



IGV-MB-04B-Rev0

Stand 02.05.2025

erstellt von

Expertengruppe Behälter (EG-B)

Cybersicherheit in Verbindung mit Telemetriesystemen

Haftungsausschluss: Diese Veröffentlichung entspricht dem Stand des technischen Wissens zum Zeitpunkt der Herausgabe.

Der Verwender muss die Anwendbarkeit auf seinen speziellen Fall und die Aktualität der ihm vorliegenden Fassung in eigener Verantwortung prüfen.

Eine Haftung des IGV und derjenigen, die an der Ausarbeitung beteiligt waren, ist ausgeschlossen.

© Der IGV genehmigt hiermit die Vervielfältigung dieses Dokuments, vorausgesetzt, der Verband wird als Quelle angegeben.

1. Einführung

Die gesetzlichen Vorgaben an die Gefährdungsbeurteilung (GBU) für Druckanlagen haben sich 2022 geändert! Mit Bekanntgabe der TRBS 1115-1 (Technische Regel für Betriebssicherheit - Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen) im November 2022 müssen Arbeitgeber/Betreiber nun auch das Thema Cyber Security berücksichtigen, um den sicheren Betrieb auch bei zunehmender Digitalisierung und Vernetzung zu gewährleisten.

Denn Software-Fehler oder Hacker-Angriffe könnten zu einer Gefährdung von Personen führen. Arbeitgeber/Anlagenbetreiber sind daher verpflichtet, nach §3 der Betriebssicherheitsverordnung (BetrSichV) für Druckanlagen das Thema Cybersicherheit zu betrachten und mögliche Gefährdungen durch Cyberbedrohungen in der GBU zu dokumentieren und gegebenenfalls Maßnahmen zu ergreifen.

Auszug aus der TRBS 1115 – Teil 1

Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen

...

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.

...

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.

...

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.

2. Fragestellung

Sind die in der Gaseindustrie verwendeten Telemetrie-Einheiten zur Visualisierung des Füllstandes und des Behälterdruckes als sicherheitsrelevante MSR-Einrichtung gemäß der TRBS 1115-1 zu betrachten?

3. Ergebnis

Die Telemetrie-Einheiten zur ausschließlichen Visualisierung des Füllstandes und des Behälterdruckes stellen keine sicherheitsrelevante MSR-Einrichtung gemäß der TRBS 1115-1 dar.

Voraussetzung ist, dass keine Daten der Telemetrie für Kundenprozesse genutzt werden. Bedeutet praktisch, es erfolgt keine direkte Einbindung in die Prozesslandschaft des Kunden.

4. Erforderliche Dokumentation:

Beispiel/Muster zur Anlagendokumentation/Prüfbuch

Dokument zur Prüfkarte:

Zusammenfassende Dokumentation zur Behandlung von Cyberbedrohungen im Rahmen der Gefährdungsbeurteilung nach § 3 der BetrSichV für Druckanlagen für Anlagenbetreiber (siehe TRBS 1115 Teil 1)

Arbeitgeber/Betreiber, (Name, Vorname): _____

Aufstellungsort der Anlage (Straße, PLZ, Ort): _____

Fabriknummer(n) / Anlagenbezeichnung: _____

Equipmentnummer: _____

Im Rahmen der Gefährdungsbeurteilung (GBU) sind alle zur Druckanlage zugehörigen Schutz- und Betriebseinrichtungen hinsichtlich möglicher Cyberbedrohungen zu betrachten.

Bitte zutreffende Antwortmöglichkeit A, B oder C ankreuzen.

- A) Nein, eine Betrachtung steht noch aus.
- B) Die Druckanlage besitzt keine Angriffsziele für Cyberbedrohungen, die Auswirkungen auf den sicheren Betrieb haben können.
- C) Die Druckanlage besitzt Angriffsziele, die möglicherweise Auswirkungen auf den sicheren Betrieb haben können.

Hinsichtlich der Cybersicherheit wurden bereits folgende Teilschritte dokumentiert:

- | | |
|---|---|
| Erfassung der schutzbedürftigen Systeme und ihrer Umgebung | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Bewertung der Auswirkungen des Verlusts der Integrität und/oder Verfügbarkeit der schutzbedürftigen Systeme | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Festlegung der erforderlichen Cybersicherheitsmaßnahmen | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Umsetzung und Wirksamkeit (Funktionsprüfung) | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Beachtung der erforderlichen Rückwirkungsfreiheit der Cybersicherheitsmaßnahmen auf die Sicherheitsfunktion | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |
| Festlegung der Prozesse zur Aufrechterhaltung des Schutzes gegen Cyberbedrohung | <input type="checkbox"/> Ja <input type="checkbox"/> Nein |

Ich bestätige, dass die vollständige Dokumentation zur Durchführung der vorgenannten Tätigkeiten bei Bedarf durch die zugelassene Überwachungsstelle eingesehen werden kann.

Ort, Datum

Unterschrift Arbeitgeber/Betreiber

Firmenstempel

5. Literaturverzeichnis:

- TRBS 1115-1
- EK-ZÜS B-002 (Rev.4)
- VCI-Statuspapier Cybersicherheit in der Chemie