Beschluss des EK ZÜS **ZÜS B-002 rev 5**

Abgestimmt im EK ZÜS	Schriftliche Abstimmung	27.05.2022
	34. Sitzung, TOP 6.2	16.11.2022
	36. Sitzung, TOP 8.10	15.11.2023
	37. Sitzung, TOP 5.2	17.04.2024
	38. Sitzung, TOP 4.2	20.11.2024
	40. Sitzung, TOP 4.1	19.11.2025

Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen von überwachungsbedürftigen Anlagen

1 Anwendungsbereich

(1) Dieser Beschluss legt für die ZÜS Mindestanforderungen für ihre Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen (Maßnahmen der Cybersicherheit, kurz CS-Maßnahmen) im Rahmen der Prüfungen gemäß § 15 oder § 16 BetrSichV der überwachungsbedürftigen Anlagen sowie, falls zutreffend, der Prüfung gemäß § 18 BetrSichV fest.

Hinweis: Um den sich ständig ändernden Bedrohungen fortlaufend zu begegnen, ist es für die Cybersicherheit wesentlich, dass diesbezüglich Strukturen und Prozesse eingerichtet und aufrechterhalten werden.

(2) In diesem Beschluss wird der Begriff „Betreiber“ verwendet.

(3) Dieser Beschluss bezieht sich ausschließlich auf Prüfungen, die der Bestätigung der Einhaltung der Vorgaben der BetrSichV dienen. Aspekte, die der Abwehr von wirtschaftlichen Schäden oder von Angriffen auf den Datenschutz (z. B. personenbezogene Daten) dienen, werden nicht berücksichtigt.

(4) Der Prüfumfang umfasst auch über sicherheitsrelevante MSR-Einrichtungen hinausgehende Teile der überwachungsbedürftigen Anlagen (z. B. Notrufeinrichtungen, Alarmierungseinrichtungen) oder andere technische Infrastrukturen, wenn für sie als Ergebnis der Gefährdungsbeurteilung ein Schutz gegen Cyberbedrohungen als erforderlich angesehen wird. Die hinsichtlich der Prüfung von CS-Maßnahmen relevanten Einrichtungen werden nachfolgend als „schutzbedürftige Einrichtungen“ (zum Begriff siehe Abschnitt 3 Absatz 2) bezeichnet.

(5) CS-Maßnahmen derjenigen IT/OT[1]-Systeme, die mit schutzbedürftigen Einrichtungen in Verbindung stehen und als Angriffswege genutzt werden können, sind Bestandteil des Prüfumfanges.

[1] OT = Operational Technology

(6) Die Beherrschung von Cyberbedrohungen setzt grundsätzlich auf einen lebenszyklusbegleitenden Prozess zur Cybersicherheit auf.

(7) Die Prüfung der Cybersicherheit gem. Abschnitt 4 dieses Beschlusses ist im Rahmen folgender Prüfungen durchzuführen:

- Anhang 2 Abschnitt 2 Nummern 3 und 4.1 BetrSichV Aufzugsanlagen
- Anhang 2 Abschnitt 3 Nummern 4.1 und 5.1 BetrSichV Explosionssicherheit
- Nach Anhang 2 Abschnitt 4 Nummern 4 und 5 BetrSichV (Prüfung vor Inbetriebnahme von Druckanlagen und wiederkehrende Anlagenprüfungen)
- Prüfbericht zur Erlaubnis nach § 18 Absatz 3 BetrSichV

Hinweis: Im Rahmen dieser Prüfungen können sich Ergebnisse des Managements der Cybersicherheit des Betreibers gemäß TRBS 1115 Teil 1 Anhang 1 zu eigen gemacht werden (vgl. TRBS 1115 Teil 1 Abschnitt 6 Abs. 4 und Abschnitt 7 Abs. 3).

(8) Schutzbedürftige Einrichtungen, die aufgrund nicht vorhandener Datenschnittstellen (sowohl kabelgebunden als auch kabellos) nicht kompromittiert werden können, benötigen keine CS-Maßnahmen.

2 Rechtliche Rahmenbedingungen

(1) Der Betreiber hat gemäß §§ 15 und 16 BetrSichV sicherzustellen, dass überwachungsbedürftige Anlagen vor Inbetriebnahme, vor Wiederinbetriebnahme nach einer prüfpflichtigen Änderung und wiederkehrend geprüft werden. Der Betreiber ist gemäß § 3 BetrSichV verpflichtet, Gefährdungen (auch die durch Cyberbedrohungen) zu beurteilen und geeignete Schutzmaßnahmen zu treffen.

(2) Die TRBS 1115 Teil 1 „Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen“ konkretisiert die Betriebssicherheitsverordnung (BetrSichV) im Hinblick auf die Ermittlung, Festlegung und Prüfung erforderlicher CS-Maßnahmen für die dauerhafte Sicherstellung der Funktionsfähigkeit von sicherheitsrelevanten Mess-, Steuer- und Regeleinrichtungen (MSR-Einrichtungen), die als technische Schutzmaßnahme für die sichere Verwendung von Arbeitsmitteln inklusive überwachungsbedürftigen Anlagen eingesetzt werden.

(3) Für die Bereitstellung von Arbeitsmitteln auf dem Markt[2] (Inverkehrbringen) gibt es noch keine verbindlichen Vorgaben zur Cybersicherheit. Deshalb sind die erforderlichen CS-Maßnahmen in der Gefährdungsbeurteilung insbesondere unter Beachtung der Anforderungen der Betriebssicherheitsverordnung zu ermitteln.

(4) Gemäß § 3 Absatz 2 Satz 2 Nr. 4 BetrSichV muss der Betreiber bei seiner Gefährdungsbeurteilung auch vorhersehbare Betriebsstörungen berücksichtigen.

In TRBS 1111 Abschnitt 4.5 sind vorhersehbare Betriebsstörungen, wie z. B. „Ereignisse, die den Arbeitsablauf behindern oder zur Einstellung der Arbeiten führen oder bei denen die für den Normalbetrieb des Arbeitsmittels getroffenen Schutzmaßnahmen teilweise oder ganz außer Kraft gesetzt sein können“, benannt. Eine solche Betriebsstörung kann auch der plötzliche Ausfall von Sicherheitsfunktionen eines Arbeitsmittels durch Fremdeinwirkung sein. Die möglichen Auswirkungen einer Kompromittierung von schutzbedürftigen OT-Einrichtungen sind daher in der Gefährdungsbeurteilung zu bewerten.

Hinweis: Ergibt sich aus der Gefährdungsbeurteilung, dass ein auf dem Markt bereit gestelltes Arbeitsmittel unter Berücksichtigung der innerbetrieblichen Einsatzbe-

[2] Redaktionsschluss August 2025

dingungen und der auszuführenden Arbeiten nicht ohne zusätzliche Schutzmaßnahmen sicher verwendet werden kann, hat der Betreiber gemäß § 5 Absatz 1 BetrSichV geeignete Schutzmaßnahmen festzulegen.

3 Begriffsbestimmungen im Sinne dieses Beschlusses

(1) Es gelten die Definitionen TRBS 1115 Teil 1.

(2) **Schutzbedürftige Einrichtungen** sind:

- Sicherheitsrelevante MSR-Einrichtungen,
- nicht sicherheitsrelevante MSR-Einrichtungen (z. B. PLT-Betriebseinrichtungen), bei denen durch die Kompromittierung ihrer Funktion auch unter Berücksichtigung von Wechselwirkungen mit anderen Anlagenteilen eine relevante Gefährdung von Beschäftigten und anderen Personen im Gefahrenbereich verursacht werden kann
- sicherheitsrelevante Einrichtungen, die keine MSR-Einrichtung sind (z. B. Notrufeinrichtungen, Notbefehlseinrichtungen), im Folgenden autarke Sicherheitseinrichtungen genannt,

soweit eine Kompromittierung durch Cyberbedrohungen möglich ist. Sowie

- Teile der IT/OT-Umgebung für die CS-Maßnahmen zum Schutz von Angriffszielen erforderlich sind.

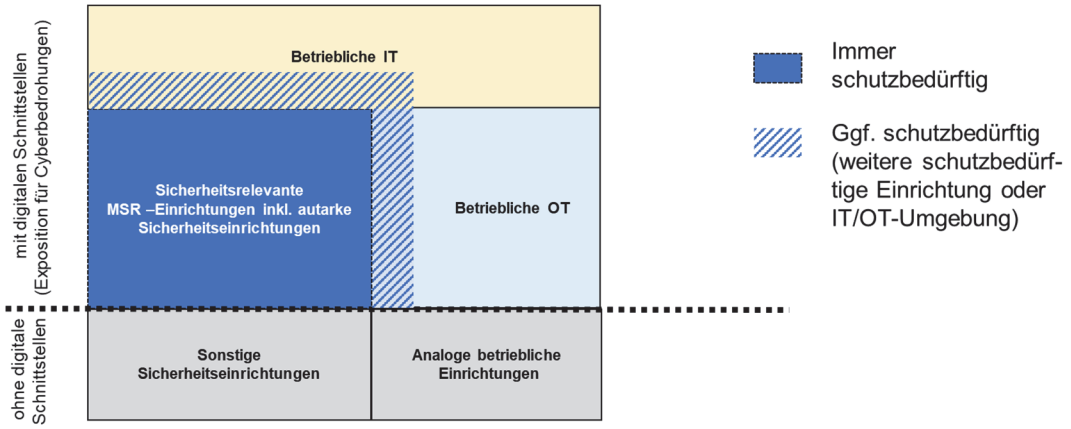

Abbildung 1: Darstellung der schutzbedürftigen Einrichtungen und der IT/OT-Umgebung

4 Prüfung der CS-Maßnahmen für schutzbedürftige Einrichtungen

Vorbemerkung:

Die folgenden Prüfschritte richten sich nach den zum Zeitpunkt der jeweiligen Prüfung geltenden Anforderungen aus der BetrSichV und dem ÜAnlG und den zugehörigen technischen Regeln, insbesondere der TRBS 1115 Teil 1 mit ihren Anhängen.

Bei jeder überwachungsbedürftigen Anlage ist zu prüfen, ob TRBS 1115 Teil 1 auf sie anzuwenden ist. Ist dies der Fall, ist eine Prüfung der CS-Maßnahmen erforderlich.

Die Überprüfung der Wirksamkeit von CS-Maßnahmen gemäß TRBS 1115 Teil 1 Abschnitt 5 und der Kontrollen gemäß TRBS 1115 Teil 1 Abschnitt 8.2 sind nicht Bestandteil der nachfolgend beschriebenen Prüfung durch die ZÜS.

Die ZÜS kann sich die durch die Anwendung eines Managements der Cybersicherheit erzeugten Ergebnisse zu eigen machen (siehe hierzu Abschnitt 4.4). Wird kein Management der Cybersicherheit nach TRBS 1115 Teil 1 Anhang 1 angewendet, kann sich die ZÜS die Ergebnisse der Überprüfung der Wirksamkeit der CS-Maßnahmen nach TRBS 1115 Teil 1 Abschnitte 5 und 8.2 durch den Betreiber zu eigen machen, wenn Durchführung und Ergebnis der Überprüfung für sie nachvollziehbar dokumentiert und plausibel sind.

Die Prüfung der Eignung von CS-Maßnahmen setzt strukturierte und dokumentierte Prozesse des Arbeitgebers zur Cybersicherheit voraus. Die Dokumentation hierzu ist zur Prüfung vorzulegen. Ein möglicher Ablauf zur Planung, Realisierung und zur zusammenfassenden Dokumentation erforderlicher CS-Maßnahmen für einzelne überwachungsbedürftige Anlagen befindet sich als Beispiel in Anhang 1.

Grundsätzlich erfolgt die Prüfung auf Vorgabe des Betreibers nach einer der zwei nachfolgenden Vorgehensweisen:

1. Einzelfallbetrachtung
   Die Prüfung der Prozesse der Cybersicherheit erfolgt einzeln für jede überwachungsbedürftige Anlage.
2. Top-Down-Betrachtung:
   Besitzt der Betreiber ein Management der Cybersicherheit gemäß TRBS 1115 Teil 1 Anhang 1 für mehrere überwachungsbedürftige Anlagen, so können die Prozesse zur Planung, Realisierung und Aufrechterhaltung der Cybersicherheit auf Ebene des Managements der Cybersicherheit durch die ZÜS zusammenfassend geprüft werden. Die Ergebnisse können in der Prüfung nach TRBS 1115 Teil 1 Abschnitt 6 und 7 zu Eigen gemacht werden.

   Hinweis: Für den Fall, dass eine Vielzahl von Anlagen bei einem Betreiber geprüft werden, besitzt dieser Weg den Vorteil einer größeren Effizienz.

Von einer Eignung der CS-Maßnahmen ist im Allgemeinen auszugehen, wenn:

- bei der Festlegung der CS-Maßnahmen berücksichtigt wurde, dass beim Betrieb von überwachungsbedürftigen Anlagen gemäß § 2 ÜAnlG ein erhebliches Risiko für die Sicherheit und Gesundheit insbesondere von Beschäftigten ausgehen kann,
- Fachkundige Personen (siehe hierzu TRBS 1115 Teil 1 Abschnitt 3.3.2) für die Festlegung der erforderlichen CS-Maßnahmen eingesetzt wurden,
- der Stand der Technik zur sicheren Verwendung z. B. durch Anwendung von Normen und Standards berücksichtigt wurde und
- bei der Festlegung der CS-Maßnahmen im Rahmen der Gefährdungsbeurteilung alle Schritte gemäß TRBS 1115 Teil 1 Abschnitte 4.1 bis 4.5 nachvollziehbar korrekt ausgeführt wurden.

4.1 Prüfung im Erlaubnisverfahren

Es ist zu prüfen, ob der Antragsteller Aspekte der Cybersicherheit in den für das Erlaubnisverfahren zu prüfenden Unterlagen entsprechend den Anforderungen der TRBS 1115 Teil 1 angemessen berücksichtigt hat.

4.2 Prüfung nach §§ 15 und 16 BetrSichV durch eine ZÜS

(1) Aus TRBS 1115 Teil 1 Abschnitte 6 und 7 ergeben sich die folgenden Prüfinhalte:

- Eignung und Funktionsfähigkeit der CS-Maßnahme,
- Plausibilität der Dokumentation und der Festlegung der erforderlichen CS-Maßnahmen,
- Feststellung, ob ein Verfahren zur Aufrechterhaltung des Cybersicherheitsniveaus vorhanden ist.

(2) Eine Konkretisierung dieser Prüfinhalte ist in TRBS 1115 Teil 1 Anhang 2 Abschnitt A2.3 enthalten.

(3) Die Prüfung der CS-Maßnahmen erfolgt durch eine Plausibilitätsprüfung der vorliegenden Unterlagen und einer Prüfung der Umsetzung und Funktionsfähigkeit der CS-Maßnahmen an einer ausreichenden Stichprobe.

(4) Die Plausibilitätsprüfung der vorliegenden Unterlagen erfolgt entweder als Einzelfallbetrachtung (siehe hierzu den Mindestumfang in Anhang 2) oder als Top-Down-Betrachtung (siehe hierzu Abschnitt 4.4).

4.3 Umgang mit bereits vorhandenen Bestätigungen der Cybersicherheit bei Prüfungen durch die ZÜS

4.3.1 Durch Hersteller bestätigter Schutz vor Cyberbedrohungen nach dem Stand der Technik

Eine Bestätigung des Schutzes vor Cyberbedrohungen durch einen Hersteller kann bei der Prüfung nach TRBS 1115 Teil 1 Abschnitt 6 berücksichtigt werden, wenn ein den Anforderungen der TRBS 1115 Teil 1 genügender Schutz gegen Cyberbedrohungen auf Basis eines etablierten Verfahrens der Cybersicherheit nach dem Stand der Technik (z. B. DIN EN IEC 62443) bestätigt wurde und plausibel ist.

4.3.2 Bestätigung der erfolgreichen Implementierung eines Informationssicherheitsmanagementsystems (ISMS) nach z. B. ISO 27001 oder eines Managements der Cybersicherheit (CSMS) nach z. B. DIN EN IEC 62443

Ein ISMS/CSMS kann bei der Prüfung der Cybersicherheit überwachungsbedürftiger Anlagen nur berücksichtigt werden, wenn eine Zertifizierung des ISMS/CSMS durch eine unabhängige Zertifizierungsstelle (Third-Party) vorhanden ist. Ist dies der Fall, ist festzustellen, welche Anforderungen der TRBS 1115 Teil 1 bereits durch die vorgelegte Zertifizierung abgedeckt und als erfüllt bestätigt wurden. Insbesondere ist dabei zu berücksichtigen, ob

- das Zertifikat den Bereich der schutzbedürftigen Systeme im Sinne dieses Beschlusses mit abdeckt,
- der Schutz von Beschäftigten und ggf. anderer Personen im Gefahrenbereich der überwachungsbedürftigen Anlage ausreichend berücksichtigt ist,
- das Zertifikat oder der Prüfungsnachweis noch Gültigkeit besitzt und
- eine Prüfung mit einer angemessenen Prüftiefe auch hinsichtlich der Funktionsfähigkeit der relevanten CS-Maßnahmen durchgeführt wurde.

4.3.3 Berücksichtigung von Ergebnissen aus Prüfungen der Cybersicherheit nach anderen Rechtsgebieten

Ergebnisse aus Prüfungen der Cybersicherheit nach anderen Rechtsgebieten können bei der Prüfung der Cybersicherheit überwachungsbedürftiger Anlagen berücksichtigt werden. Hierfür ist festzustellen, welche Anforderungen der TRBS 1115 Teil 1 bereits durch die vorgelegten Nachweise abgedeckt und im Rahmen einer unabhängigen Prüfung als anforderungsgerecht bestätigt wurden. Insbesondere ist dabei zu berücksichtigen, ob

- das Zertifikat oder der Prüfungsnachweis den Bereich der schutzbedürftigen Systeme im Sinne dieses Beschlusses mit abdeckt,
- der Schutz von Beschäftigten und ggf. anderer Personen im Gefahrenbereich der überwachungsbedürftigen Anlage ausreichend berücksichtigt ist,
- das Zertifikat oder der Prüfungsnachweis noch Gültigkeit besitzt und
- eine Prüfung mit einer angemessenen Prüftiefe auch hinsichtlich der Funktionsfähigkeit der relevanten CS-Maßnahmen durchgeführt wurde.

4.4 Zu eigen machen von Ergebnissen eines nicht-zertifizierten Managements der Cybersicherheit (CSMS)

Gemäß TRBS 1115 Teil 1 besteht im Rahmen von Prüfungen die Möglichkeit, sich Ergebnisse eines CSMS des Betreibers zu eigen zu machen (vgl. TRBS 1115 Teil 1, Abschnitt 6 Absatz 4 und Abschnitt 7 Absatz 3). Dieses setzt jedoch voraus, dass das CSMS für die zu prüfende überwachungsbedürftige Anlage wirksam, und die übernommenen Ergebnisse für die ZÜS nachvollziehbar sind. Hierzu ist durch die ZÜS eine Plausibilitätsprüfung des CSMS hinsichtlich der Erfüllung der Anforderungen gem. TRBS 1115 Teil 1 Anhang 1 Abschnitt A 1.2.1 und Abschnitt A 1.2.2 erforderlich. Eine solche Plausibilisierung kann auch für mehrere überwachungsbedürftige Anlagen erfolgen.

Als konkretisierende Hilfestellung für eine Plausibilitätsprüfung kann unter Anderem der Anhang 1 „Themenkatalog“ des „VCI-Statuspapiers zur Cybersicherheit in der Prozessindustrie – Umsetzung und Prüfung“ verwendet werden.

4.5 Datum der ersten Anwendung dieses Beschlusses

Der EK-ZÜS-Beschluss B-002 rev 5 ist spätestens ab dem 1. April 2026 anzuwenden.

5 Mängeleinstufung

Nachfolgend sind ergänzend zu den bestehenden Vorgaben für die Mängeleinstufung Beispiele für eine Mängeleinstufung im Rahmen der Prüfung der Cybersicherheit dargestellt.

Geringfügiger Mangel:	Die Dokumentation zur Behandlung von Cyberbedrohungen ist unvollständig oder fehlerhaft oder es gibt Defizite bei der Umsetzung der festgesetzten CS-Maßnahmen, die nicht einem erheblichen Mangel entsprechen.
Erheblicher Mangel:	Die Maßnahmen der Cybersicherheit sind nicht in ordnungsgemäßen Zustand (z. B. schutzbedürftige Systeme sind für Akteure im Sinne TRBS 1115 Teil 1 Anhang 2 Abschnitt B.1 Absatz 5 Satz 1 über ungeschützte Schnittstellen zugänglich) und es sind unverzüglich entsprechende Maßnahmen erforderlich.
Gefährlicher Mangel:	Eine Kompromittierung von schutzbedürftigen Einrichtungen, die zu Gefährdungen führen kann, ist bereits erfolgt.

Anhang 1

Beispielhafter Ablauf zur Planung und Realisierung erforderlicher CS-Maßnahmen

Hinweis: Handelt es sich beim Betrachtungsgegenstand um ein verwendungsfertiges System zur Umsetzung einer Sicherheitsfunktion mit durch den Hersteller bestätigter Cybersicherheit, ist gemäß TRBS 1115 Teil 1 eine Planung und Realisierung von CS-Maßnahmen durch den Betreiber nicht erforderlich. Maßgeblich für die Cybersicherheit im Betrieb ist in diesem Fall die Einhaltung der Vorgaben des Herstellers, die z. B. in Form einer Betriebsanleitung dargelegt sind.

Die folgenden Schritte beschreiben einen Ablauf zur Ermittlung der erforderlichen CS-Maßnahmen.

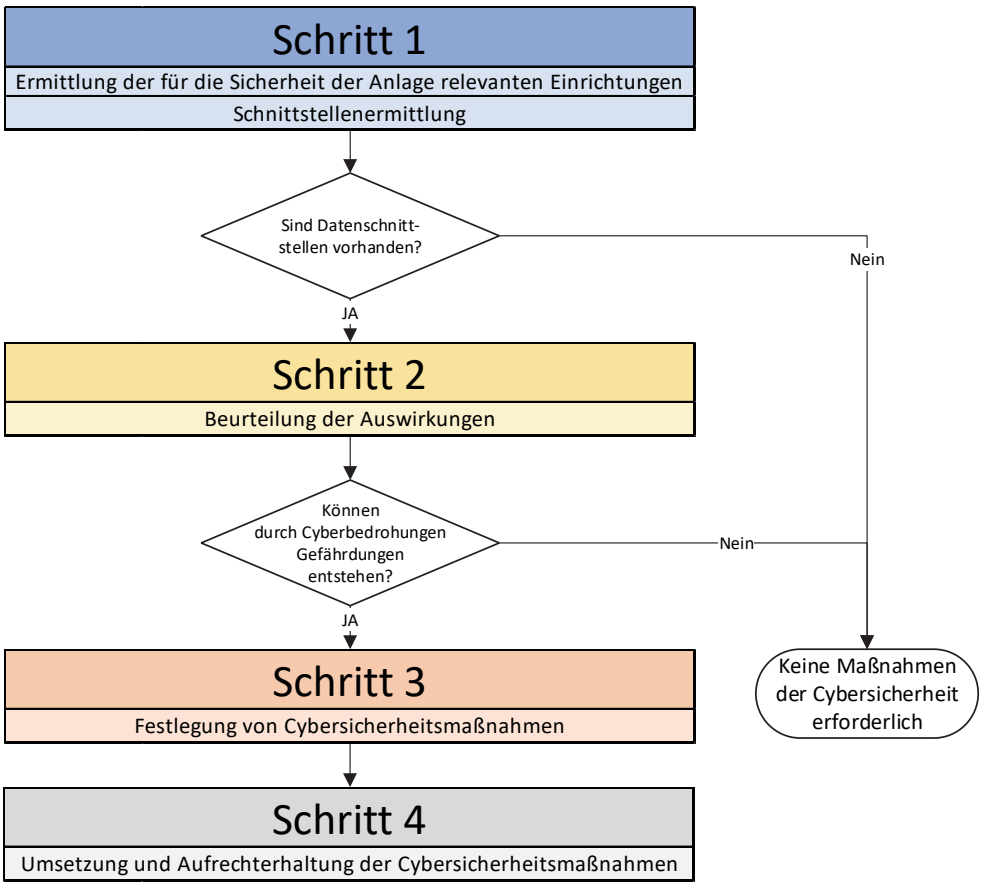

Abbildung 2: Ablauf zur Ermittlung der erforderlichen CS-Maßnahmen

Auf eine detaillierte Beurteilung der Auswirkungen von Cyberbedrohungen (Schritt 2) kann verzichtet werden, wenn pauschal ein anforderungsgerechter Schutzbedarf festgelegt wird.

Eine Konkretisierung der Inhalte der Schritte 1 bis 4 ist in den folgenden Tabellen enthalten.

Beispielhafte zusammenfassende Dokumentation des Prozesses zur Planung und Realisierung der CS-Maßnahmen:

Schritt 1	
Ermittlung der für die Sicherheit der überwachungsbedürftigen Anlage relevanten Einrichtungen	**Schnittstellenermittlung**
Benennung der jeweiligen sicherheitsrelevanten MSR-Einrichtung / Schutzeinrichtung / des Ausrüstungsteils mit Sicherheitsfunktion, autarken Sicherheitseinrichtung oder des Anlagenteils, das hinsichtlich möglicher Auswirkungen von Cyberbedrohungen auf den sicheren Zustand der überwachungsbedürftigen Anlage zu untersuchen ist	**Benennung der an der Einrichtung vorhandenen Daten-Schnittstellen**
Einrichtung A	
Einrichtung B	
...	

Schritt 2			
Beurteilung der Auswirkungen von Cyberbedrohungen			
Benennung der betrachteten Einrichtung	**Kurzbeschreibung der Schutzfunktion / des Schutzziels**	**Durch die Folgen einer Manipulation (z. B. Fehl-Auslösung, Blockierung der Auslösung oder Parameter- oder Funktionsänderungen) können grundsätzlich Gefährdungen entstehen. (Ja/Nein) Wenn „Ja“ bitte beschreiben.**	**Es gibt folgende nicht digitale Maßnahmen, um die Folgen der Manipulation auf ein ungefährliches Maß zu reduzieren. (Eintragung nur, wenn zutreffend erforderlich)**
Einrichtung A			
Einrichtung B			
...			

Schritt 3					
Festlegung von Cybersicherheitsmaßnahmen					
Benennung der schutzbedürftigen Einrichtungen	**Die Elemente gemäß TRBS 1115 Teil 1 Abschnitt 3.2 sind im erforderlichen Umfang erfasst. (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)**	**Die Standardmaßnahmen der TRBS 1115 Teil 1 Abschnitt 4.5.2 Absatz 2 wurden im erforderlichen Umfang berücksichtigt. (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)**	**Eine Festschreibung der erforderlichen Cybersicherheitsmaßnahmen ist erfolgt. (Ja/Nein) (Spezifikation der Cybersicherheit) (zzgl. Verweis auf Dokumentationsort)**	**Wenn Herstellervorgaben zur Cybersicherheit vorhanden sind, werden diese berücksichtigt. (Ja/Nein)**	**Ein Verfahren zur Aufrechterhaltung des Cybersicherheits-niveaus ist festgelegt. (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)**
Einrichtung x					
Einrichtung x					
.....					

Schritt 4		
Umsetzung und Aufrechterhaltung der Cybersicherheitsmaßnahmen		
Benennung der schutzbedürftigen Einrichtungen	**Organisatorische Maßnahmen der Cybersicherheit sind in einer Betriebsanweisung festgeschrieben (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)**	**Technische Maßnahmen der Cybersicherheit sind nachweislich funktionsfähig/wirksam (Ja/Nein) (siehe hierzu TRBS 1115 Teil 1 Abschnitt 5 und 8.2)**
Einrichtung x		
Einrichtung x		
...		

Andere Darstellungsformen (z. B. mit Gruppierungen von mehreren sicherheitsrelevanten MSR-Einrichtungen, Typisierungen von gleichartigen sicherheitsrelevanten MSR-Einrichtungen) oder inhaltsspezifische Verweise auf bereits etablierte Prozesse oder Dokumentationen können je nach Komplexität der überwachungsbedürftigen Anlage sinnvoll sein. Entscheidend für die Durchführbarkeit der Prüfung ist die Verfügbarkeit der oben genannten erforderlichen Informationen.

Anhang 2

Mindestumfang der Dokumentationsprüfung zu den CS-Maßnahmen im Rahmen einer Einzelfallbetrachtung

Prüfschritt Nr.	Prüffrage	Ist eine Aussage/ein Inhalt zu den u. g. Sachverhalten in Dokumentation des Betreibers vorhanden?	Prüfung § 15 BetrSichV oder erstmalige Prüfung der CS-Maßnahmen		Prüfung § 16 BetrSichV	
			ZÜS	Übernahme der Ergebnisse möglich	ZÜS	Übernahme der Ergebnisse möglich
1	Wurden Cyberbedrohungen gemäß TRBS 1115 Teil 1 bei der Gefährdungsbeurteilung berücksichtigt?	Berücksichtigung der Cybersicherheit gemäß TRBS 1115 Teil 1 in der Gefährdungsbeurteilung	X		–	
2	Sind die sicherheitsrelevanten MSR-Einrichtungen und weitere schutzbedürftige Einrichtungen erfasst und dokumentiert?	Auflistung der schutzbedürftigen Einrichtungen	X		–	
3	Wurde berücksichtigt, dass bei überwachungsbedürftigen Anlagen gemäß ÜAnlG stets von einem erheblichen Risiko für Sicherheit und Gesundheit von Beschäftigten und anderen Personen im Gefahrenbereich auszugehen ist?	Schriftliche Bestätigung, durch Übernahme der linksstehenden Aussagen in die GBU oder CS-Risikoanalyse	X		–	
4	Erfolgte die Festlegung der Maßnahmen durch fachkundige Personen entsprechend TRBS 1115 Teil 1 Abschnitt 3.3.2?	Liste der beteiligten fachkundigen Personen	X		–	
5	Wurde der Stand der Technik herangezogen?	Angaben zu den zugrunde gelegten einschlägigen Normen und Standards z. B.: EN 62443-ff ICS –Security- Kompendium IEC 27019	X		–	
6	Wurden Maßnahmen mit den Mindestinhalten nach TRBS 1115 Teil 1 4.5.2 im erforderlichen Umfang festgelegt?	Schriftliche Festlegung der CS-Maßnahmen	X		–	

Prüfschritt Nr.	Prüffrage	Ist eine Aussage/ein Inhalt zu den u. g. Sachverhalten in Dokumentation des Betreibers vorhanden?	Prüfung § 15 BetrSichV oder erstmalige Prüfung der CS-Maßnahmen		Prüfung § 16 BetrSichV	
			ZÜS	Übernahme der Ergebnisse möglich	ZÜS	Übernahme der Ergebnisse möglich
7	Gibt es Vorgaben von Herstellern und wenn ja, wurden diese bei der Festlegung der CS-Maßnahmen berücksichtigt?	Bestätigung anhand einer Dokumentation z. B. der Überprüfung nach TRBS 1115 Teil 1 Abschnitt 5	X	X	–	
8	Sind Art und Umfang sowie Fristen der Überprüfungen und Kontrollen der Maßnahmen schriftlich festgelegt?	Bestätigende Angaben in der Dokumentation.	X		X	
9	Wird sichergestellt, dass CS-Maßnahmen die Sicherheitsmaßnahmen nicht negativ beeinflussen? (Rückwirkungsfreiheit)	Bestätigende Angaben in der Dokumentation.	X	X	–	
10	Werden neue Erkenntnisse zur Cybersicherheit in die Gefährdungsbeurteilung eingebunden?	Dokumentiertes Verfahren zur Aufrechterhaltung der Cybersicherheit	X		–	
11	Sind Unterweisungen von Beschäftigten zur Cybersicherheit durchgeführt?	Bestätigende Angaben in der Dokumentation.	X		X	X
12	Liegt für die CS-Maßnahmen gemäß Nr. 6 ein Nachweis der Wirksamkeit gemäß TRBS 1115 Teil 1 Abschnitt 5 vor?	Schriftliche Bestätigung	X	X	–	
13	Liegt für die CS-Maßnahmen gemäß Nr. 6 eine Bestätigung der Funktionsfähigkeit gem. TRBS 1115 Teil 1 Abschnitt 8.2 vor?	Schriftliche Bestätigung	–		X	X
14	Wurden nach Aussage des Betreibers prüfpflichtige Änderungen am Arbeitsmittel mit Einfluss auf die Cybersicherheit durchgeführt? (z. B. aufgrund neuer Erkenntnisse)	Aussage des Betreibers	–		X	

Inhaltsverzeichnis