TÜVNORD

Inspired by Knowledge

Cybersicherheitsdokument

gemäß TRBS 1115 Teil 1

tuev-nord.de/cybersicherheit

Anlagenbezeichnung

Name Anlagenbetreiber

Version	Autor	Änderung	Datum

Anhang 1: Cybersicherheitsbetrachtung der sicherheitsrelevanten Einrichtungen

1. Erläuterungen

TÜV NORD stellt Ihnen mit diesem Dokument eine Möglichkeit zur Verfügung, die Cybersicherheitsbetrachtungen Ihrer überwachungsbedürftigen Anlage (üA) einfach und übersichtlich zu dokumentieren. Die Inhalte dieses Dokuments entsprechen den aktuellen Anforderungen der Technischen Regel für Betriebssicherheit 1115 Teil 1 (TRBS 1115-1) und dem zugehörigen EK ZÜS Beschluss B 002 rev 3. Bitte halten Sie Ihre Unterlagen zur Cybersicherheit am Prüfungstag bereit, um einen reibungslosen Ablauf der Prüfung zu gewährleisten.

Die TRBS 1115-1 erhalten Sie kostenlos unter:
https://www.baua.de/DE/Angebote/Regelwerk/TRBS/TRBS-1115-Teil-1.html
Zudem finden Sie unsere Zusammenfassung der TRBS 1115-1 in leichter Sprache unter:
Inhalte_der_TRBS_1115-1_einfache_Sprache_2024-03-07a__002_.pdf (tuev-nord.de)

1.1 Ist Cybersicherheit für meine Anlage prüfpflichtig?

Wenn Sie sich nicht sicher sind, ob Cybersicherheit für Ihre Anlage und deren Prüfung relevant ist, haben Sie die Möglichkeit, dies durch die Beantwortung der drei Fragen entlang des Ablaufdiagramms (https://www.tuev-nord.de/pdf/Ablaufdiagramm_TUEV_NORD.pdf) herauszufinden.

a) Sollten Sie zu dem Ergebnis kommen, dass Cybersicherheit für Ihre Anlage nicht relevant ist, erleichtern Sie die Anlagenprüfung, indem Sie das unterschriebene Ablaufdiagramm zusammen mit Ihren anderen Unterlagen am Prüfungstag bereithalten. Bitte beachten Sie, dass nach Änderungen an der Anlage eine erneute Bewertung erforderlich ist.

b) Sollten Sie jedoch zu dem Ergebnis kommen, dass eine Cybersicherheitsbetrachtung erforderlich ist, können Sie diese mit unserem Cybersicherheitsdokument dokumentieren. In diesem Fall fahren Sie bitte mit der Cybersicherheitsbetrachtung gemäß Abschnitt 1.2 fort.

Zum Verständnis
Sicherheitsrelevante Mess-, Steuer-und Regel-Einrichtungen (sMSR-Einrichtung) beziehen sich hier auch auf: Schutzeinrichtungen, PLT-Sicherheitsfunktionen (SIF), Ausrüstungsteile mit Sicherheitsfunktion, autarke Sicherheitseinrichtungen oder Anlagenteile, welche hinsichtlich möglicher Auswirkungen von Cyberbedrohungen auf den sicheren Anlagenzustand zu untersuchen sind.

1.2 Cybersicherheitsbetrachtung der sicherheitsrelevanten Einrichtungen

Mit der Vorlage im Anhang 1 zur Cybersicherheitsbetrachtung der sicherheitsrelevanten Einrichtungen bietet TÜV NORD Ihnen die Möglichkeit, die Cybersicherheitsbetrachtung Ihrer Anlage strukturiert zu dokumentieren. Durch diese Dokumentation können Sie die gesetzlichen Anforderungen zum Thema Cyberbedrohungen für überwachungsbedürftige Anlagen erfüllen und somit einen reibungslosen Prüfungsablauf sicherstellen.

Anleitung zur Anwendung des Dokuments: Cybersicherheitsbetrachtung der sicherheitsrelevanten Einrichtungen (Anhang 1)

Tragen Sie zunächst die Bezeichnung und die Bestandteile Ihrer sMSR-Einrichtung in die Übersichtstabelle ein. Die vorgegebene Gliederung sieht die Unterteilung in Messeinrichtung (Sensor), Steuerung (Logik) und Regeleinrichtung (Aktor) vor. Bei Bedarf kann von dieser Gliederung abgewichen werden (z. B. bei Frequenzumrichtern). So erhalten Sie einen schnellen Zugriff auf die einzelnen Cybersicherheitsbetrachtungen, entlang der zugehörigen Identifikationsnummern (ID). Übertragen Sie anschließend die ID aus der Übersichtstabelle auf das jeweilige Blatt der Cybersicherheitsbetrachtung. Beachten Sie, dass für jede für die Sicherheit der Anlage relevante Einrichtung ein Dokument/Blatt auszufüllen ist.

Schritte 1.1 – 1.2

1.1 Übernehmen Sie die Bestandteile Ihrer sMSR-Einrichtung aus der Übersichtstabelle. Ordnen Sie den jeweiligen Komponenten die entsprechenden Schnittstellen (z.B. USB, Bluetooth, (W-LAN, Bussysteme etc.) zu.

1.2 Wurden keine Schnittstellen ermittelt, kreuzen Sie bitte „Nein“ an, unterschreiben das Dokument und tragen in der Übersichtstabelle „Nicht relevant, daher Ende nach Schritt 1.2“ ein. Die Betrachtung dieser sMSR-Einrichtung ist damit beendet. Beginnen Sie mit der nächsten sMSR-Einrichtung erneut in der Übersichtstabelle.

Schritte 2.1 – 2.4

Schritt 2 kann übersprungen werden, wenn in Schritt 3 pauschale Maßnahmen ergriffen werden.

2.1 Beschreiben Sie die Schutzfunktion bzw. das Schutzziel, das die sMSR-Einrichtung erfüllen soll. Beispiel: „Nach Detektion eines Drucks über 2 Bar am Sensor P1 wird die Speisepumpe sofort abgeschaltet, um ein Überlaufen des Behälters zu verhindern.“

2.2 Beschreiben Sie mögliche sicherheitstechnisch relevante Folgen einer Manipulation der Einrichtung, wie Fehlauslösungen, Blockierungen der Auslösung oder Änderungen von Parametern und Funktionen. Diese Manipulationsfolgen sind ohne Berücksichtigung bereits bestehender oder geplanter Cybersicherheitsmaßnahmen darzustellen.

Wenn keine Gefährdungen durch Manipulation auftreten können, kreuzen Sie bitte unter 2.2 „Nein“ an, unterschreiben das Dokument und tragen in der Übersichtstabelle „Nicht relevant, daher Ende nach Schritt 2.2“ ein. Die Betrachtung dieser sMSR-Einrichtung ist damit beendet. Beginnen Sie mit der nächsten sMSR-Einrichtung erneut in der Übersichtstabelle.

2.3 Wenn gemäß 2.2 Gefährdungen auftreten können, beschreiben Sie bitte unter 2.3 die nicht-digitalen Gegenmaßnahmen (z. B. ein ausreichend großes Überlaufbecken als nicht-digitale Maßnahme zur Überfüllsicherung), sofern solche vorhanden sind.

2.4 Dokumentieren Sie unter 2.4, ob die Folgen einer Manipulation der sicherheitsrelevanten Einrichtung, unter Berücksichtigung der nicht-digitalen Maßnahmen, weiterhin zu einer Gefährdung führen können. Wenn dies nicht der Fall ist, kreuzen Sie bitte unter 2.4 „Nein“ an, unterschreiben das Dokument und tragen in der Übersichtstabelle „Nicht relevant, daher Ende nach Schritt 2.4“ ein. Die Betrachtung dieser sMSR-Einrichtung ist damit beendet. Beginnen Sie mit der nächsten sMSR-Einrichtung erneut in der Übersichtstabelle.

Schritte 3 und 4

Gehen Sie in Schritt 3 und 4 gemäß den Fragestellungen in der Cybersicherheitsbetrachtung vor.

3.4 Herstellerangaben: Die abgefragten Informationen können beispielsweise Vorgaben aus den Betriebsanleitungen der einzelnen Komponenten umfassen, wie die Deaktivierung von Funkverbindungen in Sicherheitsanwendungen.

3.5 Verfahren zur Aufrechterhaltung des Niveaus der Cybersicherheit: Dies können z. B. Festlegungen zur regelmäßigen Durchführung und Aktualisierung einer Gefährdungsbeurteilung und Festlegungen zur Funktionsprüfung von Cybersicherheitsmaßnahmen sein.

Nach Abschluss unterschreiben Sie das Dokument und kreuzen in der Übersichtstabelle „Ja, ist CySi-Relevant“ an.

Anhang 1: Cybersicherheitsbetrachtung der sicherheitsrelevanten Einrichtungen

Übersichtstabelle: Übersicht der für die Sicherheit der Anlage relevanten Einrichtung (sMSR-Einrichtungen)

ID	Einrichtung/Benennung/SIF	Bestandteile der für die Sicherheit der Anlage relevanten Einrichtung	CySi-Relevanz	Datum
		M: ____ S: ____ R: ____	☐ Ja, ist CySi Relevant ☐ Nicht relevant, daher Ende nach Schritt: ____	
		M: ____ S: ____ R: ____	☐ Ja, ist CySi Relevant ☐ Nicht relevant, daher Ende nach Schritt: ____	
		M: ____ S: ____ R: ____	☐ Ja, ist CySi Relevant ☐ Nicht relevant, daher Ende nach Schritt: ____	
		M: ____ S: ____ R: ____	☐ Ja, ist CySi Relevant ☐ Nicht relevant, daher Ende nach Schritt: ____	
		M: ____ S: ____ R: ____	☐ Ja, ist CySi Relevant ☐ Nicht relevant, daher Ende nach Schritt: ____	
		M: ____ S: ____ R: ____	☐ Ja, ist CySi Relevant ☐ Nicht relevant, daher Ende nach Schritt: ____	
		M: ____ S: ____ R: ____	☐ Ja, ist CySi Relevant ☐ Nicht relevant, daher Ende nach Schritt: ____	

Übersichtstabelle: Übersicht der für die Sicherheit der Anlage relevanten Einrichtung (sMSR-Einrichtungen)

ID	Einrichtung/Benennung/SIF	Bestandteile der für die Sicherheit der Anlage relevanten Einrichtung	CySi-Relevanz	Datum
		M: ____ S: ____ R: ____	☐ Ja, ist CySi Relevant ☐ Nicht relevant, daher Ende nach Schritt: ____	
		M: ____ S: ____ R: ____	☐ Ja, ist CySi Relevant ☐ Nicht relevant, daher Ende nach Schritt: ____	
		M: ____ S: ____ R: ____	☐ Ja, ist CySi Relevant ☐ Nicht relevant, daher Ende nach Schritt: ____	
		M: ____ S: ____ R: ____	☐ Ja, ist CySi Relevant ☐ Nicht relevant, daher Ende nach Schritt: ____	
		M: ____ S: ____ R: ____	☐ Ja, ist CySi Relevant ☐ Nicht relevant, daher Ende nach Schritt: ____	
		M: ____ S: ____ R: ____	☐ Ja, ist CySi Relevant ☐ Nicht relevant, daher Ende nach Schritt: ____	
		M: ____ S: ____ R: ____	☐ Ja, ist CySi Relevant ☐ Nicht relevant, daher Ende nach Schritt: ____	

ID: _____

Cybersicherheitsbetrachtung der Einrichtung: _____

1.1) Bestandteile der sMSR- Einrichtung und deren Schnittstellen

M: _____ Schnittstelle: _____

S: _____ Schnittstelle: _____

R: _____ Schnittstelle: _____

1.2) sMSR-Einrichtung enthält Schnittstellen

☐ Ja → Weiter zu 2.1 oder direkt zu 3.1
☐ Nein → Ende

2.1) Beschreibung der Schutzfunktion bzw. des Schutzziel der sMSR-Einrichtung

_____

_____

2.2) Können grundsätzlich Gefährdungen durch Manipulation entstehen

☐ Nein → Ende
☐ Ja

Falls „Ja“ → Beschreibung der sicherheitstechnisch relevanten Folgen einer Manipulation der Einrichtung

_____

_____

2.3) Beschreibung von nicht-digitalen Gegenmaßnahmen

_____

_____

2.4) Können unter Berücksichtigung von 2.3 Gefährdungen durch Cyberbedrohungen entstehen?

☐ Nein → Ende
☐ Ja → Weiter

3.1) Sind die Elemente gemäß TRBS 1115-1* Abschnitt 3.2 erfasst?

☐ Nein
☐ Ja → Dokumentationsort: _____

3.2) Sind die Maßnahmen der TRBS 1115-1 Abschnitt 4.5.2 im erforderlichen Umfang berücksichtigt?

☐ Nein
☐ Ja → Dokumentationsort: _____

Weiter auf nächster Seite

3.3) Sind die erforderlichen Maßnahmen als „Cybersicherheitsspezifikation“ festgeschrieben?

☐ Nein
☐ Ja → Dokumentationsort: _____

3.4) Liegen Herstellerangaben vor und werden diese berücksichtigt?

☐ Keine Herstellerangaben vorhanden
☐ Nein, liegen vor aber werden nicht berücksichtigt
☐ Ja → Dokumentationsort: _____

3.5) Ist ein Verfahren zur Aufrechterhaltung des Niveaus der Cybersicherheit festgelegt?

☐ Nein
☐ Ja → Dokumentationsort: _____

4.1) Sind die organisatorischen Cybersicherheitsmaßnahmen in einer Betriebsanweisung festgeschrieben?

☐ Nein
☐ Ja → Dokumentationsort: _____

4.2) Sind die technischen Cybersicherheitsmaßnahmen nachweislich funktionsfähig/wirksam?**

☐ Nein
☐ Ja → Dokumentationsort: _____

Bemerkungen

_____

_____

_____

_____ _____

Ort, Datum Unterschrift des Anlagenbetreibers

* Die TRBS 1115 Teil 1 erhalten Sie kostenlos unter https://www.baua.de/DE/Angebote/Regelwerk/TRBS/TRBS-1115-Teil-1.html

** Die Begriffe „funktionsfähig“ und „wirksam“ werden in der TRBS 1115-1 Abschnitt 5 und 8.2 erläutert

ID: _____

Cybersicherheitsbetrachtung der Einrichtung: _____

1.1) Bestandteile der für die Sicherheit der Anlage relevanten Einrichtung und deren Schnittstellen

M: _____ Schnittstelle: _____

S: _____ Schnittstelle: _____

R: _____ Schnittstelle: _____

1.2) MSR-Einrichtung enthält Schnittstellen

☐ Ja → Weiter zu 2.1 oder direkt zu 3.1
☐ Nein → Ende

2.1) Beschreibung der Schutzfunktion bzw. des Schutzziel der sicherheitsrelevanten Einrichtung

_____

_____

2.2) Können grundsätzlich Gefährdungen durch Manipulation entstehen

☐ Nein → Ende
☐ Ja

Falls „Ja“ → Beschreibung der sicherheitstechnisch relevanten Folgen einer Manipulation der Einrichtung

_____

_____

2.3) Beschreibung von nicht-digitalen Gegenmaßnahmen

_____

_____

2.4) Können unter Berücksichtigung von 2.3 Gefährdungen durch Cyberbedrohungen entstehen?

☐ Nein → Ende
☐ Ja → Weiter

3.1) Sind die Elemente gemäß TRBS 1115-1* Abschnitt 3.2 erfasst?

☐ Nein
☐ Ja → Dokumentationsort: _____

3.2) Sind die Maßnahmen der TRBS 1115-1 Abschnitt 4.5.2 im erforderlichen Umfang berücksichtigt?

☐ Nein
☐ Ja → Dokumentationsort: _____

Weiter auf nächster Seite

3.3) Sind die erforderlichen Maßnahmen als „Cybersicherheitsspezifikation“ festgeschrieben?

☐ Nein
☐ Ja → Dokumentationsort: _____

3.4) Liegen Herstellerangaben vor und werden diese berücksichtigt?

☐ Keine Herstellerangaben vorhanden
☐ Nein, liegen vor aber werden nicht berücksichtigt
☐ Ja → Dokumentationsort: _____

3.5) Ist ein Verfahren zur Aufrechterhaltung des Niveaus der Cybersicherheit festgelegt?

☐ Nein
☐ Ja → Dokumentationsort: _____

4.1) Sind die organisatorischen Cybersicherheitsmaßnahmen in einer Betriebsanweisung festgeschrieben?

☐ Nein
☐ Ja → Dokumentationsort: _____

4.2) Sind die technischen Cybersicherheitsmaßnahmen nachweislich funktionsfähig/wirksam?**

☐ Nein
☐ Ja → Dokumentationsort: _____

Bemerkungen

_____

_____

_____

_____ _____

Ort, Datum Unterschrift des Anlagenbetreibers

* Die TRBS 1115 Teil 1 erhalten Sie kostenlos unter https://www.baua.de/DE/Angebote/Regelwerk/TRBS/TRBS-1115-Teil-1.html

** Die Begriffe „funktionsfähig“ und „wirksam“ werden in der TRBS 1115-1 Abschnitt 5 und 8.2 erläutert