Umsetzung Anforderungen Cyber-Sicherheit TRBS 1115-1

Ralf Schmitt
TÜV Rheinland Industrie Service GmbH

TÜVRheinland®
Genau. Richtig.

Anwendungsbereich TRBS 1115-1

Allgemein

Die Technische Regel konkretisiert die Betriebssicherheitsverordnung im Hinblick auf die Ermittlung und Festlegung erforderlicher Cybersicherheitsmaßnahmen für die dauerhafte Sicherstellung der Funktionsfähigkeit von sicherheitsrelevanten Mess-, Steuer- und Regeleinrichtungen (MSR-Einrichtungen), die als technische Schutzmaßnahme für die sichere Verwendung

- eines Arbeitsmittels inklusive
- einer überwachungsbedürftigen Anlage

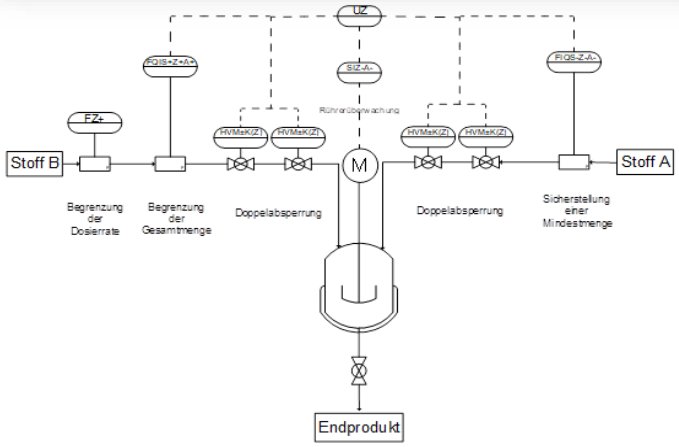
eingesetzt werden.

Ergänzend zur TRBS 1201 beschreibt sie auch:

- die Durchführung von Prüfungen und Kontrollen zur Cybersicherheit sowie
- das Vorgehen bei Änderungen von Arbeitsmitteln im Zusammenhang mit der Cybersicherheit von sicherheitsrelevanten MSR-Einrichtungen.

Welche Anlagen sind betroffen

Spezifische Betrachtung im Gefahrenfeld Druck



Prinzipskizze der verfahrenstechnischen Einrichtungen und der steuerungstechnischen Zusammenhänge für das Beispiel Rührreaktor

1. Alle technischen Schutzmaßnahmen, die im Sinne der TRBS 2141 mit steuerungstechnischer Netzwerkanbindung oder netzwerkfähigen MSR-Einrichtungen realisiert wurden. Hierzu zählen auch steuerungstechnische Einrichtungen oder Anlagenteile wie
   - frequenzgeregelte Fördereinrichtungen
   - Einrichtungen zur unmittelbaren Druckbegrenzung (Abschaltung Druckerzeugung)

2. Alle netzwerkfähigen Einrichtungen mit autarker elektronischer Steuereinheit, wie z. B. Ausrüstungsteile mit Sicherheitsfunktion gemäß Richtlinie 2014/68/EU, wie z. B. gesteuerte Sicherheitseinrichtungen und Begrenzungseinrichtungen

Was sind Cyberbedrohungen

Spezifische Betrachtung im Gefahrenfeld Explosionsschutz

1. Ex-Einrichtungen entsprechend TRGS 725

2. Alle netzwerkfähigen Einrichtungen mit autarker elektronischer Steuereinheit, wie z. B.

   - automatische Regalbediengeräte
   - Gaswarneinrichtungen
   - Lüftungsanlagen
   - Inertisierungseinrichtungen
   - Notauseinrichtung
   - Löscheinrichtungen incl. Brandmeldeeinrichtung

3. Alle netzwerkfähigen Anlagenteile, wie z. B.
   - Ventile,
   - Armaturen,
   - Überfüllsicherungen,
   - Grenzwertgeber

Was sind Cyberbedrohungen

Spezifische Betrachtung im Aufzüge

- PESSRAL
  (programmable electronic system in safety related applications for lift),
- Notrufsysteme


Summer AUS
Erkunden
Verzög. AB
Akustik AB- / Anstellen
Rücksetzen
Anwesend
ÜE AB / AN
SST AB / AN
Weitere Meldungen
Gruppen In Alarm
FEUER
STÖRUNG
Abschaltung
Gruppentest
Betrieb
Voralarm Melder
Systemstörung
Akustik AB / gestört
ÜE AB / gestört
Feuerwehr gerufen
Anwesend
Verzögerung läuft
Technischer Alarm
Störung Löschanlage
Löschanlage ausgelöst
BMZ NF3000
EN 54-2 EN 54-4
VdS 5201020
NOTIFIER®
by Honeywell

Begriffe

Definition (TRBS1115-1)

Cyberbedrohung

bezeichnet gem. Verordnung (EU) 2019/881 einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.

Hinweis: Unter „Umständen“ können z. B. Sicherheitslücken verstanden werden.

IT/OT-Umgebung

Die IT/OT-Umgebung 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.

IT-Systeme

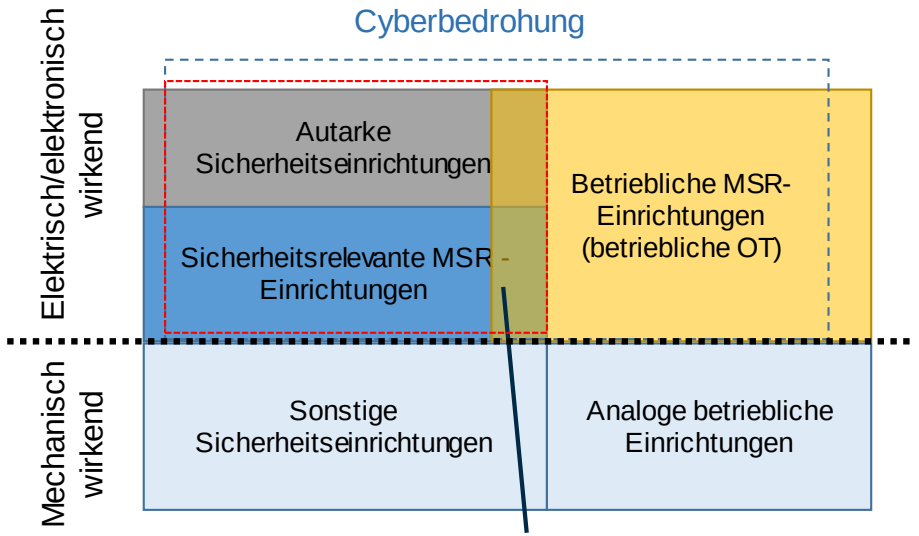
sind die Hard- und Softwarekomponenten zur elektronischen Datenverarbeitung (IT - Information Technology).

OT-Systeme (OT - Operational Technology)

sind die Hard- und Softwarekomponenten zur Steuerung, Regelung, Überwachung und Kontrolle von Maschinen, Anlagen und Prozessen.

Begriffe

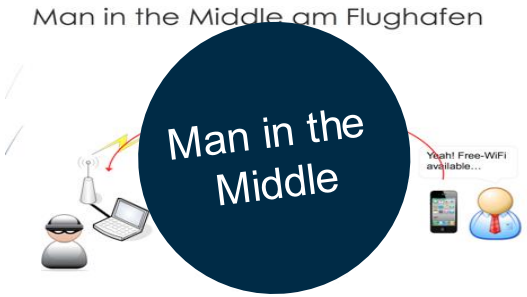
Beispiele Geräte (Assets)

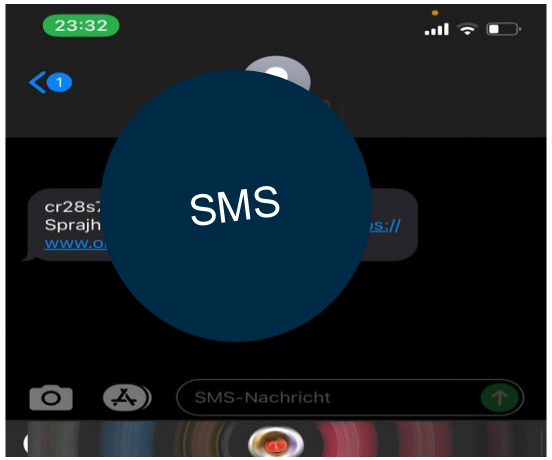


Schutzbedürftige -Einrichtungen
Betriebliche OT, die Rückwirkungen auf sicherheitsrelevante MSR- oder autarke Sicherheitseinrichtung haben kann.

Begriffe

Zugriffsmöglichkeiten

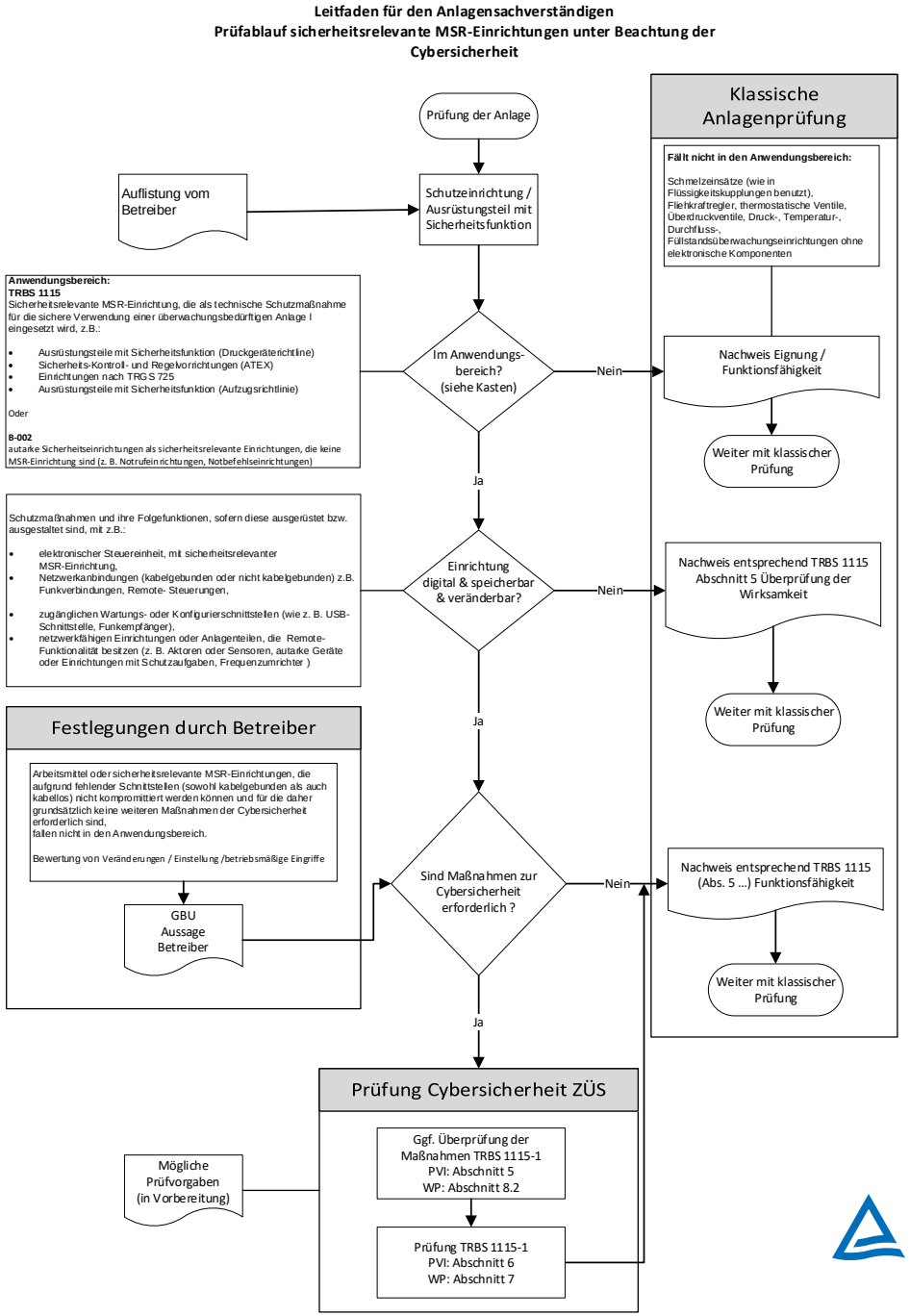




USB-Stick

Cyberbedrohungen

Wann sind die sicherheitsrelevanten MSR-Einrichtungen bei den Prüfungen hinsichtlich der TRBS 1115-1 zu berücksichtigen?



Prüfung des Arbeitsmittels / Anlage

Befinden wir uns im Anwendungsbereich?

➔ JA, sicherheitsrelevante MSR-Einrichtung, Ausrüstungsteile mit Sicherheitsfunktion (Wasserstandsbegrenzer, Druckbegrenzer, Temperaturbegrenzer).

Sind die Einrichtungen digital & speicherbar & veränderbar?

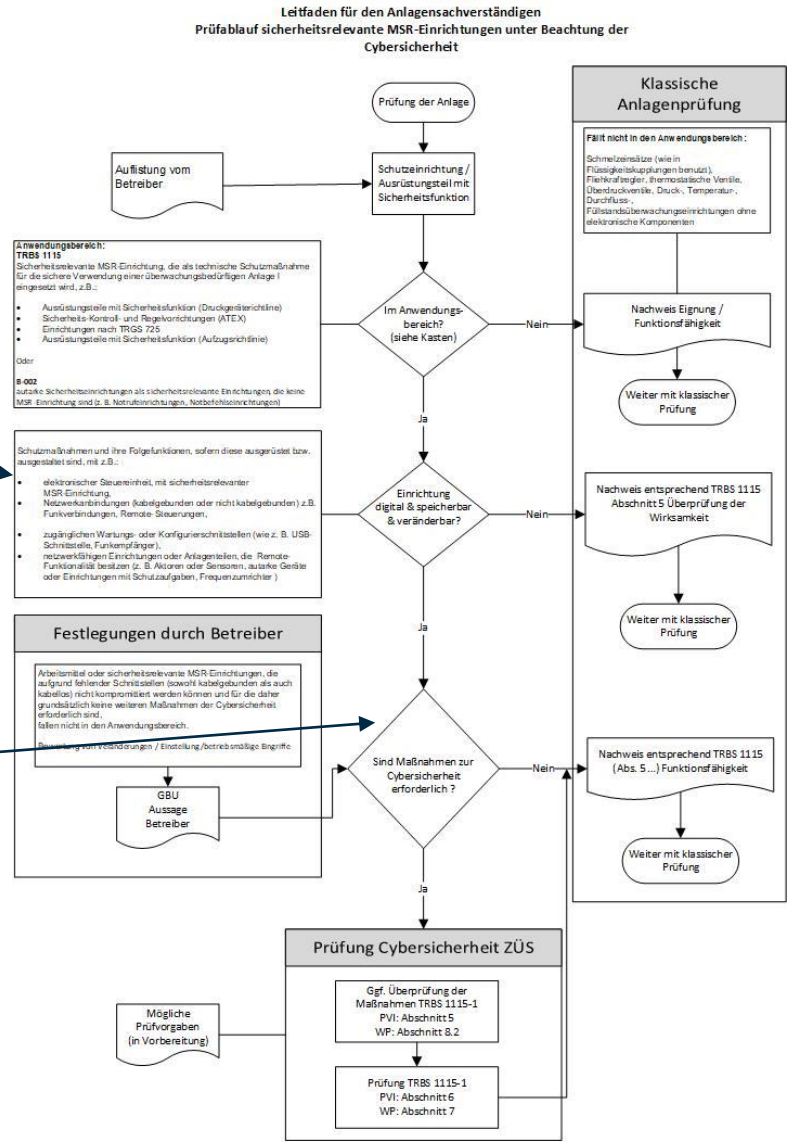
➔ Zum Teil ja (Druckbegrenzer, Temperaturbegrenzer). Netzwerkanbindung vorhanden (nicht kabelgebunden), Wartungsschnittstellen/Konfigurationsschnittstellen. Der Servicetechniker erklärte mir, dass er von der Ferne aus über eine Schnittstelle in ein Wartungssystem sich einwählen kann. Dort könnte er Werte und das System überprüfen. Grenzwerte verändern erfolgt laut seiner Aussage aber nur vor Ort. Der Mitarbeiter vom Krankenhaus hat „nur" Zugriff auf das Anwenderprogramm (läuft über das Krankenhausnetzwerk). Hier können keine Werte verstellt werden.

➔ Bei einem der Elektrodampferzeuger war ein Druckschalter von Danfoss verbaut (siehe Bild unten). Fällt somit raus und geht in das Feld *Nachweis entsprechend TRBS 1115 Abschnitt 5 Überprüfung der Wirksamkeit -> Weiter mit klassischer Prüfung*

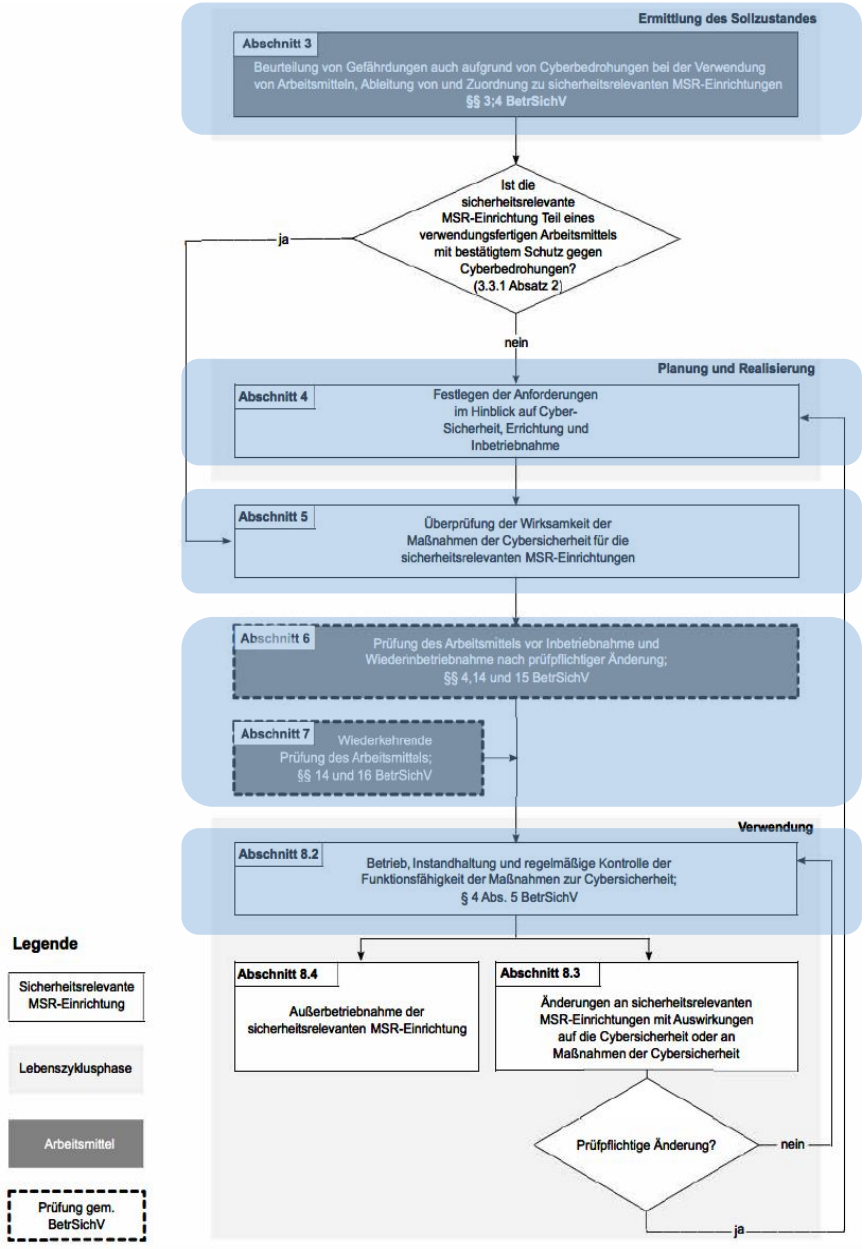
Sind Maßnahmen zur Cybersicherheit erforderlich?

➔ Fällt mir in diesem Fall schwer zu beurteilen. Eine Schnittstelle ist zwar vorhanden und Grenzwertgeber und Temperaturbegrenzer sind digital & speicherbar, aber da der Servicetechniker mir versicherte, dass nur vor Ort die Grenzwerte geändert werden können, tendiere ich eher zu Nein. Es gibt zwar eine Schnittstelle in das System. Allerdings unter der Voraussetzung, dass jemand vor Ort über das Bedienfeld den Zugang frei gibt. Des Weiteren müsste sich jemand in das Wartungssystem von MMM noch einwählen.

Genau das sind die Maßnahmen !!!



TÜVRheinland®
Genau. Richtig.



Schritte innerhalb der TRBS 1115-1

Abschnitt 3:
GBU Gefährdungen beurteilen und Maßnahmen ableiten.

Abschnitt 4:
Umsetzung der Maßnahmen

Abschnitt 5:
Überprüfung der Wirksamkeit der Maßnahmen vor erstmaliger Verwendung

Abschnitt 6 +7:
Prüfung des Arbeitsmittels / überwachungsbedürftige Anlage

Abschnitt 8.2:
Regelmäßige Kontrolle der Funktionsfähigkeit

Gefährdungsbeurteilung Cyberbedrohungen

Wieso jetzt noch eine GBU für die Cybersicherheit?
Durch den steigenden Vernetzungsgrad können sicherheitsrelevante MSR-Einrichtungen zunehmend zum Ziel von Cyberbedrohungen werden.

Wer wird für die GBU benötigt?
Die Fachkundigen Personen also die, die es können.
Dabei sind insbesondere folgende Kenntnisse erforderlich:

- gesetzliche Anforderungen, Vorschriften sowie Normen zur Cybersicherheit
- Arbeitsprozesse zur Bewertung und Aufrechterhaltung der Cybersicherheit (z. B. Erfahrung mit einem Informationssicherheitsmanagement oder eine IT-Risikobeurteilung)
- Typische Schwachstellen und Cyberbedrohungen für das Arbeitsmittel und daraus resultierende Folgen
- spezifische Kenntnis über das jeweilige Unternehmen
- Kenntnisse über Maßnahmen zum Schutz vor Cyberbedrohungen

Gefährdungsbeurteilung Cyberbedrohungen

Was sind die möglichen Auswirkungen von Cyberbedrohungen?

- Beeinflussung der Verfügbarkeit
  z. B. Deaktivieren oder Blockieren der Funktion von sicherheitsrelevanten MSR-Einrichtungen,
  Eingriff in die Steuerung,
  Unterdrückung von Alarmierungen,

- Verletzung der Integrität
  z. B. unberechtigte Änderung von

  Daten,
  Messwerte,
  Betriebsparameter,

- Verletzung der Vertraulichkeit
  z. B. Abfluss von Daten einschließlich Passwörter und Signaturen

Gefährdungsbeurteilung

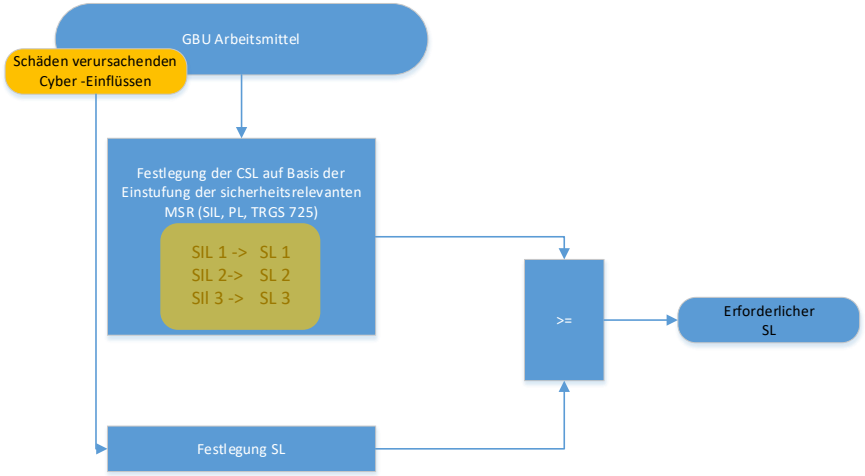
Festlegung von Maßnahmen und Realisierung

Die Festlegung der Maßnahmen sollte zwecks Nachweis der Eignung auf Basis einer der folgenden Grundlagen basieren:

- BSI Grundschutz / ICS – Kompendium
- IEC 62443-3
- ISO 270019
- VDI 2180
- …

Maßnahmen gegen Cyberbedrohungen

Gefährdungsbeurteilung



GBU: Gefährdungsbeurteilung
MSR: Messen, Steuern, Regeln
SIL: Safety Integritiy Level
SL: Security Level
PL: Peformance Level

Entsprechend den möglichen Gefährdungen werden für jede sicherheitsrelevante MSR-Einrichtung die Anforderungen an ihre Zuverlässigkeit festgelegt.

Die Cybersicherheitsmaßnahmen müssen geeignet sein, um die Funktionsfähigkeit der sicherheitsrelevanten MSR-Einrichtungen zu schützen und an deren Zuverlässigkeit angepasst sein.

Die Maßnahmen der Cybersicherheit orientieren sich an der erforderlichen Zuverlässigkeit der sicherheitsrelevanten MSR-Einrichtung

Maßnahmen gegen Cyberbedrohungen

Beispiel SL-T nach IEC 62443-3-3

Eintrittswahrscheinlichkeit		Auswirkung /Schadensereignis			
		leichte Verletzung einer oder mehrerer Personen	schwere irreversible Verletzung einer oder mehrerer Personen; Unterbrechungen möglich	Tod mehrerer Personen Erheblicher Zeit - und Ressourcenaufwand	sehr viele Todesopfer Erhebliche Beeinträchtigung der Betriebsabläufe
		(< 1 Mio. €)	(1 Mio. € - 10 Mio. €)	(> 10 Mio. €)	
	Unwahrscheinlich (es ist unwahrscheinlich, dass der Angriff erfolgt)	Gering **SL-T 1**	Mittel **SL-T 2**	Mittel **SL-T 2**	Hoch **SL-T 3**
	Möglich (der Angriff wird wahrscheinlich auftreten)	Gering **SL-T 1**	Mittel **SL-T 2**	Hoch **SL-T 3**	Extrem **SL-T 4**
	Wahrscheinlich (der Angriff wird auftreten)	Mittel **SL-T 2**	Hoch **SL-T 3**	Hoch **SL-T 3**	Extrem **SL-T 4**

Individuelle Festlegung

Nach IEC 62443-3-3 wird der SL-T in fünf Stufen unterteilt:

- **SL 0**: Keine besonderen Anforderungen und kein Sicherheitsschutz notwendig
- **SL 1**: Schutz gegen gelegentliche oder zufällige Verstöße
- **SL 2**: Schutz gegen vorsätzliche Verstöße durch einfache Mittel mit geringem Ressourcenaufwand, allgemeinen Fähigkeiten und geringer Motivation
- **SL 3**: Schutz gegen vorsätzliche Verstöße durch hochentwickelte Mittel mit moderatem Ressourcenaufwand, IACS-spezifischen Fähigkeiten und moderater Motivation
- **SL 4**: Schutz gegen vorsätzliche Verstöße durch hochentwickelte Mittel mit erweitertem Ressourcenaufwand, IACS-spezifischen Fähigkeiten und hoher Motivation

Gefährdungsbeurteilung Cyberbedrohungen

Was ist noch zu ermitteln?

- Art und Umfang sowie Fristen der Prüfungen,
- Anlässe regelmäßiger Kontrollen der Funktionsfähigkeit der Maßnahmen zur Cybersicherheit sowie deren Art und Umfang
- Wie werden neue Erkenntnissen in die GBU eingebunden.

Kommunikation mit den Fachkundigen

Achtung:

- die Ansätze der Betrachtungen sind unterschiedlich
- Begriffe werden teils unterschiedlich verwendet

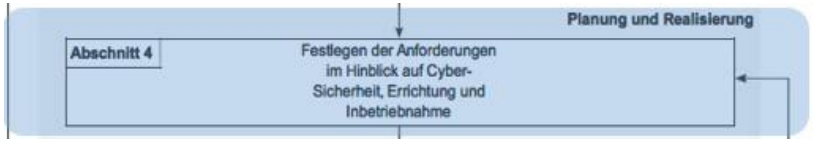
Risikobeurteilung nach IEC 62443 berücksichtigen schon vorhandenen Maßnahmen

Gefährdungsbeurteilung nach BetrSichV Betrachtung ohne vorhanden Maßnahmen

Ziele:

- Festlegung Soll-Zustand
- Auswahl der Maßnahmen

Planung und Realisierung



Für die Festlegung der erforderlichen Cybersicherheitsmaßnahmen ist wie folgt vorzugehen:

1. Erfassung aller Elemente sicherheitsrelevanten MSR-Einrichtungen und der IT/OT-Umgebung

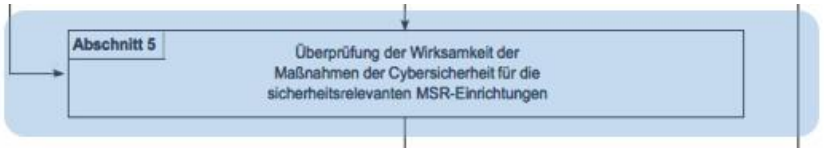
2. Erfassung und Bewertung von Bedrohungen der Integrität und Verfügbarkeit
   der sicherheitsrelevanten MSR-Einrichtungen,

3. Auswahl und Umsetzung von Cybersicherheitsmaßnahmen unter Beachtung der Auslegungsgrundsätze,

4. Festlegungen der einzuhaltenden Fristen oder Anlässe für die Durchführung von Aktualisierungen (z. B. Updates der Virensignaturen) und Kontrollen.

5. Festlegung eines Vorgehens zur regelmäßigen Ermittlung von Schwachstellen in der IT/OT-Umgebung und den Cyberbedrohungen.

Überprüfung der Wirksamkeit



Was ist das Ziel der Überprüfung?

ist die Bestätigung, dass die erforderliche Cybersicherheit der sicherheitsrelevanten MSR-Einrichtung gegeben ist.

Was sind die Bestandteile der Überprüfung?

- Entsprechend die Maßnahmen der Spezifikation?
- Sind die Beschäftigten über die organisatorischen Cybersicherheitsmaßnahmen unterwiesen und erforderlichenfalls nach den Angaben in der Betriebsanleitung bzw. der Spezifikation eingearbeitet?
- Sind alle Cybersicherheitskomponenten funktionsfähig incl. Anwenderprogramme und Ausrüstung?
- Entsprechen die Maßnahmen den festgelegten Beurteilungskriterien?

Prüfung des Arbeitsmittels / Anlage

Prüfung des Arbeitsmittels vor Inbetriebnahme und Wiederinbetriebnahme nach prüfpflichtiger Änderung nach §§ 14 und 15 BetrSichV

Es ist zu prüfen, ob die vorgesehenen Maßnahmen der Cybersicherheit geeignet und funktionsfähig sind.
Welche Fragen sind zu stellen?

- Ist eine GBU mit Berücksichtigung der Cyberbedrohungen vorhanden?
- Sind die sicherheitsrelevanten MSR-Einrichtungen erfasst und dokumentiert?
- Sind die digitalen sicherheitsrelevanten MSR-Einrichtungen hinsichtlich der möglichen Auswirkungen von Cyberbedrohungen bewertet? Wurde ein angemessenes Maß zur Cyber-Sicherheit festgelegt? (z.B. SL-T)
- Sind Festlegungen von Cybersicherheitsmaßnahmen getroffen worden sowie Art und Umfang Fristen ihrer Kontrollen und Prüfungen?
- Sind die Maßnahmen geeignet, wurde z.B. eine Norm zur Umsetzung herangezogen? (z.B. IEC 62443, IEC 27019 …)
- Wurden die Vorgaben für die organisatorischen Cybersicherheitsmaßnahmen in Betriebsanweisungen umgesetzt?
- Liegt eine Dokumentation zur Überprüfung der Wirksamkeit der Maßnahmen der Cybersicherheit nach Abschnitt 5 der TRBS 1115-1 vor?
- Ist ein ein Verfahren vorhanden, das bei der Festlegung der Maßnahmen der Informationssicherheit anlassbezogen neue Erkenntnisse berücksichtigt, die z. B. aus Cyber-Sicherheitsvorfällen oder dem fortschreitenden Stand der Cybersicherheitstechnik hervorgehen?

Prüfung des Arbeitsmittels / Anlage

Wiederkehrende Prüfung von Arbeitsmitteln mit sicherheitsrelevanten MSR-Einrichtungen nach §§ 14 und 16 BetrSichV

Es ist zu prüfen, ob Vorgaben zur regelmäßigen Kontrolle der Funktionsfähigkeit der Maßnahmen der Cybersicherheit sicherheitsrelevante MSR-Einrichtungen und ihrer IT/OT-Umgebung vorliegen.

Es ist festzustellen, ob:

- die vorgesehenen Maßnahmen der Cybersicherheit weiterhin geeignet und funktionsfähig sind.
- prüfpflichtige Änderungen an sicherheitsrelevanten MSR-Einrichtungen des Arbeitsmittels / Anlage hinsichtlich der Auswirkungen auf die erforderlichen Maßnahmen der Cybersicherheit bewertet wurden,
- prüfpflichtige Änderungen an den Maßnahmen der Cybersicherheit hinsichtlich möglicher Auswirkungen auf die sicherheitsrelevanten MSR-Einrichtungen bewertet wurden, und
- anlassbezogene neue Erkenntnisse zu Cyberbedrohungen, z. B. nach bekanntgewordenen Sicherheitslücken oder aus dem fortschreitenden Stand der Cybersicherheitstechnik berücksichtigt, und falls erforderlich Anpassungen an den Maßnahmen der Cybersicherheit vorgenommen wurden.
- Der Prüfer muss nachvollziehen, wie die geforderte Kontrollen Eignung und Funktionsfähigkeit der Maßnahmen der Cybersicherheit weiterhin erreicht wird. Alternativ kann durch den Arbeitgeber / Betreiber ein qualifiziertes Management der Cybersicherheit vorgelegt werden.

Vielen Dank für Ihre Aufmerksamkeit

TÜV Rheinland Industrie Service GmbH
Ralf Schmitt
Am Grauen Stein
51105 Köln

Mobil: **+49 171 9918823**

Mail: **Ralf.Schmitt@de.tuv.com**

TÜVRheinland®
Genau. Richtig.