Cybersicherheit: Aktuelle Anforderungen an den Schutz der Anlagensicherheit

13. Sicherheitswissenschaftliches Forum und 16. VDSI-Forum NRW, Wuppertal
26. September 2024 | Christoph Thust

EVONIK
Leading Beyond Chemistry

Anlagen unterliegen zahlreichen Rechts-vorschriften

Safety und Security sind Querschnittsthemen

(hier: Security=Cybersicherheit)

EVONIK
Leading Beyond Chemistry

Technische Aspekte Normung

EVONIK
Leading Beyond Chemistry

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

Sensoren erfassen den Anlagenstatus

- Z. B. Füllstandsgrenzschalter

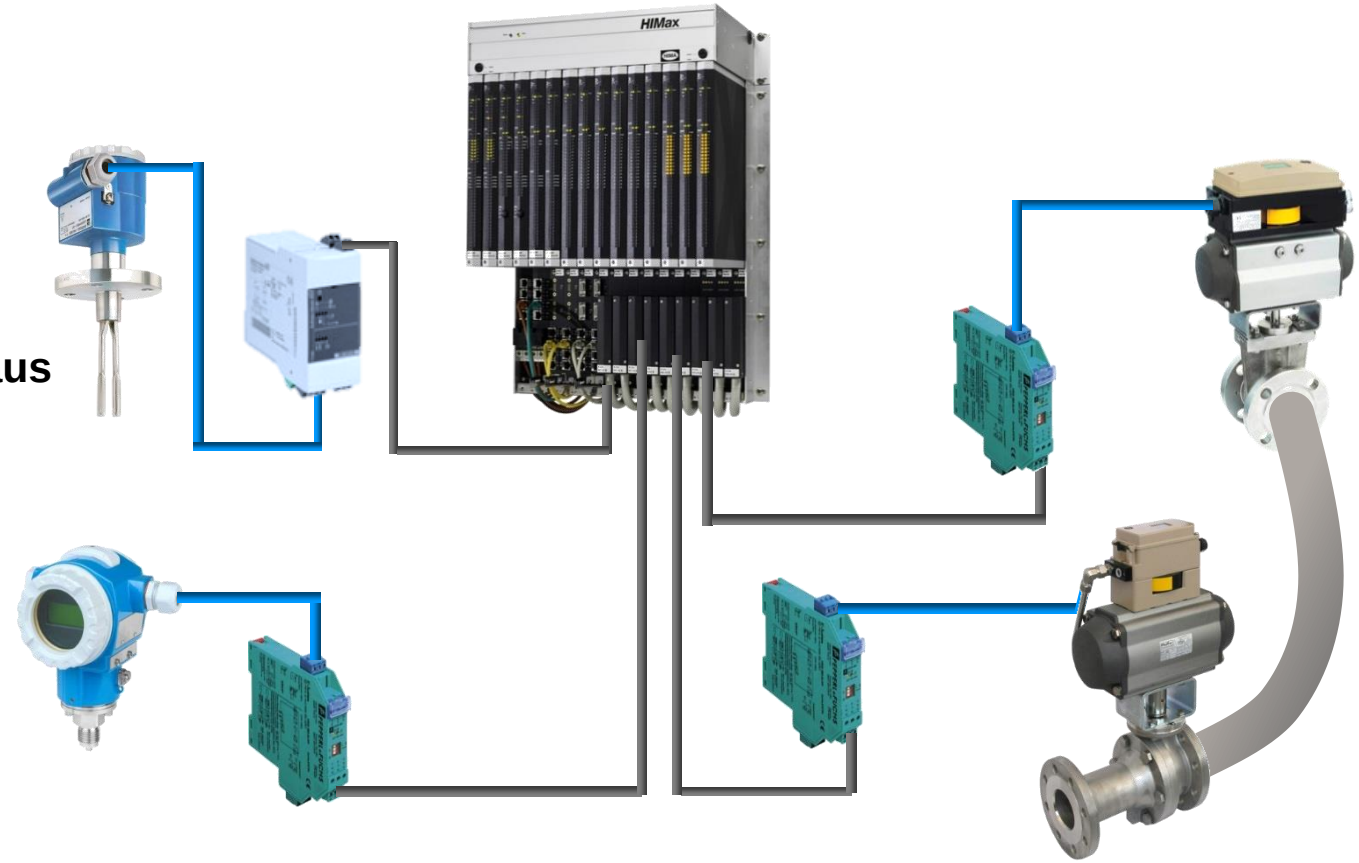
Signalverarbeitung

- Z. B. sicherheitsgerichtete Steuerung

Aktoren lösen den sicheren Zustand aus

- Z. B. Ventile

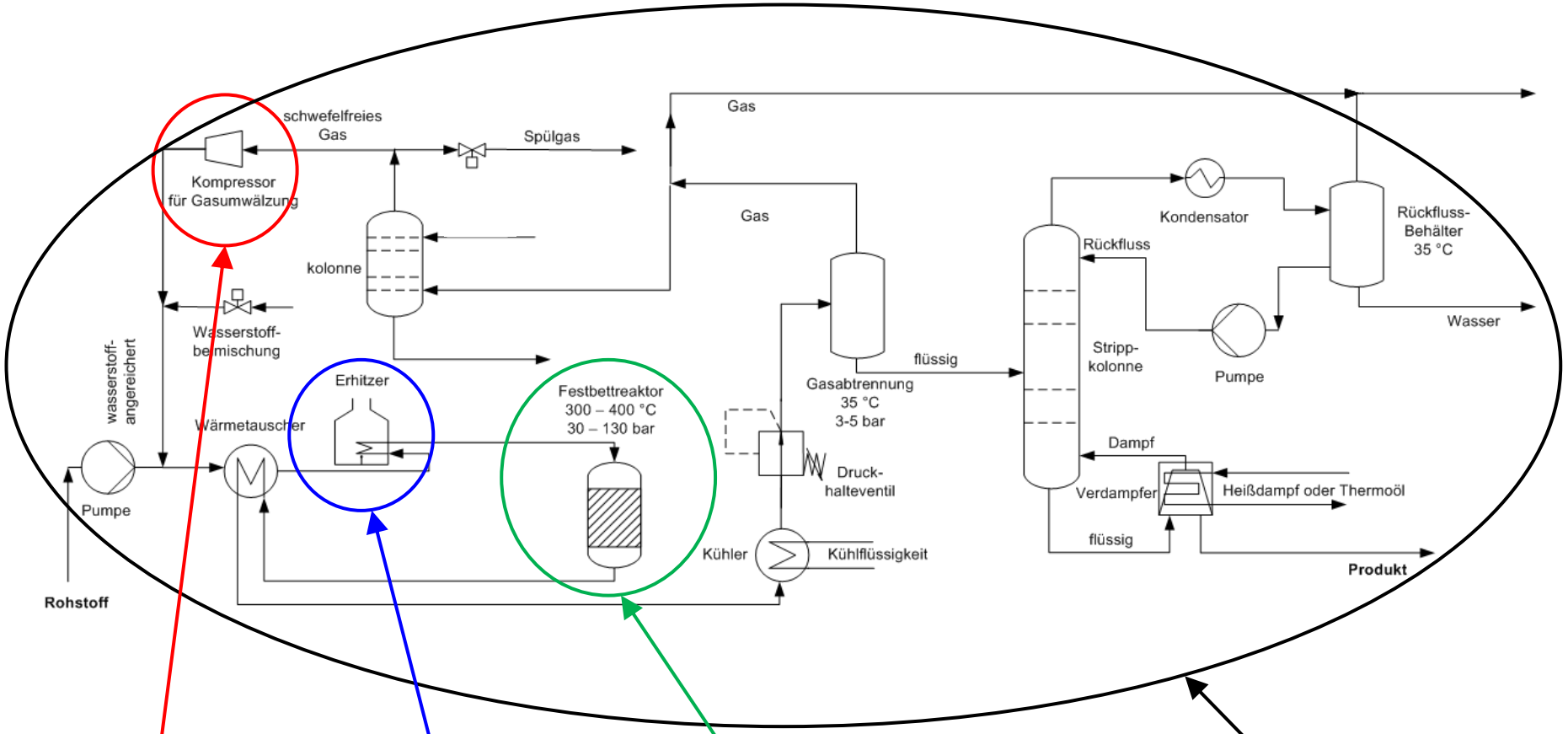
Redundanter Aufbau abhängig vom Gefährdungspotenzial



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

EVONIK
Leading Beyond Chemistry

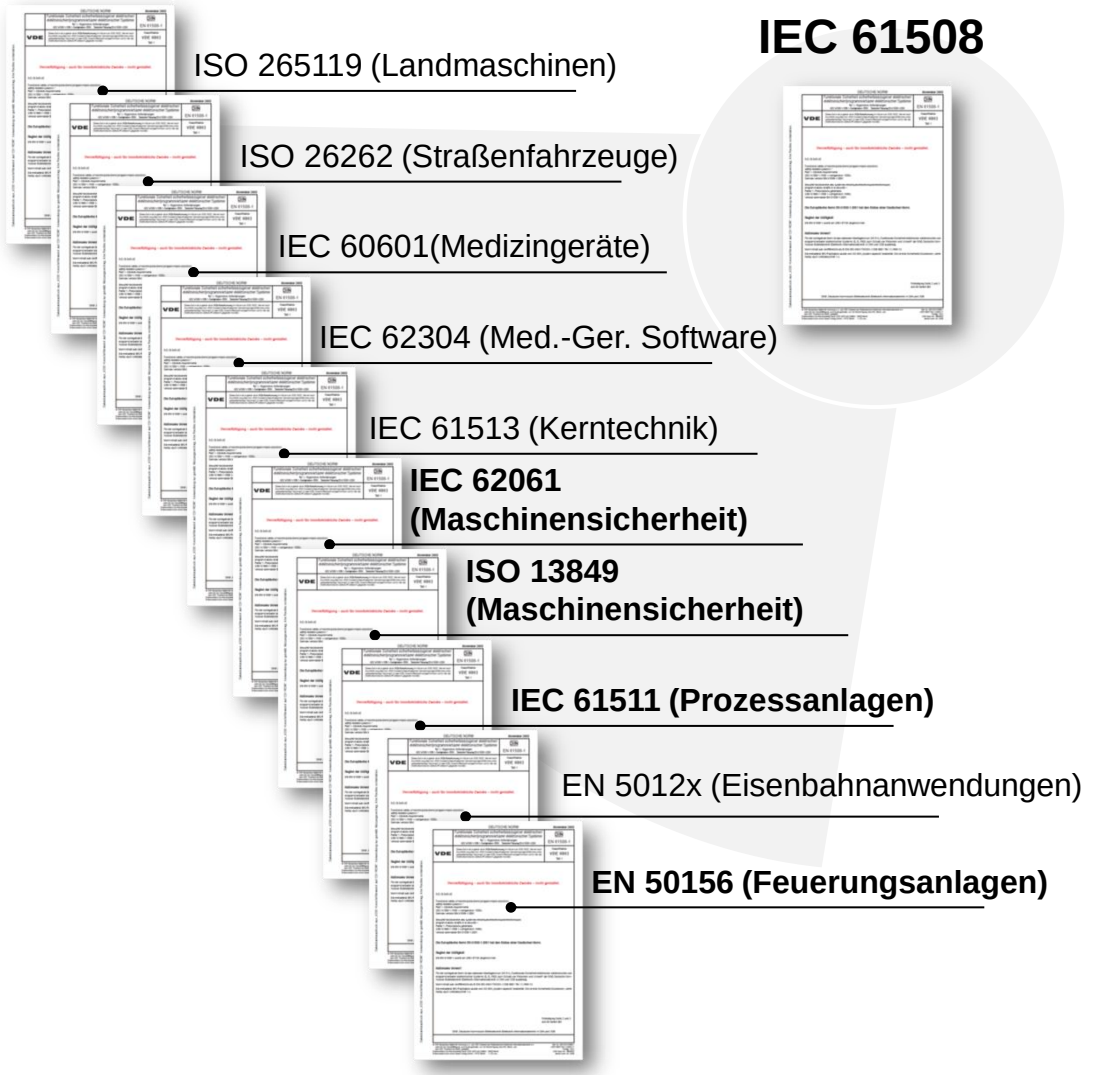
Funktionale Sicherheit in einer verfahrenstechnischen Anlage



EVONIK Leading Beyond Chemistry

Internationale Standardisierung der funktionalen Sicherheit

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



EVONIK
Leading Beyond Chemistry

Rechtliche Aspekte

Gesetzliches, Behördliches, Prüfungen

EVONIK
Leading Beyond Chemistry

Rechtliche Schnittstellen der Anlagensicherheit

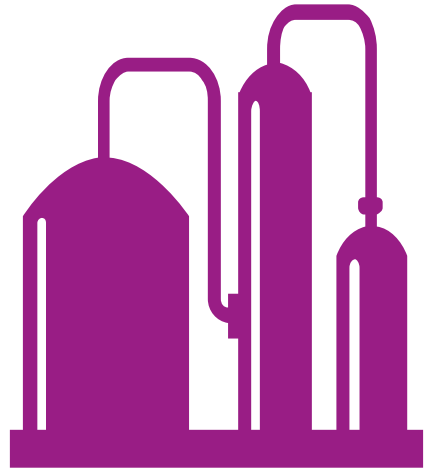
- Anlagen unterliegen i. d. R. mehreren Rechtsvorschriften gleichzeitig
  - **Anlagen**recht: Überwachungsbedürftige Anlagen (ÜAnlG, BetrSichV), Betriebsbereiche (StörfallV), AwSV-Anlagen (WHG, AwSV)
  - **Produkt**recht: Gesamtheit von Maschinen, Druckgeräte-Baugruppe, ATEX-Baugruppe
- Jedes Anlagenrecht 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

EVONIK
Leading Beyond Chemistry

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)**



EVONIK
Leading Beyond Chemistry

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)

EVONIK
Leading Beyond Chemistry

Schnittstelle zwischen BSIG und StörfallV seit 2021

Meldeverpflichtungen nach BSIG erfordern ministerienübergreifende Abstimmung der zuständigen Behörden

EVONIK
Leading Beyond Chemistry

BSIG („IT-Sicherheitsgesetz 2.0“)

IT-Produkte
„IT-Sicherheitskennzeichen“

Ist nicht KRITIS!

„Unternehmen im besonderen öffentlichen Interesse“
„UBI“

„UBI 1“
Rüstungs-betriebe

„UBI 2“
Unternehmen von „erheblicher, volkswirtschaftlicher Bedeutung“

„UBI 3“
Unternehmen, die Betriebsbereich obere Klasse gem. **Störfall**verordnung betreiben

Fokus

Kommunikationstechnik des Bundes
+ erweiterte BSI-Befugnisse

Kritische Versorger

+ „verschärfte“ Anforderungen

Anbieter digitaler Dienste

EVONIK Leading Beyond Chemistry

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.		
	Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit 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
Ordnungs-widrigkeit	bei Meldeversäumnis		bei Meldeversäumnis

EVONIK Leading Beyond Chemistry

Cybersicherheit im rechtlichen Umfeld der Anlagensicherheit

EVONIK
Leading Beyond Chemistry

Übersicht der wesentlichen Dokumente für Cybersicherheit 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 veröff 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 / StörfallV

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 Bundeslandgrenzen hinweg

*) GSP - Grundschutzprofil

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

Inhalt

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

Anhang 1 Management der Cybersicherheit

Anhang 2 Regelwerke und Normen

EVONIK Leading Beyond Chemistry

EK ZÜS*) beschließt zeitlich gestaffelte Prüftiefe der Cybersicherheit – Stufe 1

- B-002 öffentlich zugänglich
  - 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 ab Frühjahr 2024

Beschluss des EK ZÜS — ZÜS B-002 rev 1

Abgestimmt im EK ZÜS	Schriftliche Abstimmung	27.05.2022
	34. Sitzung, TOP 6.2	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)

EVONIK Leading Beyond Chemistry

EK ZÜS*) beschließt zeitlich gestaffelte Prüftiefe der Cybersicherheit – Stufe 2

- Abstimmung zu Prüfungen der Cybersicherheit **Stufe 2** im Erfahrungskreis der zugelassenen Überwachungs-stellen (EK ZÜS) erfolgt
- Öffentlicher Beschluss dazu in 04/24 aktualisiert
- EK ZÜS Beschluss B-002

Beschluss des EK ZÜS — **ZÜS B-002 rev 3**

Abgestimmt im EK ZÜS	Schriftliche Abstimmung	27.05.2022
	34. Sitzung, TOP 6.2	16.11.2022
	36. Sitzung, TOP 8.10	15.11.2023
	37. Sitzung, TOP 5.2	17.04.2024

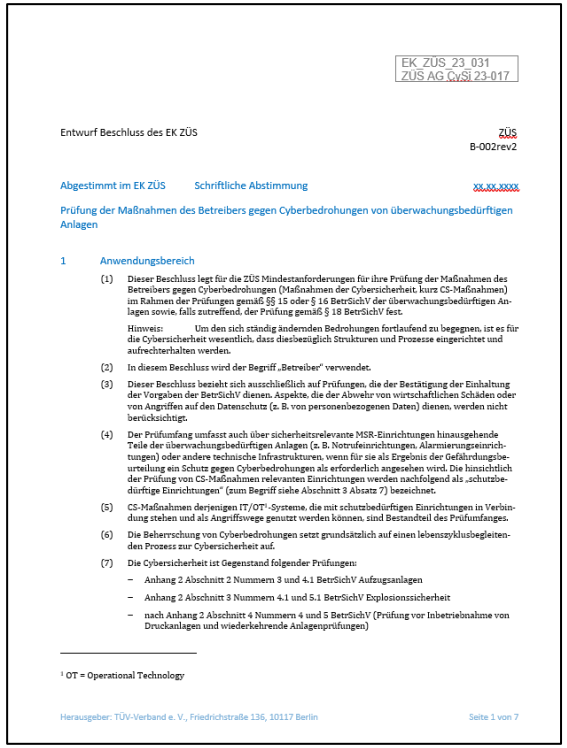
Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen von überwachungsbedürftigen Anlagen

1 Anwendungsbereich

(1) Dieser Beschluss legt für die ZÜS Mindestanforderungen für ihre Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen (Maßnahmen der Cybersicherheit, kurz CS-Maßnahmen) im Rahmen der Prüfungen gemäß § 15 oder § 16 BetrSichV der überwachungsbedürftigen Anlagen sowie, falls zutreffend, der Prüfung gemäß § 18 BetrSichV fest.

EVONIK Leading Beyond Chemistry

Veröffentlichung der Bewertungstabelle



EK_ZÜS_23_031
ZÜS AG CySi 23-017

Entwurf Beschluss des EK ZÜS — ZÜS B-002rev2

Abgestimmt im EK ZÜS — Schriftliche Abstimmung — xx.xx.xxxx

Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen von überwachungsbedürftigen Anlagen

1 Anwendungsbereich

(1) Dieser Beschluss legt für die ZÜS Mindestanforderungen für ihre Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen (Maßnahmen der Cybersicherheit, kurz CS-Maßnahmen) im Rahmen der Prüfungen gemäß §§ 15 oder § 16 BetrSichV der überwachungsbedürftigen Anlagen sowie, falls zutreffend, der Prüfung gemäß § 18 BetrSichV fest.

Hinweis: Um den sich ständig ändernden Bedrohungen fortlaufend zu begegnen, ist es für die Cybersicherheit wesentlich, dass diesbezüglich Strukturen und Prozesse eingerichtet und aufrechterhalten werden.

(2) In diesem Beschluss wird der Begriff „Betreiber" verwendet.

(3) Dieser Beschluss bezieht sich ausschließlich auf Prüfungen, die der Bestätigung der Einhaltung der Vorgaben der BetrSichV dienen. Aspekte, die der Abwehr von wirtschaftlichen Schäden oder von Angriffen auf den Datenschutz (z. B. von personenbezogenen Daten) dienen, werden nicht berücksichtigt.

(4) Der Prüfumfang umfasst auch über sicherheitsrelevante MSR-Einrichtungen hinausgehende Teile der überwachungsbedürftigen Anlagen (z. B. Notrufeinrichtungen, Alarmierungseinrichtungen) oder andere technische Infrastrukturen, wenn für sie als Ergebnis der Gefährdungsbeurteilung ein Schutz gegen Cyberbedrohungen als erforderlich angesehen wird. Die hinsichtlich der Prüfung von CS-Maßnahmen relevanten Einrichtungen werden nachfolgend als „schutzbedürftige Einrichtungen" (zum Begriff siehe Abschnitt 3 Absatz 7) bezeichnet.

(5) CS-Maßnahmen derjenigen IT/OT[1]-Systeme, die mit schutzbedürftigen Einrichtungen in Verbindung stehen und als Angriffswege genutzt werden können, sind Bestandteil des Prüfumfanges.

(6) Die Beherrschung von Cyberbedrohungen setzt grundsätzlich auf einen lebenszyklusbegleitenden Prozess zur Cybersicherheit auf.

(7) Die Cybersicherheit ist Gegenstand folgender Prüfungen:

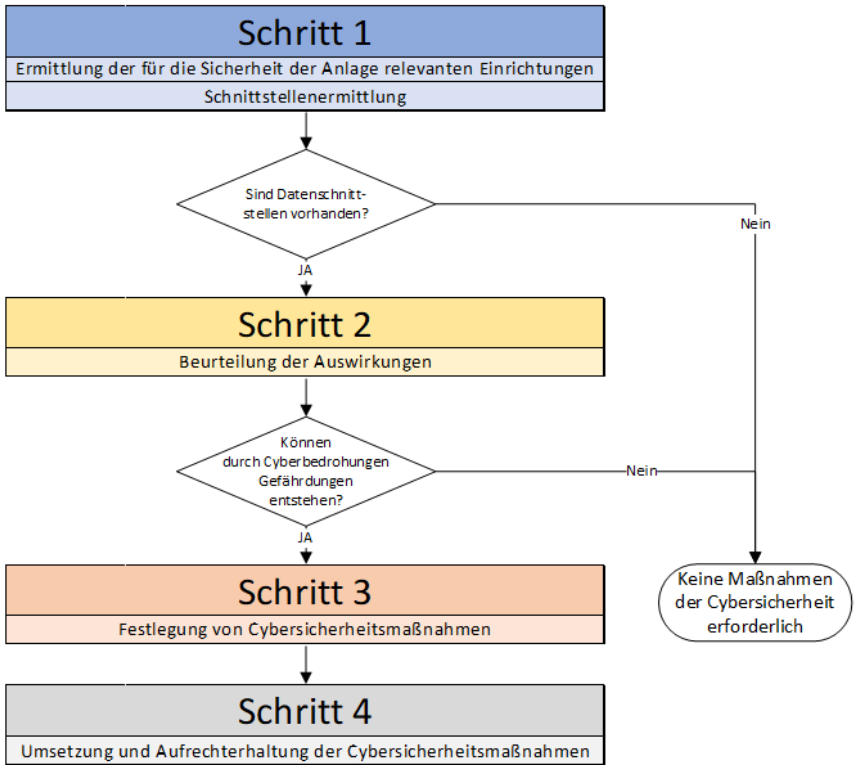
- Anhang 2 Abschnitt 2 Nummern 3 und 4.1 BetrSichV Aufzugsanlagen
- Anhang 2 Abschnitt 3 Nummern 4.1 und 5.1 BetrSichV Explosionssicherheit
- nach Anhang 2 Abschnitt 4 Nummern 4 und 5 BetrSichV (Prüfung vor Inbetriebnahme von Druckanlagen und wiederkehrende Anlagenprüfungen)

[1] OT = Operational Technology

Herausgeber: TÜV-Verband e. V., Friedrichstraße 136, 10117 Berlin — Seite 1 von 7

B-002

Ablaufplan



Beispielhafte Dokumentation

Schritt 1

Ermittlung der für die Sicherheit der Anlage relevanten Einrichtungen	Schnittstellenermittlung
Benennung der jeweiligen sicherheitsrelevanten MSR-Einrichtung / Schutzeinrichtung / des Ausrüstungsteils mit Sicherheitsfunktion, autarken Sicherheitseinrichtung oder des Anlagenteils, das hinsichtlich möglicher Auswirkungen von Cyberbedrohungen auf den sicheren Zustand der Anlage zu untersuchen ist	Benennung der an der Einrichtung vorhandenen Daten-Schnittstellen
Einrichtung A	
Einrichtung B	
...	

Schritt 2

Beurteilung der Auswirkungen von Cyberbedrohungen			
Benennung der betrachteten Einrichtung	Kurzbeschreibung der Schutzfunktion / des Schutzziels	Durch die Folgen einer Manipulation (z.B. Fehl-Auslösung, Blockierung der Auslösung oder Parameter- oder Funktionsänderungen) können grundsätzlich Gefährdungen entstehen. (Ja/Nein) Wenn ja bitte beschreiben.	Es gibt folgende nicht digitale Maßnahmen, um die Folgen der Manipulation auf ein ungefährliches Maß zu reduzieren. (Eintragung nur, wenn zutreffend erforderlich)
Einrichtung A			
Einrichtung B			
...			

Schritt 3

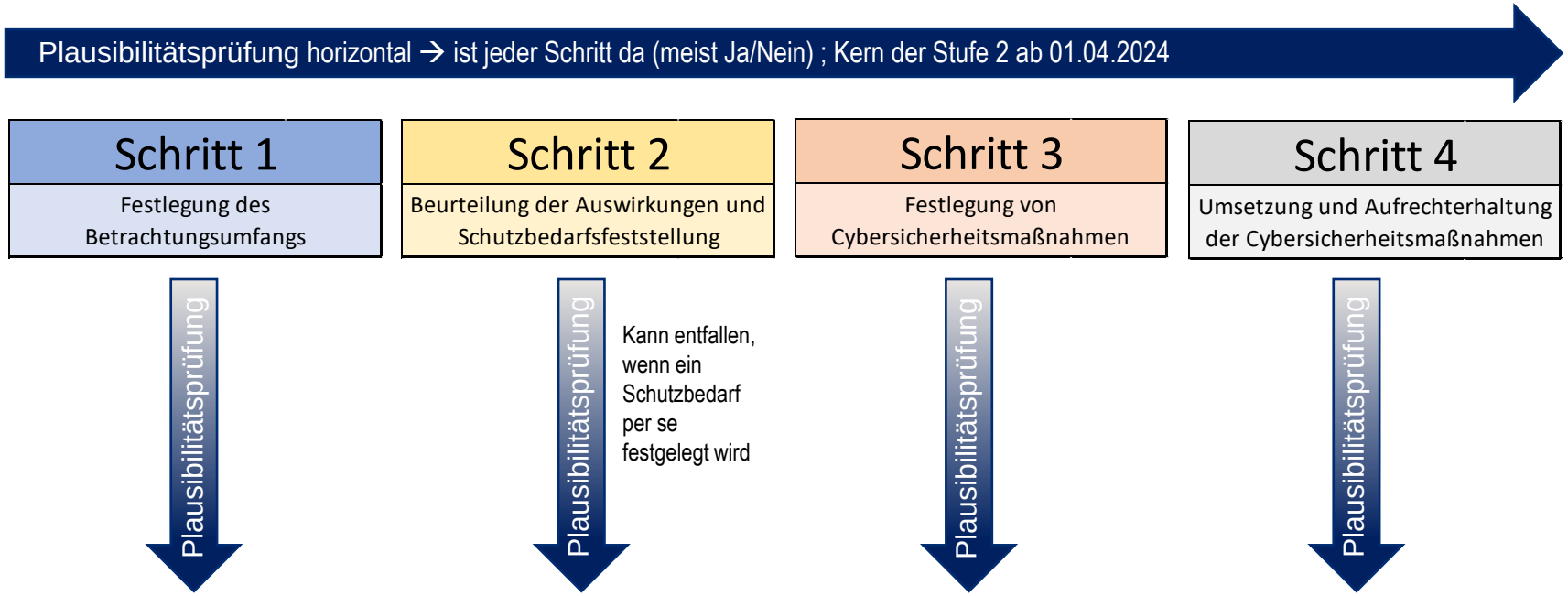
Festlegung von Cybersicherheitsmaßnahmen					
Benennung der schutzbedürftigen Einrichtungen	Die Elemente gemäß TRBS 1115-1 Abschnitt 3.2 sind im erforderlichen Umfang erfasst. (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)	Die Standardmaßnahmen der TRBS 1115-1 Abschnitt 4.5.2 Absatz 2 wurden im erforderlichen Umfang berücksichtigt. (Ja/~~Nein~~) (zzgl. Verweis auf Dokumentationsort)	Eine Festschreibung der erforderlichen Cybersicherheitsmaßnahmen ist erfolgt. (Ja/Nein) (Spezifikation der Cybersicherheit) (zzgl. Verweis auf Dokumentationsort)	Wenn Herstellervorgaben zur Cybersicherheit vorhanden sind, werden diese berücksichtigt. (Ja/Nein)	Ein Verfahren zur Aufrechterhaltung des Cybersicherheits-niveaus ist festgelegt. (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)
Einrichtung x					
Einrichtung x					
....					

Schritt 4

Umsetzung und Aufrechterhaltung der Cybersicherheitsmaßnahmen		
Benennung der schutzbedürftigen Einrichtungen	Organisatorische Maßnahmen der Cybersicherheit sind in einer Betriebsanweisung festgeschrieben (Ja/Nein) (zzgl. Verweis auf Dokumentationsort)	Technische Maßnahmen der Cybersicherheit sind nachweislich funktionsfähig/wirksam (Ja/Nein) (siehe hierzu TRBS 1115-1 Abschnitt 5 und 8.2)
Einrichtung x		
Einrichtung x		
....		

- Ergänzung des Ablaufdiagramms und der Beispieldokumentationsvorlage
- Weiterentwicklung von Textteilen ohne inhaltliche Neuausrichtung (bessere Verständlichkeit)
- Redaktionelle Anpassungen

Prüfung der Stufe 2



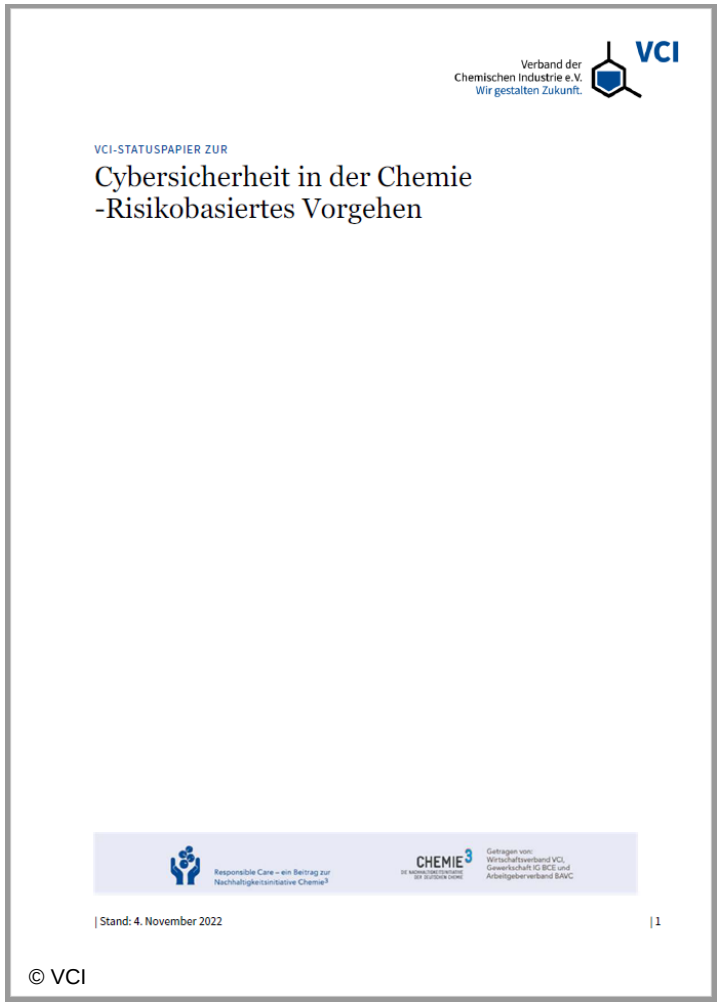
Plausibilitätsprüfung vertikal → entsprechen die Ergebnisse des Schritts (Dokumentation) dem, was ich erwarte? (Stichprobe hinsichtlich Vollständigkeit und Richtigkeit; Zukünftig erfahrungsabhängige Anpassung der Prüftiefe)

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

EVONIK Leading Beyond Chemistry

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

EVONIK
Leading Beyond Chemistry

Cybersicherheit in der Chemie - Risikobasiertes Vorgehen (Merkmale 3)

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 Schutzzielen 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

EVONIK
Leading Beyond Chemistry

VCI-STATUSPAPIER ZUR

Cybersicherheit in der Chemie - Risikobasiertes Vorgehen (Merkmale 4)

Sehr hoher Schutzbedarf

Für Sicherheitsfunktionen ≥ 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 ausreichendend Abdeckungsgrad auch für die vorgenannten Sicherheitsfunktionen und Prozessleitsysteme bzw. betrieblichen Einrichtungen bietet.
Bei der Bewertung vorhandener Cyberschutzmaßnahmen sind alle beteiligten Komponenten zu

EVONIK
Leading Beyond Chemistry

VCI-STATUSPAPIER ZUR

Cybersicherheit in der Chemie - Risikobasiertes Vorgehen (Fragenkatalog)

Anhang 1 – Themenkatalog

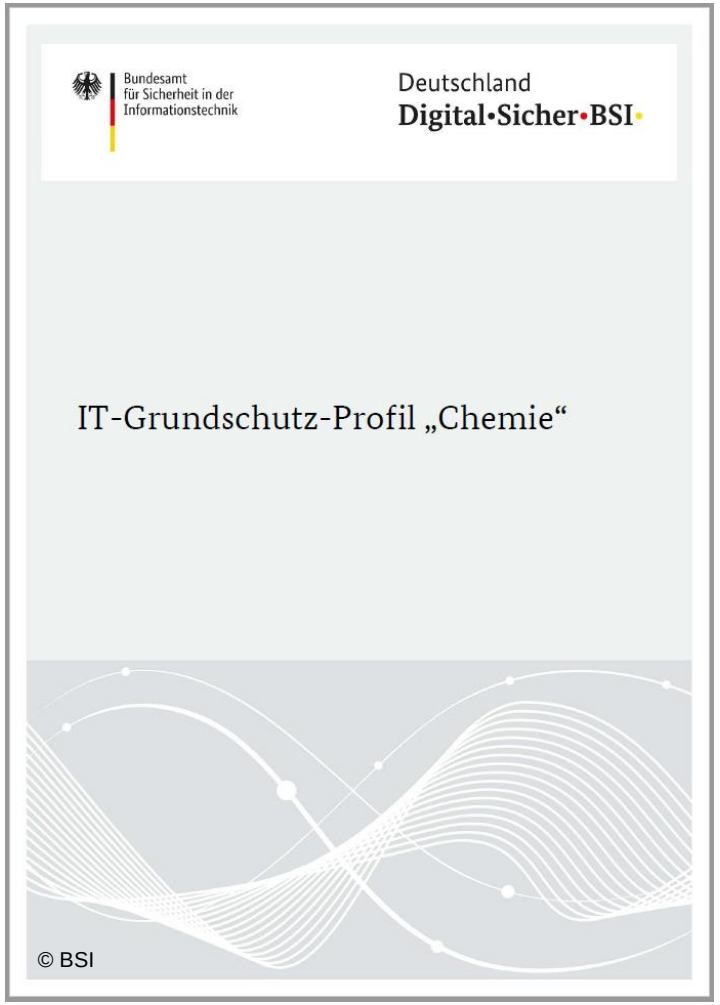
Der untenstehende Themenkatalog enthält praktische Fragen für eine strukturierte Vorgehensweise zur Festlegung der Cyberschutzmaßnahmen. Die Fragen ermöglichen den Einstieg in eine Erstbewertung der Cybersicherheit im Sinne dieses Dokumentes. Eine negative Antwort stellt dabei einen erklärungsbedürftigen 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

EVONIK Leading Beyond Chemistry

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



EVONIK
Leading Beyond Chemistry

BDI-Papier zu Cybersicherheitsregulierungen veröffentlicht 02/24

01. Februar 2024

EVONIK
Leading Beyond Chemistry

BDI-Papier zu Cybersicherheitsregulierungen - Hintergründe

Anlagensicherheit betroffen 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 (ÜAnlG)
  - Anforderungen an die Cybersicherheit in zukünftiger Überwachungsbedürfige Anlagenverordnung (ÜAnlV), AMBV (Arbeitsmittelbenutzungsverordnung, Nachfolge BetrSichV)

EVONIK Leading Beyond Chemistry

BDI-Papier zu Cybersicherheitsregulierungen – Vorschläge

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

Referentenentwurf zur Änderung der (41. BImSchV), Anhörungsverfahren 03/2024

Referentenentwurf zur Änderung der Bekanntgabeverordnung (41. BImSchV) | Sachverständige Cybersicherheit Anhörung der beteiligten Kreise nach § 51 BImSchG

- Innerhalb der Bundesregierung noch nicht abgestimmt und noch nicht beschlossen
- Frist für Stellungnahme: 29. März 2024
  - https://www.bmuv.de/gesetz/referentenentwurf-einer-verordnung-zur-aenderung-der-bekanntgabeverordnung
- 6 Stellungnahmen (2 x Länder, 4 x Industrie) veröffentlicht. Wesentliche Aspekte:
  - Vergleichbarkeit der Fachkompetenz zur Abwendung krimineller Cyberbedrohungen mit Kompetenzen der bisherigen Fachgebiete kaum möglich
  - Möglichkeit der Einbindung weiterer (Cyber-)Sachverständiger durch vorhandene Verordnung bereits gegeben
  - Anerkennungsrolle eher bei BSI
  - Inhaltsgleiche Kopplung von Cybersicherheitsanforderungen zu weiteren Rechtsgebieten (ÜAnlG, etc.)
  - Unnötiger Bürokratieaufbau

EVONIK Leading Beyond Chemistry

Referentenentwurf zum NIS2UmsuCG, Anhörungsverfahren 05/2024

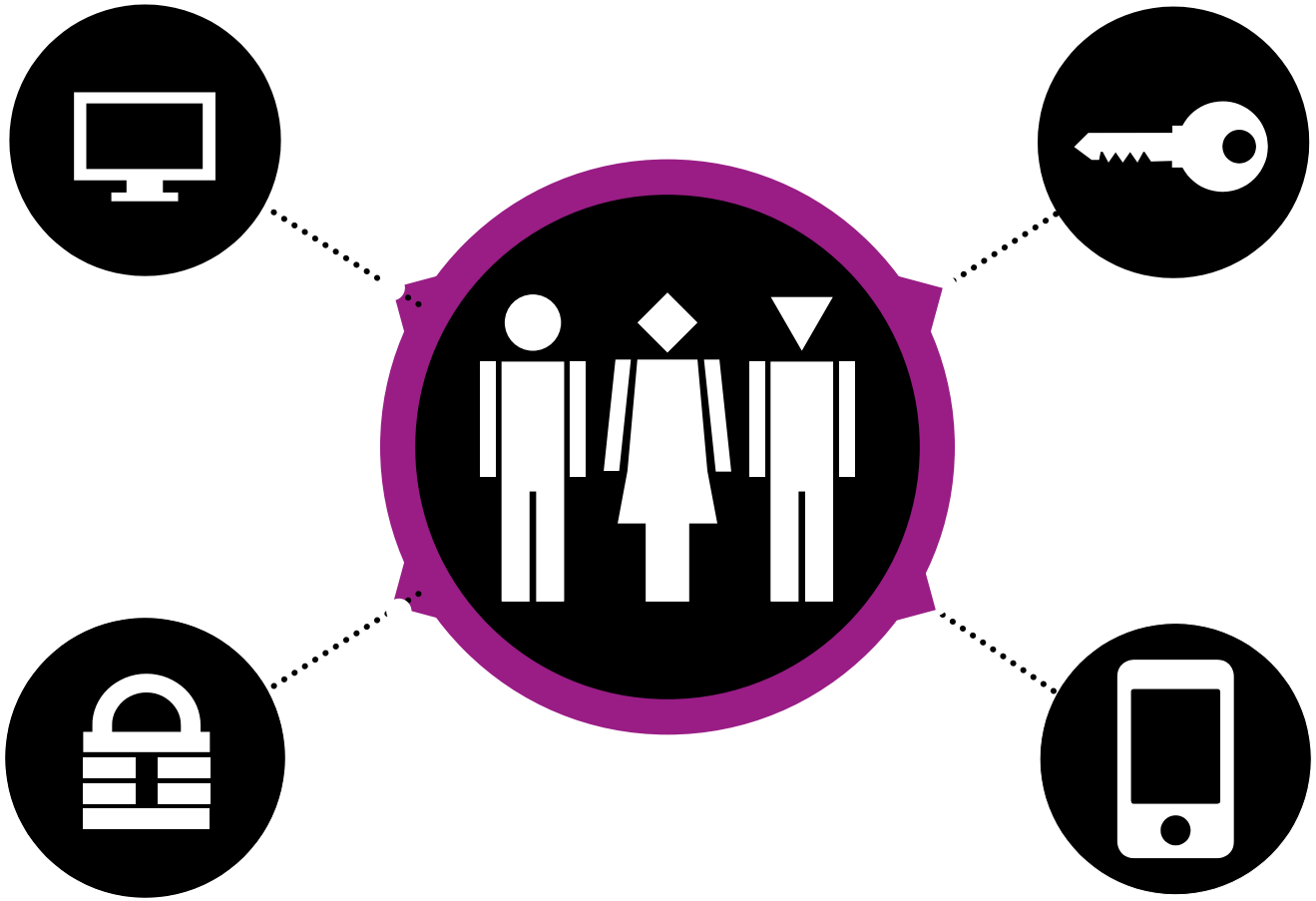
Referentenentwurf zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

- Innerhalb der Bundesregierung noch nicht abgestimmt und noch nicht beschlossen
- Frist für Stellungnahme: 28. Mai 2024
  https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis2umsucg.html
- NIS2UmsuCG, Anlage 2, *Sektoren wichtiger Einrichtungen*
  - u. a. Produktion, Herstellung und Handel mit chemischen Stoffen
- § 58 Ermächtigung zum Erlass von Rechtsverordnungen
  - BMI bestimmt i. W. durch Rechtsverordnung ohne Bundesratszustimmung Details zur Ausgestaltung im Einvernehmen mit weiteren Ressorts, z. B. BMWK, BMF, BMJ, BMAS, BMVg, BMEL, BMG, BMDV, BMBF, BMUV
  - Themen z. B.
    - Sicherheitskennzeichnung von Produkten
    - Cybersicherheitszertifizierungen

EVONIK Leading Beyond Chemistry

Auffälligkeiten bei Prüfungen in der betrieblichen Praxis

Passwortschutz
- Engineering Station nicht gesperrt



Zugriffsberechtigung
- Passwort wird weitergegeben

Zutrittsberechtigung
- Offenes Blockieren der Schaltraumtür mit Keil/Kabelbinder

Tragbare Medien
- Laden des Smartphones an der Engineering Station

EVONIK Leading Beyond Chemistry

Kontakt

Christoph Thust

VP and Senior Advisor Plant Safety | Process Technology & Engineering

Evonik Operations GmbH | Technology & Infrastructure

christoph.thust@evonik.com