TRBS 1115 -1: Lösungsansätze für die Explosionssicherheit

Ralf Schmitt

TÜVRheinland®
Genau. Richtig.

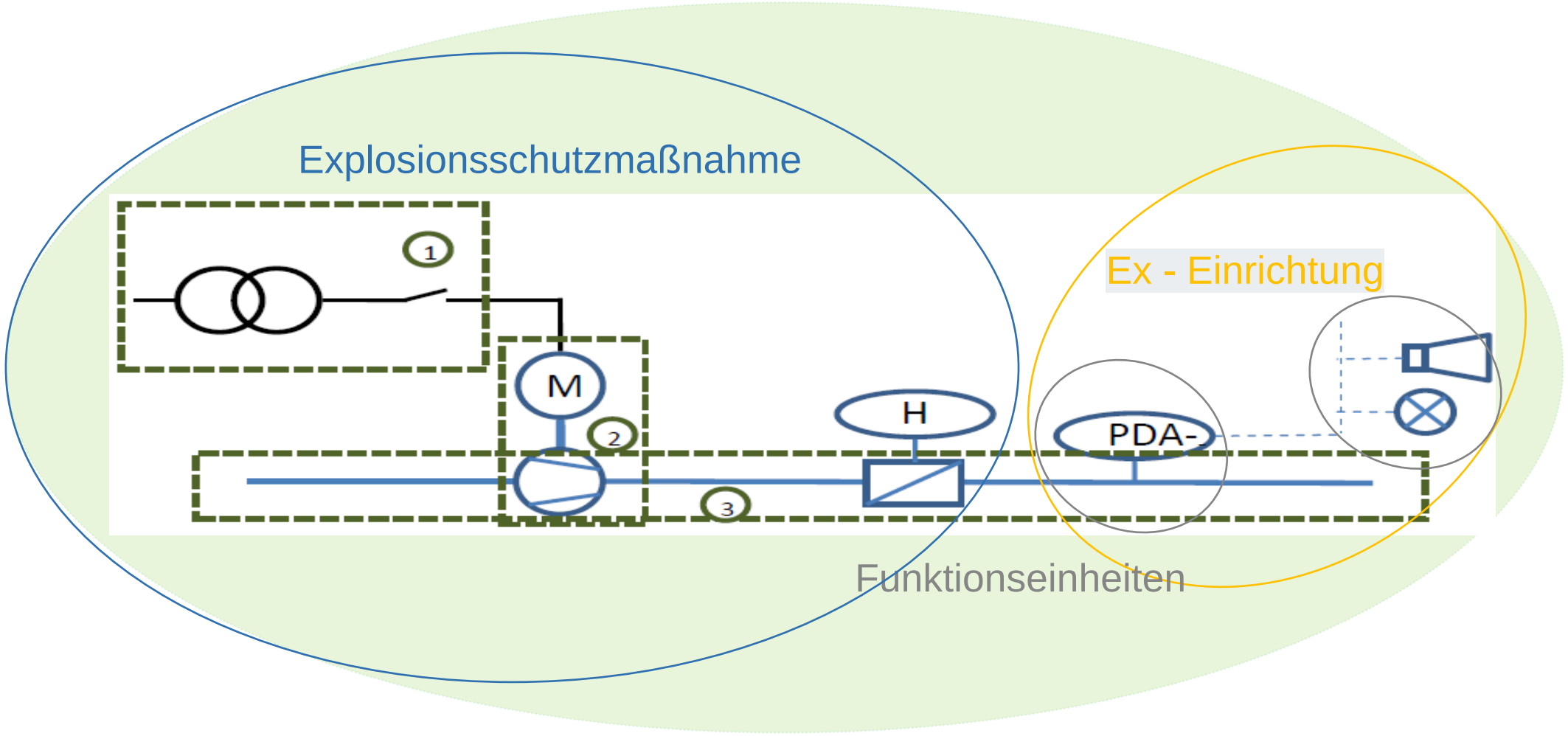
Rauchen schadet Ihrer Anlage

E-Zigarette: Aufladung per USB als Sicherheitsrisiko Foto: KENZO TRIBOUILLARD/ AFP

Diese Zigarette kann beim Aufladen irreparablen Schaden an Ihrer SPS ausrichten !

TÜVRheinland®
Genau. Richtig.

Einführung



Lüftungsanlage für primären Ex-Schutz

Einführung

Technische Ausführung von Ex-Einrichtungen mit einer Klassifizierungsstufe (K1)

Beim **komplexen** Funktionseinheiten kann von einer ausreichenden Zuverlässigkeit ausgegangen werden, wenn:

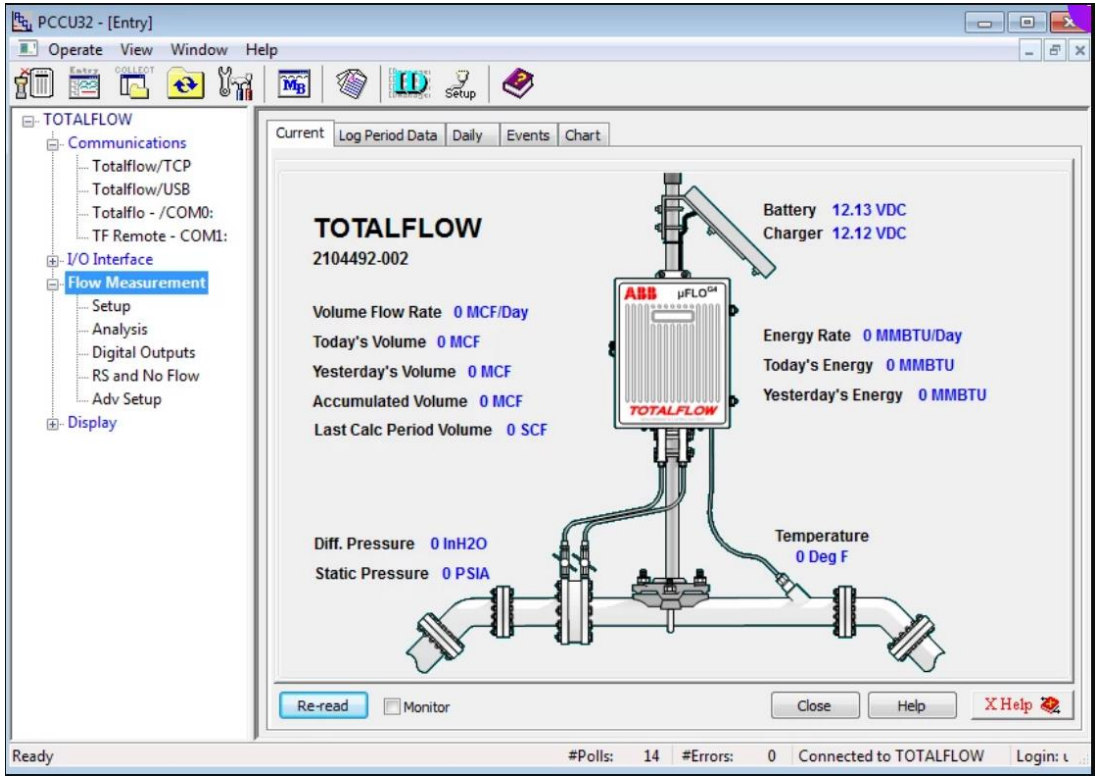
1. Erfüllung einschlägiger MSR-Industriestandards für den Zusammenbau der Bauteile,
2. Eignung für den Einsatzfall (z.B. umgebungs- und stoffbedingte Einflussgrößen),
3. Positive Erfahrung im Betriebseinsatz, z.B. durch Verwendung bewährter Technik,
4. Wartung und Inspektion im Rahmen eines Prüfkonzeptes durch Fachpersonal (§ 10 Abs. 2 BetrSichV) und
5. Verfolgung von Fehlern und Störungen und soweit erforderlich Ableitung von Korrekturmaßnahmen.

Für **PLS/SPS** sind zentralen Risiken zu betrachten und zu minimieren, Geeignete Maßnahmen sind festzulegen z.B.:

1. Betreuung und Überwachung des PLS/SPS durch fachkundige und autorisierte Personen,
2. Zugriffsschutz, d.h. Änderungsmöglichkeit nur für autorisierte Personen,
3. Maßnahmen der **Informationssicherheit (Cybersicherheit)** für das PLS liegen vor,
4. Management zur Autorisierung, Durchführung und Prüfung von Änderungen (Management of Change) liegt vor,
5. Ständige betriebliche Verwendung des PLS, wodurch die Beobachtung des PLS gewährleistet ist,
6. Geräte gehen bei Energieausfall in einen vordefinierten Zustand.

Einführung

Reale Gefährdung



November 10, 2022 By Pierluigi Paganini Posted In Breaking News Security

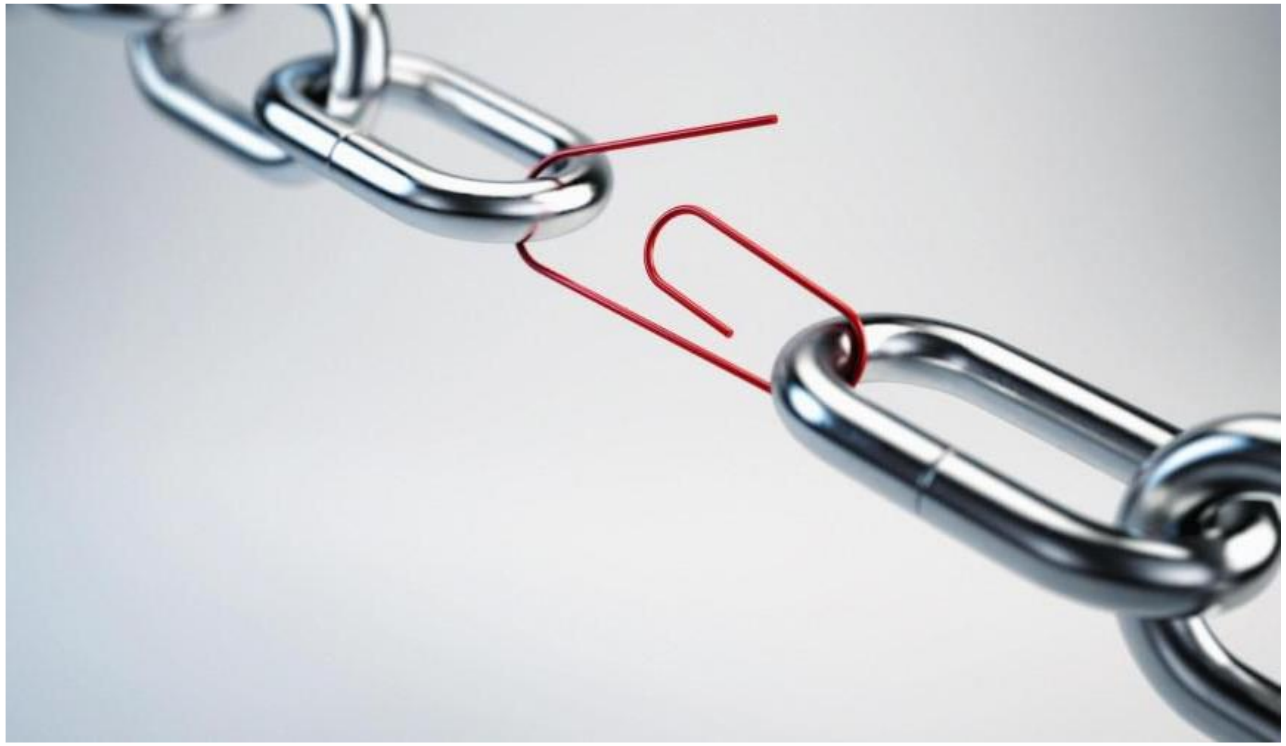
Schwachstelle bei ABB Totalflow-Durchflussrechner und Fernsteuerungen.

Systeme werden von Öl- und Gasunternehmen auf der ganzen Welt eingesetzt.

Angreifer können Schwachstelle ausnutzen, Code aus der Ferne auszuführen.

Einführung

Was hat Einfluss auf die Cybersicherheit?



- Der Mensch
- Das Team
- Das Ziel
- Das Bugdet
- Die Vorgaben

TRBS 1115 Teil 1 Cybersicherheit für sicherheitsrelevante MSR-Einrichtungen

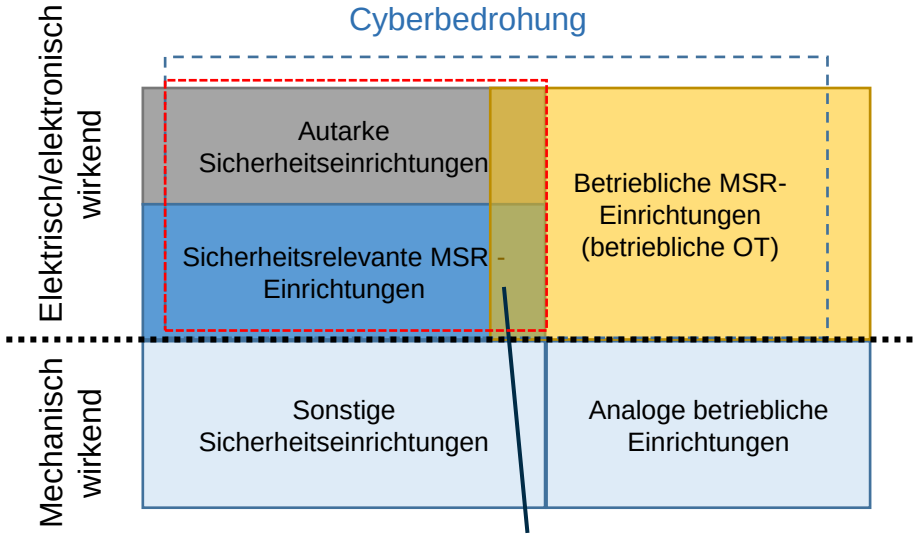
Arbeitsmittel, überwachungsbedürftige Anlagen oder technische Gebäudeausrüstungen sind zunehmend digitaler und miteinander vernetzt.
Sie stellen daher immer häufiger ein attraktives Ziel für Cyberangriffe dar.

Anforderungen:
TRBS 1115 Teil 1: „Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen“

Was bedeutet es für den Arbeitsschutz in Betrieben, wenn es darum geht, Cybersicherheitsmaßnahmen festzulegen, umzusetzen und zu prüfen?

TRBS 1115 Teil 1 Cybersicherheit für sicherheitsrelevante MSR-Einrichtungen

Welche Assets sind betroffen



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

TÜVRheinland®
Genau. Richtig.

TRBS 1115 Teil 1 Cybersicherheit für sicherheitsrelevante MSR-Einrichtungen

Erweiterte Sicht auf das Thema

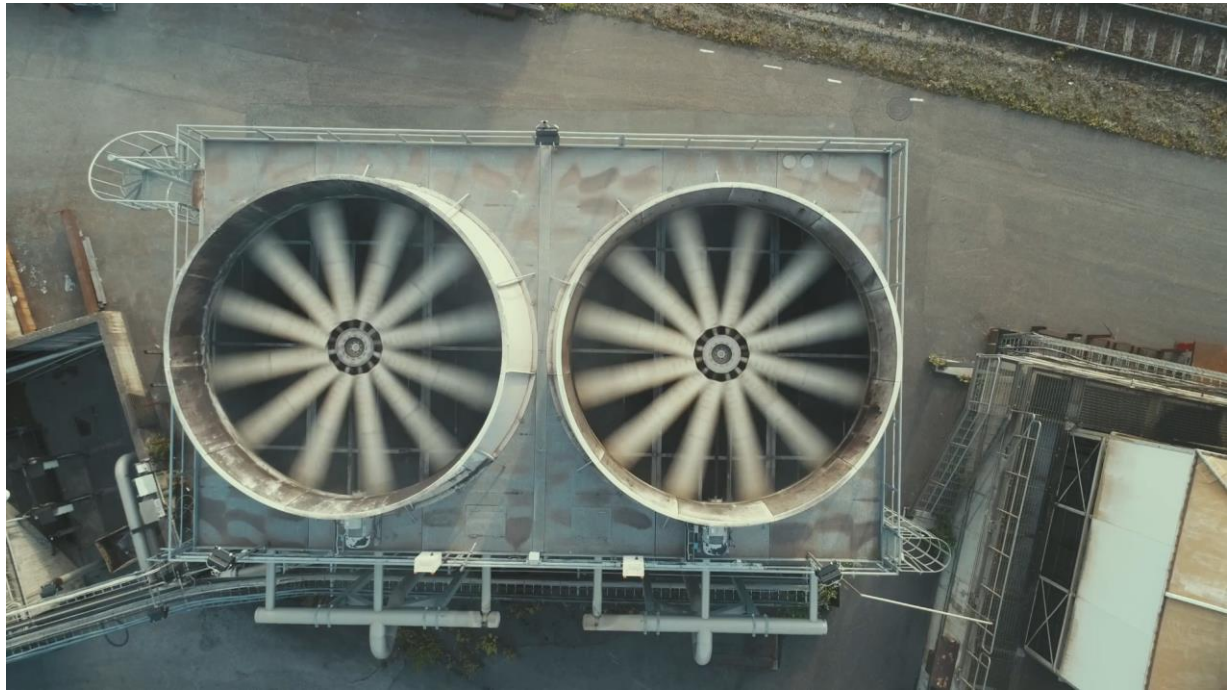
… Störungen reichen von Komforteinschränkungen, wenn Beleuchtung oder Klimatisierung der Büros beeinträchtigt ist, bis hin

zu gefährlichen Situationen, die Menschenleben gefährden können.

TÜVRheinland®
Genau. Richtig.

TRBS 1115 Teil 1 Cybersicherheit für sicherheitsrelevante MSR-Einrichtungen

Erweiterte Sicht auf das Thema

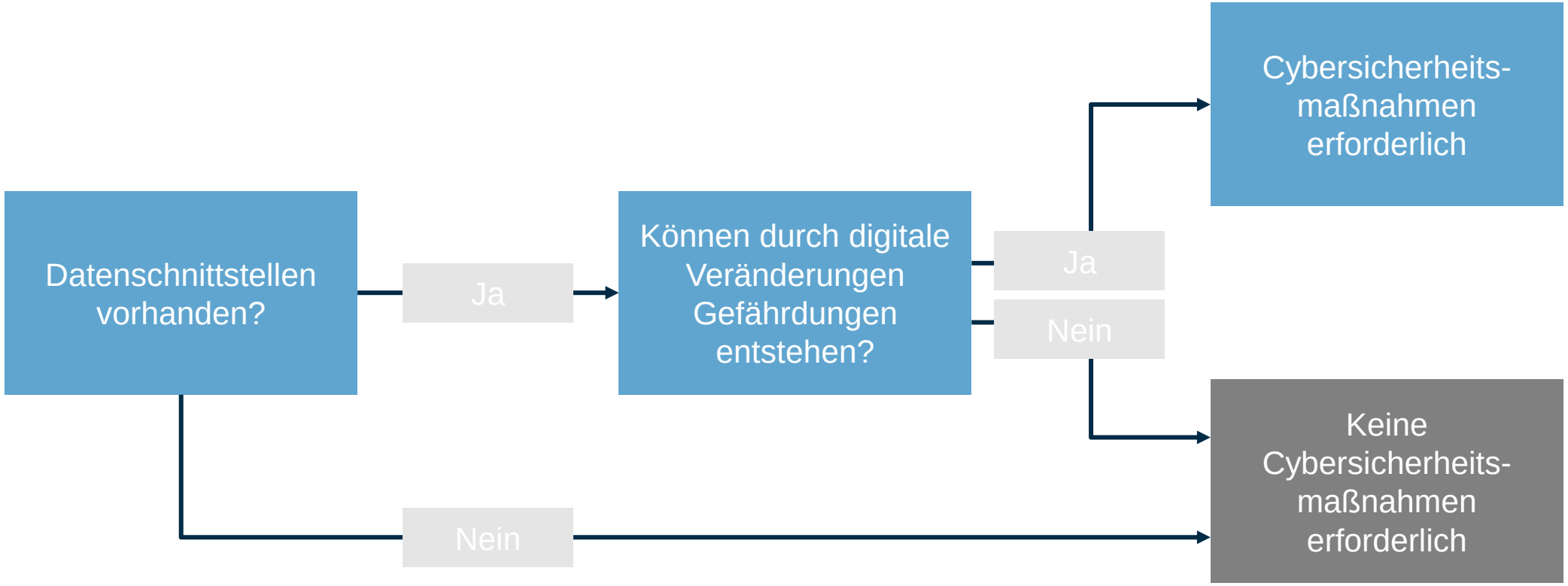


Technische Gebäudeausrüstung insbesondere:

- Brandmelde- und Alarmierungsanlagen (BMA),
- Löschanlagen,
- Kälte- und Klimaanlagen,
- Fluchttürensteuerung,
- Zutrittssysteme,
- Strom- / Energieversorgung und Energiemanagement,
- Gebäudeautomation und Gebäudeleittechnik,
- Lüftungsanlagen

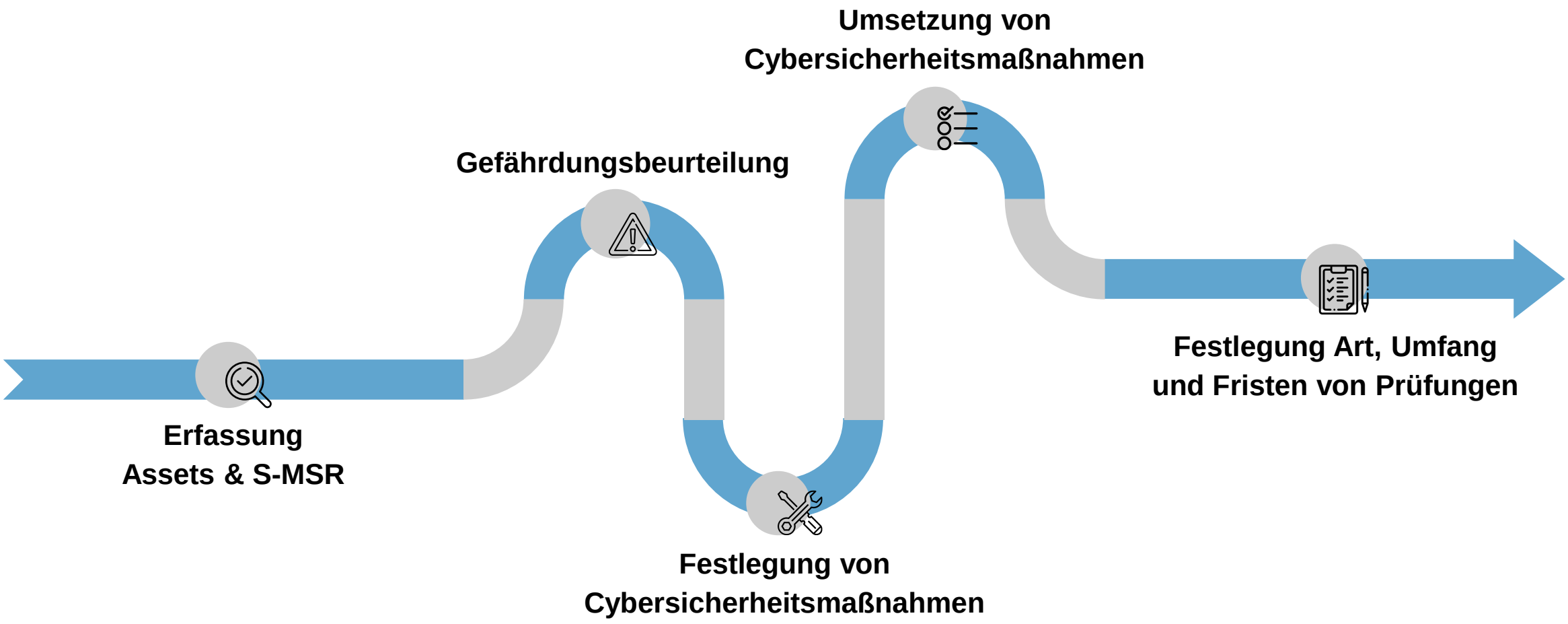
Gefährdungsbeurteilung

Erste Schritte



Gefährdungsbeurteilung

Fünf Schritte zur Erstellung der Gefährdungsbeurteilung Cybersicherheit



TÜVRheinland®
Genau. Richtig.

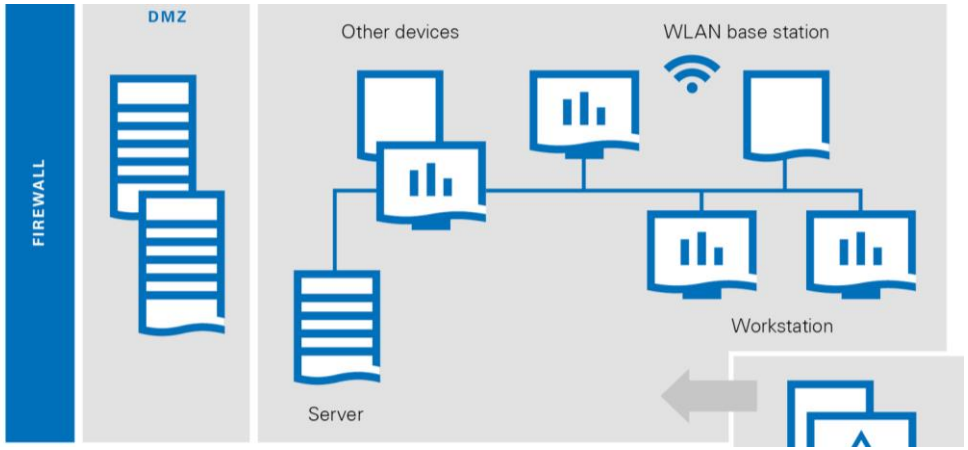
Gefährdungsbeurteilung

Auswahl & Umsetzung von Cybersicherheitsmaßnahmen

Schritt 1				Schritt 2					Schritt 3				
Feststellung der sicherheitsrelevanten Systeme			Schnittstellenermittlung	Beurteilung der Auswirkng					Festlegung Cybersicherheitsmaßnahmen				
Anlagenteil	Bezeichnung Sicherheitskreis	sicherheitsrelevanten MSR-Einrichtungen / Systeme / Schutzeinrichtungen die digital -veränderbar-speicherbar sind und über eine Schnittstelle verfügen	Auflistung der Daten-Schnittstellen	Kurzbeschreibung Schutzfunktion / Schutzaufgabe Schutzziel	Folgen einer Manipulation der Schutzfunktion	Können Gefährdungen durch die Manipulation entstehen?	Wurden technische Ersatzmaßnahmen gegen diese Gefährdung getroffen?	Welche technische Ersatzmaßnahme wurde getroffen?	Wurden Maßnahmen nach TRBS 1115-1 4.5.2 getroffen?	Verweis auf deren Dokumentation	Erfolgte eine Festschreibung zusätzlicher Cybersicherheits-maßnahmen (Spezifikation)?	Verweis auf deren Dokumentation	Festgelegtes Maß der Zuverlässigkeit
Allgemein		Druckbegrenzer	USB	Druckbegrenzung	Blockieren der Auslösung	Ja	Nein		Nein		Nein		
Klimaanlage	T1	System A	LAN	Temperaturbegrenzung	Blockieren der Auslösung	Ja	Nein		Ja	Ordner 3	Nein		SL-T 2
H2 Tankstelle	PL1	Druckbegrenzer	USB	Druckbegrenzung	Folgen Manipulation	Ja	Nein		Ja	Ordner 5	Ja	Ordner 6	hoch
		S-SPS	LAN		Blockieren der Auslösung	Ja							
		Ausgabemodul	Keine vorhanden		Manipulation nicht möglich	Nein							
		System A											

Gefährdungsbeurteilung

Notwendige Informationen und Unterlagen



- Schematische Darstellung der Anlage
- Netzwerkplan
- Auflistung der sicherheitsrelevanten MSR-Einrichtungen
- Auflistung und Erfassung der Assets
- Funktionsbeschreibung der Anlage

Fachkunde

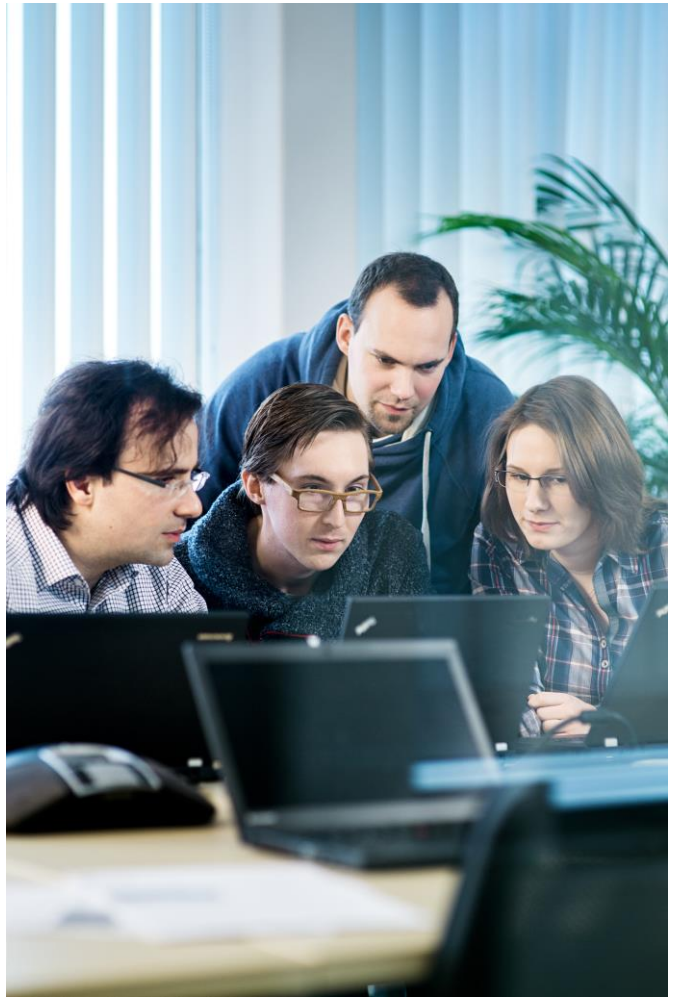
Welche Kenntnisse sind erforderlich?

Folgende Kenntnisse sind grundsätzlich erforderlich:

- gesetzlicher Anforderungen und Vorschriften sowie Normen zur Cybersicherheit sowie Branchenkenntnisse
- über das jeweilige Unternehmen
  (z.B. Umgang mit Updates, Protokollierung, Überwachung)
- Managements der Cybersicherheit
  Technologien,
  Prozesse zum Umgang mit Updates,
  Protokollierung,
  Überwachung.
- Maßnahmen zum Schutz vor Cyberbedrohungen

Fachkunde

Welche Kenntnisse sind erforderlich?



Falls der Arbeitgeber für eine sicherheitsrelevante MSR-Einrichtung eigenständig Cybersicherheitsmaßnahmen ermittelt und umsetzt, sind zusätzlich folgende Kenntnisse erforderlich:

- Informationssicherheitsmanagement,
- Vorgehensweisen zur Ermittlung von relevanten Cybergefährdungen auf Basis der Cyberbedrohungen und Schwachstellen,
- Vorgehensweisen zur systemspezifischen Auswahl von geeigneten Cybersicherheitsmaßnahmen, z. B.
    - Hardwarearchitektur und Segmentierung
    - Zugangs- und Zugriffskontrolle,
    - sichere Installation und Änderung von Cybersicherheitsmaßnahmen,
    - Funktionsreduktion und Härtung,
    - Überwachung von Hardware, Software und ihrer Kommunikation,
    - Notfallmanagement (z. B. response and recover, Disaster Recovery)

Anforderungen Gefährdungsbeurteilung

- Die Anforderungen an die Zuverlässigkeit für sicherheitsrelevante MSR-Einrichtung wird in der GBU festgelegt.

Ziele:
Einhaltung der festgelegten Funktionsfähigkeit und Zuverlässigkeit der sicherheitsrelevanten MSR-Einrichtungen

- Die Mindestinhalten nach TRBS 1115-1 4.5.2 müssen berücksichtig sein
- ein erhebliches Schadensausmaß ist als Anforderung heranzuziehen (ÜAnlG)
- Fachkundige Personen erstellen die GBU
- der Stand der Technik (Normen und Standards) werden herangezogen
- Festlegung von konkreten Maßnahmen mit Vorgaben der Fristen und Prüfumfängen

Schritte zur Umsetzung der TRBS 1115-1: Gefährdungsbeurteilung

Wichtig für die Festlegung der Cybersicherheits-Maßnahmen

- Die Mindestinhalten nach TRBS 1115-1 4.5.2 müssen berücksichtig sein
- ein erhebliches Schadensausmaß ist als Anforderung heranzuziehen (ÜAnlG)
- Fachkundige Personen erstellen die GBU
- der Stand der Technik (Normen und Standards) werden herangezogen

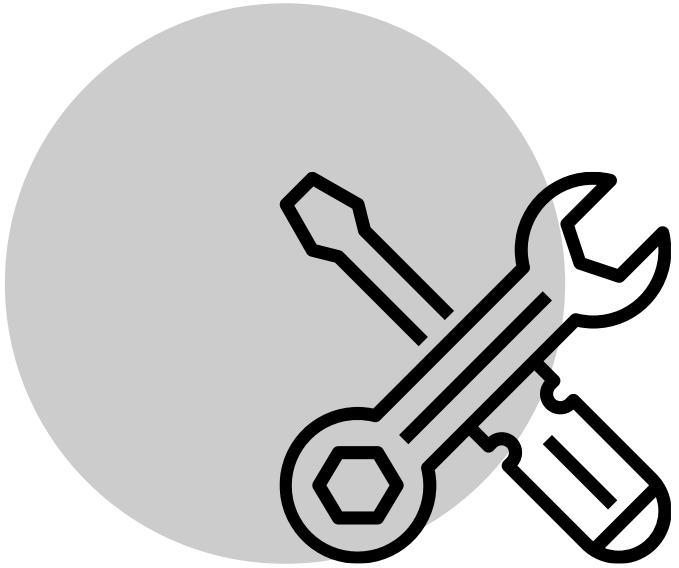
Anforderungen Gefährdungsbeurteilung

Empfehlung

- Einbindung der Fragestellungen in: HAZOP, ROGA, GBU, Sicherheitsgespräche und Explosionsschutzdokumente,
- Frage: wie kann es durch Cyberangriffe zu Situationen kommen, die eine Anlage in einen unsicheren Zustand führen?
- Beurteilung: welche Auswirkung hat eine Kompromittierung der sicherheitsrelevanten MSR?
- Festlegung der erforderlichen Cybersicherheit zur Sicherstellung der Zuverlässigkeit der MSR-Einrichtung z.B. Security – Level Target (SL-T)
- Berücksichtigung TRBS 1115-1 mit Anforderungen an die zu treffenden Maßnahmen

Schritte zur Umsetzung der TRBS 1115-1: Gefährdungsbeurteilung

Auswahl & Umsetzung von Cybersicherheitsmaßnahmen



Segmentierung

Fernzugriffs-möglichkeit

Regelungen zu Zugang und Zugriff

Härtung von Komponenten

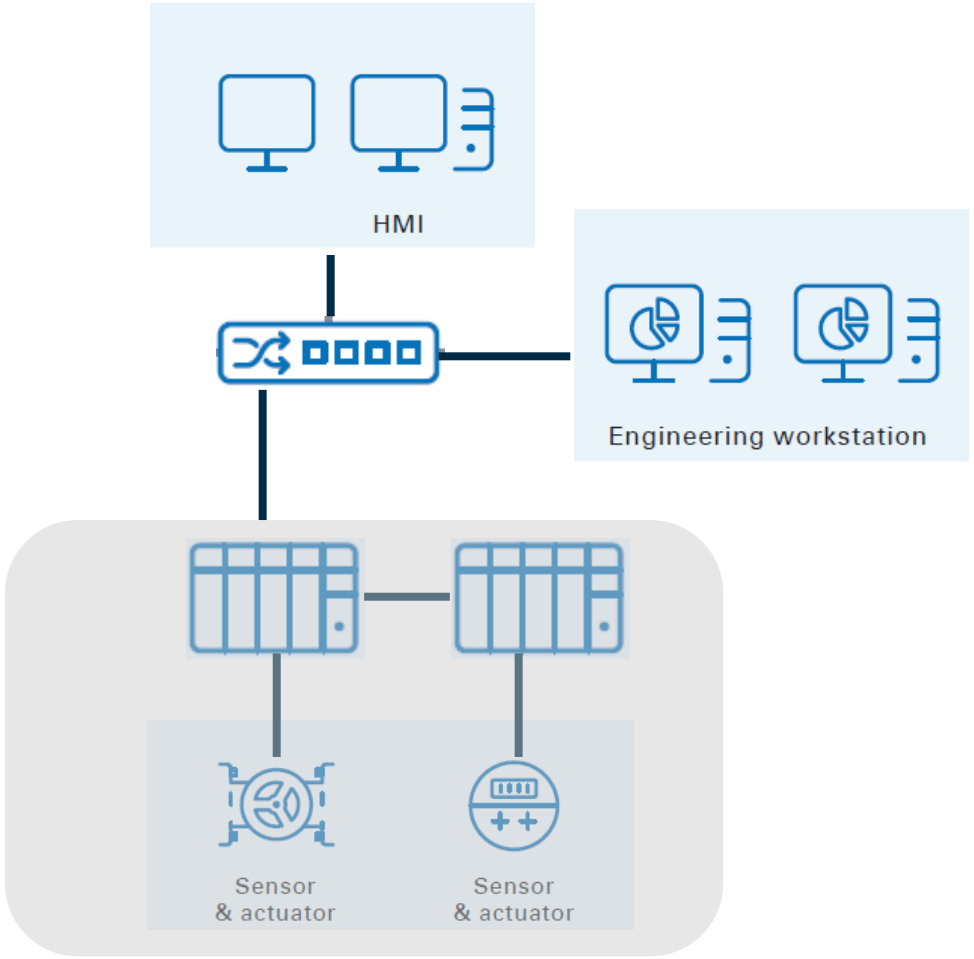
Unabhängigkeit von sicherheits-relevanten MSR-Einrichtungen

Überwachung

Notfall-management

Beispiele

Beispiel 1



Arbeitsmittel

Anlagenbeschreibung:

Das Arbeitsmittel besitzt externe Schnittstellen. Das Arbeitsmittel ist über ein arbeitsmittelbezogenes Netzwerk mit dem Konfigurationsgerät und einer Bedienstation mit Touch-Display verbunden (Inselbetrieb).

Eine Änderung von Parametern ist lokal am Arbeitsmittel oder über das Netzwerk mittels des Konfigurationsgerätes und der Bedienstation vorgesehen.

Das Arbeitsmittel verfügt über eine nicht-kompromittierbare Not-Befehlseinrichtung

Bewertung

Das Arbeitsmittel fällt wegen der für den Nutzer vorhandenen Schnittstellen unter den Anwendungsbereich der TRBS 1115 Teil 1.

Das Konfigurationsgerät, die Bedienstation und das Netzwerk müssen mitbetrachtet werden, da eine Kompromittierung die Sicherheitsfunktion beeinträchtigen kann

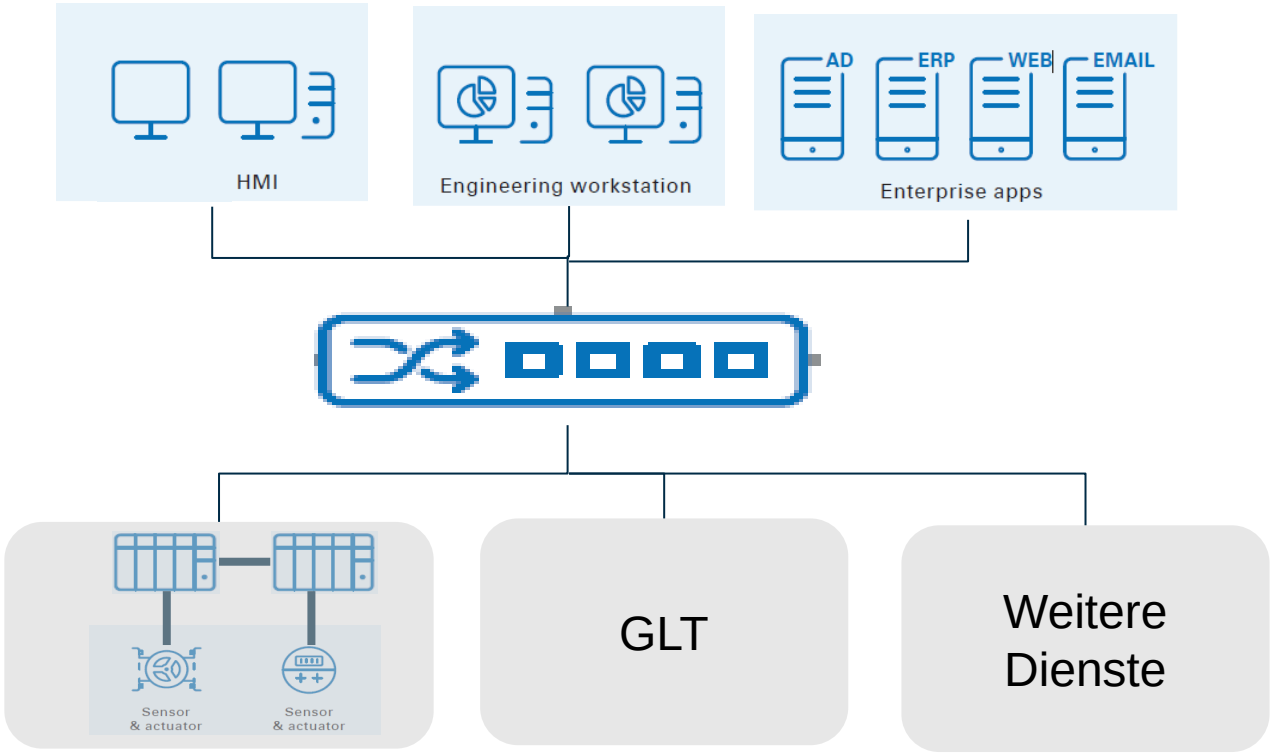
Beispiel

Beispiel 1

1	SEGMENTIERUNG UND FERNZUGRIFFSMÖGLICHKEIT	Es wird sichergestellt, dass sich in dem Netzwerk nur das Arbeitsmittel, das Konfigurationsgerät und die Bedienstation befinden.
2	REGELUNGEN ZU ZUGANG UND ZUGRIFF	Der Zugang und Zugriff für die externen Schnittstellen am Arbeitsmittel, für das Konfigurationsgerät und die Netzwerkkomponenten wird auf jeweils berechtigte Personen eingeschränkt. Dies erfordert unter anderem eine sichere Authentifizierung. Die Maßnahmen gelten auch für Wartungsdienstleister
3	HÄRTUNG VON KOMPONENTEN	Nicht benötigte Hardwareschnittstellen deaktiviert oder blockiert. Die Maßnahmen gelten auch für Wartungsdienstleister Die Konfiguration für das Arbeitsgerät, Konfigurationsgerät, Bedienstation und Netzwerkkomponenten so, dass ein unberechtigter Zugriff verhindert wird.
4	UNABHÄNGIGKEIT VON SICHERHEITSRELEVANTEN MSR-EINRICHTUNGEN	Unabhängigkeit der sicherheitsrelevanten MSR-Einrichtungen wurde durch den Hersteller berücksichtigt
5	ÜBERWACHUNG	Die Integrität der sicherheitsrelevanten MSR-Einrichtung und des Konfigurationsgeräts wird regelmäßig kontrolliert. Die Verwendung des Konfigurationsgeräts am Arbeitsmittel kann nachvollzogen werden. Die Maßnahmen gelten auch für Wartungsdienstleister
6	NOTFALLMANAGEMENT	Wenn einer Kompromittierung erkannt wird, wird das Arbeitsmittel durch die nicht-kompromittierbare Not-Befehlseinrichtung in den sicheren Zustand versetzt .Vor der Wiederinbetriebnahme ist sicherzustellen, dass keine Spuren vom Angriff im System verblieben sind

Beispiele

Beispiel 2



Arbeitsmittel

Anlagenbeschreibung:

Das Arbeitsmittel besitzt externe Schnittstellen. Das Arbeitsmittel ist dauerhaft über ein Netzwerk mit dem Konfigurationsgerät und einer Bedienstation mit Touch-Display verbunden.

Einzelne „Weitere Dienste“ haben Zugriff auf die Konfiguration des Arbeitsmittels.

Schnittstellen einzelner Teilkomponenten des Arbeitsmittels sind extern zugänglich.

Ein Ändern von Parametern ist lokal am Arbeitsmittel oder externe Schnittstellen möglich.

Bewertung

Die Bewertung muss auf Basis von etablierten Verfahren. Hierfür können beispielsweise die ISO270019, die IEC/ISO 62443-ff, die Vorgehensweise des IT-Grundschutzes des BSI oder andere gleichwertige Vorgehensweisen nach dem Stand der Technik herangezogen werden.

Beispiel

Beispiel 2

1 SEGMENTIERUNG UND FERNZUGRIFFSMÖGLICHKEIT

2 REGELUNGEN ZU ZUGANG UND ZUGRIFF

3 HÄRTUNG VON KOMPONENTEN

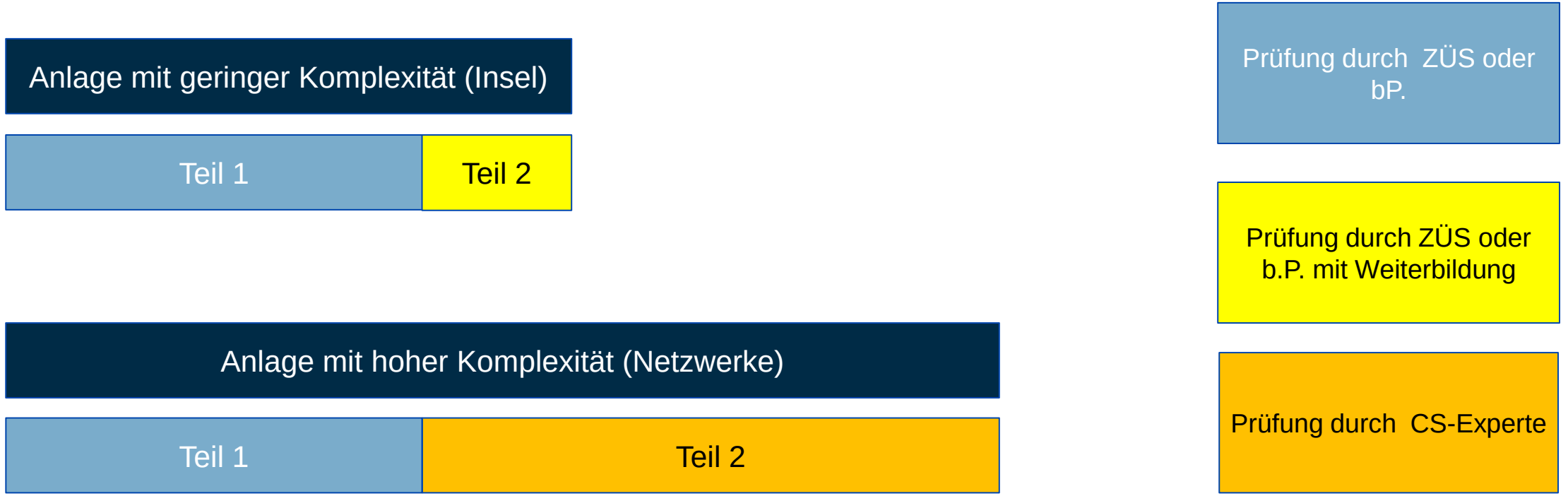
4 UNABHÄNGIGKEIT VON SICHERHEITSRELEVANTEN MSR-EINRICHTUNGEN

5 ÜBERWACHUNG

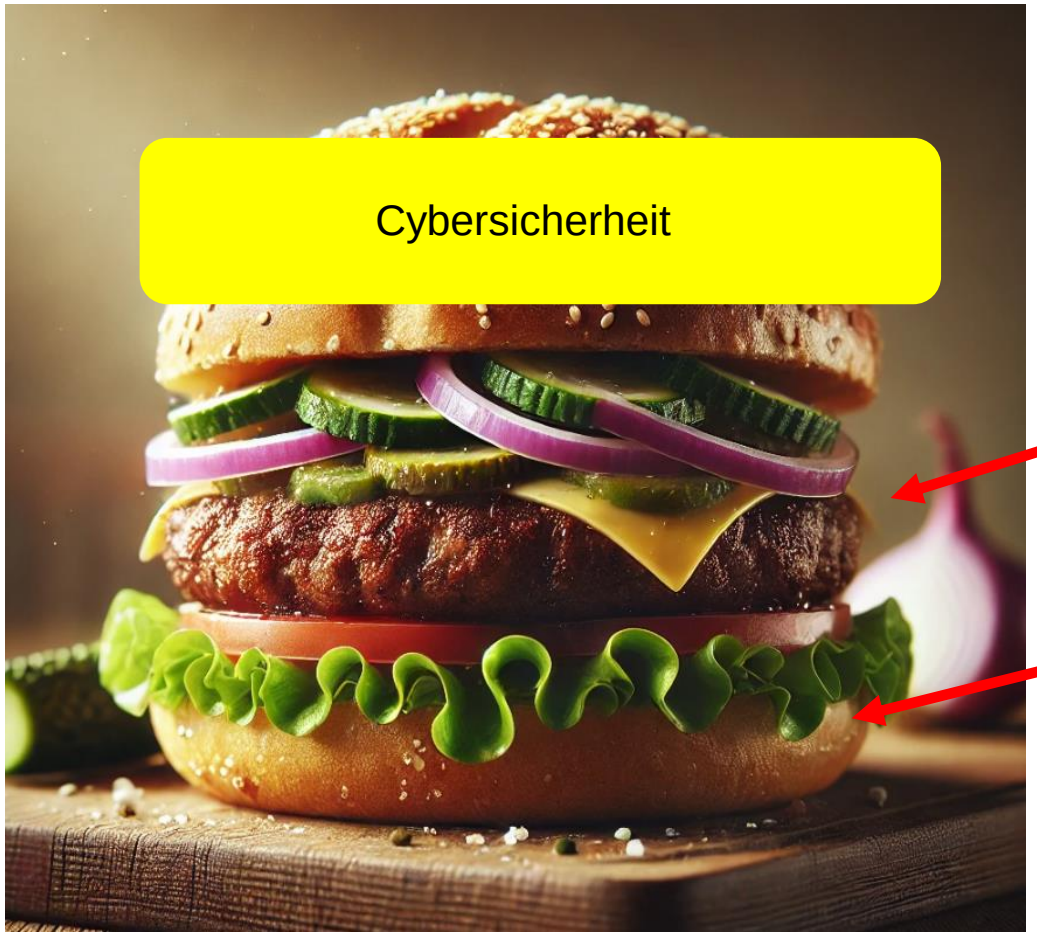
6 NOTFALLMANAGEMENT

Eine detaillierte Beurteilung ist erforderlich.
Z.B. IEC 62443-3-2 oder ICS-Security Kompendium

Prüfung vor Inbetriebnahme und wiederkehrend



Zusammenfassung Explosionssicherheit



Chat GPT

- Maßnahmen des Explosionsschutzes
  primär,
  sekundär,
  konstruktiv
- TRGS 725 sicherheitsrelevante MSR - Einrichtung

Danke für Ihre Aufmerksamkeit

TRGS 725 & TRBS 1115 Teil 1:
Lösungsansätze für die Explosionssicherheit

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

Mobiltelefon 0171-9918823
ralf.schmitt@de.tuv.com

TÜVRheinland®
Genau. Richtig.