LANUV
Kompetenz für ein lebenswertes Land

Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen

KAS-51 und Co.

Anforderungen und Auswirkungen der aktuellen Regelwerke

M. Sc. Stephan Gebhard

FB 74: Umwelttechnik und Anlagensicherheit für Chemie und Mineralölraffination

KAS 51 und Co.

- Kurzvorstellung
- Abgrenzung 12.BImSchV / IT-SIG
- KAS-51
- Neuerungen der VDI/VDE 2180
- Exkurs NA 163
- Industrie 4.0

KAS 51 und Co.

- **Kurzvorstellung**
- Abgrenzung 12.BImSchV / IT-SIG
- KAS-51
- Neuerungen der VDI/VDE 2180
- Exkurs NA 163
- Industrie 4.0

Zur Person

Stephan Gebhard

2007 – 2014:

- Bachelorstudium Umweltschutz
- Masterstudium Umweltingenieurwesen
- Zertifikatsstudium Umweltrecht

Seit 2015:
Gutachter im Bereich Anlagensicherheit des LANUV NRW Fachliche Schwerpunkte:

- IT-OT Konvergenz
- IT-Sicherheit
- Prozessleittechnik

In 2019:
Referent im Umweltministerium NRW, Bereich Anlagensicherheit

2016 - 2020:
Berufsbegleitendes Fernstudium IT-Sicherheit

LANUV NRW

Landesamt für Natur, Umwelt und Verbraucherschutz NRW

- Landesoberbehörde im Ressort des Ministeriums für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz (MULNV) NRW
- Technisch-wissenschaftliche Fachbehörde
- Rund 1200 Mitarbeiter an 19 Standorten in NRW
- Gegliedert in 8 Abteilungen, untergliedert in Fachbereiche
- Anlagensicherheit:
  - Fachbereich 73: Umwelttechnik und Anlagensicherheit für Energieerzeugung, Steine/Erden, Metalle, Landwirtschaft
  - **Fachbereich 74: Umwelttechnik und Anlagensicherheit für Chemie und Mineralölraffination**
  - Fachbereich 75: Umwelttechnik und Anlagensicherheit für Gefahrstofflagerung und -verladung

LANUV NRW

Landesamt für Natur, Umwelt und Verbraucherschutz NRW

Tätigkeiten und Arbeitsfelder (Auszug)

- Begutachtung von Sicherheitsberichten, Beurteilung von Sicherheitskonzepten etc.
- Fachliche Beratung in Fragen zur Anlagensicherheit und Störfallverordnung für Ministerien, Behörden, etc.
- Bekanntgabe von Sachverständigen gemäß § 29b BImSchG
- Anerkennung von Lehrgängen für die Immissionsschutz- und Störfallbeauftragten gemäß der 5. BImSchV
- Ausrichten von Seminaren, Mitarbeit in Gremien etc.

KAS 51 und Co.

- Kurzvorstellung
- **Abgrenzung 12.BImSchV / IT-SIG**
- KAS-51
- Neuerungen der VDI/VDE 2180
- Exkurs NA 163
- Industrie 4.0

12. BImSchV

Herkunft

Deutsche Umsetzung der Seveso III Richtlinie (Richtlinie 2012/18/EU) durch eine Verordnung der Umweltverwaltung

Auslöser

Mehrere schwere Unfälle (sogenannte Störfälle) in den 1970er Jahren, z.B. in Flixborough 1974 oder in Seveso 1976

Ziel

Beherrschung der Gefahren schwerer Unfälle mit gefährlichen Stoffen

Anwendungsbereich

Betriebsbereiche (der unteren und / oder oberen Klasse)

IT-Sicherheitsgesetz

Zuständigkeit des Bundesinnenministeriums

- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz aka IT-SIG)
- Ausführung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), hinterlegt im BSI-Gesetz (BSIG)
- Konkretisiert durch die Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV)

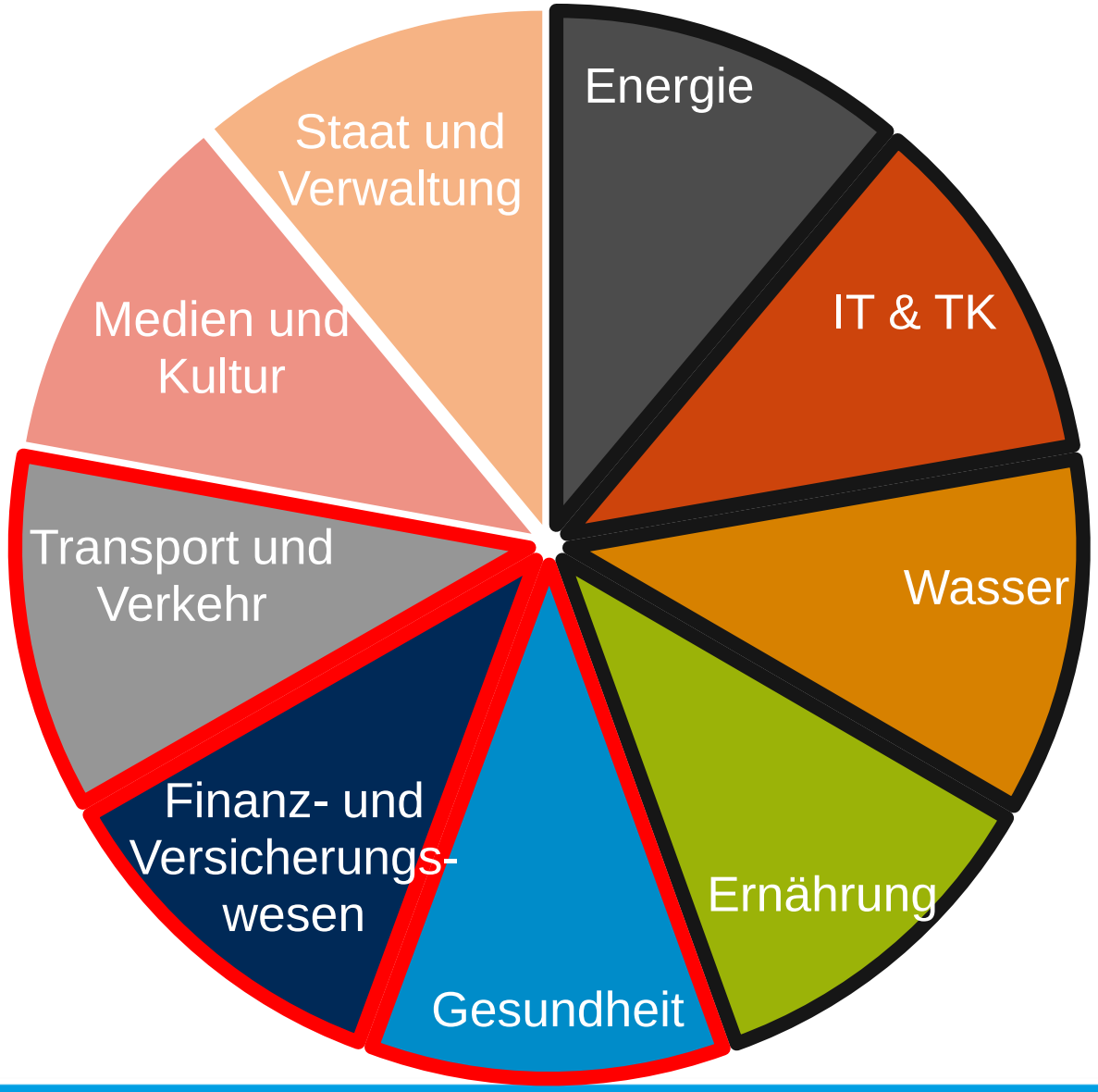
Hintergrund

Schutz der Versorgungssicherheit und der sogenannten Kritischen Infrastrukturen

Kriterien der Kritische Infrastrukturen

- Mindestens 500.000 durch die „Anlage“ versorgte Personen
- Sektorenzugehörigkeit der „Anlage“

Sektorenaufteilung nach BSI-KritisV



Stand:

- „**Korb I**“ 04.2016:
  Energie,
  Informationstechnik und Telekommunikation
  Wasser, Ernährung

- „**Korb II**“. 07.2017:
  Transport und Verkehr,
  Gesundheit
  Finanz- und Versicherungswesen

- Strittig (nicht Bestandteil der aktuellen BSI-KritisV)
  Staat und Verwaltung,
  Medien und Kultur
  sowie die Rolle von diversen Substrukturen (z. B. Zulieferbetrieben)

Abgrenzung 12. BImSchV / BSI-KritisV

Zuständigkeit

- **12. BImSchV**: Umweltverwaltungen der Länder
- **BSI-KritisV:** Innenministerium (Ausführung BSI) des Bundes

Primäres Ziel

- **12. BImSchV**: Schutz der Bevölkerung vor gefährlichen Zuständen durch eine / von einer Anlage
- **BSI-KritisV:** Versorgungssicherheit der Bevölkerung

Betrachtungsansatz in der IT-Sicherheit

- **12. BImSchV**: Fokussiert auf die PLT- und MSR-Einrichtungen
- **BSI-KritisV:** Ganzheitlicher Ansatz für das Unternehmen

KAS 51 und Co.

- Kurzvorstellung
- Abgrenzung 12.BImSchV / IT-SIG
- **KAS-51**
- Neuerungen der VDI/VDE 2180
- Exkurs NA 163
- Industrie 4.0

KAS-51

Die KAS

Die Kommission für Anlagensicherheit (KAS) ist ein unabhängiges Gremium zur Beratung der deutschen Bundesregierung bzw. des zuständigen Bundesministeriums in Fragen der Sicherheit von Anlagen im Sinne des Bundes-Immissionsschutzgesetzes (BImSchG).

Zusammensetzung:

- Bundesbehörden
- Landesbehörden (Immissions- und Arbeitsschutz)
- Gewerkschaften & Berufsgenossenschaften
- Sachverständige
- Wirtschaftsvertreter
- Wissenschaftsvertreter
- Umweltverbände

KAS-51

Aus dem SFK-GS-38 wird der KAS-51

Hintergrund:

- Der ursprüngliche SFK-GS-38 erschien 2002 in der Folge der Attentate vom 11. September 2001 in New York (9/11)
- Fokus liegt auf dem Schutz des Außenperimeters

Defizite des alten Leitfadens:

- Fehelende Betrachtung von heute wichtigen/ relevanten Themenfeldern
- Veraltete rechtliche Grundlage (Seveso-II-Richtlinie)

Veraltet

~~Angriffe über die elektronische Verne[illegible]ehmen („Cyberattacke“) werden für weniger gefährdend erachtet. Ein Zugang zu den Rechnern, welche die Anlagen direkt steuern (und nur diese sind für die Anlagensicherheit relevant), ist in der Regel von außen außerordentlich schwierig~~

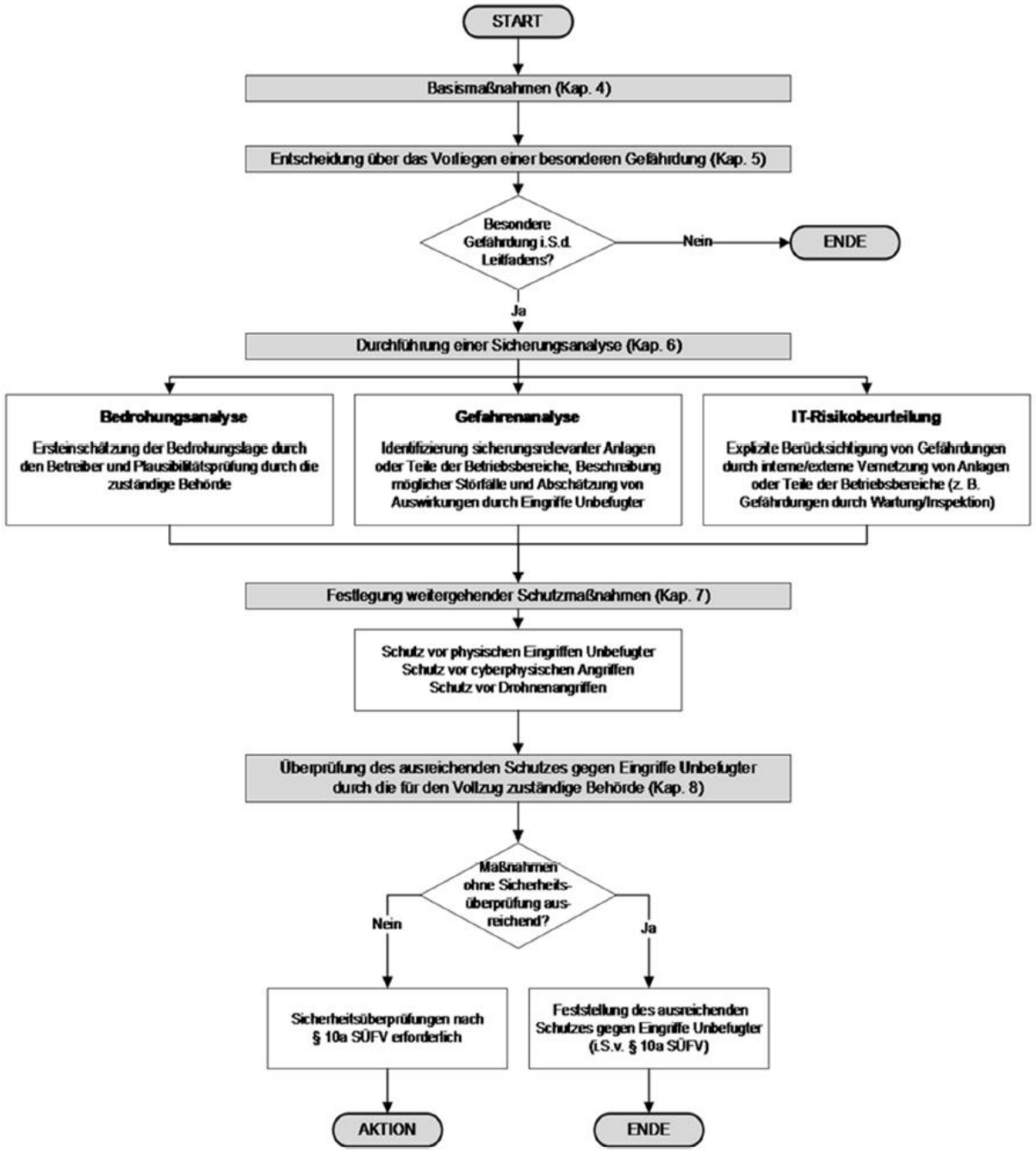
KAS-51

Überarbeitung des SFK-GS-38

- Anpassung an die aktuelle Rechtslage (Seveso-III)
- Einbezug neuer Erkenntnisse
- Neustrukturierung der Inhalte
- Einbezug der Themen:
  - Cyber-Security
  - Drohnen

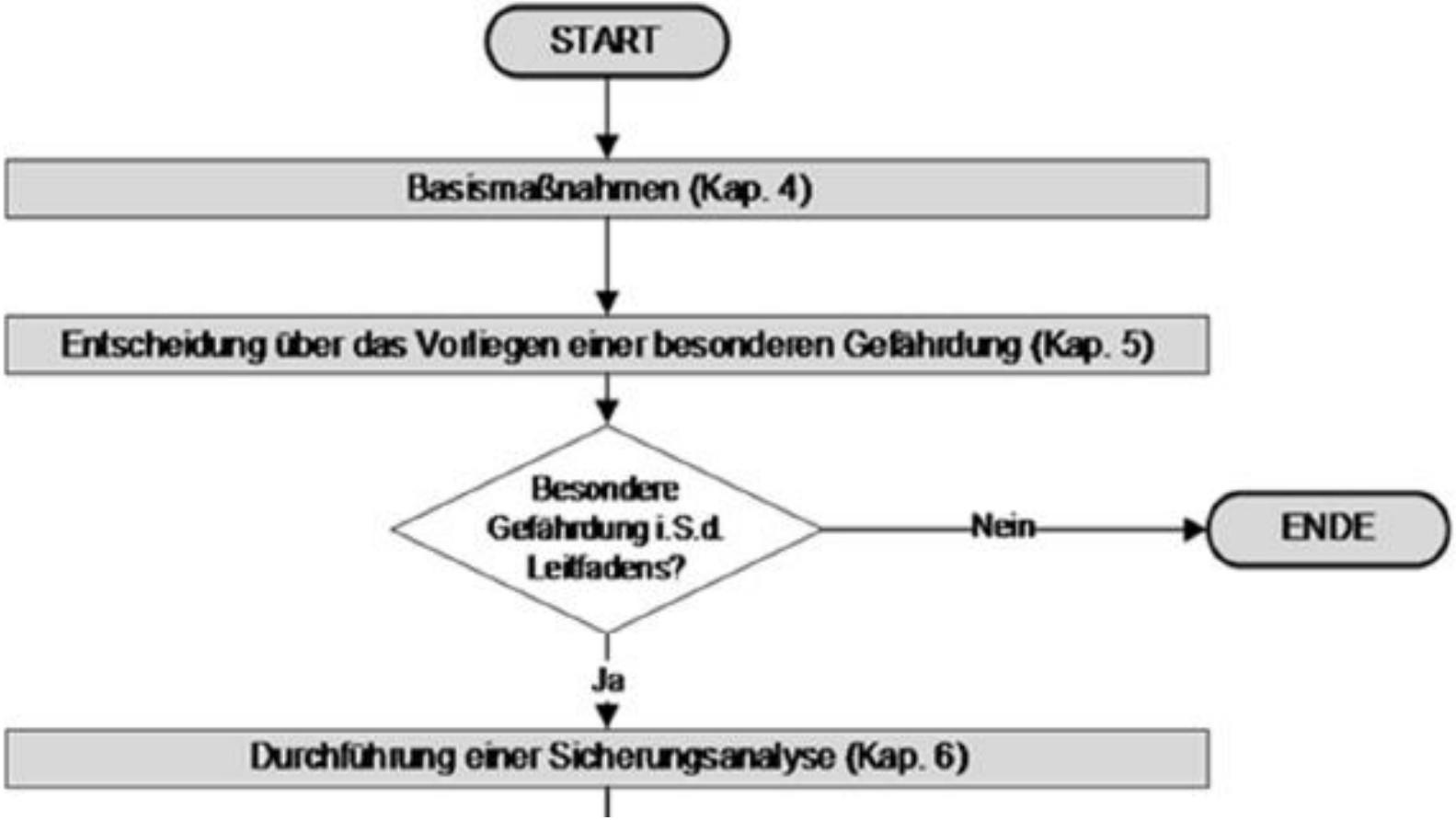
KAS-51

Struktur



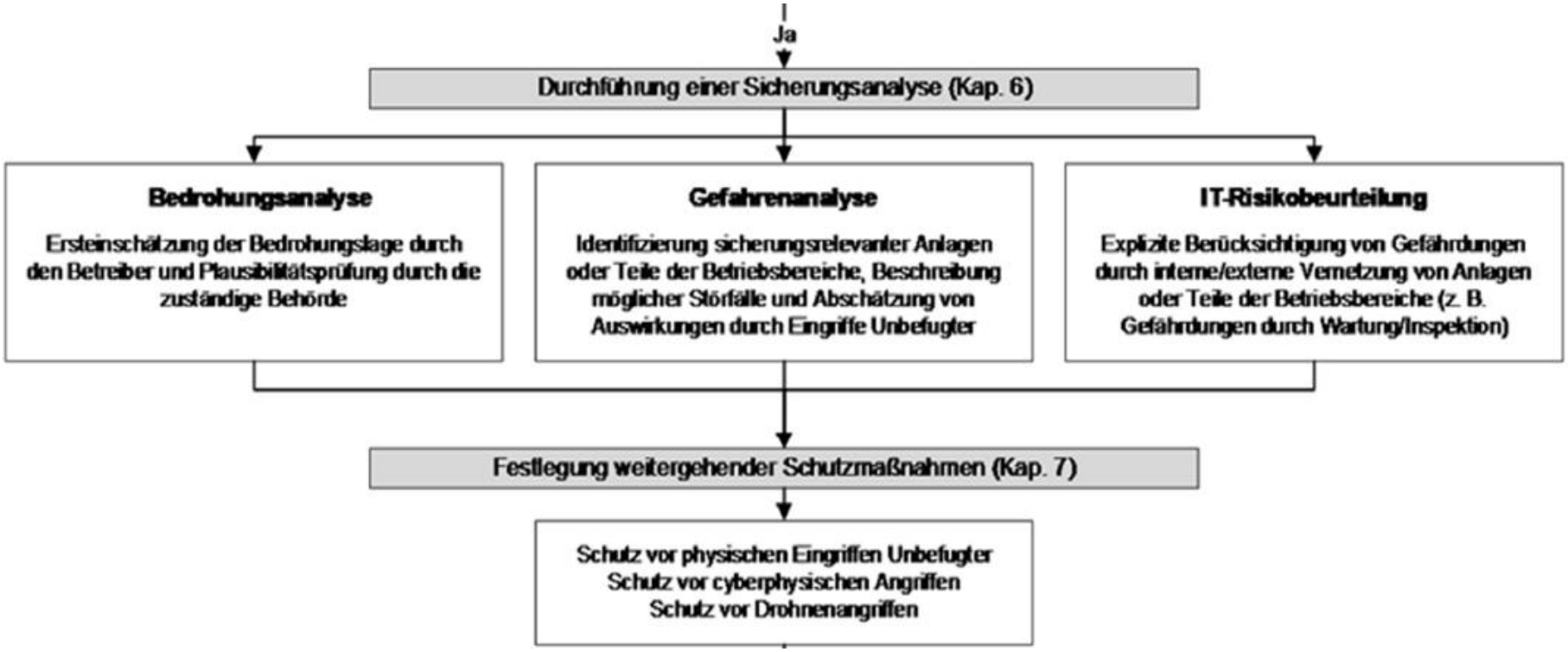
KAS-51

Struktur



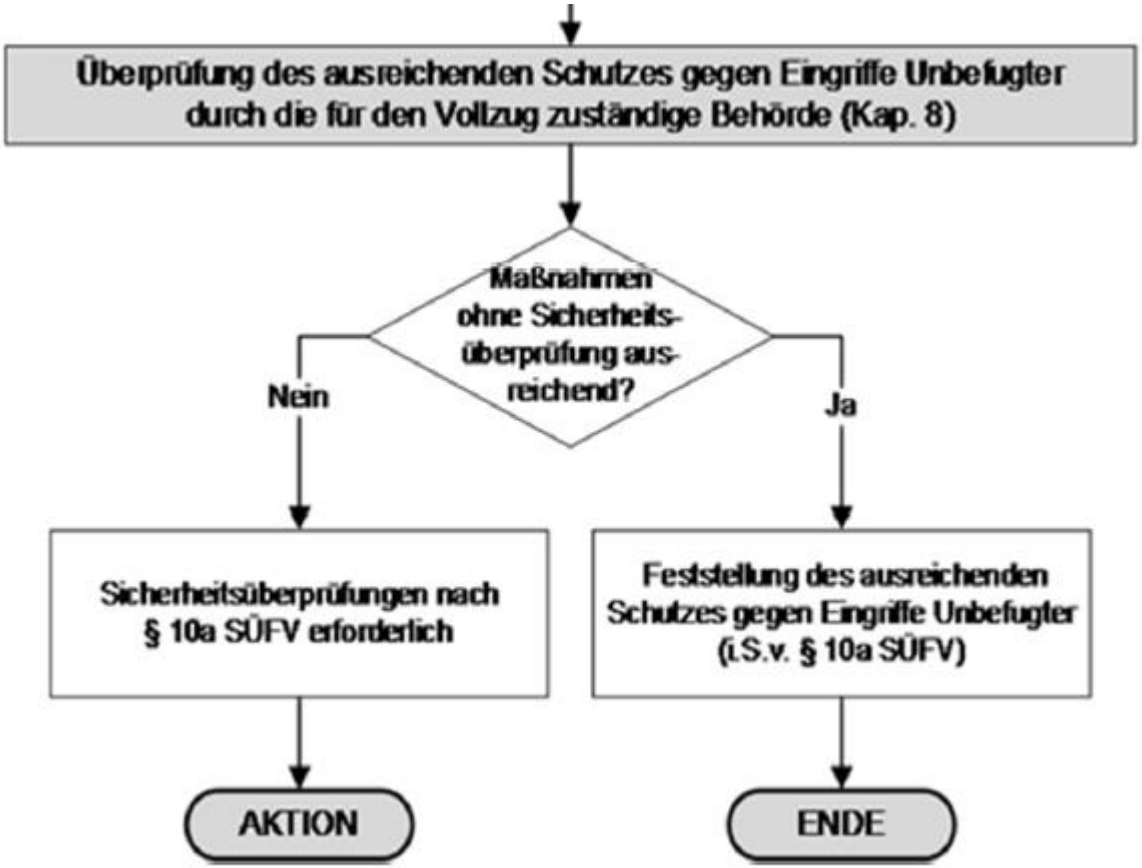
KAS-51

Struktur



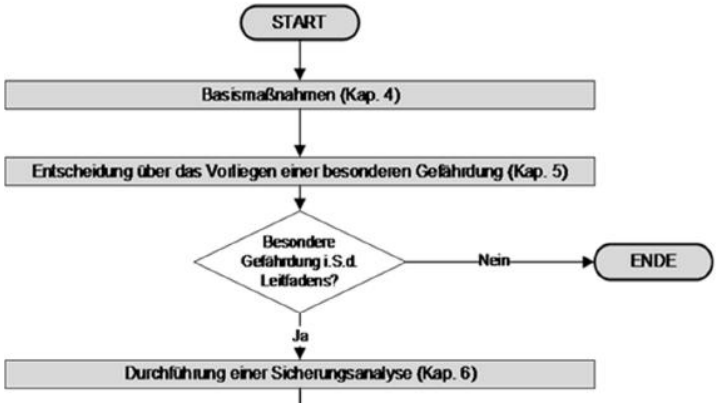
KAS-51

Struktur



KAS-51

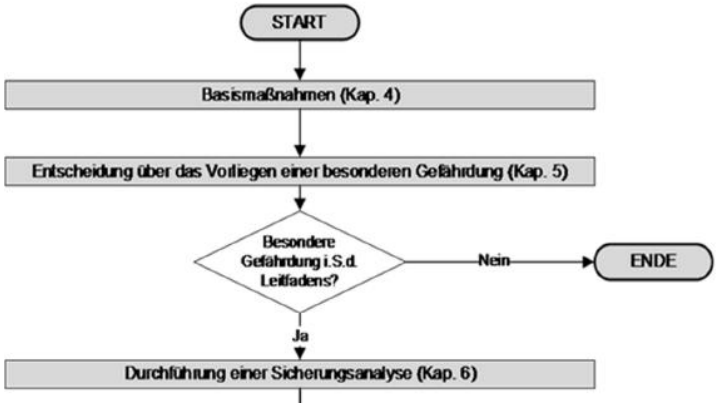
Basismaßnahmen
(gelten für alle ohne Ausnahme)



- Festlegung von Verantwortlichkeiten
- Zugangs- und Zutrittsmanagement und -überwachung
- Zugriffsmanagement auf Prozesssteuerung/Sicherheitssteuerung
- Manipulationserkennung und –schutz
- Regelungen für Fremdpersonal und fremdvergebene Dienstleistungen
- Sensibilisierung/Schulung eigener Mitarbeiter
- Reaktion auf neue Schwachstellen und IT-Bedrohungen

KAS-51

Entscheidung über das Vorliegen einer besonderen Gefährdung



- Einzelfallentscheidung der zuständigen Behörde
- „Daumenregel“:

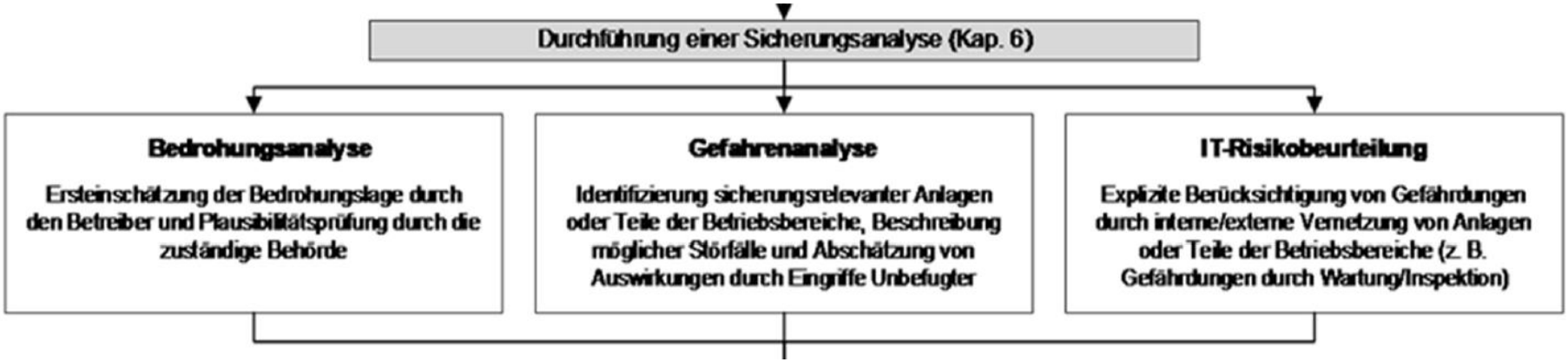
Betriebsbereichen der unteren Klasse → oftmals keine „besondere Gefährdung“

Betriebsbereichen der oberen Klasse → oftmals eine „besondere Gefährdung“

- Aber: Durchlässigkeit in beide Richtungen bleibt

KAS-51

Sicherheitsanalyse



Bestandteile:

- **Bedrohungsanalyse**: Einschätzung der Bedrohungslage
  (politische Lage, soziale nationale und produktspezifische Besonderheiten etc.)
- **Gefahrenanalyse:** Klassische Gefahrenanalyse
- **IT-Risikobeurteilung**

KAS-51

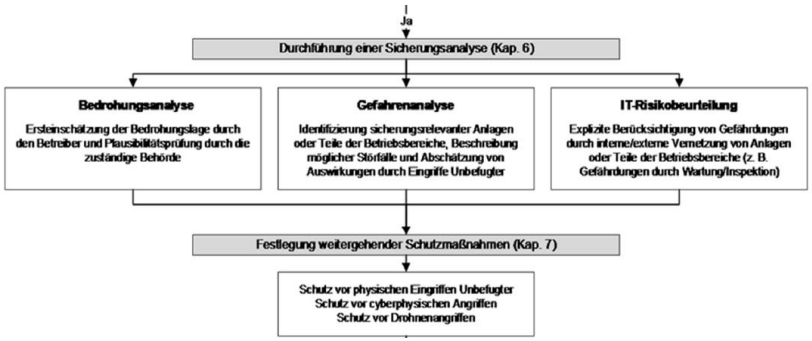
IT-Risikobeurteilung

- erfasst Schwachstellen aus Sicht der IT-Sicherheit für alle Assets
- erfasst IT-Gefährdungen aus Sicht der IT-Sicherheit
- identifiziert die möglichen Auswirkungen der IT-Gefährdungen auf die Integrität und Verfügbarkeit der sicherheitstechnischen Funktionen (nach DIN EN 61511)
- bewertet diese anhand der Wahrscheinlichkeit des Ausnutzens der IT-Schwachstelle

Durchführung nach: IEC 62443, DIN ISO/IEC 27001, NA 163, ….

KAS-51

Festlegung weitergehender Schutzmaßnahmen



- Schutz vor Außentätern
- Schutz vor Innentätern
- Einführung eines Sicherungsmanagements
- Schutz vor cyberphysischen Angriffen (Anhang 2)
- Schutz vor Drohnenangriffen (Anhang 3)
- Geheimhaltung von Unterlagen

KAS-51

Exkurs Anhang 2: IT-Sicherheit

Schutz vor cyberphysischen Angriffen

Behandelte Themen

- IT-Security ist Führungsaufgabe
- Sensibilisierung und Unterweisung
- Asset Register und Netzwerkarchitektur
- IT-Sicherheit bei der Errichtung von Anlagen
- Reaktion auf neue Schwachstellen und Bedrohungen
- Erkennung von IT-Sicherheitsvorfällen
- Maßnahmen nach IT-Sicherheitsvorfällen

KAS-51

Exkurs Anhang 2 (Beispiel)

Reaktion auf neue Schwachstellen und Bedrohungen

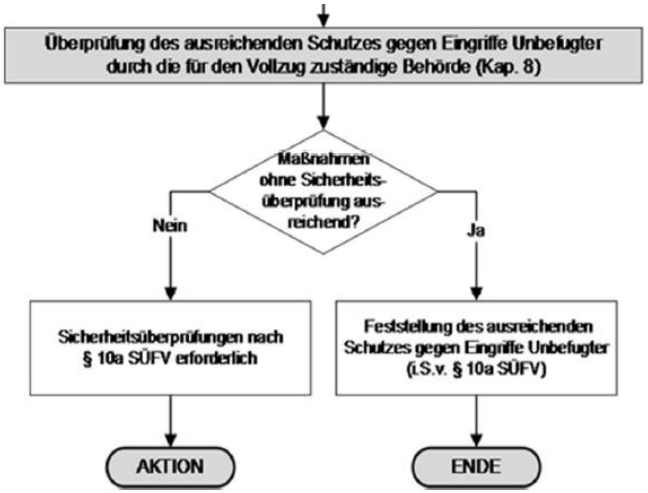
- Es sind Konzepte und Abläufe festzulegen, wie auf neue Schwachstellen und IT-Bedrohungen reagiert wird. Dazu gehören u. A. der Umgang mit Updates und der Schutz vor Schadsoftware.

Kontrollfragen:

- *Über welche Wege werden Informationen zu neuen Schwachstellen und IT-Bedrohungen erfasst, die den Betriebsbereich betreffen?*
- *Wie wird auf neue Schwachstellen reagiert?*
- *Gibt es Vorgaben bezüglich der Reaktion auf neue Schwachstellen und IT-Bedrohungen (z.B. Patch- und Updatemanagement)?*
- *In welchem zeitlichen Rahmen werden Schutzmaßnahmen ergriffen?*

KAS-51

Überprüfung durch die Behörde



- Die zuständige Behörde prüft die Sicherungsanalyse und die Qualität der Umsetzung
- Bei Feststellung des ausreichenden Schutzes ist keine separate Sicherheitsüberpüfung nach § 10a Sicherheitsüberprüfungs-feststellungsverordnung (SÜFV) erforderlich
- Der Sicherheitsbericht dient dem Betreiber insoweit als Rechtssicherheitsnachweis

KAS 51 und Co.

- Kurzvorstellung
- Abgrenzung 12.BImSchV / IT-SIG
- KAS-51
- **Neuerungen der VDI/VDE 2180**
- Exkurs NA 163
- Industrie 4.0

Neuerungen der VDI/VDE 2180

Funktionale Sicherheit in der Prozessindustrie

Allgemeines:

- Runderneuert in 04/2019 (als Folge der Konkretisierung der Normen IEC 61508 und IEC 61511)
- Geänderte Systematik bei der Einteilung von PLT-Systemen

Alter Begriff	Neuer Begriff
PLT-Betriebseinrichtung (Messen, Steuern, Regeln)	PLT-Betriebseinrichtung (**PLT-B**) (Messen, Steuern, Regeln, Alarmieren, Melden, Schalten)
PLT-Überwachungseinrichtung (Alarmieren, Melden, Schalten)	
Hochverfügbare PLT-Überwachungseinrichtung	PLT-Betriebseinrichtung mit Sicherheitsfunktion (**PLT-BS**) (Risikominderung bis Faktor 10)
PLT-Schutzeinrichtung	PLT-Sicherheitseinrichtung (**PLT-S**) (Risikominderung > Faktor 10, SIL 1 bis SIL 4)

- Stärkung der Probabilistik und Deterministik
- Neuer Schwerpunkt: Cyber-Security

Neuerungen der VDI/VDE 2180

Kapitel 8 Cyber-Security

(Aus Gründen des Copyrights können die einzelnen Auszüge der Norm nicht 1:1 wiedergegeben werden, es folgt eine kurze inhaltliche Auflistung der im Vortrag erläuterten Punkte)

- Eine IT-Risikobeurteilung muss durchgeführt werden (Blatt 1, S. 38 ff.)
- IT-Risikobeurteilung soll die Bereiche Hardware, Software, Daten, Verbindungen, Prozesse, Organisationen, Personen umfassen (Blatt 1 S. 39)

Neuerungen der VDI/VDE 2180

Kapitel 8 Cyber-Security

(Aus Gründen des Copyrights können die einzelnen Auszüge der Norm nicht 1:1 wiedergegeben werden, es folgt eine kurze inhaltliche Auflistung der im Vortrag erläuterten Punkte)

- Die IT-Risikobeurteilung soll folgende Teilschritte beinhalten:
  - Erfassen der Elemente des Systems
  - Erfassen und Bewerten von Bedrohungen der Integrität der PLT-Sicherheitsfunktion
  - Definieren von Maßnahmen, um den Bedrohungen in geeigneter Weise zu begegnen
  - Wirksamkeitsüberprüfung der Maßnahmen (Blatt 1 S. 39)

Neuerungen der VDI/VDE 2180

Kapitel 8 Cyber-Security

(Aus Gründen des Copyrights können die einzelnen Auszüge der Norm nicht 1:1 wiedergegeben werden, es folgt eine kurze inhaltliche Auflistung der im Vortrag erläuterten Punkte)

- Ausgehend von der Schnelllebigkeit der Thematik ist ein kontinuierliche Überwachungsprozesse zu etablieren (Blatt 1 S. 39)
- Ein IT-Absicherungskonzept kann (unter bestimmten Bedingungen) beispielsweise mittels NA 163 + VDI/VDE 2182 realisiert werden (Blatt 1 S. 40)

KAS 51 und Co.

- Kurzvorstellung
- Abgrenzung 12.BImSchV / IT-SIG
- KAS-51
- Neuerungen der VDI/VDE 2180
- **Exkurs NA 163**
- Industrie 4.0

Exkurs NAMUR Arbeitsblatt 163

Ausgangslage

- Bestehende Ansätze für eine IT-Risikoanalyse sind oft sehr Zeit- und Personalintensiv (z.B. IEC 62443)
- Es gibt in der Summe viele „einfache“ PLT-Sicherheitseinrichtungen

Anforderungen

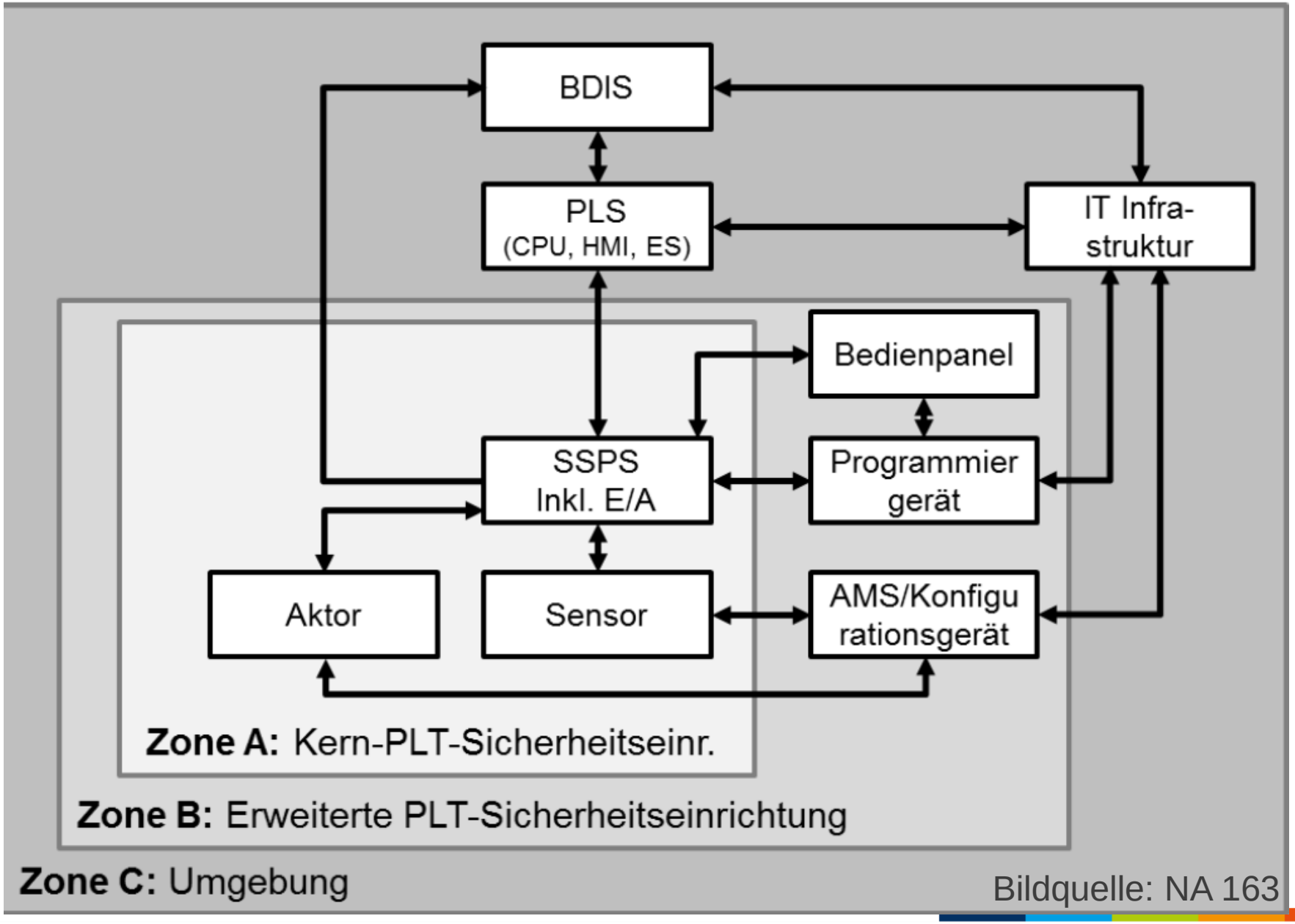
- Sicheres Einhalten von Gesetzen und Regelwerken
- Durchführung durch nicht IT-Fachleute (PLT- Ingenieur/in als Zielgruppe) möglich
- Zeiterfordernis < 1 Tag pro Anlage

Exkurs NAMUR Arbeitsblatt 163

Ansatz

- Anwendung der IT-Risikobeurteilung der IEC 62443
- Verständigung auf allgemeingültige Basisparameter
  - SIL 1 bis 3
  - Niedrige Anforderungsrate (low demand)
  - Zonierter (segmentierter) Aufbau des Netzwerkes

Exkurs NAMUR Arbeitsblatt 163



Bildquelle: NA 163

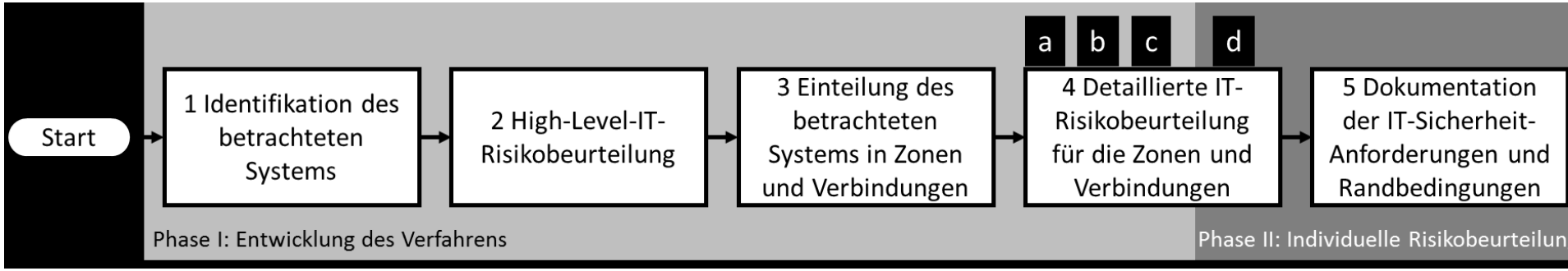
Exkurs NAMUR Arbeitsblatt 163

Ansatz

- Anwendung der IT-Risikobeurteilung der IEC 62443
- Verständigung auf allgemeingültige Basisparameter
  - SIL 1 bis 3
  - Niedrige Anforderungsrate (low demand)
  - Zonierter (segmentierter) Aufbau des Netzwerkes
  - Rückwirkungsfreiheit der PLT-Sicherheitseinrichtung gegenüber der Umgebung
    - → Trennung der PLT-Sicherheitseinrichtung von der Umgebung
  - „ Assume the breach“-Ansatz für Zone C
    - → Es ist immer davon auszugehen, dass die Umgebung (Zone C) kompromittiert ist. Die PLT-Sicherheitseinrichtung muss Maßnahmen bereithalten, die ihre Integrität auch unter solchen Rahmenbedingungen gewährleistet.

Exkurs NAMUR Arbeitsblatt 163

IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen



1. **Identifikation des betrachteten Systems**
2. **High-Level-IT Risikobeurteilung**
3. **Einteilung des betrachteten Systems in Zonen und Verbindungen**
4. **Detaillierte IT-Risikobeurteilung**
5. **Dokumentation**

Großteils vorgegeben durch die NA 163

Abarbeitung durch die Checkliste der NA 163

Quelle: NA 163 Seite 4

Exkurs NAMUR Arbeitsblatt 163

Beispiel

Nr.	Erläuterung	Empfohlen / Möglich	Ergebnis	Abweichung	Verbesserungs - empfehlung
5	**Maßnahmen für Engineering Station, Field Entry Panel, AMS**				
5.1.1	Die Komponente (z.B. Engineering Station) wird ausschließlich für Zwecke der PLT-Sicherheitseinrichtung genutzt. Z.B. die Erstellung und Übertragung von Anwenderprogrammen auf das Logiksystem bzw. die Konfiguration von Feldgeräten genutzt.				
	Erläuterung: Eine Nutzung für weitere Zwecke würde die Installation von Software und Diensten nach sich ziehen, die Schwachstellen mit sich bringen. Darüber hinaus müsste der Kreis der Zugriffsberechtigten erweitert werden. Zielsetzung ist hier, „nur so viel wie nötig, so wenig wie möglich“ (z.B. keine Office-Software und Hilfsprogramme, Browser etc.).	empfohlen			

Quelle: Checkliste zur NA 163

KAS 51 und Co.

- Kurzvorstellung
- Abgrenzung 12.BImSchV / IT-SIG
- KAS-51
- Neuerungen der VDI/VDE 2180
- Exkurs NA 163
- **Industrie 4.0**

Industrie 4.0

Historischer Kontext

- Industrie 1.0: Erste Massenproduktion durch Maschinen; um ca. 1800. Einsatz menschlicher Kraft, Wasser und Dampf
- Industrie 2.0: Elektrizität als Antriebskraft; Ende 19. Jahrhundert. Umsetzung der Fließbandarbeit im großen Rahmen (Automobilbranche)
- Industrie 3.0: Automatisierung durch Elektronik und IT; ab den 1970er. Einsatz von Industrierobotern im großen Rahmen (Automobilbranche)
- Industrie 4.0: Vernetzung von Produktionsabläufen sowie deren Teilschritte, heute.

Bildquelle der Vortragsabbilung: https://www.yokogawa-blog.de/de/industrie-4-0

Industrie 4.0

Sicht der Behörde

- Sehr Inhomogener Level der einzelnen Firmen (bezogen auf den Stand der Digitalisierung):
  - Zumeist zwischen Industrie 2.0 und 4.0
  - Oftmals Mischungen innerhalb des Betriebsbereiches oder innerhalb einzelner Anlagen (Stichwort „Retrofit“)
  - Unterschiedliche Wünsche / Ansprüche / Erwartungshaltungen, insbesondere zwischen Ingenieuren/innen und Marketing
  - Gesamtkonzepte und Leuchtturmprojekte

Industrie 4.0

Sicht der Behörde

- Relativ große Unsicherheiten bezogen auf die IT-Sicherheit:
  - Schnelllebigkeit der Security Branche
  - Fehlende / unterschiedliche Regularien und Vorgaben
    - Insbesondere bei International tätigen Unternehmen kommen national unterschiedliche Interessen dazu, z.B. Verfassungsschutz vs. Homeland Security
  - Personalprobleme, Budgetlimitierungen
  - Kommunikationsprobleme (oft historisch bedingt): z. B. zwischen IT und OT

Industrie 4.0

Sicht der Behörde

- Oft vorgefundene Mängel / Probleme:
  - Informationen veraltet / überholt / unvollständig
  - Security vs. Obscurity
  - Zu klein gewählter Ansatz / falsch gewählter Ansatz
  - Nicht betrachtete Schnittstellen
  - Fokussieren auf Vorteile einer neuen Technologie

    → Unterschätzen der damit einhergehenden Nebenwirkungen / Nachteile
  - Fehlendes „Know How“

Industrie 4.0

Wohin geht die Reise? – Ein Blick in die Glaskugel

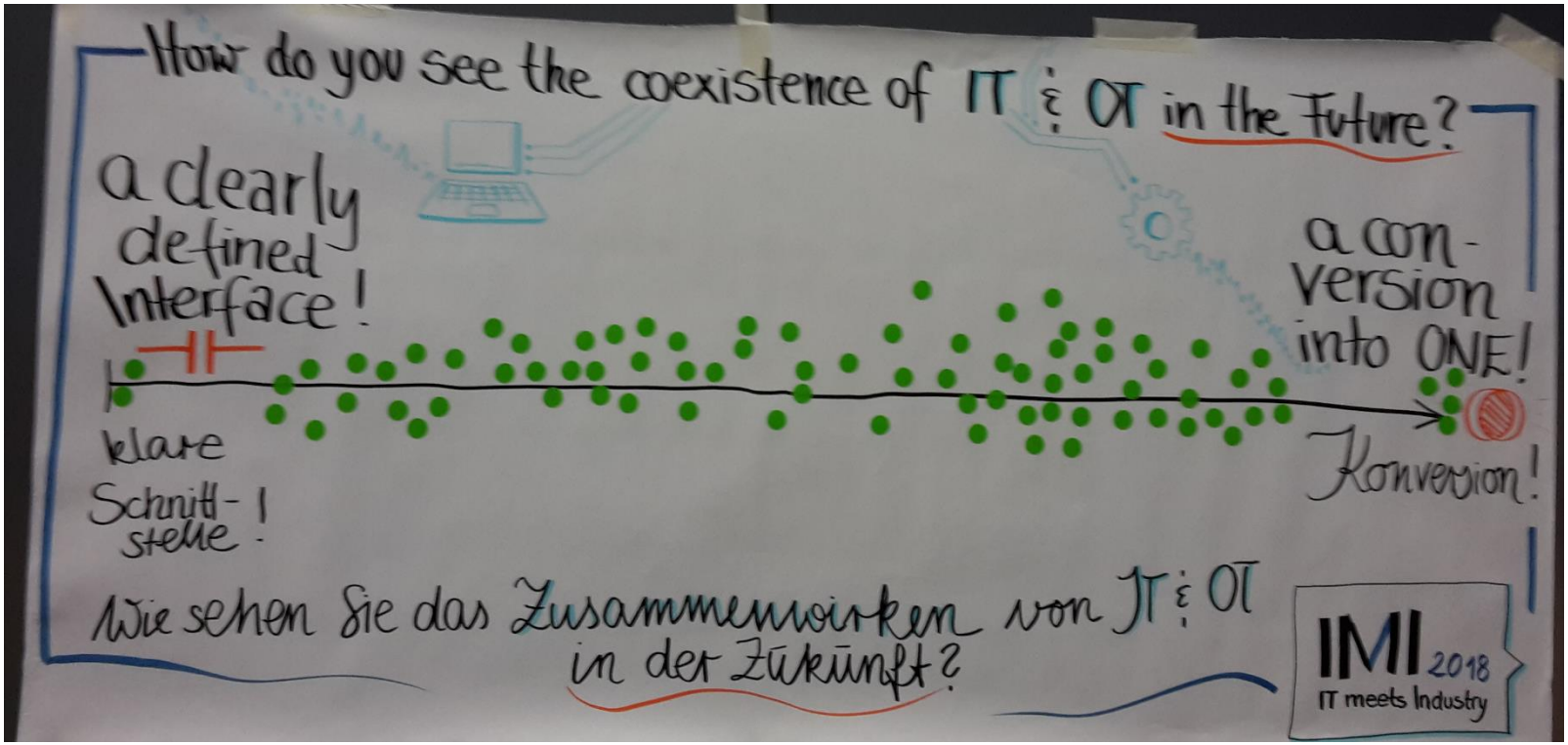


Bild mit freundlicher Genehmigung von Anapur

Industrie 4.0

Wohin geht die Reise? – Aktuelle Projekte in der Industrie (Auszug)

- Anlagenparametrierung und –controlling aus der Cloud
- Augmented-Reality in der Instandhaltung
- Drohnen im Betriebsbereich
- Ethernet als neuer Standard
- Fernwartung
- IIoT
- Predictive maintenance
- Smart Overpressure Protection Device (SmOP)
- Smarte Gefahrstofflagerung
- WLAN (oder andere Funknetze) im Betriebsbereich

Vielen Dank!

Kontakt

M. Sc. Stephan Gebhard

Fachbereich 74
Umwelttechnik und Anlagensicherheit
für Chemie und Mineralölraffination

**Landesamt für Natur, Umwelt
und Verbraucherschutz NRW**

Dienstort: Wallneyer Straße 6,
45133 Essen

Postanschrift: Postfach 101052,
45610 Recklinghausen

Telefon / E-Mail
+49 (0)201 7995-1924
Stephan.Gebhard@lanuv.nrw.de