten Verwendung des Arbeitsmittels gewährleistet sein. Dazu gehören auch Maßnahmen der Instandhaltung nach § 10 BetrSichV, z. B. regelmäßiger Wechsel von Passwörtern. Für die Zeitdauer ausgeschalteter oder eingeschränkt verfügbarer Cybersicherheitsmaßnahmen, z. B. für den Fall von Fernwartung, sind Ersatzmaßnahmen anzuwenden.

(2) Die Anlässe regelmäßiger Kontrollen der Funktionsfähigkeit der Maßnahmen zur Cybersicherheit sowie deren Art und Umfang werden in der Gefährdungsbeurteilung ermittelt. Bei der Ermittlung ist zu berücksichtigen, dass ggf. automatisierte Kontroll- oder Diagnoseeinrichtungen hierzu genutzt werden können.

(3) Tätigkeiten zur Aufrechterhaltung der Cybersicherheit dürfen nur von fachkundigen, beauftragten und unterwiesenen Beschäftigten oder von vergleichbar qualifizierten Auftragnehmern durchgeführt werden.

(4) Personen, die für Betrieb und Instandhaltung der Cybersicherheitsmaßnahmen verantwortlich sind, müssen insoweit Zugang zu den Spezifikationen der Cybersicherheitsmaßnahmen (z. B. IT-Sicherheitshandbuch) erhalten, wie es für die Aufrechterhaltung der Funktionsfähigkeit der Maßnahmen erforderlich ist.

8.3 Änderungen an sicherheitsrelevanten MSR-Einrichtungen mit Auswirkungen auf die Cybersicherheit oder an Cybersicherheitsmaßnahmen

(1) Der Arbeitgeber hat zu beurteilen, ob es sich bei einer Änderung um eine prüfpflichtige Änderung im Sinne der BetrSichV handelt (§ 10 Absatz 5 Satz 3 BetrSichV). Bei der Beurteilung einer Änderung sind auch die Aspekte der Cybersicherheit mit zu berücksichtigen. Bei einer prüfpflichtigen Änderung sind die geänderten Teile nach Abschnitt 6 zu prüfen.

(2) Die folgenden Änderungen an Cybersicherheitsmaßnahmen sind keine prüfpflichtige Änderung im Sinne der BetrSichV:

1. Anpassungen an bestehenden Cybersicherheitsmaßnahmen wie Parameteränderungen oder Updates, sofern die Anpassungen der Aufrechterhaltung der Wirksamkeit dienen,
2. funktionsidentischer Austausch von Komponenten,

wenn der Arbeitgeber die ordnungsgemäße Montage der Hardware sowie die korrekte Installation oder Modifikation der Software durch fachkundige Personen und geeignete organisatorische Abläufe sicherstellt.

(3) Im Falle einer prüfpflichtigen Änderung an sicherheitsrelevanten MSR-Einrichtungen muss der Arbeitgeber ermitteln, ob die Cybersicherheitsmaßnahmen nach Abschnitt 4 neu festzulegen sind.

(4) Eine prüfpflichtige Änderung an Cybersicherheitsmaßnahmen erfordert eine Bewertung nach Abschnitt 4 hinsichtlich ihrer Auswirkungen auf den Schutz der sicherheitsrelevanten MSR-Einrichtungen vor Cyberbedrohungen sowie auf die Rückwirkungsfreiheit (z. B. Beeinflussung der Datenübertragung der sicherheitsrelevanten MSR-Einrichtungen).

(5) Änderungen an Cybersicherheitsmaßnahmen sind zu dokumentieren. Dabei ist eine Kontrolle der Funktionsfähigkeit (§ 4 Absatz 5 BetrSichV) durchzuführen.

8.4 Außerbetriebnahme der sicherheitsrelevanten MSR-Einrichtung

(1) Werden Cybersicherheitsmaßnahmen dauerhaft außer Betrieb genommen (z. B. bei Wegfall der Gefährdung), ist sicherzustellen, dass die Außerbetriebnahme rückwirkungsfrei auf die verbleibenden Cybersicherheitsmaßnahmen erfolgt.

(2) Ausgesonderte sicherheitsrelevante MSR-Einrichtungen oder ihre IT-Umgebung sind so zu entsorgen, dass ein Verlust der Vertraulichkeit von Informationen, z. B. gespeicherte Passwörter auf einem Speicherchip im Elektroschrott, keine Auswirkungen auf die Cybersicherheit für die Verwendung vorhandener sicherheitsrelevanter MSR-Einrichtungen haben kann.

(3) Die Außerbetriebnahme ist zu dokumentieren.

(4) Die Beschäftigten sind über die geänderte Situation zu unterweisen.

Anhang 1

Management der Cybersicherheit

A1.1 Anwendungsbereich

Dieser Anhang gilt für die erforderlichen Maßnahmen des Arbeitgebers, der ein Management der Cybersicherheit zum Erreichen der Anforderungen der BetrSichV im Betrieb einführen und aufrechterhalten will.

A1.2 Anforderungen an das Management der Cybersicherheit

A1.2.1 Allgemeines

(1) Ein Management der Cybersicherheit kann separat oder als Teil eines Managements der funktionalen Sicherheit bzw. als Teil eines Informationssicherheitsmanagements implementiert werden.

(2) Wenn der Arbeitgeber ein Management der Cybersicherheit einführt, müssen insbesondere die folgenden Schritte durchgeführt bzw. geeignete Regelungen festgelegt und die zugehörigen Inhalte dokumentiert werden (vgl. z. B. BSI 200-2):

1. Initiierung des Informationssicherheitsprozesses
2. Erstellung einer Leitlinie zur Cybersicherheit auf Basis der sicherheitstechnischen Anforderungen
3. Organisation des Sicherheitsprozesses
4. Erstellung einer Cybersicherheitskonzeption
5. Umsetzung der Cybersicherheitskonzeption und Überprüfung der Wirksamkeit der Cybersicherheitsmaßnahmen
6. Aufrechterhaltung des Cybersicherheitsniveaus und Verbesserung

(3) Wenn der Arbeitgeber ein Management der Cybersicherheit einführt, muss er dieses über den gesamten Sicherheitslebenszyklus etablieren und regelmäßig auf seine Wirksamkeit überprüfen.

(4) Für das Management der Cybersicherheit sind die Festlegung der beteiligten Personen und deren erforderliche Fachkunde, der Verantwortlichkeiten und der zu nutzenden Werkzeuge und Methoden, der Dokumentation sowie qualitätssichernde Maßnahmen und deren dokumentierte Umsetzung erforderlich.

A1.2.2 Wirksamkeit des Managements der Cybersicherheit

Bei Verwendung eines Managements der Cybersicherheit ist zum Nachweis der Wirksamkeit regelmäßig ein Audit durchzuführen, mit dem der Arbeitgeber überprüft, ob die Maßnahmen und Verfahren zum Erreichen der Cybersicherheit wirksam durchgeführt wurden und angemessen sind.

Anhang 2

Erläuterungen und Beispiele für erforderliche Cybersicherheitsmaßnahmen

A2.1 Allgemeine Hinweise

(1) Diese TRBS beschreibt Anforderungen an die Ermittlung und Festlegung erforderlicher Cybersicherheitsmaßnahmen von sicherheitsrelevanten MSR-Einrichtungen. Da langjährige Erfahrungen zur Cybersicherheit bei vielen Arbeitgebern noch nicht vorliegen können, sollen diese Anforderungen durch die nachfolgenden Erläuterungen und Beispiele konkretisiert und der Arbeitgeber bei der Umsetzung unterstützt werden.

(2) Durch Cyberbedrohungen ergeben sich zusätzliche Wege zum Auftreten von Gefährdungen. Ergänzend zu den Betrachtungen der funktionalen Sicherheit, die berücksichtigen, dass durch zufällige oder systematische Fehler Gefährdungen auftreten können, sind bei Cyberbedrohungen vorsätzliche Handlungen zu berücksichtigen, die zu bisher nicht betrachteten Kombinationen von Fehlern und schlussendlich zum Auftreten von Gefährdungen führen können. Dieses muss durch ergänzende Betrachtungen und die Festlegung geeigneter Cybersicherheitsmaßnahmen verhindert werden.

(3) Diese TRBS beschreibt den Prozess zur Ermittlung, Umsetzung und Prüfung erforderlicher Cybersicherheitsmaßnahmen für sicherheitsrelevante MSR-Einrichtungen. Für den sicheren Betrieb eines Arbeitsmittels kann es jedoch unter Umständen nicht ausreichend sein, die Umsetzungen von Cybersicherheitsmaßnahmen auf sicherheitsrelevante MSR-Einrichtungen zu beschränken. Insbesondere ist dies dann der Fall, wenn im Rahmen der Gefährdungsbeurteilung bereits darüberhinausgehende Einrichtungen für den sicheren Betrieb des Arbeitsmittels als erforderlich ermittelt wurden und diese digitale Bestandteile aufweisen. Im Rahmen der Gefährdungsbeurteilung ist deshalb zu ermitteln, ob und wenn ja welche weiteren Teile des Arbeitsmittels für dessen sichere Verwendung geschützt werden müssen (siehe hierzu Abschnitt 1 Absatz 1 Satz 3 dieser TRBS). Alle Einrichtungen, für die Cybersicherheitsmaßnahmen als erforderlich angesehen werden, werden als schutzbedürftige Einrichtungen bezeichnet. Insbesondere können hierzu ergänzend zu sicherheitsrelevanten MSR-Einrichtungen zählen:

1. sicherheitsrelevante Einrichtungen, die keine MSR-Einrichtung sind (z. B. Notrufeinrichtungen, Notbefehlseinrichtungen), soweit eine Kompromittierung durch Cyberbedrohungen möglich ist,
2. Die IT/OT-Umgebung (z. B. Service-/Programmiergeräte, Gateways) der vorgenannten Systeme, die Einfluss auf die Cybersicherheit der vorgenannten Systeme haben,
3. nicht sicherheitsrelevante MSR-Einrichtungen (z. B. PLT-Betriebseinrichtungen), bei denen durch die Kompromittierung ihrer Funktion durch Cyberbedrohungen auch unter Berücksichtigung von Wechselwirkungen mit anderen Teilen von Arbeitsmitteln eine relevante Gefährdung von Beschäftigten und anderen Personen im Gefahrenbereich verursacht werden kann.

(4) Die Behandlung von Cyberbedrohungen gemäß dieser TRBS ist als Teil der Gefährdungsbeurteilung zu verstehen. Da sich für die Erstellung der Gefährdungsbeurteilung in vielen Branchen und Unternehmen bereits Standards etabliert haben und die Dokumentation zur Behandlung von Cyberbedrohungen (siehe hierzu Abschnitt 3.4) umfangreich ausfallen kann, ist es ausreichend, in der Gefährdungsbeurteilung auf eine unterlagerte Dokumentation zur Behandlung von Cyberbedrohungen zu verweisen.

Hinweis: Bei der Bewertung von Cyberbedrohungen ist die Nutzung von Statistiken bisher bekannt gewordener Vorfälle nicht ausreichend

(5) Bei der Anwendung dieser TRBS sind Cyberbedrohungen durch die folgenden Akteure zu berücksichtigen:

1. nicht zutritts-/zugangsberechtigte Personen, die über dauerhafte oder temporäre datentechnische Verbindungen aus der Ferne agieren,
2. zutritts-/zugangsberechtigte Personen, die durch vernünftigerweise vorhersehbare Fehlanwendung Cyberangriffe unterstützen oder erst ermöglichen (z. B. unzulässige Verwendung eines USB-Sticks).

Ob ergänzend hierzu Cyberbedrohungen durch kriminelle Handlungen zutritts-/zugangsberechtigter Personen zu berücksichtigen sind, ist durch den Arbeitgeber unter Berücksichtigung der möglichen Auswirkungen von Cyberbedrohungen zu bewerten.

(6) Sollen bestehende Managementsysteme, Strukturen oder Prozesse zur Cybersicherheit für die Erfüllung dieser TRBS genutzt werden, sind insbesondere folgende Fragen zu beantworten:

1. Erfassen die bestehenden Vorgaben alle Einrichtungen, für die Cybersicherheitsmaßnahmen als erforderlich angesehen werden, um das Auftreten von Gefährdungen zu verhindern (siehe auch Absatz 3 Satz 4)?
2. Sind die festgelegten Cybersicherheitsmaßnahmen ausreichend, um den Schutz von Beschäftigten und bei überwachungsbedürftigen Anlagen auch von anderen Personen im Gefahrenbereich anforderungsgerecht sicherzustellen?

Das Ergebnis ist nachvollziehbar zu dokumentieren.

A2.2 Beispiele

Die nachfolgend dargestellten Beispiele bieten eine Orientierung für den als erforderlich anzusehenden Umfang an Cybersicherheitsmaßnahmen gemäß Abschnitt 4.5.2 dieser TRBS nach dem Stand der Technik.

Die Beispiele beschreiben Szenarien von Arbeitsmitteln, die hinsichtlich des Umfangs der vorhandenen Schnittstellen gemäß Abschnitt 1 Absatz 4 und des Grads der Vernetzung unterschiedlich gestaltet sind. Die behandelten Beispiele unterscheiden sich in ihrem Vernetzungsgrad wie folgt:

Tab. A2.1: Beispiele für erforderliche Cybersicherheitsmaßnahmen

	externe Schnittstellen	**Drahtgebundene Schnittstelle ohne weitere Vernetzung**	**drahtlose Schnittstelle ohne weitere Vernetzung**	**Drahtgebundene Schnittstelle und Vernetzung im Inselbetrieb**	**Drahtgebundene oder drahtlose Überwachung über OT-Netz**	**Drahtgebundene oder drahtlose Steuerung über OT-Netz**
A2.2.1	-	-	-	-	-	-
A2.2.2	x	x	-	-	-	-
A2.2.3	x	-	x	-	-	-
A2.2.4	x	-	-	x	-	-
A2.2.5	x	-	-	-	x	-

A2.2.6	x	-	-	-	x	x

Für die Beispiele wurden Annahmen getroffen, um die Komplexität zu reduzieren. Die Beispiele ersetzen nicht die erforderliche individuelle Betrachtung jedes einzelnen Arbeitsmittels. In den Beispielen werden keine internen Schnittstellen zwischen verschiedenen Teilen eines Arbeitsmittels (z. B. Verbindungen zwischen Sensor – Logik – Aktor) sicherheitsrelevanter MSR-Einrichtungen betrachtet.

Hinweis: Diese Schnittstellen müssen, sofern sie nicht bereits durch den Hersteller betrachtet wurden, separat vom Arbeitgeber behandelt werden.

Im Beispiel A2.2.5 wird neben der zusätzlichen Vernetzung zu weiteren Diensten auch angenommen, dass die Not-Befehlseinrichtung kompromittierbar ist.

A2.2.1 „Arbeitsmittel ohne externe Schnittstellen“

A2.2.1.1 Beschreibung

Das Arbeitsmittel besitzt keine drahtgebundenen oder drahtlosen Schnittstellen (beispielsweise USB, Ethernet oder Bluetooth), durch die das Arbeitsmittel erreicht werden kann (im Weiteren „externe Schnittstellen“ genannt).

Abb. A2.1 Arbeitsmittel ohne externe Schnittstellen

Ein Ändern von Parametern ist lokal am Arbeitsmittel möglich.

A2.2.1.2 Bewertung

Das Arbeitsmittel fällt nicht in den Anwendungsbereich dieser TRBS. Aufgrund der fehlenden externen Schnittstellen sind keine Cyberbedrohungen möglich.

A2.2.2 „Arbeitsmittel mit drahtgebundenen Schnittstellen ohne weitere Vernetzung“

A2.2.2.1 Beschreibung

Das Arbeitsmittel besitzt nur drahtgebundene externe Schnittstellen. Die Schnittstellen können nur lokal genutzt werden. Das Arbeitsmittel wird nicht vernetzt betrieben.

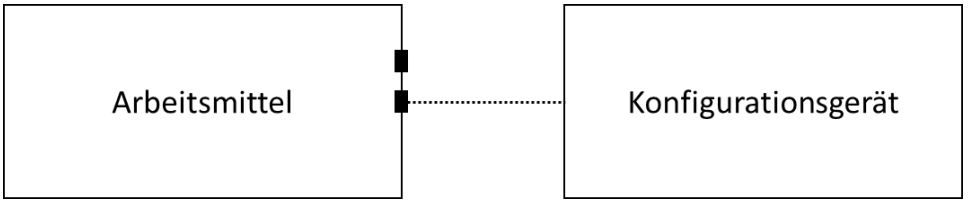

Abb. A2.2 Arbeitsmittel mit drahtgebundenen Schnittstellen ohne weitere Vernetzung

Ein Ändern von Parametern ist lokal am Arbeitsmittel und über die Schnittstellen möglich. Der Zugriff auf die externe Schnittstelle erfolgt mittels eines definierten Konfigurationsgeräts.

Das Arbeitsmittel verfügt über eine nicht-kompromittierbare Not-Befehlseinrichtung (z. B. Not-Aus- oder Not-Halt-Schaltung, Trennung der Energieversorgung).

A2.2.2.2 Bewertung

Das Arbeitsmittel fällt wegen der vorhandenen externen Schnittstellen in den Anwendungsbereich dieser TRBS.

Das Konfigurationsgerät muss mitbetrachtet werden, da eine Kompromittierung des Konfigurationsgeräts die Sicherheitsfunktion beeinträchtigen kann. Es können beispielsweise sicherheitsrelevante Parameter geändert werden.

Segmentierung

Es wird sichergestellt, dass das Arbeitsmittel und das Konfigurationsgerät nicht dauerhaft verbunden sind.

Regelungen für Zugang und Zugriff

Der Zugang und Zugriff für die externen Schnittstellen am Arbeitsmittel und für das Konfigurationsgerät wird auf berechtigte Personen eingeschränkt.

Die Regelungen bezüglich des Konfigurationsgeräts werden auch gegenüber zutritts-/zugangsberechtigten Dritten (z. B. Wartungsdienstleistern) umgesetzt.

Härtung von Komponenten

Nicht benötigte Hardwareschnittstellen werden deaktiviert oder blockiert.

Die Regelungen für das Konfigurationsgerät werden auch gegenüber zutritts-/zugangsberechtigten Dritten (z. B. Wartungsdienstleistern) umgesetzt.

Unabhängigkeit von sicherheitsrelevanten MSR-Einrichtungen

Die nach dieser TRBS geforderte Unabhängigkeit der sicherheitsrelevanten MSR-Einrichtungen wurde durch den Hersteller berücksichtigt und wird durch den Arbeitgeber aufrechterhalten.

Überwachung

Die Integrität der sicherheitsrelevanten MSR-Einrichtung und des Konfigurationsgeräts wird regelmäßig kontrolliert.

Die Verwendung des Konfigurationsgeräts am Arbeitsmittel kann nachvollzogen werden.

Die Regelungen bezüglich des Konfigurationsgeräts werden auch gegenüber zutritts-/zugangsberechtigten Dritten (z. B. Wartungsdienstleistern) umgesetzt.

Notfallmanagement

Wenn eine Kompromittierung erkannt wird, wird das Arbeitsmittel durch die nicht-kompromittierbare Not-Befehlseinrichtung in den sicheren Zustand versetzt.

Vor der Wiederinbetriebnahme ist sicherzustellen, dass keine Spuren vom Angriff im System verblieben sind.

A2.2.3 „Arbeitsmittel mit drahtlosen Schnittstellen ohne weitere Vernetzung“

A2.2.3.1 Beschreibung

Das Arbeitsmittel besitzt als externe Schnittstelle ausschließlich eine drahtlose Verbindung zu einer Bedienstation zur Steuerung des Arbeitsmittels (Inselbetrieb). Programmierungen oder Parametrierungen sind über die Bedienstation oder die drahtlose Verbindung nicht möglich.

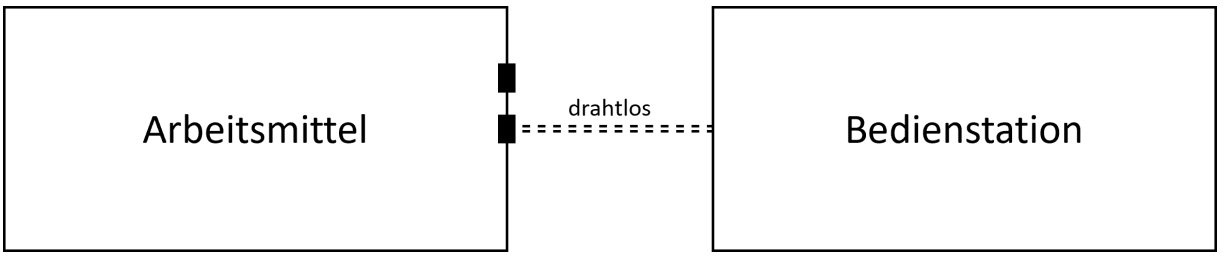

Abb. A2.3 Arbeitsmittel mit drahtlosen Schnittstellen ohne weitere Vernetzung

A2.2.3.2 Bewertung

Das Arbeitsmittel fällt wegen der für den Nutzer vorhandenen Schnittstelle unter den Anwendungsbereich dieser TRBS.

Die Bedienstation und die drahtlose Verbindung müssen mitbetrachtet werden, da eine Kompromittierung die Sicherheitsfunktion beeinträchtigen kann. Besitzt das Arbeitsmittel zusätzlich eine Konfigurationsschnittstelle, sind für diese die Vorgaben gemäß Beispiel A2.2.2 anzuwenden.

Segmentierung

Es ist durch den Hersteller bestätigt, dass mit der drahtlosen Verbindung nur das Arbeitsmittel und die Bedienstation verbunden sein können.

Regelungen für Zugang und Zugriff

Ein Verbindungsaufbau zum Arbeitsmittel ist ausschließlich über die zugehörige Bedienstation möglich. Die Datenkommunikation erfolgt verschlüsselt.

Die Bedienstation wird vor dem Zugriff Unbefugter geschützt. Dies erfolgt durch physischen Schutz (z. B. verschlossene Aufbewahrung) oder durch logischen Schutz (z. B. PIN/Passwort).

Härtung von Komponenten

Nicht benötigte Hardwareschnittstellen werden am Arbeitsmittel und der Bedienstation deaktiviert oder blockiert.

Der Arbeitgeber konfiguriert das Arbeitsmittel und die Bedienstation so, dass ein unberechtigter Zugriff verhindert wird. Dies erfordert unter anderem eine sichere Authentifizierung.

Die Regelungen für das Arbeitsmittel und die Bedienstation werden auch gegenüber zutritts-/zugangsberechtigten Dritten (z. B. Wartungsdienstleistern) umgesetzt.

Unabhängigkeit von sicherheitsrelevanten MSR-Einrichtungen

Die nach dieser TRBS geforderte Unabhängigkeit der sicherheitsrelevanten MSR-Einrichtungen wurde durch den Hersteller berücksichtigt.

Überwachung

Die Funktionsfähigkeit der sicherheitsrelevanten MSR-Einrichtung wird regelmäßig kontrolliert.

Notfallmanagement

Wenn eine Kompromittierung erkannt wird, wird das Arbeitsmittel durch die nicht-kompromittierbare Not-Befehlseinrichtung in den sicheren Zustand versetzt.

Vor der Wiederinbetriebnahme ist sicherzustellen, dass keine Spuren vom Angriff im System verblieben sind.

A2.2.4 „Arbeitsmittel mit drahtgebundenen Schnittstellen und Vernetzung im Inselbetrieb“

A2.2.4.1 Beschreibung

Das Arbeitsmittel besitzt externe Schnittstellen. Das Arbeitsmittel ist über ein arbeitsmittelbezogenes Netzwerk mit dem Konfigurationsgerät und einer Bedienstation mit Touch-Display verbunden (Inselbetrieb).

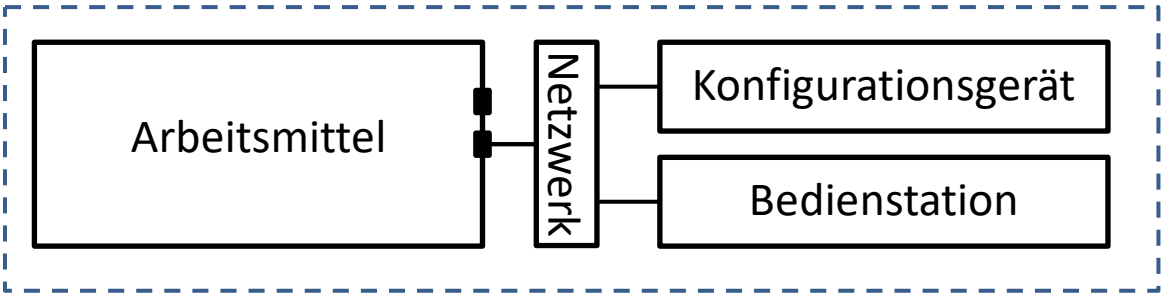

Abb. A2.4 Arbeitsmittel mit drahtgebundenen Schnittstellen und Vernetzung im Inselbetrieb

Eine Änderung von Parametern ist lokal am Arbeitsmittel oder über das Netzwerk mittels des Konfigurationsgerätes und der Bedienstation vorgesehen.

Das Arbeitsmittel verfügt über eine nicht-kompromittierbare Not-Befehlseinrichtung.

A2.2.4.2 Bewertung

Das Arbeitsmittel fällt wegen der für den Nutzer vorhandenen Schnittstellen unter den Anwendungsbereich dieser TRBS.

Das Konfigurationsgerät, die Bedienstation und das Netzwerk müssen mitbetrachtet werden, da eine Kompromittierung die Sicherheitsfunktion beeinträchtigen kann.

Segmentierung

Es wird sichergestellt, dass sich in dem Netzwerk nur das Arbeitsmittel, das Konfigurationsgerät und die Bedienstation befinden.

Regelungen für Zugang und Zugriff

Der Zugang und Zugriff für die externen Schnittstellen am Arbeitsmittel, für das Konfigurationsgerät und die Netzwerkkomponenten wird auf berechtigte Personen eingeschränkt. Dies erfordert unter anderem eine sichere Authentifizierung.

Die Regelungen für Arbeitsmittel, Konfigurationsgerät, Bedienstation und Netzwerkkomponenten werden auch gegenüber zutritts-/zugangsberechtigte Dritten (z. B. Wartungsdienstleistern) umgesetzt.

Härtung von Komponenten

Nicht benötigte Hardwareschnittstellen werden am Arbeitsmittel, Konfigurationsgerät, Bedienstation und Netzwerkkomponenten deaktiviert oder blockiert.

Der Arbeitgeber konfiguriert das Arbeitsgerät, Konfigurationsgerät, Bedienstation und Netzwerkkomponenten so, dass ein unberechtigter Zugriff verhindert wird. Dies kann z. B. durch Deaktivierungen erfolgen.

Die Regelungen für Arbeitsmittel, Konfigurationsgerät, Bedienstation und Netzwerkkomponenten werden auch gegenüber zutritts-/zugangsberechtigten Dritten (z. B. Wartungsdienstleistern) umgesetzt.

Unabhängigkeit von sicherheitsrelevanten MSR-Einrichtungen

Die nach dieser TRBS geforderte Unabhängigkeit der sicherheitsrelevanten MSR-Einrichtungen wurde durch den Hersteller berücksichtigt.

Überwachung

Die Integrität der sicherheitsrelevanten MSR-Einrichtung, der Bedienstation und des Konfigurationsgeräts wird regelmäßig kontrolliert.

Die Verwendung des Konfigurationsgeräts am Arbeitsmittel kann nachvollzogen werden.

Die Regelungen für das Konfigurationsgerät werden auch gegenüber zutritts-/zugangsberechtigte Dritten (z. B. Wartungsdienstleistern) umgesetzt.

Notfallmanagement

Wenn eine Kompromittierung erkannt wird, wird das Arbeitsmittel durch die nicht-kompromittierbare Not-Befehlseinrichtung in den sicheren Zustand versetzt.

Vor der Wiederinbetriebnahme ist sicherzustellen, dass keine Spuren vom Angriff im System verblieben sind.

A2.2.5 „Arbeitsmittel mit drahtgebundener oder drahtloser Überwachung über OT-Netz“

A2.2.5.1 Beschreibung

Das Arbeitsmittel besitzt externe Schnittstellen. Das Arbeitsmittel ist dauerhaft über ein Netzwerk mit dem Konfigurationsgerät und einer Bedienstation mit Touch-Display verbunden.

Das Arbeitsmittel sendet Statusinformationen über das Netzwerk an weitere Dienste.

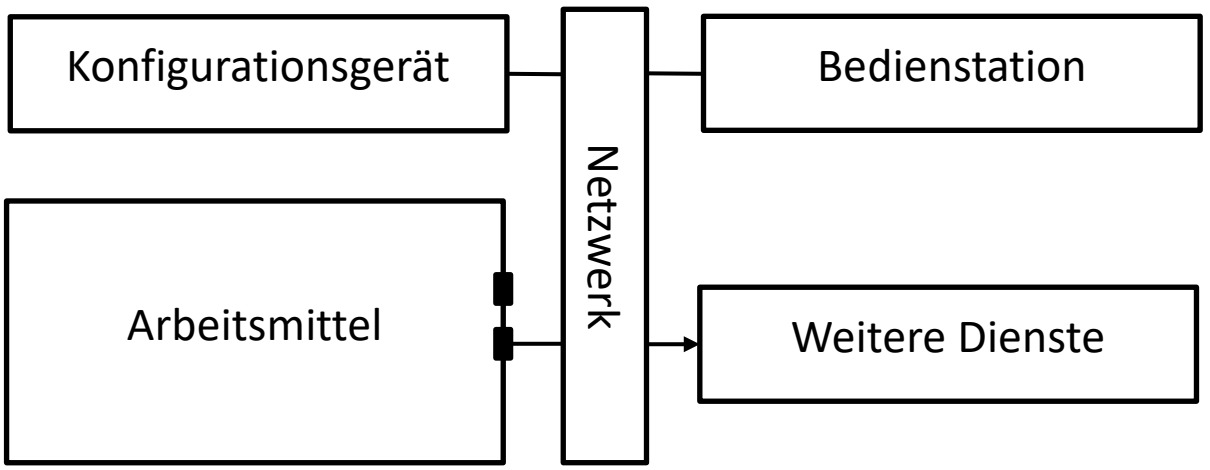

Abb. A2.5 Arbeitsmittel mit drahtgebundener oder drahtloser Überwachung über OT-Netz

Ein Ändern von Parametern ist lokal am Arbeitsmittel oder über die externen Schnittstellen möglich. Weitere Dienste können beispielweise ERP-Systeme oder auch andere Arbeitsmittel sein, die eigenständige Systeme darstellen, jedoch auf die Informationen des Arbeitsmittels angewiesen sind.

Das Arbeitsmittel verfügt über einen digitalen Not-Aus/Not-Halt, der auf die sicherheitsrelevante MSR-Einrichtung einwirkt (d. h., dass die Not-Befehlseinrichtung kompromittierbar ist).

A2.2.5.2 Bewertung

Segmentierung

Der Arbeitgeber stellt sicher, dass

1. der Zugriff auf das Arbeitsmittel über das Netzwerk auf das Konfigurationsgerät und die Bedienstation eingeschränkt sind und
2. das Arbeitsmittel Informationen an die weiteren Dienste senden kann, jedoch keine Informationen oder Befehle weiterer Dienste entgegennehmen kann, z. B. durch Einsatz einer Datendiode.

Regelungen für Zugang und Zugriff

Der Arbeitgeber schränkt für das Arbeitsmittel, die externen Schnittstellen am Arbeitsmittel, das Konfigurationsgerät und die Netzwerkkomponenten den Zugang und Zugriff auf berechtigte Personen ein.

Härtung von Komponenten

Nicht benötigte Hardwareschnittstellen werden am Arbeitsmittel, Konfigurationsgerät, Bedienstation und Netzwerkkomponenten deaktiviert oder blockiert.

Der Arbeitgeber konfiguriert das Arbeitsgerät, Konfigurationsgerät, Bedienstation und Netzwerkkomponenten so, dass ein unberechtigter Zugriff verhindert wird. Dies erfordert unter anderem eine sichere Authentifizierung.

Die Regelungen für Arbeitsmittel, Konfigurationsgerät, Bedienstation und Netzwerkkomponenten werden auch gegenüber zutritts-/zugangsberechtigten Dritten (z. B. Wartungsdienstleistern) umgesetzt.

Unabhängigkeit von sicherheitsrelevanten MSR-Einrichtungen

Die nach dieser TRBS geforderte Unabhängigkeit der sicherheitsrelevanten MSR-Einrichtungen wurde durch den Hersteller berücksichtigt.

Überwachung

Die Integrität der sicherheitsrelevanten MSR-Einrichtung, der Bedienstation und des Konfigurationsgeräts wird regelmäßig kontrolliert.

Die Verwendung des Konfigurationsgeräts am Arbeitsmittel kann nachvollzogen werden.

Die Regelungen für das Konfigurationsgerät werden auch gegenüber zutritts-/zugangsberechtigten Dritten (z. B. Wartungsdienstleistern) umgesetzt.

Der Arbeitgeber überwacht zusätzlich, dass keine unerlaubte Kommunikation zwischen dem Arbeitsmittel und den weiteren Diensten stattfindet.

Notfallmanagement

Bei einer Kompromittierung einer sicherheitsrelevanten MSR-Einrichtung oder von deren Kommunikationspartnern durch eine Schadsoftware können folgende Maßnahmen erforderlich sein:

1. Anwendung eines Notfallplans (siehe hierzu Abschnitt 4.5.2 Absatz 2 Nummer 6 Buchstabe a),
2. gezielte Deaktivierung der Kommunikation von und zu kompromittierten Einrichtungen und
3. Sicherstellung vor der Wiederinbetriebnahme, dass die Sicherheitslücke behoben ist und keine Spuren vom Angriff im System verblieben sind.

Beschäftigte sind zum erforderlichen Verhalten und zum Notfallplan zu unterweisen.

A2.2.6 „Arbeitsmittel mit drahtgebundener oder drahtloser Steuerung über OT-Netz“

A2.2.6.1 Beschreibung

Das Arbeitsmittel besitzt externe Schnittstellen. Das Arbeitsmittel ist dauerhaft über ein Netzwerk mit dem Konfigurationsgerät und einer Bedienstation mit Touch-Display verbunden.

Das Arbeitsmittel sendet Statusinformationen über das Netzwerk an weitere Dienste.

Einzelne „Weitere Dienste“ haben Zugriff auf die Konfiguration des Arbeitsmittels.

Schnittstellen einzelner Teilkomponenten des Arbeitsmittels sind extern zugänglich.

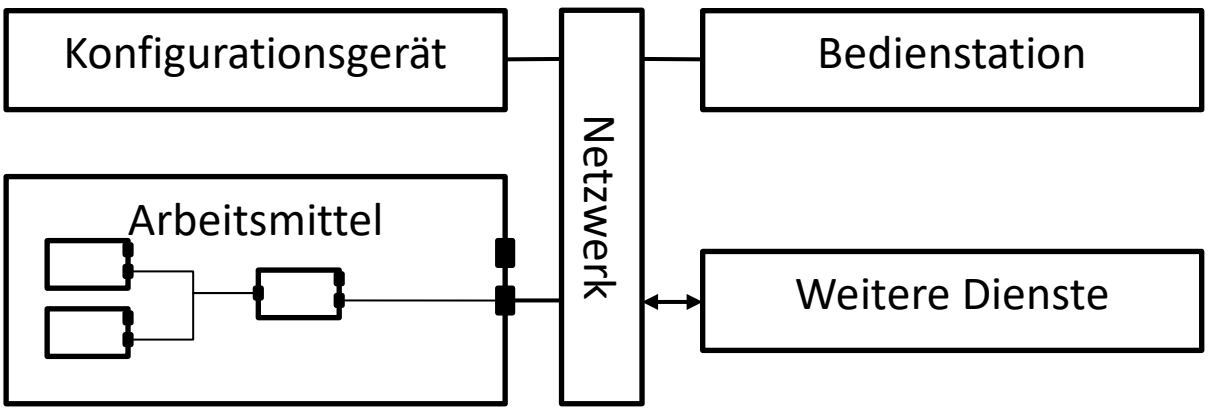

Abb. A2.6 Arbeitsmittel mit drahtgebundener oder drahtloser Steuerung über OT-Netz

Ein Ändern von Parametern ist lokal am Arbeitsmittel oder externe Schnittstellen möglich. Das Konfigurationsgerät ist ein Laptop.

A2.2.6.2 Bewertung

Das Arbeitsmittel fällt wegen der für den Nutzer vorhandenen digitalen Schnittstellen unter den Anwendungsbereich dieser TRBS.

Aufgrund der Komplexität und der Variabilität möglicher Cybersicherheitskonzepte bei diesem Beispiel muss eine systemspezifische detaillierte Betrachtung auf Basis von etablierten Verfahren zur Beurteilung von Cybersicherheitsrisiken durchgeführt werden. Hierfür können beispielsweise die ISO 27001/2, die IEC/ISO 62443-2-1, die Vorgehensweise des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder andere gleichwertige Vorgehensweisen nach dem Stand der Technik herangezogen werden.

A2.3 Prüfung und Kontrollen von Cybersicherheitsmaßnahmen

A2.3.1 Prüfungen von Cybersicherheitsmaßnahmen

(1) Die Prüfungen der der Cybersicherheitsmaßnahmen gemäß Abschnitt 6 und 7 dieser TRBS werden mit dem Ziel durchgeführt, deren Eignung und die Funktionsfähigkeit bestätigen zu können, und ist als Teilprüfung der Prüfung des Arbeitsmittels zu sehen.

(2) Im Rahmen der Prüfung der Eignung ist zu prüfen, ob ein Sollzustand festgelegt wurde, der hinsichtlich der Cybersicherheitsmaßnahmen dem Stand der Technik entspricht. Da die Festlegung eines anforderungsgerechten Sollzustands der Cybersicherheit Ergebnis eines Prozesses ist (vgl. Abschnitt 4), ist von einer Eignung der Cybersicherheitsmaßnahmen auszugehen, wenn alle Schritte gemäß Abschnitt 4 nachvollziehbar korrekt ausgeführt wurden. Insbesondere folgende Aspekte sind hierbei zu prüfen:

1. Sind die sicherheitsrelevanten MSR-Einrichtungen und weitere schutzbedürftige Einrichtungen erfasst und dokumentiert?
2. Wurden Auswirkungen eines möglichen Verlusts der Integrität (siehe hierzu Abschnitt 4.5.2 Absatz 1 Nummer 2) und Verfügbarkeit (siehe hierzu Abschnitt 4.5.2 Absatz 1 Nummer 1) der schutzbedürftigen Systeme durch Cyberbedrohungen ermittelt und die ggf. hierdurch entstehenden Gefährdungen für Sicherheit und Gesundheit von Beschäftigten und ggf. anderen Personen im Gefahrenbereich bewertet?

   Hinweis 1: Die Bewertung der möglichen Auswirkungen erfolgt ohne Berücksichtigung von bereits bestehenden oder geplanten Cybersicherheitsmaßnahmen.

   Hinweis 2: Überwachungsbedürftige Anlagen sind gemäß § 2 Nummer 1 Buchstabe b) ÜAnlG solche Anlagen, von denen beim Betrieb erhebliche Risiken für die Sicherheit und die Gesundheit insbesondere Beschäftigter ausgehen kann.
3. Sind nachvollziehbare Festlegungen von Cybersicherheitsmaßnahmen für die Einrichtungen getroffen, um die geforderte Funktionsfähigkeit sicherzustellen, und sind sie plausibel?
4. Gibt es eine dokumentierte Festlegung der erforderlichen Maßnahmen der Cybersicherheit (z. B. IT-Sicherheitskonzept und IT-Sicherheitsspezifikation)? Wenn ja, wurden die Standardmaßnahmen aus Abschnitt 4.5.2 Absatz 2 berücksichtigt?
5. Sind Herstellervorgaben vorhanden und wenn ja, wurden diese berücksichtigt?
6. Gibt es Verfahren zur Aufrechterhaltung des Cybersicherheitsniveaus (z. B. Aufspielen von Software-Updates oder sicherheitsrelevanten Patches)?
7. Wurden die Vorgaben für die organisatorischen Cybersicherheitsmaßnahmen in Betriebsanweisungen umgesetzt?
8. Wurde die mögliche Beeinträchtigung der Funktion der schutzbedürftigen Systeme durch die festgelegten Cybersicherheitsmaßnahmen und deren Umsetzung betrachtet (Rückwirkungsfreiheit)?

9. Sind ausreichende Festlegungen zur Prüfung und zur Kontrolle der Funktionsfähigkeit der Cybersicherheitsmaßnahmen getroffen worden?

(3) Die Prüfung der Funktionsfähigkeit beinhaltet insbesondere,

1. ob der Ist-Zustand dem Schutzkonzept der Cybersicherheit und der Spezifikation der Cybersicherheit entspricht,
2. ob Prüfungen gemäß den Festlegungen nach Abschnitt 3.4 zu Prüfungen der Cybersicherheitsmaßnahmen umgesetzt wurden und
3. ob die organisatorischen Cybersicherheitsmaßnahmen umgesetzt wurden.

Hinweis: Im Rahmen dieser Prüfungen können sich Ergebnisse des Managements der Cybersicherheit des Arbeitgebers gemäß Anhang 1 zu eigen gemacht werden (vgl. Abschnitt 6 Absatz 4 und Abschnitt 7 Absatz 3).

A2.3.2 Kontrollen

(1) Durch den Arbeitgeber sind gemäß § 4 Absatz 5 Satz 3 BetrSichV ergänzend zu Prüfungen auch regelmäßige Kontrollen der Funktionsfähigkeit der Cybersicherheitsmaßnahmen durch fachkundige, beauftragte und unterwiesene Beschäftigte oder durch vergleichbar qualifizierte Auftragnehmer (siehe Abschnitt 8.2 Absatz 3) durchzuführen. Art und Umfang der Kontrollen werden in der Gefährdungsbeurteilung festgelegt.

Hinweis: Um die Ergebnisse der regelmäßigen Kontrollen der Funktionsfähigkeit der Cybersicherheitsmaßnahmen für die Prüfungen gemäß §§ 14 bis 16 BetrSichV nutzen zu können, wird eine ausreichende Dokumentation der Kontrollen empfohlen.

(2) In Abhängigkeit der festgelegten Cybersicherheitsmaßnahmen kann z. B. kontrolliert werden, ob

1. Barrieren eines physischen Schutzes gegeben (z. B. abgeschlossener Serverschrank) sind,
2. Firewalls und Antiviren-Software aktiv und auf dem neuesten Stand sind,
3. ungewöhnliche oder unzulässige Aktivitäten in Netzwerken und zugehörigen Systemen aufgetreten sind (siehe hierzu auch Abschnitt 4.5.2 Absatz 2 Nummer 5),
4. Hash-Werte/Checksummen unverändert sind,
5. Zugriffskontrollen (Authentifizierung und Autorisierung) aktiv sind,
6. Verschlüsselungsmechanismen aktiv sind,
7. organisatorische Cybersicherheitsmaßnahmen eingehalten werden.

(3) Automatisierte Überwachungseinrichtungen zur Feststellung ungewöhnlicher oder unzulässiger Aktivitäten in Netzwerken können zur Kontrolle der Funktionsfähigkeit der Cybersicherheitsmaßnahmen eingesetzt werden. In diesem Fall sind die Systemmeldungen zyklisch oder anlassbezogen nach Vorgaben des Arbeitgebers durch diesen auszuwerten.

Anhang 3

Regelwerke und Normen

In den folgenden Regelwerken und Normen sind Vorgehensweisen und Methoden für die Ermittlung und Umsetzung von erforderlichen Cybersicherheitsmaßnahmen beschrieben:

[1] IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik (BSI))

[2] ICS-Security-Kompendium (Bundesamt für die Sicherheit in der Informationstechnik (BSI))

[3] BSI-Standard 200-1 „Managementsysteme für Informationssicherheit (ISMS)“

[4] BSI-Standard 200-2 „IT-Grundschutz-Methodik“

[5] BSI-Standard 200-3 „Risikomanagement“

[6] Normen der Reihe ISO/IEC 27000 „Information technology – Security techniques“

[7] Normen der Reihe IEC 62443 „Industrial communication networks – Network and system security“

Link zum kostenlosen Download von Informationen des BSI:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

Link zum kostenlosen Download von TRBS: https://www.baua.de/trbs

Link zu kostenlosen Informationen der DGUV: https://cert.dguv.de/