Beschluss des EK Rof **B-001 rev 1**

Abgestimmt im EK Rof	schriftlich Abstimmung	12.07.2024
	10. Sitzung	06.03.2025

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 schutzbedürftiger 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 Berücksichtigung 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.

3 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

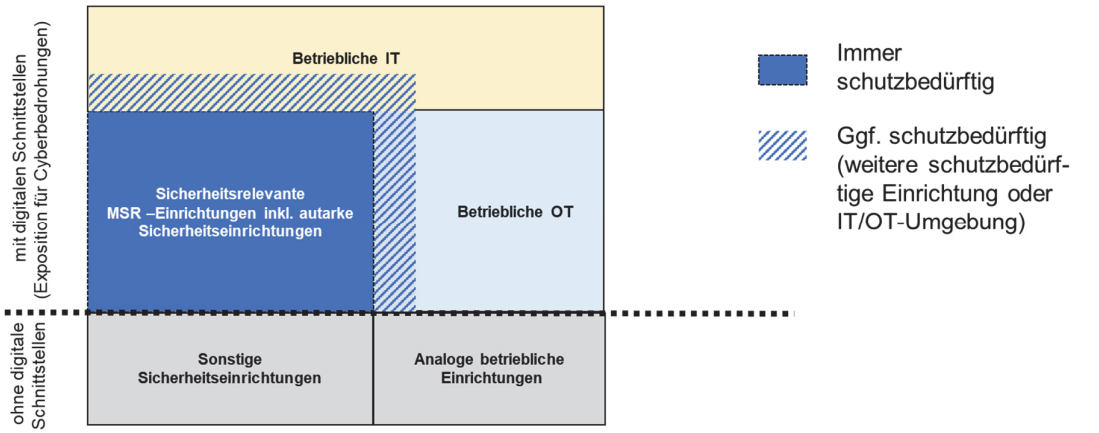

Abbildung 1: Darstellung der schutzbedürftigen Einrichtungen und der IT/OT-Umgebung

(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. 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 sind.

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

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 1115-1 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) Die Prüfung der Eignung der CS-Maßnahmen erfolgt in Form einer Plausibilitätsprüfung des Prozesses gemäß TRBS 1115-1 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) Ab 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 erst zu einem späteren Zeitpunkt.

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 zu einem späteren Zeitpunkt.

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

4.4.1 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 1115-1 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 nur berücksichtigt werden, wenn eine Zertifizierung des ISMS/CSMS durch eine unabhängige Zertifizierungsstelle (Third-Party) vorhanden ist und die Zertifizierung die Anforderungen der TRBS 1115-1 abdeckt.

Ein ISMS/CSMS kann bei der Prüfung der Cybersicherheit berücksichtigt werden, wenn das ISMS/CSMS insbesondere

– den Bereich der schutzbedürftigen Systeme im Sinne dieses Beschlusses mit abdeckt und
– der Schutz von Personen und Umwelt ausreichend berücksichtigt ist.

Insbesondere diese Punkte sind im Rahmen einer Plausibilitätsprüfung im erforderlichen Umfang zu hinterfragen.

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

Gemäß TRBS 1115-1 besteht im Rahmen von Prüfungen die Möglichkeit, sich Ergebnisse eines CSMS des Betreibers zu eigen zu machen (vgl. TRBS 1115-1, Abschnitt 6 Abs. 4 und Abschnitt 7 Abs. 3). Dieses setzt jedoch voraus, dass das CSMS wirksam und die Belastbarkeit der übernommenen Ergebnisse für die Prüfstelle nachvollziehbar ist. Hierzu ist durch die Prüfstelle eine Plausibilitätsprüfung des CSMS hinsichtlich der Erfüllung der Anforderungen gemäß TRBS 1115-1 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.
Erheblicher Mangel:	Es gibt ungeschützte Verbindungen von schutzbedürftigen Systemen in unzureichend geschützten Bereichen, die zu Gefährdungen führen können.
Gefährlicher Mangel:	Eine Kompromittierung von schutzbedürftigen Systemen, die zu Gefährdungen führen kann, ist bereits erfolgt.

Inhaltsverzeichnis