Baden-Württemberg
Ministerium für Umwelt, Klima
und Energiewirtschaft

DWA-BW
NACHBAR
SCHAFTEN

DWA
Klare Konzepte. Saubere Umwelt.
Landesverband
Baden-Württemberg

THEMENBERICHT **EXPLOSIONSSCHUTZ.03** MSR-EINRICHTUNGEN RICHTIG SCHÜTZEN – CYBERSICHERHEIT GEZIELT OPTIMIEREN



03.2026 // DWA-BW NACHBARSCHAFTEN – BEST PRACTICE

Einleitung

Die NIS-2-Richtlinie und die aktualisierte Technische Regel für Betriebssicherheit (TRBS) 1115-1 verknüpfen IT-Sicherheit eng mit dem Arbeitsschutz. Die TRBS 1115-1 konkretisiert die Betriebssicherheitsverordnung (BetrSichV), um die Mess-, Steuer- und Regelungstechnik- (MSR-) Einrichtungen gegen Cyber-Bedrohungen abzusichern. Beide Regelwerke fordern von Betreibern ein hohes Maß an Cyber-Resilienz. Grund: Cyberangriffe können direkte Auswirkungen auf die Anlagensicherheit haben, insbesondere wenn sie in explosionsgefährdeten Bereichen die Wirksamkeit von Schutzfunktionen beeinträchtigen.

Hintergrund

Die zunehmende Digitalisierung und Vernetzung industrieller Anlagen erhöht die Angriffsfläche für Cyber-Bedrohungen. Werden sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen beeinträchtigt, können Sicherheitsfunktionen ausfallen oder unzulässig beeinflusst werden. Dadurch können Gefahren für die Beschäftigten und die Anlagen entstehen.



© GORODENKOFF/STOCK.ADOBE.COM

BEISPIELE:

- manipulierte Gaswarnanlagen können Abschaltungen verhindern
- veränderte Lüftungssteuerung führt zu mangelhafter Belüftung von Ex-Bereichen
- manipulierte SIL-Schutzfunktionen verhindern die Sicherheitsabschaltung.

Daher hat der Gesetzgeber mit der TRBS 1115-1 ›Cybersicherheit für sicherheitsrelevante MSR-Einrichtungen‹ den Stand der Technik konkretisiert, der bei der Gefährdungsbeurteilung, der Festlegung von Maßnahmen und bei Prüfungen anzuwenden ist.

Was fordert die TRBS 1115-1?

Die Kernforderung der Regel

Betreiber müssen prüfen, ob Cyber-Bedrohungen die Sicherheitsfunktionen ihrer Anlagen beeinträchtigen können. Wenn ja, müssen sie geeignete technische und organisatorische Maßnahmen ergreifen und dokumentieren. Das betrifft nicht die klassische IT-Sicherheit im Büro, sondern die Frage: Können Cyber-Bedrohungen die zuverlässige Funktion sicherheitsrelevanter MSR-Einrichtungen und damit den Schutz von Menschen und Anlagen gefährden?



© GORODENKOFF/STOCK.ADOBE.COM

Welche Anlagen sind betroffen?

Die TRBS 1115-1 gilt für Anlagen mit sicherheitsrelevanten MSR-Einrichtungen. Im Explosionsschutz sind das typischerweise:

- Gaswarneinrichtungen mit automatischer Abschaltung
- Steuerungen für Lüftungsanlagen in Ex-Bereichen
- Inertisierungssysteme mit Überwachung
- NOT-AUS-Systeme und Verriegelungen
- Prozessleitsysteme mit sicherheitsrelevanten Funktionen
- PLT-Sicherheitseinrichtungen (SIL-Kreise)

Entscheidend ist die sicherheitsrelevante Funktion im Sinne der BetrSichV. Reine Prozesssteuerungen ohne Sicherheitsfunktion sind nicht betroffen.

BEISPIEL 1:

Rechengebäude (Ex-Zone 2): Die Lüftung wird mit einem Strömungswächter überwacht. Dieser Strömungswächter ist eingebunden in die MSR-Technik und über das Prozessleitsystem (PLS) kann der Lüftermotor gesteuert werden. Da die Lüftungssteuerung relevant für den Explosionsschutz ist, muss ein Schutzkonzept erstellt werden, für den Fall, dass ein Ferneingriff oder ein Fehler im PLS auftritt.

BEISPIEL 2:

Die Gaswarnanlage im Rechengebäude ist an die SPS-Steuerung angeschlossen. Über die SPS oder das PLS werden gewisse sicherheitsrelevante Aggregate gesteuert. Rolltore gehen auf, die Lüftung geht an oder es werden Aggregate abgeschaltet. Bei einem ›Cyberangriff‹ können sicherheitsrelevante Aggregate nicht mehr abgeschaltet oder gesteuert werden.

Festlegung der Anforderungen

Entsprechend der möglichen Gefährdungen müssen für jede Sicherheitsfunktion, die von einer MSR-Einrichtung ausgeführt werden soll, die Anforderungen an ihre Zuverlässigkeit festgelegt werden. Dies kann z. B. auf Basis des Sicherheitsintegritätslevels (SIL) oder Performance Levels (PL) erfolgen.

Zu berücksichtigen sind – neben den Anforderungen an die sicherheitsrelevante Funktion – zusätzliche Anforderungen, die sich aus den Randbedingungen des Einsatzortes ergeben.

DAZU GEHÖREN BEISPIELSWEISE:

1. Explosionsschutz
2. elektrische Schutzklassen
3. Blitzschutz
4. klimatische Bedingungen sowie Aufstellungsbedingungen

Schutzkonzept bezogen auf sicherheitsrelevante MSR-Einrichtungen

Der Arbeitgeber hat die Wirksamkeit von Schutzmaßnahmen vor der erstmaligen Verwendung eines Arbeitsmittels zu überprüfen (siehe § 4 Absatz 5 BetrSichV und TRBS 1111 Abschnitt 5.7). Dies bedeutet für sicherheitsrelevante MSR-Einrichtungen, dass die Wirksamkeit der entsprechenden Schutzmaßnahmen in Anlehnung an TRBS 1111 Abschnitt 4.2 Absatz 7 angenommen werden kann, wenn sie nach Angaben in der Betriebsanleitung und nach dem Ergebnis der Gefährdungsbeurteilung, insbesondere hinsichtlich der vom Arbeitgeber vorgesehenen Verwendung, vorhanden und aktiviert sind.

Festlegung von Schutzmaßnahmen

Die Ermittlung des Sollzustandes und die Festlegung von Schutzmaßnahmen erfolgt als Explosionsschutzkonzept im Rahmen der nach § 6 GefStoffV vorgeschriebenen Gefährdungsbeurteilung unter Berücksichtigung der technischen Regeln TRGS 720 bis TRGS 727.

Die Anforderungen aus Abschnitt 4 zur Planung, Realisierung und Dokumentation können durch Einhaltung der Anforderungen aus den Anhängen 2 und 3 der TRGS 725 erfüllt werden.

In Bezug auf die Funktionsfähigkeit der Ex-Einrichtungen dienen die Prüfungen insbesondere dazu, passive (unentdeckte) Fehler durch geeignete Maßnahmen (z. B. Prüfroutinen oder Funktionstests) zu erkennen. Der Arbeitgeber muss die sicherheitstechnischen Maßnahmen in Bezug auf die Cybersicherheit nach TRBS 1115 Teil 1:

- Bei neuen Erkenntnissen zu Cyber-Bedrohungen z. B. aus veröffentlichten oder firmeninternen Cybersicherheitsvorfällen und Schwachstellenmeldungen oder aus einschlägigen Veröffentlichungen festlegen und
- bei Änderungen des Stands der Technik der Cybersicherheit überprüfen.

Cybersicherheit im Lebenszyklus

Die Cybersicherheit muss für den ganzen Lebenszyklus der sicherheitsrelevanten MSR-Technik gewährleistet sein. Betroffen sind:

1. Hardware,
2. Software,
3. Daten/Informationen und
4. Schnittstellen

sowie die mit deren Verwendung verbundenen

1. Prozesse,
2. Richtlinien,
3. Organisationen sowie
4. Personen und die
5. IT-/OT-Umgebung.

Was ist die informations- und betriebstechnische Umgebung (IT/OT-Umgebung)?

Die IT-/OT-Umgebung im Sinne der TRBS 1115-1 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.



© XIAOLIANGGE/STOCK.ADOBE.COM

HINWEIS 1: Die IT-/OT-Umgebung kann als möglicher Angriffsweg einen Einfluss auf die Zuverlässigkeit der sicherheitsrelevanten MSR-Einrichtungen besitzen.

HINWEIS 2: IT-Systeme sind die Hard- und Softwarekomponenten zur elektronischen Datenverarbeitung (IT – Information Technology). OT-Systeme sind die Hard- und Softwarekomponenten zur Steuerung, Regelung, Überwachung und Kontrolle von Maschinen, Anlagen und Prozessen (OT – Operational Technology).

Welche Rolle spielt die Instandhaltung?

Instandhaltung im Sinne der TRBS 1115-1 umfasst die für die Aufrechterhaltung der Cybersicherheit erforderlichen Tätigkeiten an der Hard- und Software der betroffenen Komponenten. Insbesondere zählen hierzu sicherheitsrelevante Software-Updates. Betreiber sollten regelmäßig prüfen, ob die Hersteller ihrer Geräte Sicherheitsupdates veröffentlicht haben (z. B. auf deren Internetseite oder über eine Meldung des BSI). Die Sicherheitsupdates sollten zeitnah durchgeführt werden.

Wiederkehrende Prüfungen

In der Regel ist eine Prüffrist von zwölf Monaten ausreichend. Das Prüfintervall kann verändert werden, wenn dies im Rahmen der Prüffristermittlung in der Gefährdungsbeurteilung dargelegt wurde. Die so ermittelten Prüfintervalle zum Nachweis der Zuverlässigkeit können im Einzelfall über die für die gesamte Ex-Maßnahme festgelegten Maximalfristen der BetrSichV hinausgehen.

Prüffristen und Prüfumfänge werden z. B. beeinflusst durch:

1. Herstellerangaben der verwendeten Komponenten,
2. die verwendete Technologie, z. B. VPS, PLS/SPS, SSPS, sowie deren Software,
3. festgelegte Anforderungen (z. B. Betriebsbewährung, SIL, Performance Level, Wartungs- und Inspektionspläne etc.),
4. die Mean-time-to-failure (MTTF) – d. h. etwa ›mittlere Lebensdauer‹,
5. die Anforderungsrate der Betriebsart (high oder low demand) oder
6. organisatorische Maßnahmen.



BEISPIEL FÜR DIE ÜBERPRÜFUNG EINER VORHANDENEN SCHUTZMASSNAHME BEI DER ERSTINBETRIEBNAHME:

1. Abschaltung der Lüftung
2. Auffahren der Toranlage
3. Abschaltung von Aggregaten
4. Überprüfung der notwendigen Schutzausrüstung
5. Einstellung der Grenzwerte
6. Übereinstimmung der Betriebsanleitung mit der Funktion der Anlage
7. Gefährdungsbeurteilung (Ex-Schutzdokument) vorhanden

Dokumentation

Entsprechend der Anforderungen des § 3 Absatz 8 BetrSichV sind auch die Cybersicherheitsmaßnahmen für sicherheitsrelevante MSR-Einrichtungen zu dokumentieren. Dazu gehören auch Art und Umfang der diesbezüglichen Festlegungen zu Prüfungen sowie deren Fristen. Eine elektronische Form der Dokumentation ist zulässig.

Fazit

Es muss ein Schutzkonzept erstellt werden. Darin müssen alle sicherheitstechnisch relevanten Abläufe dokumentiert werden. Das heißt konkret: Es muss eine verantwortliche Person für den IT-/OT-Bereich benannt werden. Festzulegen ist auch das Verhalten der Mitarbeitenden bei einem erkannten Cyberangriff sowie die organisatorische Regelung, wenn es in Ex-Bereichen zu Fehlern oder zu Abschaltungen oder Störungen kommt. Außerdem sollte dokumentiert werden, welche Mitarbeitenden für die verschiedenen Tätigkeiten ausgebildet und geschult sind.

Alle im Netzwerk verbauten Geräte sind mit Gerätetyp und Softwarestand aufzulisten. Für alle Geräte muss regelmäßig geprüft werden, ob es ein Sicherheitsupdate gibt. Wenn ja, sollte dieses dann zeitnah installiert werden.

Der Umgang mit USB-Sticks von Fremdfirmen oder auch von internen Stellen muss geprüft werden, mit dem Ziel, zu verhindern, dass über diesen Weg Schadsoftware ins interne Netz kommt.



Bezugsquellen

- TRBS 1115-1, Technische Regel für Betriebssicherheit (TRBS), https://www.baua.de/DE/Angebote/Regelwerk/TRBS/TRBS-1115-Teil-1
- Verordnung (EU) 2019/881, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881
- TRBS 1111, https://www.baua.de/DE/Angebote/Regelwerk/TRBS/TRBS-1111
- TRGS 720 bis TRGS 727, Technische Regeln für Gefahrstoffe (TRGS), https://www.baua.de/DE/Angebote/Regelwerk/TRGS/TRGS.html
- Betriebssicherheitsverordnung (BetrSichV), http://www.gesetze-im-internet.de/bundesrecht/betrsichv_2015/gesamt.pdf
- Bundesamt für Sicherheit in der Informationstechnik (BSI), www.bsi.bund.de

HERAUSGEBER:
DWA-Landesverband Baden-Württemberg
Rennstraße 8, 70499 Stuttgart, Tel: 0711 99589-100
Email: info@dwa-bw.de
www.dwa-bw.de

AUTOR DIESER AUSGABE:
Stadtentwässerung Reutlingen
Andreas Schorpp
Wannweiler Straße 71, 72770 Reutlingen

Gefördert durch
Baden-Württemberg
Ministerium für Umwelt, Klima und Energiewirtschaft

STAND: 01.11.2026