Beschluss des EK Rof **B-001 rev 2**

Abgestimmt im EK Rof	schriftlich Abstimmung	12.07.2024
	10. Sitzung	06.03.2025
	schriftliche Abstimmung	23.04.2026

Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen von Rohrfernleitungsanlagen

1 Anwendungsbereich

(1) Dieser Beschluss legt für die Prüfstellen Mindestanforderungen für ihre Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen (Maßnahmen der Cybersicherheit, kurz CS-Maßnahmen) im Rahmen der Prüfungen gemäß § 5 RohrFLtgV von Rohrfernleitungsanlagen fest.

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

(3) Der Prüfumfang umfasst im Wesentlichen sicherheitsrelevante MSR-Einrichtungen von Rohrfernleitungsanlagen. Er kann sich aber um nicht sicherheitsrelevante MSR-Einrichtungen und für die Sicherheit relevante Einrichtungen, die keine MSR-Einrichtung sind, erweitern, wenn als Ergebnis einer sicherheitstechnischen Beurteilung der Rohrfernleitungsanlage durch den Betreiber festgestellt wurde, dass durch die Kompromittierung dieser Einrichtungen mittelbar oder unmittelbar eine Gefährdung von Menschen oder der Umwelt verursacht werden kann. Die hinsichtlich der Prüfung von CS-Maßnahmen relevanten Einrichtungen werden nachfolgend als „schutzbedürftige Einrichtungen“ (zum Begriff siehe Abschnitt 3 Absatz 7) bezeichnet.

(4) Wurden CS-Maßnahmen an IT/OT-Systemen, die mit schutzbedürftigen Einrichtungen datentechnisch in Verbindung stehen, als notwendig identifiziert, um diese Systeme zu schützen („defence in depth“) (siehe auch hierzu TRBS 1115 Teil 1), sind diese bei der Prüfung der zugehörigen schutzbedürftigen Einrichtung ebenfalls zu berücksichtigen.

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

(6) Schutzbedürftige Einrichtungen, die aufgrund nicht vorhandener Datenschnittstellen (sowohl kabelgebunden als auch kabellos) nicht kompromittiert werden können, benötigen keine Maßnahmen der Cybersicherheit.

2 Begriffsbestimmungen im Sinne dieses Beschlusses

(1) **Cybersicherheit** ist das Vorhandensein des erforderlichen Schutzes von schutzbedürftigen Einrichtungen vor Cyberbedrohungen, soweit deren Informationstechnik durch Cyberbedrohungen kompromittiert werden kann und sie dem Schutz von Beschäftigten und anderen Personen im Gefahrenbereich dienen.

(2) **Cyberbedrohung** ist die intendierte Bedrohung der datentechnischen Integrität von Rohrfernleitungsanlagen einschließlich der Verfügbarkeit ihrer sicherheitsrelevanten MSR-Einrichtungen mit Methoden und Werkzeugen der Informationstechnik.

(3) **Maßnahmen** der **Cybersicherheit (CS-Maßnahmen)** sind Maßnahmen zum Schutz vor Cyberbedrohungen.

(4) **Sicherheitseinrichtungen** sind gemäß TRBS 1201 Einrichtungen zur Verhinderung von unzulässigen oder instabilen Betriebszuständen von Arbeitsmitteln. Dazu können auch MSR-Einrichtungen zählen.

(5) **MSR-Einrichtungen** sind Einrichtungen, die dem Messen physikalischer Größen und dem auf dieser Grundlage erfolgenden Regeln oder Steuern von Arbeitsmitteln dienen. MSR-Einrichtungen können betrieblichen und/oder sicherheitstechnischen Zwecken dienen.

Hinweis: In anderen Regelwerken werden MSR-Einrichtungen auch als PLT- oder PLS-Einrichtungen bezeichnet.

(6) **Sicherheitsrelevante MSR-Einrichtungen** sind gemäß TRBS 1201 Mess-, Steuer- und Regeleinrichtungen an Arbeitsmitteln inkl. überwachungsbedürftigen Anlagen, die deren sicherer Verwendung dienen. Sie bestehen aus Sensor-, Aktor- und Logikeinheiten sowie zugehörigen Verbindungseinrichtungen und unterliegen üblicherweise auch Anforderungen an ihre funktionale Sicherheit.

(7) **Schutzbedürftige Einrichtungen** ist der Sammelbegriff für

- 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.

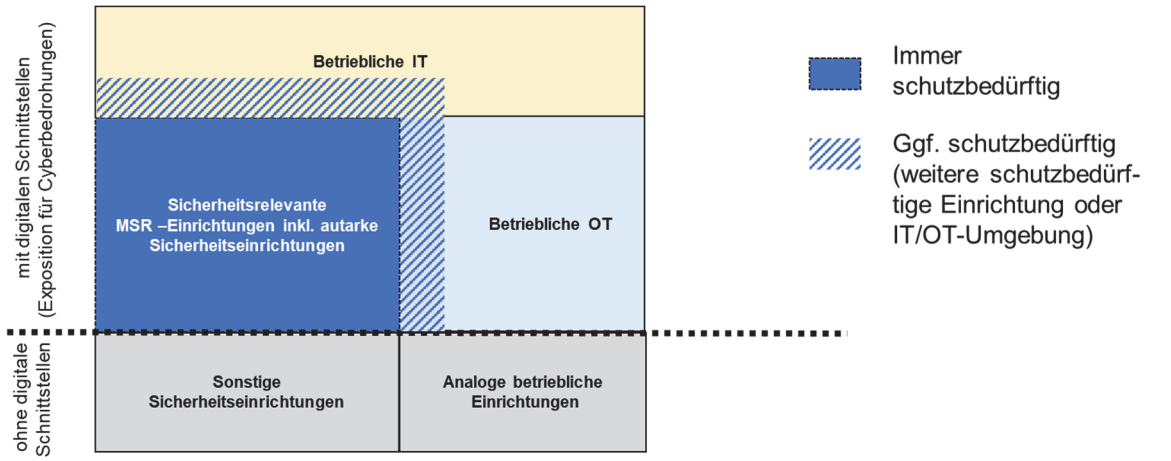

Abbildung 1: Darstellung der schutzbedürftigen Einrichtungen und der IT/OT-Umgebung

(8) **Kompromittierung** ist der unberechtigte datentechnische Zugriff auf eine schutzbedürftige Einrichtung mit dem Ziel der Manipulation der Funktion.

(9) Die **Umgebung** sind IT/OT-Komponenten und Systeme, die weder direkt noch indirekt der schutzbedürftigen OT-Einrichtung zuzuordnen sind, aber mit dieser in Verbindung stehen (z. B. Betriebsdateninformationssystem, Visualisierung des Sicherheitsfunktion-Zustands, Service-IT für z. B. Patchmanagement, Domain Control und Virenschutz, Internet) und daher als Angriffswege dienen können.

3 Grundsätze der Prüfung

(1) Um eine durch die Kompromittierung ausgelöste unmittelbare oder mittelbare Gefährdung von Menschen oder der Umwelt durch die Rohrfernleitungsanlage zu vermeiden, müssen die schutzbedürftigen Einrichtungen einer Rohrfernleitungsanlage gegen durch Kompromittierung ausgelöste Störungen gesichert sein.

(2) Die sicherheitsrelevanten MSR-Einrichtungen und autarken Sicherheitseinrichtungen von Rohrfernleitungsanlagen und ihre Folgefunktionen müssen auch unter Beachtung der jeweils vom Betreiber festgelegten CS-Maßnahmen geeignet und funktionsfähig sein.

(3) Der Betreiber hat gemäß § 4 Abs. 2 RohrFLtgV und § 3 Absatz 7 BetrSichV seine festgelegten CS-Maßnahmen regelmäßig und anlassbezogen in Abhängigkeit der allgemeinen Cyberbedrohungslage oder nach Cybersicherheits-Vorfällen zu überprüfen, ggf. anzupassen und zu dokumentieren.

(4) Die Prüfaussage richtet sich nach den zum Zeitpunkt der jeweiligen Prüfung geltenden Anforderungen aus der Prüfungsgrundlage (RohrFLtgV) und der zugehörigen technischen Regel TRFL. Technische Regeln zur Betriebssicherheit (TRBS) werden in geeigneter Form berücksichtigt.

4 Prüfung der CS- Maßnahmen für schutzbedürftige Einrichtungen

Vorbemerkung:

Die folgenden Prüfschritte durch eine Prüfstelle richten sich nach den zum Zeitpunkt der jeweiligen Prüfung geltenden Anforderungen aus der Prüfungsgrundlage (RohrFLtgV) und der zugehörigen technische Regel TRFL bei der Prüfung einer Rohrfernleitungsanlage durch eine Prüfstelle. Die TRBS 1115 Teil 1 wurde hierbei zugrunde gelegt. Die Einführung der einzelnen Prüfschritte nach diesem Abschnitt erfolgt zeitlich gestaffelt.

Bei Prüfungen der Prüfstelle wird die Prüfung der CS-Maßnahmen im Zuge der Prüfung gemäß Abschnitt 1 Absatz 1 der sicherheitsrelevanten MSR-Einrichtungen sowie der autarken Sicherheitseinrichtungen durchgeführt. Die gemäß TRBS 1115 Teil 1 festgelegten CS-Maßnahmen bei betrieblichen MSR-Einrichtungen, die als schutzbedürftige Einrichtungen identifiziert wurden, sowie der Umgebung sind hierbei zusätzlich zu berücksichtigen.

Können keine nachvollziehbaren und ausreichend aktuellen Nachweise der Eignung und Funktionsfähigkeit von CS-Maßnahmen vorgelegt werden, sind vertiefende Prüfungen durch die Prüfstelle (nach entsprechender Beauftragung) erforderlich.

Die Prüfstelle kann sich die durch die Anwendung eines Managements der Cybersicherheit erzeugten Ergebnisse zu eigen machen (siehe hierzu Abschnitt 4.5). Wird kein Management der Cybersicherheit nach TRBS 1115-1 Anhang 1 angewendet, kann sich die Prüfstelle die Ergebnisse der Überprüfung der Wirksamkeit der CS-Maßnahmen zu eigen machen, wenn Durchführung und Ergebnis der Überprüfung für sie plausibel und nachvollziehbar dokumentiert sind.

Die Prüfung der Eignung von CS-Maßnahmen setzt einen strukturierten und dokumentierten Prozess des Arbeitgebers voraus. Die Dokumentation hierzu ist zur Prüfung vorzulegen.

Ein möglicher Ablauf zur Planung, Realisierung und zur zusammenfassenden Dokumentation erforderlicher CS-Maßnahmen für einzelne Rohrfernleitungsanlagen 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 Rohrfernleitungsanlagen der Zweck der RohrFLtgV berücksichtigt ist,
- 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 ausgeführt wurden.

4.1 Prüfung im Anzeige- oder Genehmigungsverfahren

Es ist zu prüfen, ob der Antragsteller CS-Maßnahmen in den für das Anzeige- oder Genehmigungsverfahren zu prüfenden Unterlagen angemessen berücksichtigt hat.

4.2 Prüfung vor Inbetriebnahme oder vor Wiederinbetriebnahme gemäß § 5 Abs. 1 Nrn. 2 und 2a RohrFLtgV

4.2.1 Allgemein

(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 2.3 enthalten.

(3) Die Prüfung der Eignung der CS-Maßnahmen erfolgt in Form einer Plausibilitätsprüfung des Prozesses gemäß TRBS 1115 Teil 1 Abschnitt 4.4.3.

4.2.2 Prüfumfang

(1) Seit dem 1. September 2024 ist zu prüfen, ob Cyberbedrohungen durch den Betreiber dokumentiert behandelt werden.

(2) Seit dem 1. April 2025 ist zu prüfen, ob Cyberbedrohungen durch den Betreiber geeignet behandelt werden, u. a. sind hierbei die in den folgenden Absätzen dargestellten Punkte zu prüfen.

a) Sind die sicherheitsrelevanten MSR-Einrichtungen und weitere schutzbedürftige Einrichtungen sowie ihre Aufgaben erfasst und dokumentiert?

b) Wurden mögliche Auswirkungen auf die Integrität und Verfügbarkeit der Einrichtungen durch Cyberbedrohungen ermittelt und bewertet?

Hinweis: Die Bewertung der möglichen Auswirkungen erfolgt ohne Berücksichtigung von bereits bestehenden oder geplanten CS-Maßnahmen.

c) Sind nachvollziehbare Festlegungen von CS-Maßnahmen für die Einrichtungen getroffen, um die geforderte Funktionsfähigkeit sicher zu stellen, und sind sie plausibel?

- Gibt es eine dokumentierte Festlegung der erforderlichen Maßnahmen der Cybersicherheit (Ja / Nein). Wenn ja, wurden die Standardmaßnahmen der TRBS 1115-1 Abschnitt 4.5.2 Absatz 2 behandelt?
- Sind Herstellervorgaben vorhanden und wenn ja, wurden diese berücksichtigt?

d) Gibt es Verfahren zur Aufrechterhaltung des Cybersicherheitsniveaus (z. B. Aufspielen von Software-Updates oder sicherheitsrelevanten Patches)?

e) Wurden die Vorgaben für die organisatorischen CS-Maßnahmen in Betriebsanweisungen umgesetzt?

f) Wurde die mögliche Beeinträchtigung der Wirksamkeit der sicherheitsrelevanten MSR-Einrichtungen und autarken Sicherheitseinrichtungen durch die festgelegten CS-Maßnahmen und deren Umsetzung betrachtet (Rückwirkungsfreiheit)?

(3) Die Prüfung der Funktionsfähigkeit der CS-Maßnahmen im geeigneten Umfang erfolgt ab dem 1. April 2027. Hilfestellungen aus dem EK ZÜS zur Prüfung der Funktionsfähigkeit der Maßnahmen der Cybersicherheit können herangezogen werden.

4.3 Wiederkehrende Prüfung

4.3.1 Allgemein

Die erstmalige Prüfung der CS-Maßnahmen bei einer Anlage, die wiederkehrend gemäß § 5 RohrFLtgV geprüft wird, erfolgt sinngemäß des Abschnittes 4.2, inklusive der dort festgelegten stufenweisen Einführung der Prüfumfänge.

4.3.2 Prüfumfang entsprechend der festgelegten Stufen

(1) Seit dem 1. September 2024 ist zu prüfen, ob Cyberbedrohungen im Rahmen der Gefährdungsbeurteilung dokumentiert behandelt werden.

(2) Ab dem 1. April 2026 ergeben sich die folgenden Prüfinhalte:

- Sind die vorgesehenen CS-Maßnahmen weiterhin geeignet?
- Liegen Vorgaben zur regelmäßigen Kontrolle der CS-Maßnahmen vor und werden diese durchgeführt?
- Sind Nachweise der Kontrolle der technischen und organisatorischen CS-Maßnahmen vorhanden?
- Werden anlassbezogene neue Erkenntnisse zu Cyberbedrohungen, z. B. nach bekanntgewordenen Sicherheitslücken oder aus dem fortschreitenden Stand der Cybersicherheitstechnik berücksichtigt?
- Wurden falls erforderlich Anpassungen an den CS-Maßnahmen vorgenommen?
- Wurden prüfpflichtige Änderungen an der überwachungsbedürftigen Anlage hinsichtlich der Auswirkungen auf die erforderlichen CS-Maßnahmen bewertet?

(3) Die Prüfung der Funktionsfähigkeit der CS-Maßnahmen im geeigneten Umfang erfolgt ab dem 1. April 2027. Hilfestellungen aus dem EK ZÜS zur Prüfung der Funktionsfähigkeit der Maßnahmen der Cybersicherheit können herangezogen werden.

4.4 Umgang mit bereits vorhandenen Bestätigungen der Cybersicherheit bei Prüfungen durch die Prüfstelle

4.4.1 Durch den 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.

4.4.2 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 von Rohrfernleitungsanlagen 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 abdeckt und als erfüllt bestätigt wurde. Insbesondere ist dabei zu berücksichtigen, ob

- das Zertifikat den Bericht der schutzbedürftigen Systeme im Sinne dieses Beschlusses mit abdeckt,
- der Schutz von Menschen und Umwelt vor schädlichen Einwirkungen durch die Rohrfernleitungsanlage 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.

4.4.3 Berücksichtigung von Ergebnissen aus Prüfungen der Cybersicherheit nach anderen Rechtsgebieten

Ergebnisse aus Prüfungen der Cybersicherheit nach anderen Rechtsgebieten können bei der Prüfung der Cybersicherheit von Rohrfernleitungsanlagen 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 Menschen und Umwelt vor schädlichen Einwirkungen durch die Rohrfernleitungsanlage 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.

4.5 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 Rohrfernleitungsanlage wirksam, und die Belastbarkeit der übernommenen Ergebnisse für die Prüfstelle nachvollziehbar sind. Hierzu ist durch die Prüfstelle eine Plausibilitätsprüfung des CSMS hinsichtlich der Erfüllung der Anforderungen gemäß 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 Rohrfernleitungsanlagen erfolgen.

Als konkretisierende Hilfestellung für eine Plausibilitätsprüfung von Auditinhalten kann unter Anderem der Anhang 1 „Themenkatalog“ des „VCI-Statuspapier zur Cybersicherheit in der Chemie“ verwendet werden.

5 Mängeleinstufung

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

Geringfügiger Mangel:	Die Dokumentation zur Behandlung von Cyberbedrohungen wurde nicht vorgelegt, 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 Systemen, 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.

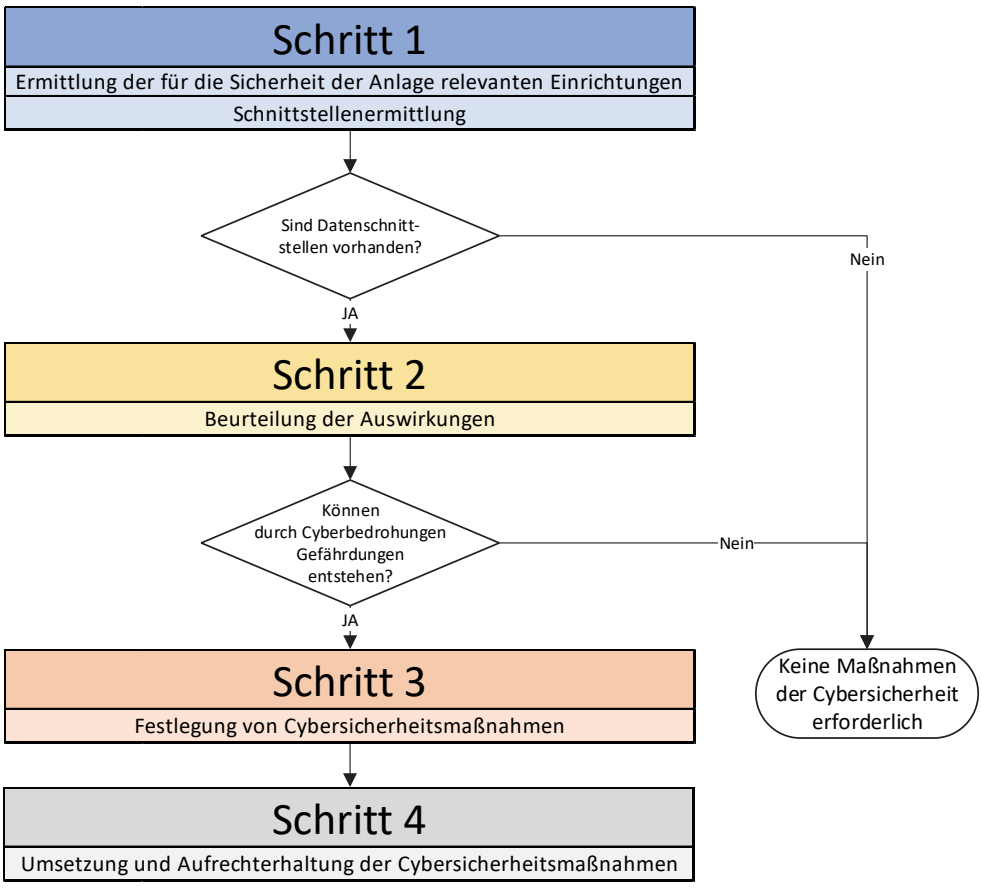

Abbildung 2: Ablauf zur Ermittlung der erforderlichen CS-Maßnahmen

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 Cybersicherheitsniveaus 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?	Erstmalige Prüfung der CS-Maßnahmen[1]		Wiederkehrende Prüfung der CS-Maßnahmen	
			Prüfstelle	Übernahme der Ergebnisse möglich	Prüfstelle	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 Rohrfernleitungsanlagen von dem Schutz von Menschen und Umwelt vor schädlichen Einwirkungen durch die Rohrfernleitungsanlage 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		–	
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?	Bestätigung in der Dokumentation oder „bestätigende Angaben“?	X		X	
9	Wird sichergestellt, dass CS-Maßnahmen die Sicherheitsmaßnahmen nicht negativ beeinflussen? (Rückwirkungsfreiheit)	Bestätigung in der Dokumentation „oder bestätigende Angaben“	X	X	–	

[1] Erfolgt im Rahmen einer Prüfung vor Inbetriebnahme, vor Wiederinbetriebnahme oder im Falle der erstmaligen Prüfung der CS-Maßnahmen im Rahmen einer wiederkehrenden Prüfung.

Prüfschritt Nr.	Prüffrage	Ist eine Aussage/ein Inhalt zu den u. g. Sachverhalten in Dokumentation des Betreibers vorhanden?	Erstmalige Prüfung der CS-Maßnahmen[1]		Wiederkehrende Prüfung der CS-Maßnahmen	
			Prüfstelle	Übernahme der Ergebnisse möglich	Prüfstelle	Übernahme der Ergebnisse möglich
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?	Aussage des Betreibers „oder 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