

Funktionale- und Cybersicherheit

Herausforderungen durch rechtliche Schnittstellen

Fachdialog Technische Sicherheit
21. Februar 2024 | Christoph Thust

Anlagen unterliegen zahlreichen Rechtsvorschriften

- Safety und Security sind Querschnittsthemen



Technische Aspekte Normung

Aufbau von Mess-, Steuer- und Regeleinrichtungen für den sicheren Betrieb von Anlagen

Sensoren erfassen den Anlagenstatus

- Z. B. Füllstandgrenzschalter

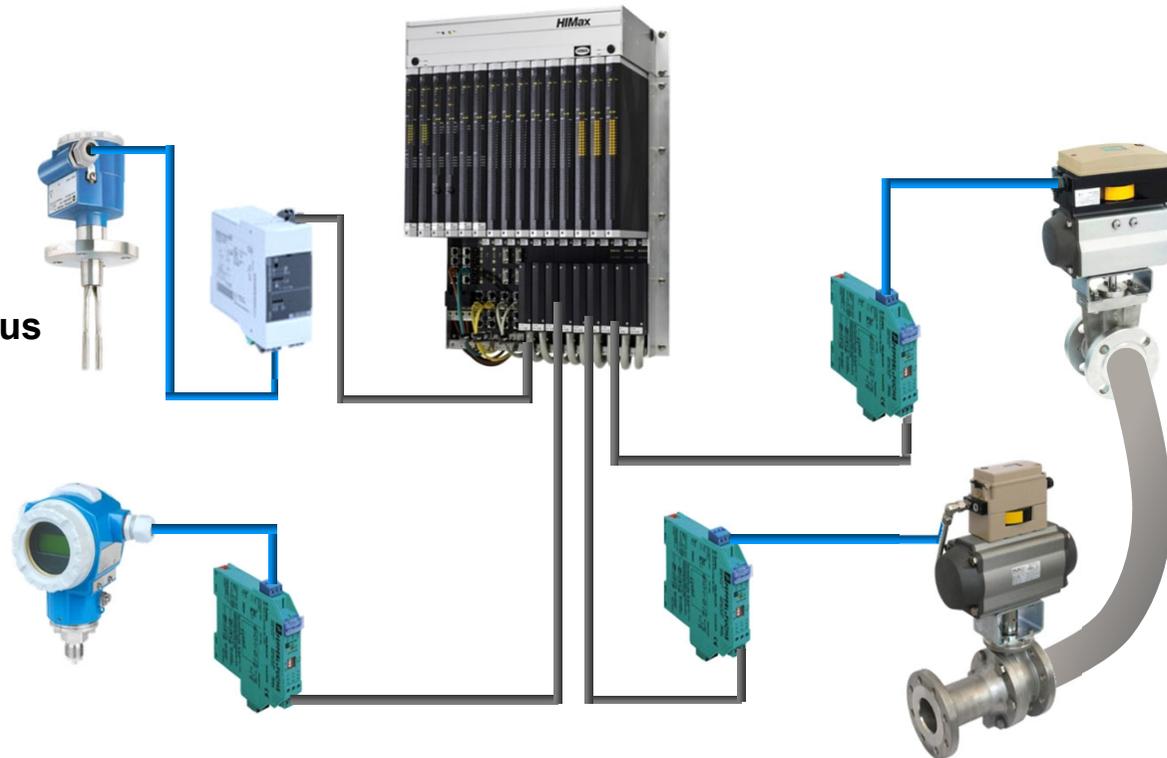
Signalverarbeitung

- Z. B. sicherheitsgerichtete Steuerung

Aktoren lösen den sicheren Zustand aus

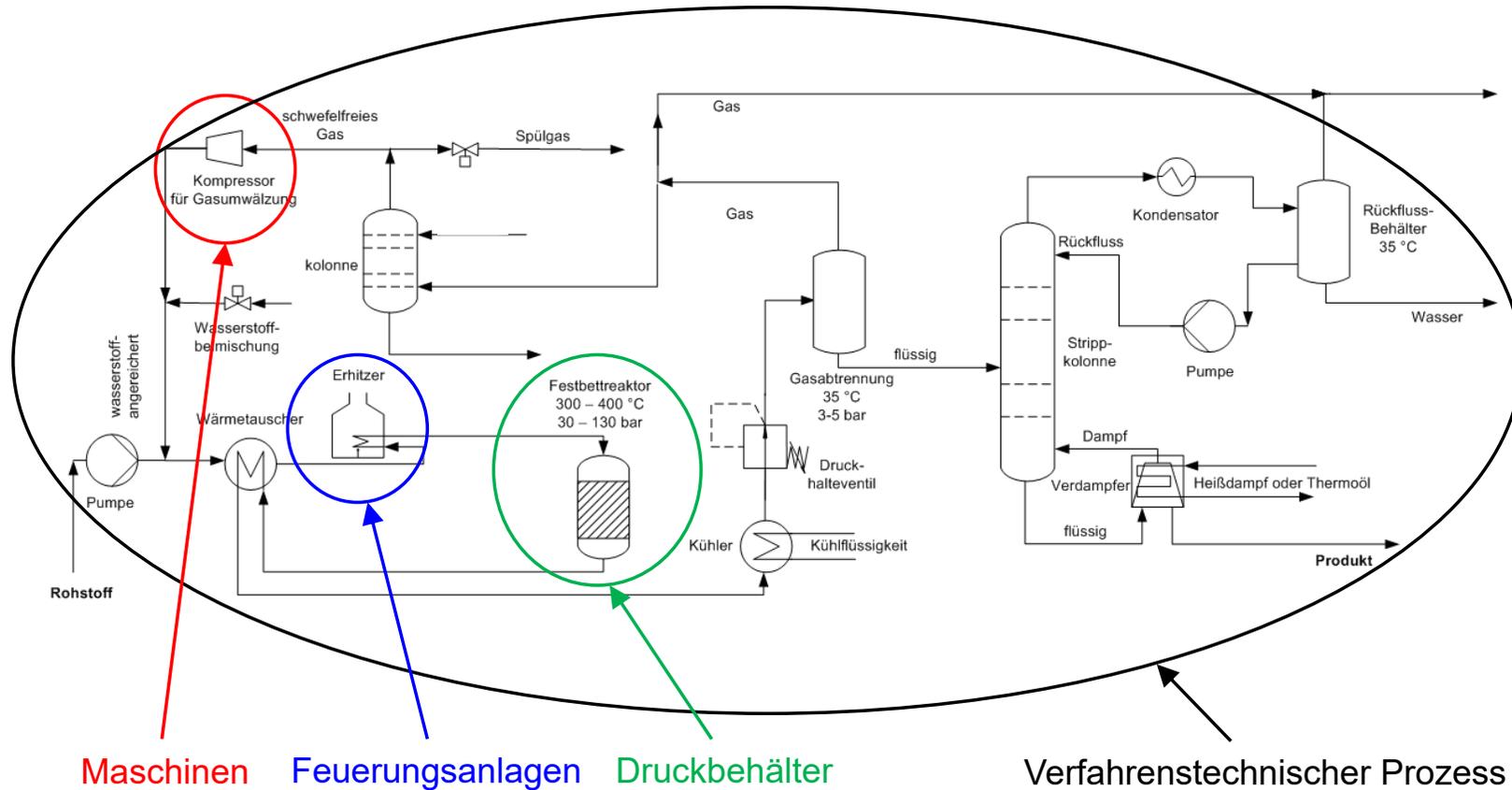
- Z. B. Ventile

Redundanter Aufbau abhängig vom Gefährdungspotenzial



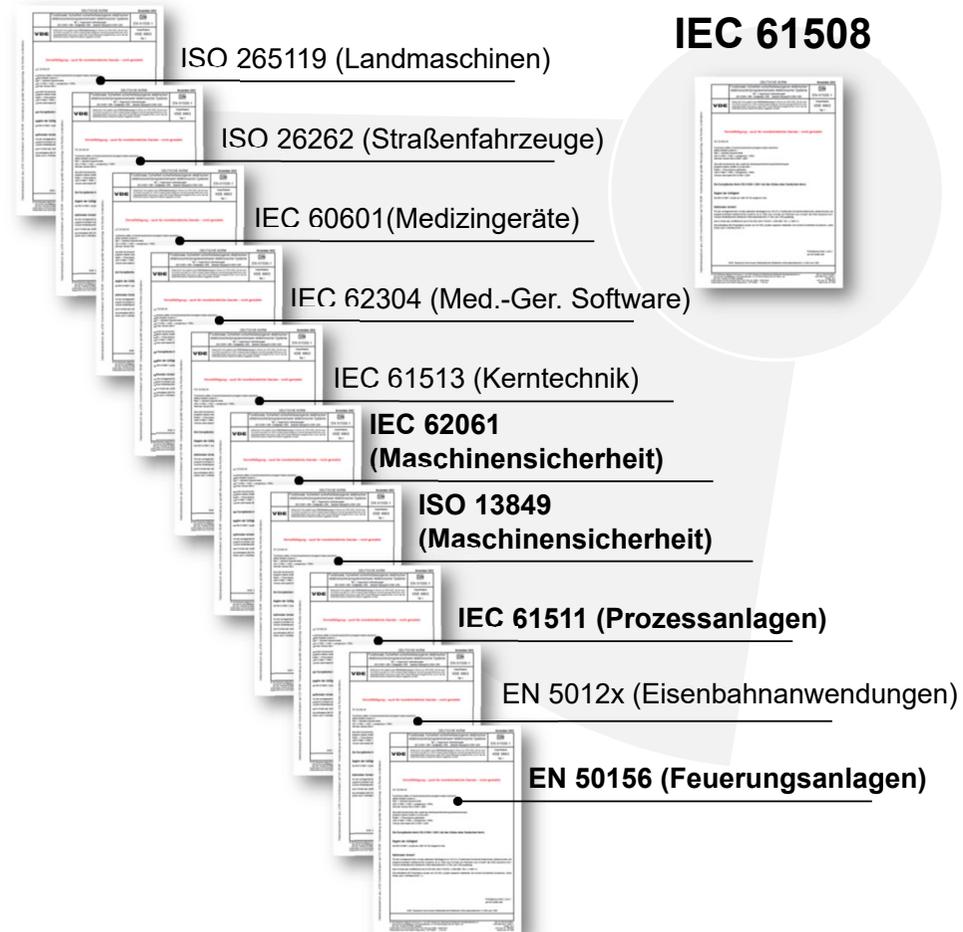
© Endress+Hauser, Pepperl+Fuchs, HIMA, SAMSON

Funktionale Sicherheit in einer verfahrenstechnischen Anlage



Internationale Standardisierung der funktionalen Sicherheit

- **1998**
IEC 61508 als Grundnorm für funktionale Sicherheit veröffentlicht
- **2010**
IEC 61508 Edition 2 veröffentlicht
- Ableitung sektorspezifischer Normen



Rechtliche Aspekte

Gesetzliches, Behördliches, Prüfungen

Rechtliche Schnittstellen der Anlagensicherheit

- Anlagen unterliegen i. d. R. mehreren Rechtsvorschriften gleichzeitig
 - **Anlagenrecht**: Überwachungsbedürftige Anlagen (ÜAnIG, BetrSichV), Betriebsbereiche (StörfallV), AwSV-Anlagen (WHG, AwSV)
 - **Produktrecht**: Gesamtheit von Maschinen, Druckgeräte-Baugruppe, ATEX-Baugruppe
- Jedes Anlagenrecht und jedes Produktrecht schafft eigene Regelungen zu Safety und Security! Warum?
- Safety und Security sind Querschnittsthemen, die unabhängig vom Rechtsgebiet und vom Schutzziel eigenen, international harmonisierten und etablierten Standards folgen
- Alle Anlagen nach **StörfallV** unterliegen auch der **BetrSichV** und sind i.d.R. überwachungsbedürftig, d.h. behördliche Überwachungspflichten und Prüfpflichten – auch für Safety und Security – liegen i. W. im Geltungsbereich des Arbeitsschutzrechtes



IT/OT-Security for Safety ist der maßgebliche rechtliche Fokus in der Prozessindustrie

Gesetzliche Anforderungen

Europäisch

Seveso-RL

Arbeitsmittelbenutzungs-RL

National

**Bundesimmissionsschutzgesetz
Störfallverordnung**

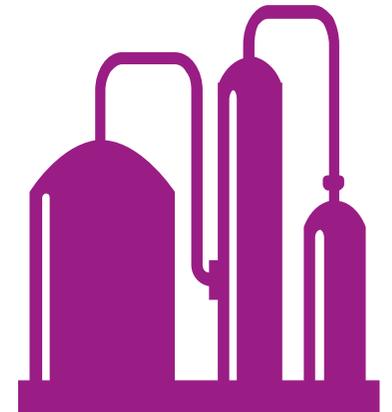
**Arbeitsschutzgesetz
Betriebssicherheitsverordnung**

**Fokus: Schutz der Bevölkerung
und der Umwelt**

**Fokus: Schutz der Arbeitnehmer
(und Dritter)**

**KAS 51 „Maßnahmen gegen Eingriffe
Unbefugter“ (11/2019)**

**TRBS 1115 Teil 1 „Cybersicherheit für
sicherheitsrelevante Mess-, Steuer- und
Regeleinrichtungen“ (03/2023)**



Gesetzliche Regelungen zur IT/OT-Security

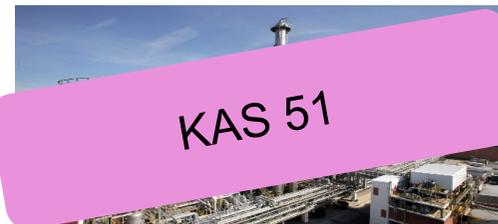
Welche Ministerien?

Wirtschaft/Verkehr
BMWK/BMDV

Inneres
BMI

Umwelt
BMUV

Arbeit
BMAS



BSIG

KAS 51

TRBS 1115,
TRBS 1115-1

Netze

- Bundesnetzagentur (BNetzA)
- Katalog zu IT-Security

Energie

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- BSI-Gesetz („IT-Sicherheitsgesetz“)
- Kritis-Verordnung

Chemie etc.

- Störfallverordnung (StörfallV)
- Regelsetzung durch Kommission für Anlagensicherheit (KAS)

Arbeitsmittel

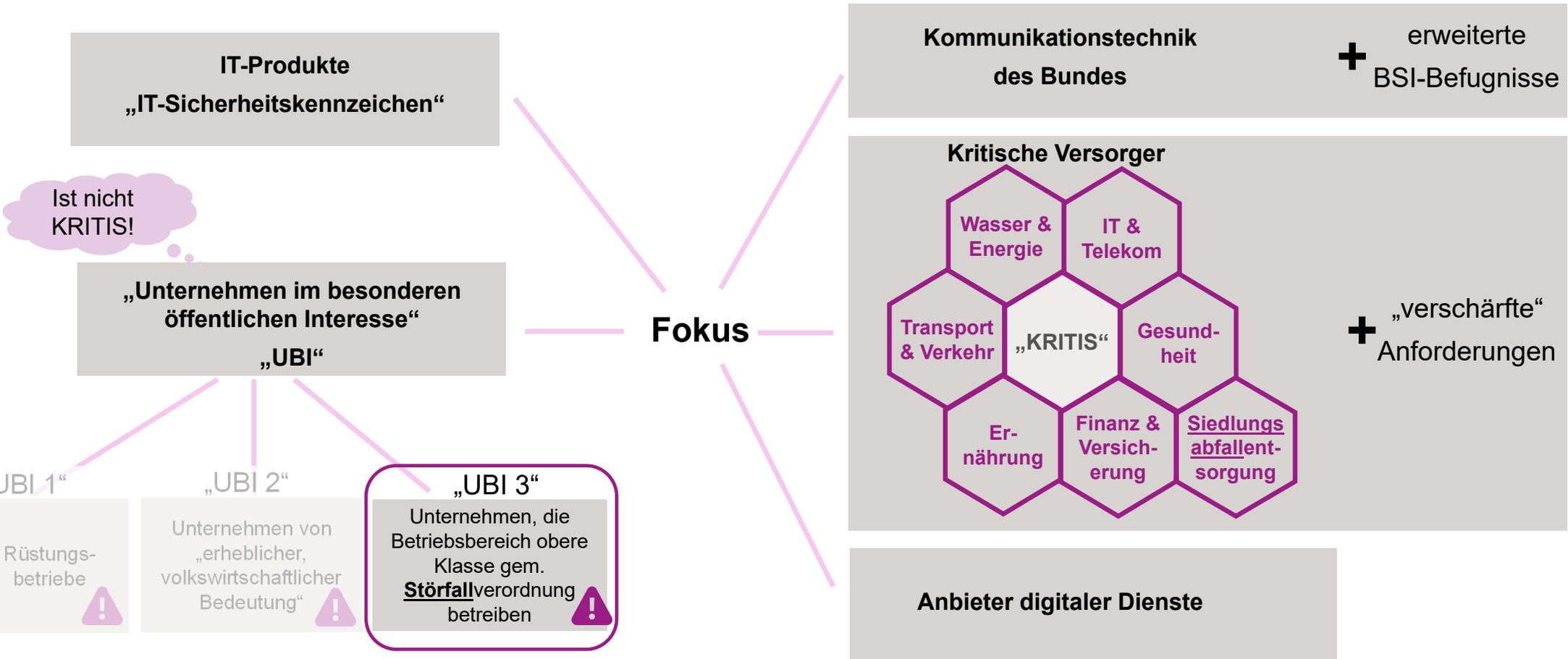
- Betriebssicherheitsverordnung (BetrSichV)
- Regelsetzung durch Ausschuss für Betriebssicherheit (ABS)

Schnittstelle zwischen BSIG und StörfallV seit 2021

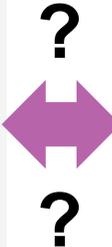
- Meldeverpflichtungen nach BSIG erfordern ministerienübergreifende Abstimmung der zuständigen Behörden



BSIG („IT-Sicherheitsgesetz 2.0“)



Gegenüberstellung der Meldepflichten nach IT-Sicherheitsgesetz und nach StörfallV

	IT-Sicherheitsgesetz § 8f => Meldung an BSI		StörfallV §19 => Meldung an zuständige Behörde
Kriterien	1. Störungen ... die zu einem Störfall ... geführt haben.		
	<p style="text-align: center;">Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit</p> 2. Erhebliche Störungen ... die zu einem Störfall ... führen können .		Ein Ereignis, das aus technischer Sicht im Hinblick auf die Verhinderung von Störfällen und die Begrenzung ihrer Folgen besonders bedeutsam ist, aber den vorstehenden mengenbezogenen Kriterien nicht entspricht. (Anhang VI Teil 1 II)
Weitere Meldewege	- -		Zuständige Behörde informiert BMUV BMUV unterrichtet Europäische Kommission
Ordnungswidrigkeit	bei Meldeversäumnis		bei Meldeversäumnis

Cybersicherheit im rechtlichen Umfeld der Anlagensicherheit

Übersicht der wesentlichen Dokumente für CyberSecurity in der Prozessindustrie in Deutschland



NAMUR



NAMUR NA 163

(IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen)
09/2017, 13 Seiten



NAMUR NA 169

(Automation Security Mgmt in der Prozessindustrie)
12/2019, 14 Seiten

VCI



VCI Leitfaden OT-Security

(revidierte Fassung nicht veröf. wg. Parallelaktivitäten), 2019

BMI / BSI



BSIG („ITSiG2.0“)



BSI Grundschutz Kompendium



BSI / VCI / NAMUR Lenkungskreis 4.18.1 VCI Statuspapier

(Risikobasiertes Mgmt der Cybersecurity in der Prozessindustrie)
11/2022, 10 Seiten
Prinzipien, systemischer Ansatz



BSI AK GSP^{*)} Chemie

(BSI + NAMUR + andere)
03/2023

Höherer techn. Detaillierungsgrad

BMUV / KAS



BImSchG / StörfallIV



KAS51

(Leitfaden Maßnahmen gg. Eingriffe Unbefugter inkl. **Anhang 2 IT-Sicherheit**)
11/2019, 37 Seiten, davon 5 Anh. 2



LANUV NRW Orientierungspapier

(Darstellung der IT-Sicherheit im Sicherheitsbericht und in den Genehmigungsunterlagen zur Anlagensicherheit)
04/2021, 21 Seiten

BMAS / ABS



BArbSchG / BetrSichV



TRBS 1115-1

(Cybersicherheit für sicherheitsrel. Mess-, Steuer- und Regeleinrichtungen)
03/2023, ~20 Seiten, (2016 gestartet als Empfehlung)



Ziel: Einheitliche Beurteilung von *Security for Safety* rechtsgebietsübergreifend und über Bundeslandesgrenzen hinweg

TRBS 1115-1 Cybersicherheit

- TRBS Cybersicherheit
 - Stakeholderpapier (Arbeitgeber, Arbeitnehmer, Berufsgenossenschaften, Bundesländer, Wissenschaft/Prüforganisationen)
 - Löst rechtliche Vermutungswirkung aus
 - Veröffentlichung 03/2023 ([LINK](#))
 - Umgang mit Cybersicherheit im Rahmen von Prüfungen an überwachungsbedürftigen Anlagen zwischen Prüforganisationen und Länderbehörden abgestimmt

Technische Regel für Betriebssicherheit	Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen	TRBS 1115-1
<p>Inhalt</p> <ul style="list-style-type: none"> 1 Anwendungsbereich 2 Begriffsbestimmungen 3 Anforderungen der Cybersicherheit an sicherheitsrelevante MSR-Einrichtungen 4 Planung und Realisierung der Ausrüstung eines Arbeitsmittels mit einer sicherheitsrelevanten MSR-Einrichtung durch den Arbeitgeber im Hinblick auf Cybersicherheit 5 Überprüfung der Wirksamkeit der Cybersicherheitsmaßnahmen 6 Prüfung des Arbeitsmittels vor Inbetriebnahme und Wiederinbetriebnahme nach prüfpflichtiger Änderung nach §§ 14 und 15 BetrSichV 7 Wiederkehrende Prüfung von Arbeitsmitteln mit sicherheitsrelevanten MSR-Einrichtungen nach §§ 14 und 16 BetrSichV 8 Verwendung und Instandhaltung <p>Anhang 1 Management der Cybersicherheit</p> <p>Anhang 2 Regelwerke und Normen</p>		

EK ZÜS*) beschließt zeitlich gestaffelte Prüftiefe der Cybersicherheit

- B-002 öffentlich zugänglich unter ([LINK](#))
 - Beschreibt grundsätzliches
 - 6.2 (1): ab 2023 „nur“ Abfrage durch Sachverständige aus den Bereichen Druck und Ex, ob Cyberbedrohungen dokumentiert behandelt werden.
 - Wenn ja: zunächst nichts weiter
 - Wenn nein: **Hinweis** „... Dokumentation wurde nicht vorgelegt“; nach Veröffentlichung der TRBS 1115-1: **Geringfügiger Mangel** „...“
- Erweiterung der Prüftiefe voraussichtlich ab Frühjahr 2024

Beschluss des EK ZÜS		ZÜS B-002 rev 1
Abgestimmt im EK ZÜS	Schriftliche Abstimmung 34. Sitzung, TOP 6.2	27.05.2022 16.11.2022
Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen von überwachungsbedürftigen Anlagen		
6.2	Prüfung vor Inbetriebnahme oder vor Wiederinbetriebnahme nach einer prüfpflichtigen Änderung	
(1)	Für eine festzulegende Übergangszeit ist zu prüfen, ob Cyberbedrohungen im Rahmen der Gefährdungsbeurteilung dokumentiert behandelt werden.	

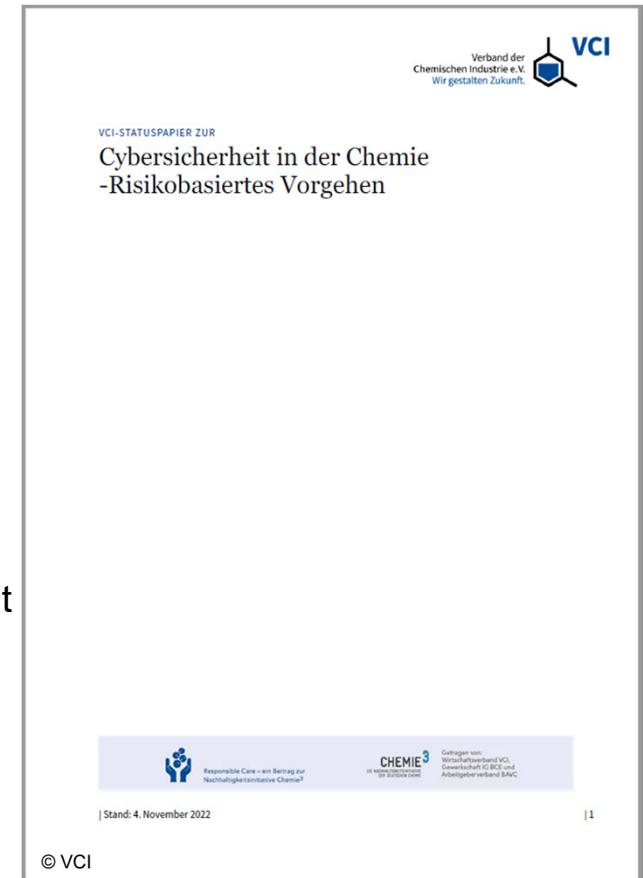
*) Erfahrungskreis der *Zugelassenen Überwachungsstellen* (gesetzlich verpflichtend)

VCI-STATUSPAPIER ZUR Cybersicherheit in der Chemie - Risikobasiertes Vorgehen

- Direkte **Betroffenheit** durch KAS 51 bei Genehmigungsverfahren
- ebenfalls **Stakeholderpapier**, beteiligt neben Chemie: BSI, LANUV NRW, TÜV-Verband

Merkmale

- Lesbarkeit des Textteils für Nicht-Experten im Bereich Cybersicherheit
 - Darstellung der rechtsformalen Einbettung des Themas in die Rechtsgebiete
 - Generische Darstellung der in der (Groß-)Industrie angewendeten Methodik
 - Kopplung der Cybersicherheitsanforderungen an sicherheitstechnisch klassifizierte PLT-Einrichtungen
- Breit abgestimmte Arbeitsgrundlage für den operativen Einstieg in die Cybersicherheit
 - BSI Fragenkatalog beschränkt auf Chemiebelange
 - Synopse KAS 51 zum BSI-Kompendium und dem in der Chemie üblicherweise verwendeten internationalen Standard IEC 62443
- Veröffentlichung Anf. November 2022 auf Webseiten des VCI ([LINK](#)) erfolgt.



VCI-STATUSPAPIER ZUR Cybersicherheit in der Chemie - Risikobasiertes Vorgehen (Merkmale 2)

Inhaltsverzeichnis

Cybersicherheit in der Chemie -Risikobasiertes Vorgehen	1
Vorwort	4
Charakteristika von Chemieanlagen und Ausgangssituation.....	4
Risikobasiertes Vorgehen.....	5
Risikobasiertes Vorgehen zur Cyberschutzbedarfsfeststellung.....	6
Bestimmung des Cyberschutzbedarfes	6
Sehr hoher Schutzbedarf	7
Hoher Schutzbedarf	7
Normaler Schutzbedarf.....	7
Einzelfallbetrachtung	7
Festlegung anlagenspezifischer Cyberschutzmaßnahmen.....	8
Anhang 1 – Themenkatalog	10

Charakteristika von Chemieanlagen und Ausgangssituation

Chemieanlagen sind individuell und komplex. Des Weiteren sind sie i. d. R. genehmigungsbedürftig. Im Rahmen des Genehmigungsverfahrens werden verschiedene Rechtsgebiete geprüft (GefStoffV, 12. BImSchV, etc.). Die Cybersicherheit mit ihren Schutzziele ist hierbei grundsätzlich relevant, sowohl wirtschaftlich als auch zum Schutz von Menschen und Umwelt. Rechtliche Verpflichtungen zur Umsetzung der erforderlichen Cybersicherheit resultieren derzeit im Wesentlichen aus dem Störfallrecht sowie aus dem Arbeitsschutzrecht, hier insbesondere der Betriebssicherheitsverordnung.

Konkretisierungen zur Cybersicherheit finden sich im untergesetzlichen Regelwerk (z. B. IEC 62443, dem ICS-Kompendium des BSI oder dem Leitfaden KAS 51) sind aber aufgrund des mangelnden Abgleichs mit den oben genannten Rechtsvorschriften nicht unmittelbar anwendbar. Insbesondere das Zusammenspiel von Methoden der klassischen Safety (SIL etc.) mit Methoden der Cybersicherheit ist zu konkretisieren, um Rechtssicherheit sowohl für die betroffenen Betreiber als auch für die zuständigen Behörden und die Prüforganisationen zu erreichen.

Dieses Dokument bezieht sich auf die in den o. g. Rechtsgebieten beschriebenen Schutzziele

Sehr hoher Schutzbedarf

Für Sicherheitsfunktionen \geq SIL 1 ist ein sehr hoher Cyberschutzbedarf erforderlich.

Hoher Schutzbedarf

Ein hoher Cyberschutzbedarf für Sicherheitsfunktionen $<$ SIL 1 (z. B. PLT-BS) ist für Einrichtungen erforderlich, die im betrieblichen PLS umgesetzt sind, da durch diese Einrichtungen eine geringere Risikoreduzierung als durch SIL-klassifizierte Einrichtungen gewährleistet wird.

Erfolgt für das Prozessleitsystem bzw. betriebliche Einrichtungen keine Einzelfallbetrachtung, so ist aus vorgenannten Gründen auch für diese Systeme von einem hohen Cyberschutzbedarf auszugehen.

In der Regel ist bereits aus Gründen der Wirtschaftlichkeit (Verfügbarkeit der Anlagen und Produktqualität) ein Cyberschutzbedarf erforderlich, der schon einen ausreichend Abdeckungsgrad auch für die vorgenannten Sicherheitsfunktionen und Prozessleitsysteme bzw. betrieblichen Einrichtungen bietet.

Bei der Bewertung vorhandener Cyberschutzmaßnahmen sind alle beteiligten Komponenten zu

VCI-STATUSPAPIER ZUR Cybersicherheit in der Chemie - Risikobasiertes Vorgehen (Fragenkatalog)

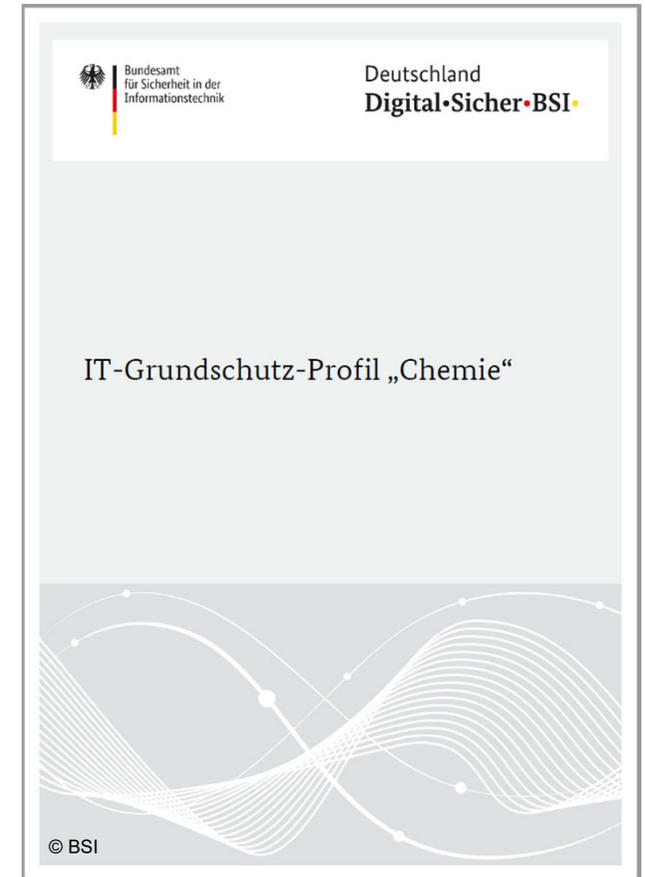
Anhang 1 – Themenkatalog

Der untenstehende Themenkatalog enthält praktische Fragen für eine strukturierte Vorgehensweise zur Festlegung der Cyberschutzmaßnahmen. Die Fragen ermöglichen den Einstieg in eine Erstbewertung der Cybersicherheit im Sinne dieses Dokumentes. Eine negative Antwort stellt dabei einen erklärungsbedürftigen Zustand dar. Eine positive Antwort sollte durch umgesetzte Prozesse und Cyberschutzmaßnahmen belegbar sein.

Themen der Cybersicherheit	Fragen	IEC62443-Bezug	BSI-Kompendium-Bezug	KAS-51-Bezug	Beispiel / Hilfestellung
1) Informationssicherheits-Management	Gibt es ein Security*-Managementsystem?	prEN IEC62443-2-1:2019: ORG 1.1: Information security management system	ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie durch die Leitung ISMS.1.A13 Dokumentation des Sicherheitsprozesses (S)	7.2.1 Einführung eines Sicherungsmanagements	z.B. basierend auf ISO27k, BSI Kompendium, IEC62443, NIST CSF
	Gibt es eine Security-Organisation?	prEN IEC62443-2-1:2019:	ISMS.1.A6 Aufbau einer geeigneten Orga	4 Festlegung von Verantwortlichkeiten	z.B. definierte und dokumentierte

BSI IT-Grundschutz-Profil „Chemie“ fertiggestellt

- Erarbeitet vom BSI unter maßgeblicher Mitwirkung der NAMUR ([LINK](#))
- Fokus auf Absicherung von PLT-Schutzeinrichtungen in Chemieanlagen gegenüber Cyberangriffen
- Detaillierte Beschreibung von Referenz- und Modellarchitekturen und Zuordnung von Bausteinen des IT-Grundschutz-Kompendiums
- 32 Seiten Haupttext + 39 Seiten Anhang
- **Ursprünglich geplante Konsolidierung mit VCI-Statuspapier konnte nicht erreicht werden**



BDI-Papier zu Cybersicherheitsregulierungen veröffentlicht



01. Februar 2024

BDI-Papier zu Cybersicherheitsregulierungen - Hintergründe

Betroffenheit der Anlagensicherheit durch

- NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)
 - Deutliche Erweiterung der Anforderungen, z. B. Meldepflichten, Billigungs-, Überwachungs- und Schulungspflicht der Risikomanagementmaßnahmen für Geschäftsleiter
 - Chemie explizit benannt
- Bundes-Immissionsschutzgesetz (BImSchG)
 - Erweiterung der Sachverständigen-Fachgebiete um IT/OT in der 41. BImSchV geplant (Auswirkung z. B. auf Genehmigungen)
- Gesetz über überwachungsbedürftige Anlagen (ÜAnIG)
 - Anforderungen an die Cybersicherheit in zukünftiger Überwachungsbedürftige Anlagenverordnung (ÜAnIV), AMBV (Arbeitsmittelbenutzungsverordnung, Nachfolge BetrSichV)

BDI-Papier zu Cybersicherheitsregulierungen – weiteres Vorgehen

Ansprache der betroffenen Bundesministerien zu folgenden Handlungsempfehlungen

- Cybersicherheitsanforderungen über Ressortgrenzen hinweg harmonisieren
- Audit-, Prüf- und Nachweispflichten bündeln
- Bundesamt für Sicherheit in der Informationstechnik (BSI) als maßgeblichen behördlichen Cybersicherheits-Ansprechpartner etablieren
- Zentrales Melde- und Informationswesen für erhebliche Cybersicherheitsvorfälle



EVONIK

Leading Beyond Chemistry