Landesamt für Natur,
Umwelt und Verbraucherschutz
Nordrhein-Westfalen

Anforderungen der Störfallverordnung und deren Umsetzung – Überprüfung des Sicherheitsmanagementsystems

Fragen und Bewertungshilfen

LANUV-Arbeitsblatt 51

LANUV
Kompetenz für ein lebenswertes Land

Anforderungen der Störfallverordnung und deren Umsetzung – Überprüfung des Sicherheitsmanagementsystems

Fragen und Bewertungshilfen

LANUV-Arbeitsblatt 51

Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen
Recklinghausen 2020

IMPRESSUM

Herausgeber	Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen (LANUV) Leibnizstraße 10, 45659 Recklinghausen Telefon 02361 305-0, Telefax 02361 305-3215 E-Mail: poststelle@lanuv.nrw.de
Bearbeitung	Birgit Richter (LANUV)
Titelfoto	Michael Kuntschner (LANUV)
Stand	April 2020
ISSN	2197-8336 (Print), 1864-8916 (Internet), LANUV-Arbeitsblätter
Informationsdienste	Informationen und Daten aus NRW zu Natur, Umwelt und Verbraucherschutz unter • www.lanuv.nrw.de Aktuelle Luftqualitätswerte zusätzlich im • WDR-Videotext
Bereitschaftsdienst	Nachrichtenbereitschaftszentrale des LANUV (24-Std.-Dienst) Telefon 0201 714488

Inhalt

1 Einführung

Nordrhein-Westfalen ist eine bedeutende Industrieregion in Deutschland, in der eine Vielzahl gefährlicher Stoffe eingesetzt oder produziert wird, die z. B. akut toxisch, entzündbar oder explosionsfähig sein können.

Eine wesentliche Grundlage für den Umgang mit gefährlichen Stoffen ist die Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes, die Störfall-Verordnung (12. BImSchV), die die Zielsetzung hat, schwere Industrieunfälle zu verhüten und die Unfallfolgen zu begrenzen. Unter diese Verordnung fallen sogenannte Betriebsbereiche, in denen gefährliche Stoffe in Mengen vorhanden sind, die die in der 12. BImSchV genannten Mengenschwellen erreichen oder überschreiten.

Ein Betriebsbereich ist der gesamte unter der Aufsicht eines Betreibers stehende Bereich und umfasst alle Anlagen innerhalb der Betriebsbereichsgrenzen. Hierbei kann es sich um eine einzelne Anlage (z. B. eine Biogasanlage, ein Gefahrgutlager, eine verfahrenstechnische Anlage oder eine Galvanik) handeln oder aber um mehrere Anlagen wie z. B. Chemieanlagen unterschiedlichen Gefahrenpotentials eines Betreibers in einem Chemiepark.

Der Betreiber eines Betriebsbereiches hat die Verpflichtung, die möglichen Gefahren mit Hilfe von systematischen Untersuchungen zu bestimmen und die erforderlichen Vorkehrungen zu treffen, um Ereignisse, wie z B. Emissionen, Brände oder Explosionen größeren Ausmaßes, die zu einer ernsten Gefahr und damit zu einem Störfall führen können, zu verhindern sowie die Folgen zu begrenzen.

Seit dem Jahr 2000 fordert die Störfall-Verordnung das Betriebsbereiche als eine Maßnahme zur Verhinderung von Störfällen über ein Sicherheitsmanagementsystem verfügen. Welche Anforderungen ein Sicherheitsmanagementsystem erfüllen muss ist im Anhang III „Sicherheitsmanagementsystem“ der Störfall-Verordnung kurz beschrieben.

Nach § 16 Störfall-Verordnung „Überwachungssystem“ ist die Überwachungsbehörde verpflichtet, die technischen, organisatorischen und managementspezifischen Systeme der Betriebsbereiche planmäßig und systematisch zu prüfen.

In NRW sind die Bezirksregierungen die zuständigen Überwachungsbehörden. Auf deren Anfrage unterstützt das LANUV NRW diese.

Zur Unterstützung bei der Überprüfung von Sicherheitsmanagementsystemen gibt es das EDV-Programm "Safety Management Valuation Programm (SMVP)", welches seit 2001 kostenfrei vom LANUV (damals LUA – Landesumweltamt) zur Verfügung gestellt wird.

Die nun vorliegende Programmversion SMVP 3.0.0.0 wurde im Jahr 2015 programmiert und berücksichtigt die rechtlichen Grundlagen der Störfall-Verordnung in ihrer Fassung vom 15. März 2017 (BGBl. I S.483). Der aktuelle Prüfkatalog (Stand Januar 2018) enthält unter der Bezeichnung "Inspektionsmodul 2017" folgende Themenbereiche:

- Quellen- / Literaturangaben
- Allgemeines zur Benutzung
- Dokumentationspflichten nach Störfall-Verordnung
- **Sicherheitsmanagementsystem - SMS**
- Corporate Governance – CG APS
- Vielstoffanlagen – VMA
- Alarmmanagement - AM

Um fachlich vernünftige Antworten auf die Fragen in SMVP zu geben und eine fundierte Bewertung der Ergebnisse zu gewährleisten, muss der Anwender oder die Anwenderin über Fachkenntnisse auf den jeweiligen Gebieten beispielsweise Sicherheitsmanagementsysteme, Vielstoffanlagen etc. verfügen.

Bei dem Themenbereich „Sicherheitsmanagementsystem – SMS“ handelt es sich um einen Fragenkatalog, der insgesamt 66 Fragen enthält, welche zur Überprüfung des SMS von den Überwachungsbehörden an die Betreiber gestellt werden können. Um die Bewertung der Fragen zu erleichtern gibt es zu jeder Frage eine Bewertungshilfe, welche die wesentlichen Aspekte zur Bewertung einer Frage erläutert.

Dieses Arbeitsblatt enthält die Inhalte des Themenbereiches „Sicherheitsmanagementsystem – SMS“, Stand August 2017, aus SMVP sowie aktualisierte Inhalte der Schrift „Zur Inspektion von Sicherheitsmanagementsystemen“ vom Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen, Essen, Stand Januar 2006 /1/ und ersetzt letztere.

Aktualisierte und ergänzende Hinweise in den Kapiteln 5 und 6 dieses LANUV-Arbeitsblattes über den Inhalt SMVP, Stand August 2017, hinaus werden in dieser kursiven Schriftform dargestellt.

2 Allgemeine Aspekte zur Überwachung von Betriebsbereichen durch die Behörden

Der dritte Abschnitt der Störfall-Verordnung nennt Behördenpflichten und enthält in den § 16 „Überwachungssystem“ und § 17 „Überwachungsplan und Überwachungsprogramm“ die Verpflichtung regelmäßig Vor-Ort-Besichtigungen in Betriebsbereichen durchzuführen und zu prüfen, ob in den Betriebsbereichen die notwendigen Maßnahmen zur Verhinderung von Störfällen sowie zur Begrenzung von Störfallauswirkungen, falls es dennoch zu einem Störfall kommt, umgesetzt wurden.

Die technischen, organisatorischen und managementspezifischen Systeme eines Betriebsbereiches sollen überprüft werden, wobei die zuständige Behörde sich insbesondere des folgenden Sachverhaltes vergewissert:

- der Betreiber hat die zur Verhinderung von Störfällen erforderlichen Maßnahmen ergriffen,
- der Betreiber hat angemessene Mittel zur Begrenzung von Störfallauswirkungen innerhalb und außerhalb des Betriebsbereiches vorgesehen,
- die Angaben im Sicherheitsbericht und in anderen Unterlagen stimmen mit der Situation vor Ort überein,
- die Informationen der Öffentlichkeit nach § 8a und § 11 ist erfolgt.

Die Inspektion eines Betriebsbereiches umfasst die Vor- und Nachbereitung – einschließlich des Berichts der Überwachungsbehörde an den Betreiber, und die Vor-Ort-Besichtigung des Betriebsbereiches.
Generell besteht die Möglichkeit Inspektionen in die folgenden zwei Schwerpunkte aufzuteilen:

- Überprüfung des Technischen Systems
- Überprüfung des Sicherheitsmanagementsystems

Die Ergebnisse der Inspektion finden ihren Niederschlag in einem Inspektionsbericht, den die Überwachungsbehörde innerhalb von vier Monaten dem Betreiber übermitteln muss. Der Bericht enthält die relevanten Feststellungen der Überwachungsbehörde sowie ggf. aus der Inspektion resultierende Folgemaßnahmen, die der Betreiber in einer angemessenen Frist umsetzen muss.

Nach § 17 der Störfall-Verordnung darf der Zeitraum zwischen zwei Vor-Ort-Besichtigungen eines Betriebsbereiches die folgenden Zeiträume nicht überschreiten, es sei denn, die Überwachungsbehörde hat auf Grundlage einer systematischen Bewertung der von Betriebsbereichen ausgehenden Gefahren von Störfällen andere Zeiträume ermittelt:

- 1 Jahr bei Betriebsbereichen der oberen Klasse,
- 3 Jahre bei Betriebsbereichen der unteren Klasse.

In Nordrhein-Westfalen gibt es mit Stand 01/2020 in Summe 609 Betriebsbereiche, ohne die Betriebsbereiche, die unter die Bergaufsicht fallen. Dabei fallen 311 Betriebsbereiche in die untere Klasse, d. h. die Betriebsbereiche müssen die Grundpflichten der Störfall-Verordnung

erfüllen und 298 Betriebsbereiche fallen in die obere Klasse, d. h. sie müssen zusätzlich die erweiterten Pflichten der Störfall-Verordnung erfüllen.

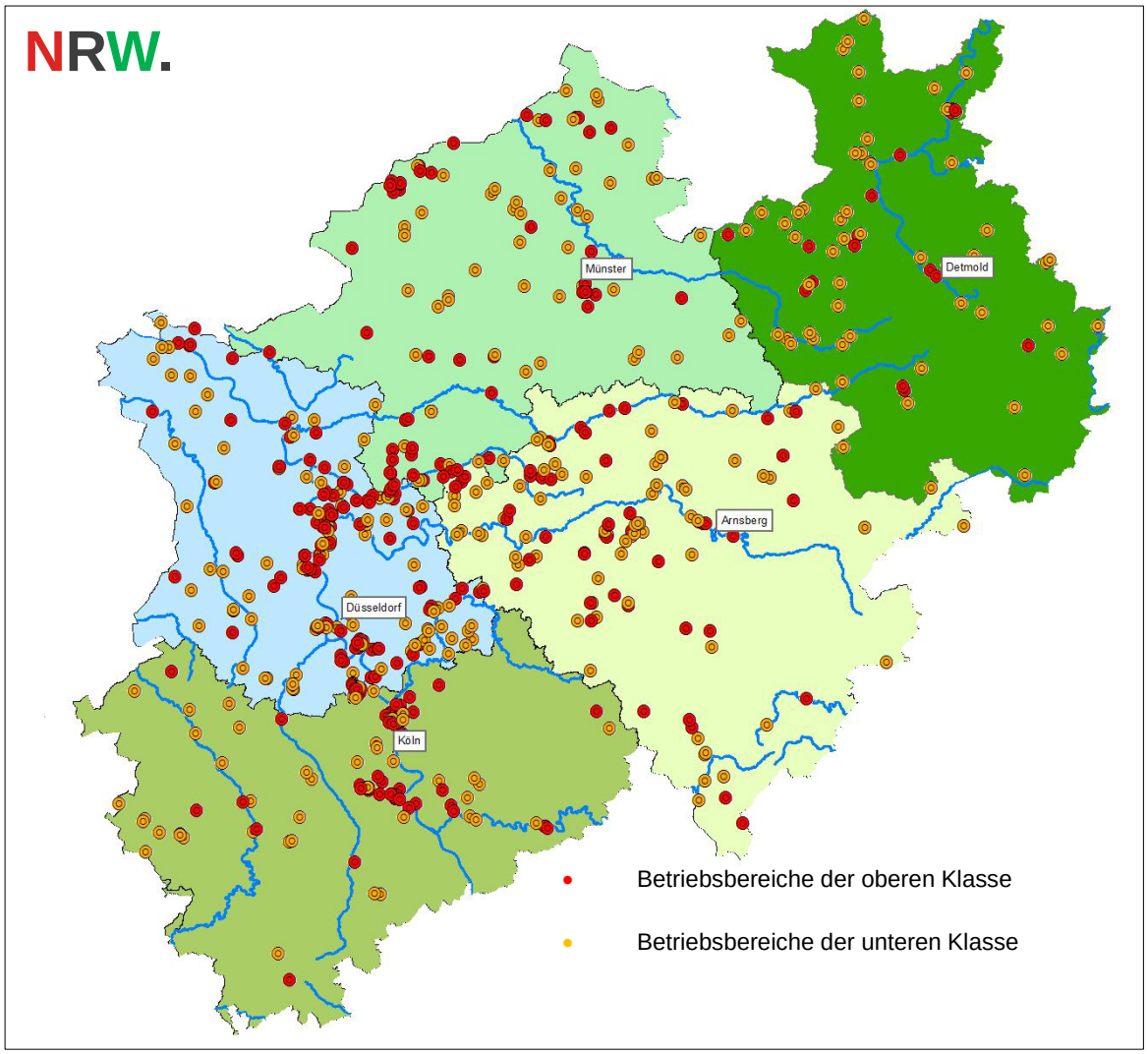

Abb. 01: Betriebsbereiche in den 5 Regierungsbezirken in NRW, Stand 01/2019

Die Bezirksregierungen in NRW als zuständige Überwachungsbehörden für Betriebsbereiche ermitteln die Überwachungszyklen für die Betriebsbereiche anhand einer systematischen Bewertung.
Für diese risikobasierte Inspektionsplanung wird die internetbasierte Anwendung IRAM (Integrated Risk Assessment Method) verwendet.

IRAM unterscheidet zwischen den beiden Arten Auswirkungskriterien und Betreiberkriterien als Bewertungskriterien und ermittelt als Ergebnis der Risikobewertung den Überwachungszyklus für die nächste Vor-Ort-Besichtigung des untersuchten Betriebsbereiches systematisch, transparent und nach einheitlichen Kriterien, solange keine sonstigen Vorkommnisse, wie z. B. meldepflichtige Ereignisse, schwerwiegende Beschwerden etc. dies außer Kraft setzen.

Auswirkungskriterien	**Betreiberbezogene Kriterien**
Kenntnis über den Betriebsbereich	Beherrschung von Betriebsstörungen und meldepflichtigen Ereignissen
Gefährliche Stoffe	
Organisation der Schadensbegrenzung	Unterlagen und Dokumente nach Störfall-Verordnung
Dominobetriebe und umgebungsbedingte Gefahren	
Benachbarte Schutzobjekte	Ergebnis und Bewertung bisheriger Überwachung
Prozessgefahren, Anlagenkomplexität	
Systeme zur Meldung und Begrenzung von Schadensereignissen	Bereitschaft des Betreibers zur Regeleinhaltung

Abb. 02: Risikokriterien „Betriebsbereiche nach Störfall-Verordnung“ in IRAM

Laut Überwachungsplan der Abteilung für Umwelt und Arbeitsschutz der Bezirksregierung Köln /2/ werden entsprechend dieser Risikobewertung im Mittel Betriebsbereiche der oberen Klasse alle zwei Jahre und Betriebsbereiche der unteren Klasse alle 4 Jahre überwacht.

3 Grundlagen zur Überprüfung von SMS

3.1 Das SMS in der Störfall-Verordnung

Alle Betriebsbereiche, die unter die Störfall-Verordnung fallen, müssen über ein Sicherheitsmanagementsystem (SMS) verfügen. Die Verpflichtung hierzu findet sich im § 8 „Konzept zur Verhinderung von Störfällen“ der Störfall-Verordnung.

§ 8
Konzept zur Verhinderung von Störfällen

(1) Der Betreiber hat vor Inbetriebnahme ein schriftliches Konzept zur Verhinderung von Störfällen auszuarbeiten und es der zuständigen Behörde auf Verlangen vorzulegen. Bei Betriebsbereichen der oberen Klasse kann das Konzept Bestandteil des Sicherheitsberichts sein.

(2) Das Konzept soll ein hohes Schutzniveau für die menschliche Gesundheit und die Umwelt gewährleisten und den Gefahren von Störfällen im Betriebsbereich angemessen sein. Es muss die übergeordneten Ziele und Handlungsgrundsätze des Betreibers, die Rolle und die Verantwortung der Leitung des Betriebsbereichs umfassen sowie die Verpflichtung beinhalten, die Beherrschung der Gefahren von Störfällen ständig zu verbessern und ein hohes Schutzniveau zu gewährleisten.

(3) Der Betreiber hat die Umsetzung des Konzeptes durch angemessene Mittel und Strukturen sowie durch ein Sicherheitsmanagementsystem nach Anhang III sicherzustellen.

(4) Der Betreiber hat das Konzept, das Sicherheitsmanagementsystem nach Anhang III sowie die Verfahren zu dessen Umsetzung zu überprüfen und soweit erforderlich zu aktualisieren, und zwar

1. mindestens alle fünf Jahre nach erstmaliger Erstellung oder Änderung,
2. vor einer Änderung nach § 7 Absatz 3 und
3. unverzüglich nach einem Ereignis nach Anhang VI Teil 1.

Abb. 03: 12. BImSchV § 8 Konzept zur Verhinderung von Störfällen (Stand 2017)

Explizit angesprochen wird das Sicherheitsmanagementsystem in der Störfall-Verordnung in den in der folgenden Abbildung aufgeführten Paragrafen und Anhängen:

Das SMS in der Störfallverordnung:

§ 8 Konzept zur Verhinderung von Störfällen

§ 9 Sicherheitsbericht

§ 16 Überwachungssystem

§ 21 Ordnungswidrigkeiten

Anhang II „Mindestangaben im Sicherheitsbericht“

Anhang III „Sicherheitsmanagementsystem“

Abb. 04: SMS in der Störfall-Verordnung (Stand 2017)

Grundsätzliche Anforderungen, die ein SMS erfüllen muss, sind im Anhang III „Sicherheitsmanagementsystem“ der Störfall-Verordnung genannt:

Anhang III Sicherheitsmanagementsystem

1. Das Sicherheitsmanagementsystem ist den Gefahren, Tätigkeiten und der Komplexität der Betriebsorganisation angemessen und beruht auf einer Risikobeurteilung. In das Sicherheitsmanagementsystem ist derjenige Teil des allgemeinen Managementsystems einzugliedern, zu dem Organisationsstruktur, Verantwortungsbereiche, Handlungsweisen, Verfahren, Prozesse und Mittel gehören, also die für die Festlegung und Anwendung des Konzepts zur Verhinderung von Störfällen relevanten Punkte. Insbesondere bei bereits nach § 32 des Umweltauditgesetzes EMAS-registrierten Standorten kann auf deren Managementstrukturen und Vorgehensweisen aufgesetzt werden.

2. Folgende Punkte werden durch das Sicherheitsmanagementsystem geregelt:
a) Organisation und Personal
Aufgaben und Verantwortungsbereiche des für die Verhinderung von Störfällen und die Begrenzung ihrer Auswirkungen vorgesehenen Personals auf allen Organisationsebenen; Maßnahmen, die zur Sensibilisierung für die Notwendigkeit ständiger Verbesserungen ergriffen werden. Ermittlung des entsprechenden Ausbildungs- und Schulungsbedarfs sowie Durchführung der erforderlichen Ausbildungs- und Schulungsmaßnahmen. Einbeziehung der Beschäftigten des Betriebsbereichs sowie des im Betriebsbereich beschäftigten Personals von Subunternehmen, soweit dies unter dem Gesichtspunkt der Sicherheit relevant ist.

b) Ermittlung und Bewertung der Gefahren von Störfällen
Festlegung und Anwendung von Verfahren zur systematischen Ermittlung der Gefahren von Störfällen bei bestimmungsgemäßem und nicht bestimmungsgemäßem Betrieb, einschließlich von Tätigkeiten, die als Unteraufträge vergeben sind, sowie Abschätzung der Wahrscheinlichkeit und der Schwere solcher Störfälle.

c) Überwachung des Betriebs
Festlegung und Anwendung von Verfahren und Anweisungen für den sicheren Betrieb, einschließlich der Wartung der Anlagen, für Verfahren und Einrichtung sowie für Alarmmanagement und zeitlich begrenzte Unterbrechungen. Berücksichtigung verfügbarer Informationen über bewährte Verfahren zur Überwachung und Prüfung, um die Wahrscheinlichkeit von Systemausfällen zu verringern. Betrachtung und Beherrschung der durch Alterung oder Korrosion von Anlagenteilen im Betriebsbereich entstehenden Risiken.
Dokumentation der Anlagenteile im Betriebsbereich, verbunden mit einer Strategie und Methodik zur Überwachung und Prüfung des Zustands dieser Anlagenteile. Gegebenenfalls Festlegung von erforderlichen Gegenmaßnahmen und angemessenen Folgemaßnahmen.

d) Sichere Durchführung von Änderungen
Festlegung und Anwendung von Verfahren zur Planung von Änderungen bestehender Anlagen oder Verfahren oder zur Auslegung einer neuen Anlage oder eines neuen Verfahrens.

e) Planung für Notfälle
Festlegung und Anwendung von Verfahren zur Ermittlung vorhersehbarer Notfälle auf Grund einer systematischen Analyse und zur Erstellung, Erprobung und Überprüfung der Alarm- und Gefahrenabwehrpläne, um in Notfällen angemessen reagieren und um dem betroffenen Personal eine spezielle Ausbildung erteilen zu können. Diese Ausbildung muss allen Beschäftigten des Betriebsbereichs, einschließlich des relevanten Personals von Subunternehmen, erteilt werden.

f) Überwachung der Leistungsfähigkeit des Sicherheitsmanagementsystems
Festlegung und Anwendung von Verfahren zur ständigen Bewertung der Erreichung der Ziele, die der Betreiber im Rahmen des Konzepts zur Verhinderung von Störfällen und des Sicherheitsmanagementsystems festgelegt hat, sowie Einrichtung von Mechanismen zur Untersuchung und Korrektur bei Nichterreichung dieser Ziele. Die Verfahren umfassen das System für die Meldung von Ereignissen, insbesondere von solchen, bei denen Schutzmaßnahmen versagt haben, sowie die entsprechenden Untersuchungen und Folgemaßnahmen, bei denen einschlägige Erfahrungen und Erkenntnisse aus innerbetrieblichen und außerbetrieblichen Ereignissen zugrunde zu legen sind. Die Verfahren können auch Leistungsindikatoren wie sicherheitsbezogene Leistungsindikatoren und andere relevante Indikatoren beinhalten.

g) Systematische Überprüfung und Bewertung
Festlegung und Anwendung von Verfahren zur regelmäßigen systematischen Bewertung des Konzepts zur Verhinderung von Störfällen und der Wirksamkeit und Angemessenheit des Sicherheitsmanagementsystems. Von der Leitung des Betriebsbereichs entsprechend dokumentierte Überprüfung der Leistungsfähigkeit des bestehenden Konzepts und des Sicherheitsmanagementsystems sowie seine Aktualisierung, einschließlich der Erwägung und Einarbeitung notwendiger Änderungen gemäß der systematischen Überprüfung und Bewertung.

Abb. 05: Anhang III Sicherheitsmanagementsystem

3.2 Wichtige Aspekte von SMS

Mit dem Instrument des Sicherheitsmanagementsystems soll ein hoher Stand der Anlagensicherheit gewährleistet werden.

Der Hintergrund für die Aufnahme von Sicherheitsmanagementsystemen als Pflicht für Betriebsbereiche liegt darin, dass vorangegangene Analysen von an die EU gemeldeten Störfällen gezeigt haben, dass in den meisten Fällen Management- bzw. organisatorische Mängel zu den Ursachen zählten.

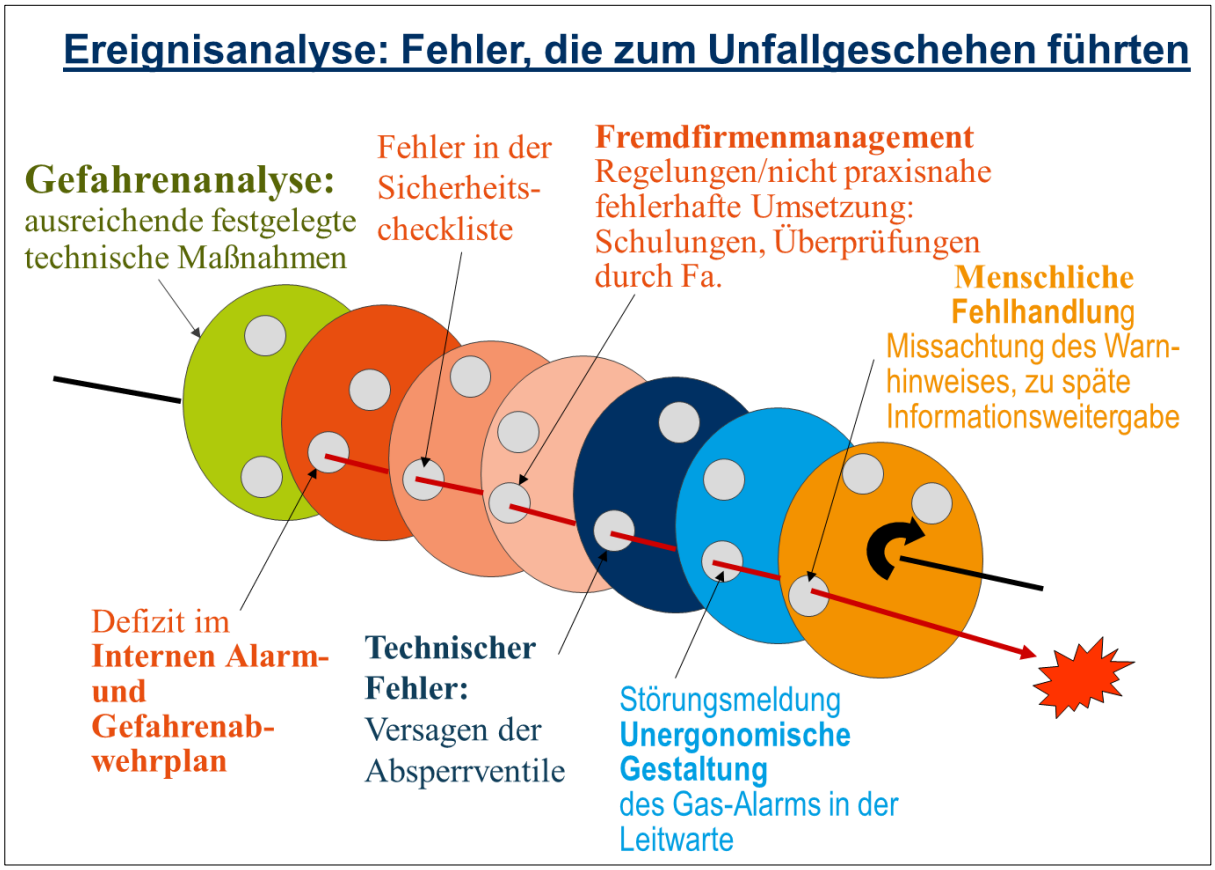

Abb. 06: Beispiel einer Ereignisanalyse

Ein SMS nach Störfall-Verordnung entspricht in seinen grundlegenden Anforderungen den generellen Anforderungen an Managementsysteme. D.h. es muss über einen prozessorientierten Ansatz, eine Struktur der Regelungen und Dokumentation und über Überprüfungszyklen, die kontinuierliche Verbesserungs- und Anpassungsprozesse gewährleisten, verfügen (siehe auch Abbildungen 07, 08 und 25).

Das SMS muss auf einer Unternehmenspolitik zur Prozess- und Anlagensicherheit im Sinne der Störfall-Verordnung basieren. Zusätzlich muss es den Gefahren, Tätigkeiten und der Komplexität des Betriebsbereiches angemessen sein. Das SMS beruht daher auf einer Risikobeurteilung.

Definition Managementsystem:

Bei einem Managementsystem handelt es sich um ein festgelegtes und dokumentiertes System aller organisatorischen Strukturen, Abläufe, Vorkehrungen, Maßnahmen und Überprüfungen zur Erreichung von festgelegten (Unternehmens-) Zielen.

Es zeichnet sich aus durch

1. einen ***prozessorientierten*** Ansatz
2. eine (hierarchische) ***Struktur der Regelungen und Dokumentation***
3. ***Überprüfungszyklen***, die kontinuierliche Verbesserungs- und Anpassungsprozesse gewährleisten.

Abb. 07: Definition Managementsystem

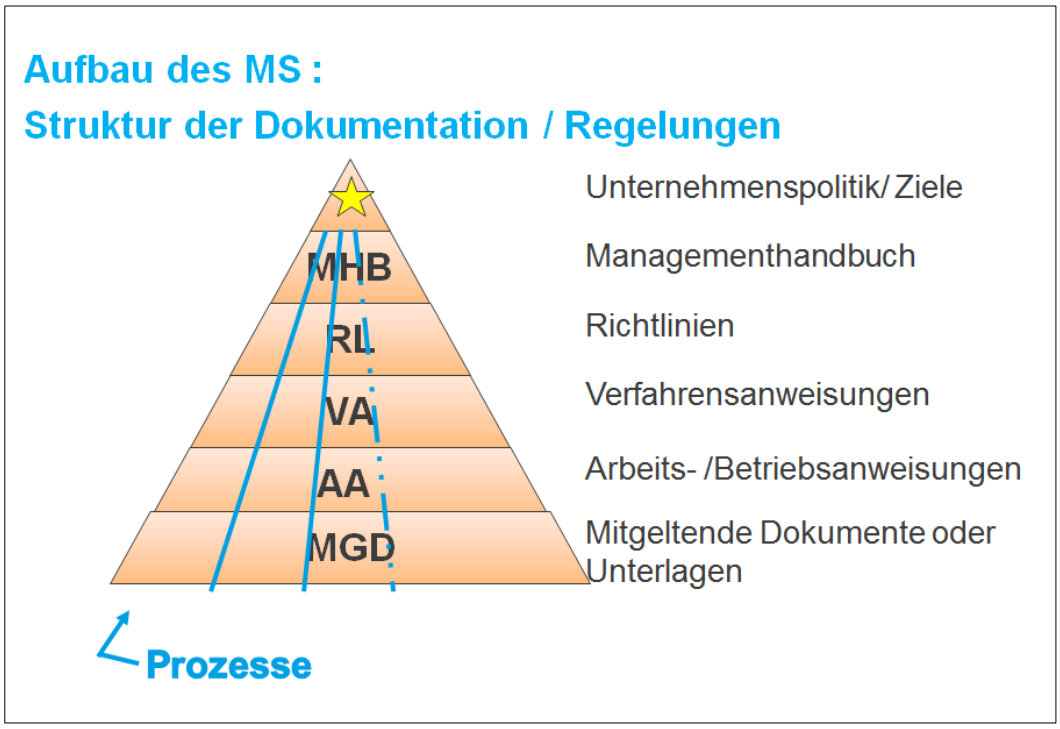

Abb. 08: Mögliche prozessorientierte Struktur der Dokumentation des MS

Das SMS muss zudem alle im Anhang III der Störfall-Verordnung aufgeführten zu regelnden Punkte aufweisen:

a. Organisation und Personal
b. Ermittlung und Bewertung der Gefahren von Störfällen
c. Überwachung des Betriebes
d. Sichere Durchführung von Änderungen
e. Planung für Notfälle
f. Überwachung der Leistungsfähigkeit des SMS
g. Systematische Überprüfung und Bewertung

Zur Unterstützung der Beurteilung von SMS hat das LANUV einen Fragenkatalog mit dazugehörigen Bewertungshilfen entwickelt – dies ist Inhalt des Kapitels 5 dieses Arbeitsblattes und zudem ein Bestandteil von SMVP. SMVP ist ein EDV-Programm, dessen Einsatz ein Beitrag zur effektiven Durchführung der Überwachung von Betriebsbereichen durch die zuständigen Behörden ist (siehe Kapitel 4 dieses Arbeitsblattes).

Zur Überprüfung der Wirkungen von SMS wurde 2008 ein vom LANUV in Auftrag gegebenes Untersuchungsvorhaben „Auswirkungen von Sicherheitsmanagementsystemen“ durchgeführt. Es beinhaltet eine Bestandsaufnahme zu Veränderungen in den Betriebsbereichen in NRW, die durch die Einführung von Sicherheitsmanagementsystemen im Jahr 2000 und deren Aufrechterhaltung stattgefunden haben und wurde vom Öko-Institut e.V., Darmstadt durchgeführt. Das Ergebnis bestätigte, dass ein gut implementiertes SMS im Betriebsbereich ein geeignetes Instrument ist, um das Sicherheitsniveau aufrechtzuerhalten und stetig weiterzuentwickeln.

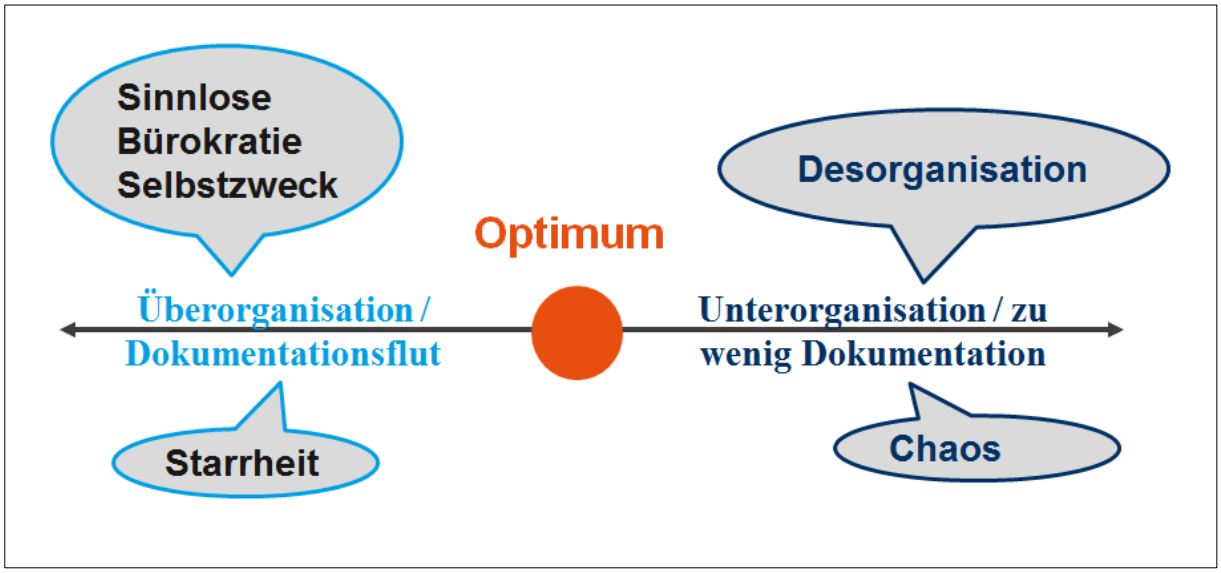

Abb. 09: Optimum bei der Anzahl von Regelungen / Dokumenten

Als Fazit des Untersuchungsvorhabens kann festgehalten werden, dass Sicherheitsmanagementsysteme deutlich zur Verbesserung der Anlagensicherheit beigetragen haben.

Auch ein positiver Einfluss von Sicherheitsmanagementsystemen auf die Sicherheitskultur in Betriebsbereichen wurde deutlich.

Es gibt eine Wechselbeziehung von Sicherheitsmanagementsystem (SMS) und Sicherheitskultur: Ein gut gelebtes SMS kann als Beleg für eine positive Sicherheitskultur betrachtet werden. Bei einer schlecht ausgeprägten Sicherheitskultur wird das SMS viele Mängel aufweisen, allerdings kann durch die Einführung oder Verbesserung eines SMS auch die Sicherheitskultur verbessert werden (siehe hierzu auch Bewertungshilfe im Kap. 5.8.3 in diesem Arbeitsblatt).

3.3 Zur Durchführung von Inspektionen

Die technischen, organisatorischen und managementspezifischen Systeme von Betriebsbereichen sollen regelmäßig durch Vor-Ort-Besichtigungen der zuständigen Überwachungsbehörden überprüft werden (siehe auch Kapitel 2 „Allgemeine Aspekte zur Überwachung von Betriebsbereichen durch die Behörden“ dieser Arbeitshilfe).

Bei der Überprüfung des Sicherheitsmanagementsystems kann die Überwachungsbehörde zur Vorbereitung der Vor-Ort-Besichtigung z. B. auf Genehmigungsunterlagen, das Konzept zur Verhinderung von Störfällen oder den Sicherheitsbericht zurückgreifen. Jedoch ist der Informationsgehalt zum Sicherheitsmanagementsystem in den vorhandenen Unterlagen meist zu gering, um eine wirksame Vorbereitung der Vor-Ort- Besichtigung des Sicherheitsmanagementsystems eines Betriebsbereiches durchzuführen. Dementsprechend werden vom Betreiber weitere Unterlagen hierfür der Überwachungsbehörde zur Verfügung gestellt. Dies sind z.B. (Auszüge von) Managementhandbüchern, Zusammenstellung von betrieblichen Regelungen, Handbuch des Sicherheitsmanagements. Bei Nutzung des EDV-Programms „Safety-Management-Valuation-Program (SMVP) können Betreiber Informationen auch elektronisch der Behörde übermitteln.

Das Programm SMVP verfügt zur Überprüfung des SMS über 66 Fragen mit Bewertungshilfen, deren Inhalte im Kapitel 5 „SMS: Fragen und Bewertungshilfen“ dieser Arbeitshilfe aufgeführt sind und die den folgenden acht Prüfgebieten (PG) zugeordnet sind:

PG 1: Konzept zur Verhinderung von Störfällen und Aufbau des SMS
PG 2: Organisation und Personal
PG 3: Ermittlung und Bewertung der Gefahren von Störfällen
PG 4: Überwachung des Betriebs
PG 5: Sichere Durchführung von Änderungen und Anlagenneuplanungen
PG 6: Planung für Notfälle
PG 7: Überwachung der Leistungsfähigkeit des Sicherheitsmanagementsystems
PG 8: Systematische Überprüfung und Bewertung

Diese acht Prüfgebiete bilden insbesondere die im Anhang III der Störfallverordnung geforderten Aspekte eines Sicherheitsmanagementsystems (SMS) ab.

Die Bewertungshilfen zu den Fragen geben in der Regel Hinweise darauf, welche Aspekte bei der Bewertung der Frage eine Rolle spielen können. Abhängig vom Einzelfall können Aspekte wegfallen oder aber zusätzliche Aspekte sehr relevant sein.

Das EDV-Programm SMVP wird im Kapitel 4 „Das EDV-Programm Safety-Management-Valuation-Program (SMVP)“ dieser Arbeitshilfe näher erläutert.

3.3.1 Zum Ablauf von Inspektionen

Im Überblick kann der Ablauf einer Störfallinspektion durch die Überwachungsbehörde wie folgt aussehen:

Ablaufschritte einer Störfallinspektion

1. **Schritt:** **Absprachen zum Vorgehen** (Termin für die Vor-Ort-Besichtigung, Unterlagen, welche der Betreiber den Überwachungsbehörden zur Vorbereitung der Vor-Ort-Besichtigung zur Verfügung stellt) – ggf. in ein einem ersten Termin vor Ort mit einer Vorstellung des Betriebsbereiches durch den Betreiber und einer ersten Besichtigung des Betriebsbereiches
2. **Schritt:** **Vorbereitung** auf die **Vor-Ort-Besichtigung**
3. **Schriftt:** **Durchführung der Vor-Ort-Besichtigung**
4. **Schritt:** **Erstellung** des **Inspektionsberichtes**
5. **Schritt:** **Ggf. Überprüfung** der durchgeführten **Folgemaßnahmen**

Abb. 10: Ablaufschritte einer Störfallinspektion

Zuständige Überwachungsbehörde für die Durchführung von Störfallinspektionen sind in Nordrhein-Westfalen die fünf Bezirksregierungen Arnsberg, Detmold, Düsseldorf, Köln und Münster. Das LANUV NRW – Arbeitsbereich Anlagensicherheit – kann von den Überwachungsbehörden bei der Durchführung der Störfallinspektionen zur Unterstützung angefordert werden. Je nach Anforderung der Überwachungsbehörden wird der Arbeitsbereich Anlagensicherheit in unterschiedlichem Maße in die Störfallinspektion von Betriebsbereichen eingebunden, so auch bei der praktischen Durchführung der Vor-Ort-Besichtigung und bei der Erstellung der Inspektionsberichte.

Beim LANUV wird bei einer Störfallinspektion mit dem Schwerpunkt Überprüfung des Sicherheitsmanagementsystems das EDV-Programm SMVP benutzt.

Abhängig von den Anforderungen der zuständigen Überwachungsbehörde wählen LANUV und die Überwachungsbehörde die Fragen aus SMVP aus, die zur Überprüfung des SMS zur Anwendung kommen sollen. In der Regel erhalten die Betreiber des zu inspizierenden Betriebsbereichs diese ausgewählten Fragen für eine Vorab-Beantwortung. Hierfür stellt SMVP eine Exportfunktion zum Austausch von Antwortdateien zur Verfügung.

Zur Vorbereitung einer Vor-Ort-Besichtigung werden vom LANUV die Fragen im Programm SMVP anhand der zur Verfügung gestellten Unterlagen über den Betriebsbereich einschließlich der Vorab-Antworten des Betreibers beantwortet.

Aus dieser ersten Beantwortung der Fragen kristallisiert sich heraus, was bei der Vor-Ort-Besichtigung besonders zu beachten ist, z. B.:

- → Welche Dokumente eingesehen werden sollten,
- → Zu beachtenden Aspekte bei der Betriebsbegehung (z. B. bestimmter Tank: Zustand, Kennzeichnung, (PLT-) Schutzeinrichtungen, Abstände zu anderen Anlagen etc.)
- → Zu beachtenden Aspekte bei Gesprächen / Interviews mit Beschäftigten des / im BB
- → Teilnahme an bestimmten Tätigkeiten im Betriebsbereich
- → Etc.

Details hierzu sind den folgenden Abbildungen 11 bis 14 zu entnehmen.

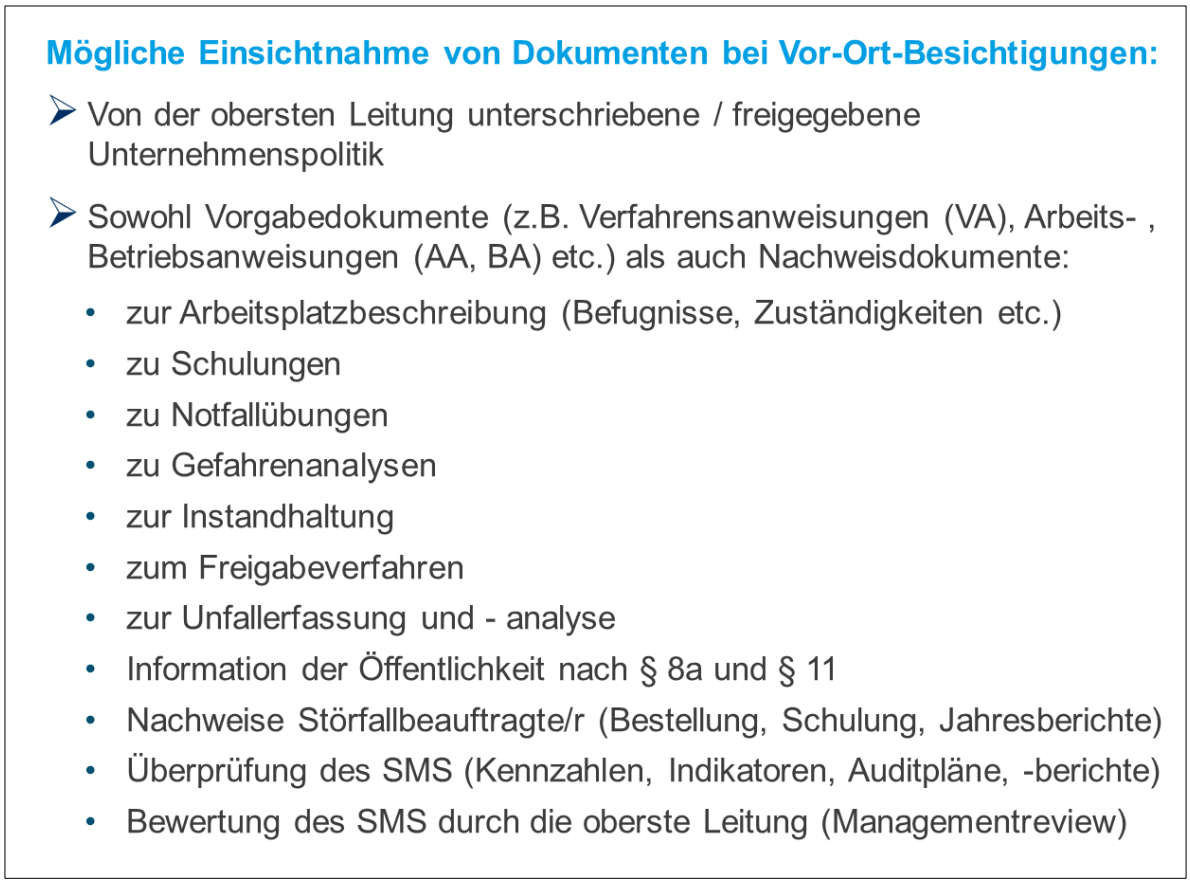

Abb. 11: Vor-Ort-Besichtigung - mögliche Einsichtnahme von Dokumenten

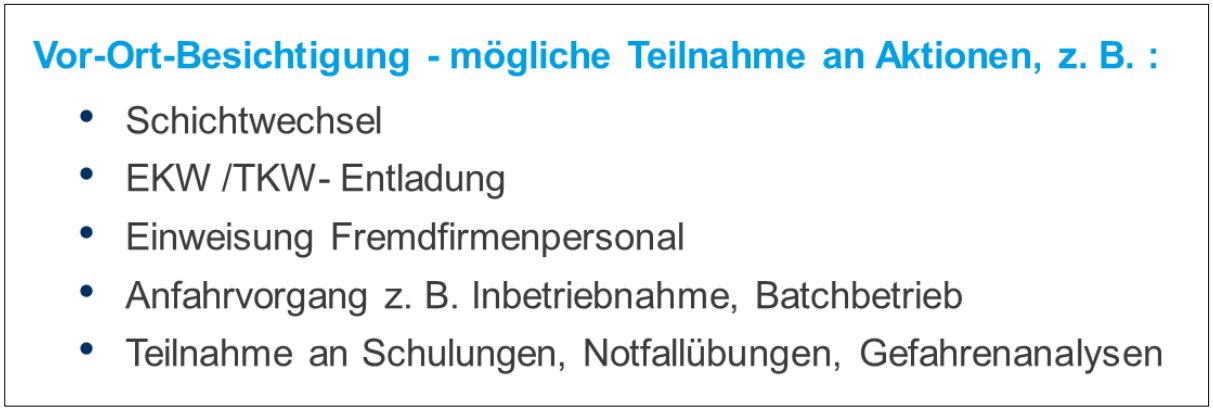

Abb. 12: Vor-Ort-Besichtigung - mögliche Teilnahme an Aktionen

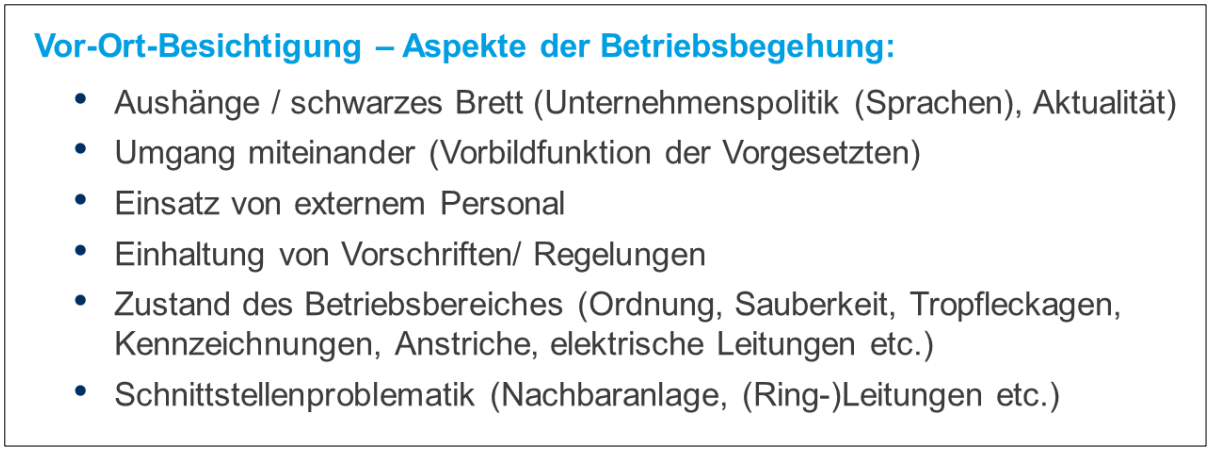

Abb. 13: Vor-Ort-Besichtigung – Aspekte bei der Betriebsbegehung

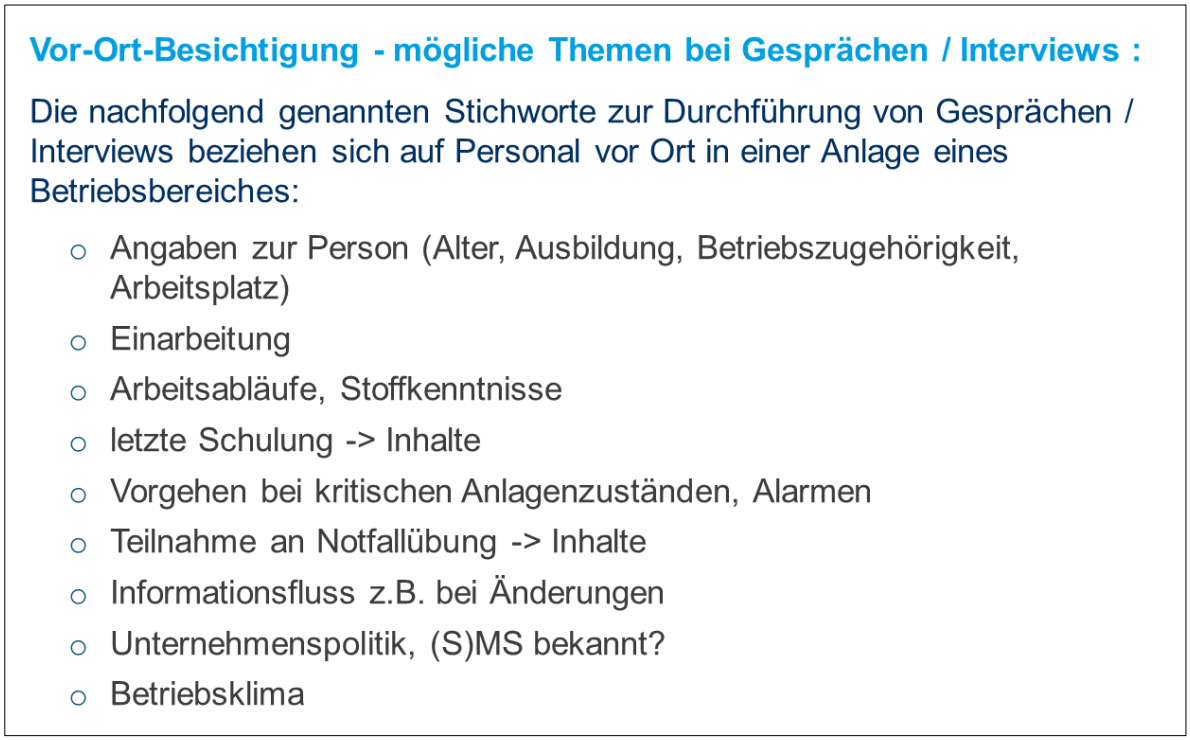

Abb. 14: Vor-Ort-Besichtigung - mögliche Themen bei Gesprächen / Interviews

Die Qualität der Ergebnisse aus den Gesprächen oder Interviews hängt in einem hohen Maß von der Kommunikationskompetenz des Inspektors oder der Inspektorin ab.

Die Ergebnisse der Vor-Ort-Inspektion werden in einem Inspektionsbericht dargestellt. Der Inspektionsbericht des LANUV beinhaltet in der Regel als Anlage den vollständigen Bericht aus dem EDV-Programm SMVP, welcher die ausgewählten Fragen, deren Vorab-Beantwortung durch den Betreiber des Betriebsbereiches sowie die Bewertungen durch das LANUV und den Begründungen für diese Bewertungen enthält.

3.3.2 Zu den Ergebnissen durchgeführter SMS-Inspektionen

Seit in Kraft treten der Seveso-II-Richtlinie im Jahr 1996 und ihrer Umsetzung auch durch die Störfallverordnung (Novellierung 3.5.2000) werden für Betriebsbereiche Sicherheitsmanagementsysteme gefordert. Dies gilt entsprechend für die zuständigen Behörden im Hinblick auf die Durchführung von Störfallinspektionen.
Wenn Anweisungen oder Regelungen zur Anlagensicherheit im Betriebsbereich existieren, heißt dies noch lange nicht, dass ein SMS im Betriebsbereich vorliegt. Ein SMS liegt vor, wenn die grundlegenden Elemente eines Sicherheitsmanagementsystems, dargestellt in den Abbildungen Nr. 15 und Nr. 16 vorhanden sind.

Das **SMS** oder das **integrierte Managementsystem** , welches auch das SMS beinhaltet, erfüllt die folgenden Anforderungen:

Es verfügt über:

1. einen **prozessorientierten Ansatz** und **beruht** auf einer **Risikobeurteilung**,
2. eine (hierarchische) **Struktur der Regelungen** und **Dokumentation**,
3. **Überprüfungszyklen**, die kontinuierliche Verbesserungs- und Anpassungsprozesse gewährleisten

Und beinhaltet die **Anforderungen der Störfall-Verordnung** einschließlich **dokumentierte Regelungen** zu

a) Organisation und Personal
b) Ermittlung und Bewertung der Gefahren von Störfällen
c) Überwachung des Betriebs
d) Sichere Durchführung von Änderungen
e) Planung für Notfälle
f) Überwachung der Leistungsfähigkeit des SMS
g) Systematische Überprüfung und Bewertung

Abb.15: Grundlegende Elemente des SMS – Teil 1

Das **SMS** oder das **integrierte Managementsystem** , welches auch das SMS beinhaltet, erfüllt die folgenden Anforderungen:

- **Unternehmenspolitik** beinhaltet **Anlagensicherheit** im Sinne der Störfall-VO,
- **Engagement der obersten Leitung** des Betriebsbereiches **zur Anlagensicherheit** im Sinne der Störfall-Verordnung liegt vor.

Abb. 16: Grundlegende Elemente des SMS – Teil 2

Die zwei wesentlichen Elemente des **Managementsystems** sind die Systematik im Hinblick auf die organisatorischen Strukturen, Abläufe, Regelungen und Verantwortlichkeiten eines Betriebsbereiches und das Vorhandensein von Überprüfungszyklen (Plan Do Check Act - Regelkreis, kontinuierliche Verbesserung).
Wenn die Elemente des SMS der Abb. Nr. 15 + Nr. 16 vorhanden und entsprechend gelebt werden, so findet dies im EDV-Programm SMVP seinen Niederschlag darin, dass die Prüfgebiete

- **„Konzept zur Verhinderung von Störfällen und Aufbau des SMS“,**
- **„Organisation und Personal“,**
- **„Überwachung der Leistungsfähigkeit des Sicherheitsmanagementsystems“,**
- **„Systematische Überprüfung und Bewertung“**

positiv bewertet werden.

Bei integrierten Managementsystemen, die nach Betreiberansicht auch das SMS nach Störfall-Verordnung beinhalten, muss geprüft werden, ob die Anforderungen der Störfall-Verordnung, insbesondere des Anhanges III erfüllt sind. Wird z. B. die Anlagensicherheit nicht explizit als Ziel in der Unternehmenspolitik genannt und findet die Anlagensicherheit auch in den weiterführenden Regelungen und Anweisungen keine oder nur selten Berücksichtigung, so kann die Aussage des Betreibers, dass die Anlagensicherheit implizit z. B. bei den Begriffen Umwelt oder Sicherheit berücksichtigt wird, nicht akzeptiert werden.

Zusammenfassend werden nun noch einmal wichtige Aspekte zur Überprüfung von Sicherheitsmanagementsystemen genannt:

1. Existieren dokumentierte Regelungen zu allen Prüfgebieten des SMS?

2. Ist ein Sicherheitsmanagementsystem vorhanden, d. h.:

a) Es ist eine **Systematik** vorhanden:

→ zwischen den verschiedenen Ebenen des SMS,
→ zwischen den Prüfgebieten?

b) Sind **Überprüfungszyklen** vorhanden:

→ der vorhandenen Regelungen (i. d. R. durch Audits),
→ des SMS-Aufbaus, der Unternehmenspolitik (i. d. R. durch Managementreviews)?
→ Gibt es Kennzahlen zur Nachverfolgung von Zielen?

c) Beruht das SMS auf einer **Risikobeurteilung**?

3. Beim Vorliegen eines integrierten MS: Wie ist das SMS berücksichtigt?

4. Existiert eine Übereinstimmung zwischen SMS-Regelungen und Betriebsalltag („Wird das SMS gelebt?“)?

5. Engagiert sich die oberste Leitung bei der Anlagensicherheit?

6. Sind Anmerkungen zur Sicherheitskultur sinnvoll?

Abb.17: Zusammenfassung: Wichtige Aspekte zur Überprüfung von SMS

Die Sicherheitskultur in einem Betriebsbereich kann auch ohne ein Sicherheitsmanagementsystem positiv geprägt sein, im Sinne, dass ein angemessenes Gefahrenbewusstsein bei den Beschäftigten vorhanden ist, sich dieses in ihrem Verhalten niederschlägt und in den bis jetzt getroffenen organisatorischen und technischen Maßnahmen im Betriebsbereich Berücksichtigung findet.

Die Vor-Ort-Besichtigung des Betriebsbereiches ermöglicht auch die Wahrnehmung der Betriebs- und Sicherheitskultur des Betriebsbereiches durch externe Personen. Diese Fremdwahrnehmung deckt sich nicht unbedingt mit der Sichtweise der Beschäftigten des Betriebsbereiches von ihrer Betriebs- und Sicherheitskultur.

Mitteilungen zur Fremdwahrnehmung der Sicherheitskultur durch die Inspektoren/innen geben den Verantwortlichen eines Betriebsbereiches die Möglichkeit betriebsblinde Flecken zu entdecken und ggf. entgegen zu steuern. Bei starken Differenzen zwischen Fremdwahrnehmung und Eigenwahrnehmung geht es nicht darum „Richtig“ oder „Falsch“ heraus zu finden, sondern diese Differenz zu untersuchen. Es kann z.B. den Fragen nachgegangen werden, warum eine gegensätzliche Wahrnehmungen der Inspektoren/innen aufgetreten sind; was würde es für den Betriebsbereich bedeuten, wenn die Fremdwahrnehmung zugrunde gelegt würde; etc..
So können auch unangenehme Hinweise zur Sicherheitskultur durch die Inspektoren/innen von den Verantwortlichen als Chance für eine Weiterentwicklung genutzt werden.

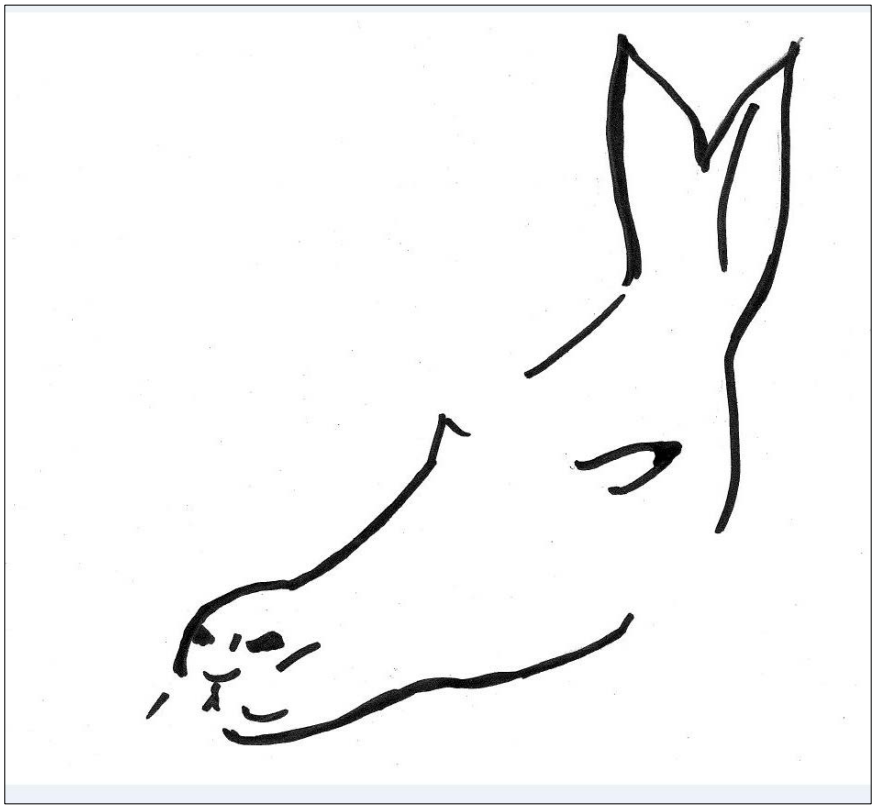

Abb. 18: Eigen- versus Fremdwahrnehmung: Esel versus Robbe

4 Das EDV-Programm Safety-Management-Valuation-Program (SMVP)

Das EDV-Programm SMVP wurde in den Jahren 1997 - 1999 in erster Linie für die Behörden in NRW als Hilfsmittel bei der Überprüfung von Sicherheitsmanagementsystemen (SMS) konzipiert, kann jedoch auch von anderen Interessierten genutzt werden.

Im Rahmen einer Vor-Ort-Besichtigung / Inspektion können aus dem Prüfkatalog des SMVP die relevanten Prüfgebiete für ein neuangelegtes Projekt ausgewählt werden. Die Prüfgebiete beinhalten Fragen die im Rahmen der Überprüfung beantwortet werden. Eine Unterstützung hierzu bieten die zugehörigen Bewertungshilfen, gleichwohl werden für die Beantwortung der Fragen entsprechende Fachkenntnisse vorausgesetzt.

Die jeweils aktuelle Programm Version SMVP (zurzeit: Version 3.0.0.0) ist frei verfügbar und kann von den Internetseiten des Landesamts für Natur, Umwelt und Verbraucherschutz NRW heruntergeladen werden.

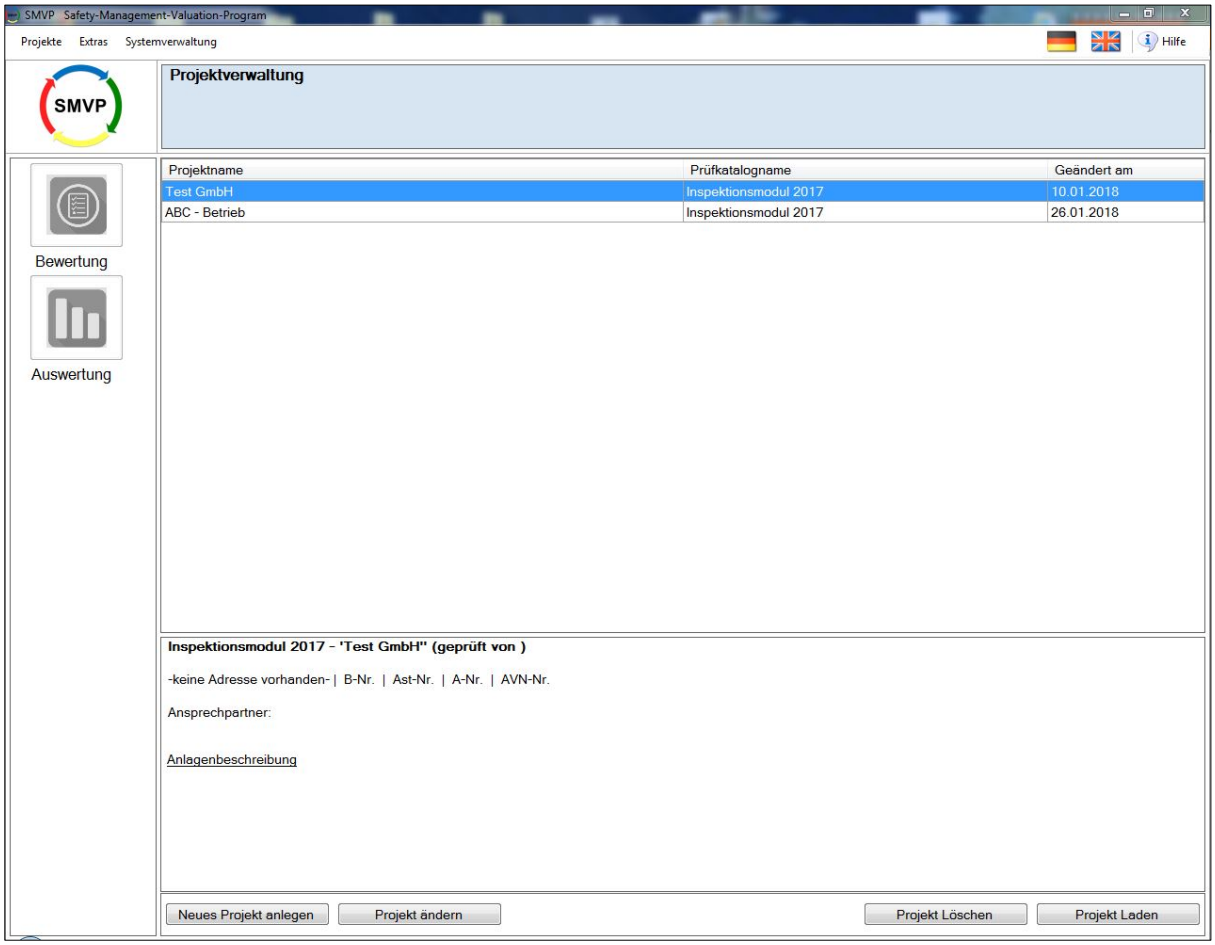

Abb. 19: Start-Maske in SMVP

Um Erweiterungen und Anpassungen – z. B. bei geänderten Rechtsgrundlagen – der Inhalte des SMVP ohne Änderung des eigentlichen Programms vornehmen zu können, arbeitet das Programm mit sog. Prüfkatalogen. Diese werden bei Bedarf durch das LANUV NRW verändert

und in unregelmäßigen Abständen auf der entsprechenden LANUV Webseite zum Herunterladen angeboten. Neue Prüfkataloge lassen sich in bestehende Programme übernehmen, ohne dass die bisherigen Daten verloren gehen. Allerdings muss bei der Nutzung von Inhalten eines neuen Prüfkatalogs ein Projekt neu angelegt werden.
Der zurzeit aktuelle Prüfkatalog (Stand Januar 2018) beinhaltet unter der Bezeichnung "Inspektionsmodul 2017" folgende Themenbereiche:

- **Quellen- /Literaturangaben**
- **Allgemeines zur Benutzung**
- **Sicherheitsmanagement - SMS**
- **Corporate Governance – CG APS**
- **Vielstoffanlagen – VMA**
- **Alarmmanagement - AM**

welche insgesamt 27 Prüfgebiete enthalten.

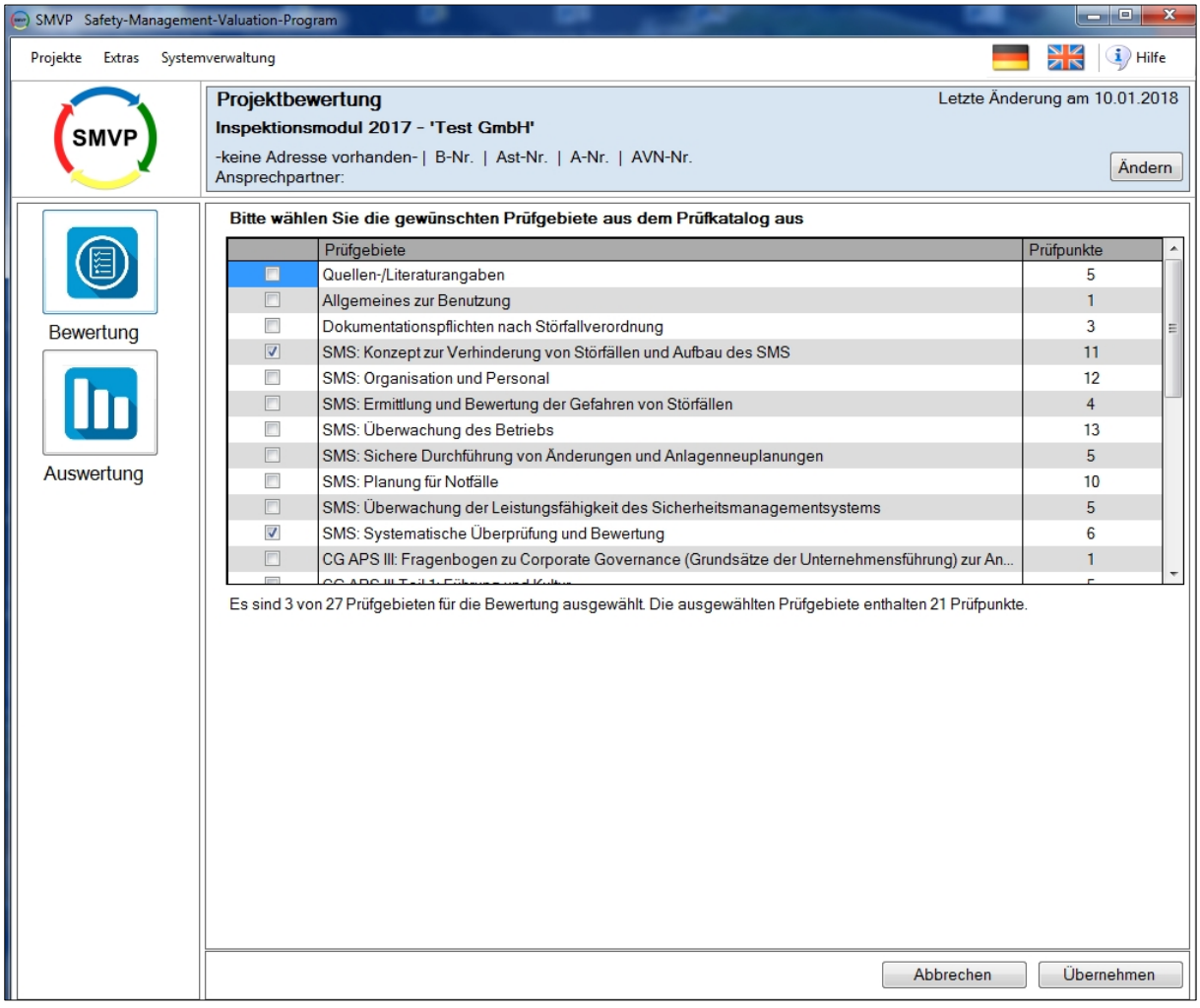

Abb. 20: Maske in SMVP: Auswahl der Prüfgebiete

Die Prüfgebiete zu den unterschiedlichen Themengebieten können für Vor-Ort-Besichtigung und Überprüfungen beliebig ausgewählt werden - standardmäßig sind erstmal alle Prüfgebiete deaktiviert. Die auswählbaren Themen sind abhängig vom zugrundeliegenden Prüfkatalog, der ausschließlich vom LANUV gepflegt und weiterentwickelt wird.

Acht Prüfgebiete unter dem Titel „SMS:“ bilden die Anforderungen der Störfall-Verordnung an ein SMS ab. Hiermit kann das SMS, welches in einem Betriebsbereich nach Störfall-Verordnung umgesetzt sein muss, überprüft werden.

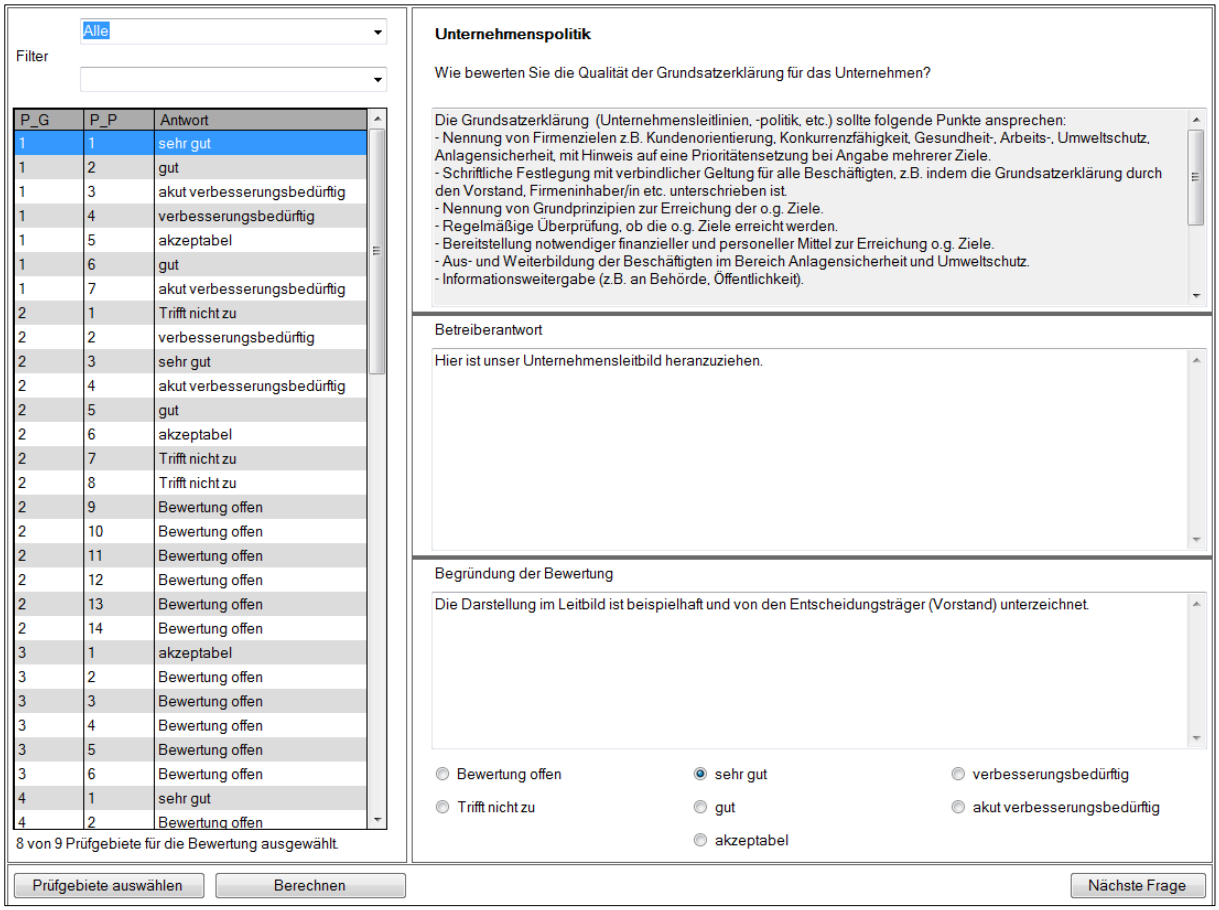

Abb. 21: Maske in SMVP: Bewertung der Fragen

Die obige SMVP-Bewertungsmaske enthält u. a. eine ausgewählte Frage und die dazugehörige Bewertungshilfe, sowie Felder für eine freie Texteingabe der Antwort durch den Betreiber eines Betriebsbereiches sowie für die Begründung der Bewertung für die Frage durch die überprüfende Person. Die Bewertung der Frage erfolgt durch einfaches Anklicken mit der linken Maustaste auf den entsprechenden Kreis einer ausgewählten aus den verfügbaren Bewertungen.

SMVP ermöglicht einen Austausch von Inhalten zu einem Projekt mittels Exportfunktionen – so kann ein Betreiber seine Antworten in SMVP der zuständigen Behörde als SMVP-Exportdatei per E-Mail übermitteln. Des Weiteren bietet SMVP die automatische Generierung von Berichten und Auswertungen und deren Export als Word-, Pdf- oder Excel-Datei an.

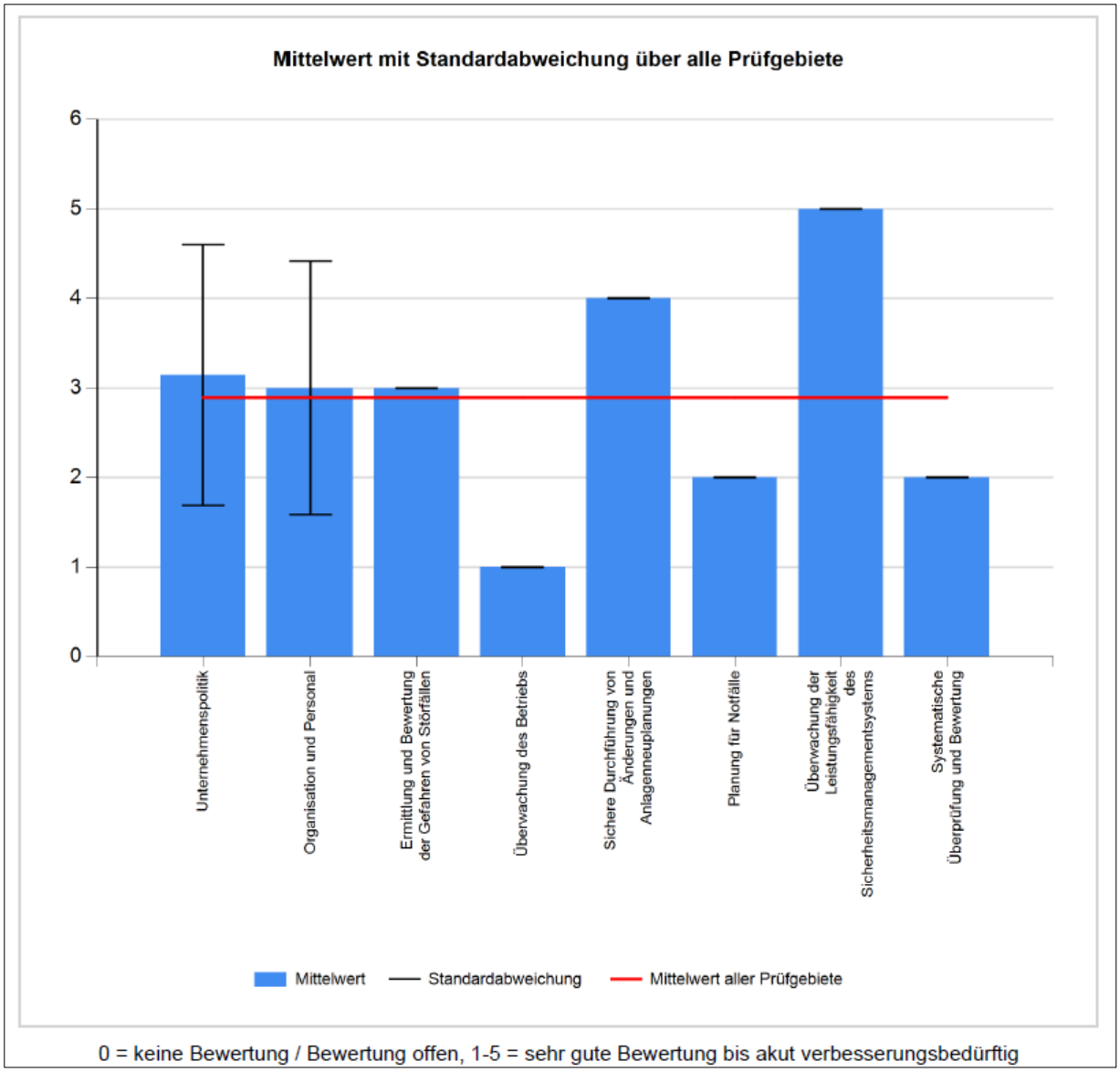

Abb. 22: Beispiel SMVP-Auswertung eines Projektes: „Mittelwert mit Standardabweichung“

Anregungen zur Weiterentwicklung des SMVP nimmt das LANUV, Arbeitsbereich Anlagensicherheit über die E-Mailadresse: SMVP@lanuv.nrw.de gerne entgegen.

5 SMS: Fragen und Bewertungshilfen

SMVP ermöglicht die Bewertung der Antwort zu einer Frage mit sehr gut, gut, akzeptabel, verbesserungsbedürftig, akut verbesserungsbedürftig und „trifft nicht zu“. Die Bewertungshilfen erläutern, welche Aspekte bei der Beantwortung einer Frage berücksichtigt werden können bzw. sollten. Sind die genannten Aspekte für den zu prüfenden Betriebsbereich relevant, so führt deren Fehlen zu einer negativen Bewertung. Ggf. werden in den Bewertungshilfen auch Bewertungskriterien für eine gute Bewertung genannt.

5.1 SMS: Konzept zur Verhinderung von Störfällen und Aufbau des SMS

Dieses Prüfgebiet enthält die folgenden Fragen:

Frage Nr. 1: Wie ist die Qualität der Unternehmenspolitik des Unternehmens im Hinblick auf die Anlagensicherheit zu bewerten?

Frage Nr. 2: Wie wird das Konzept zur Verhinderung von Störfällen bewertet?

Frage Nr. 3: Wie ist der Aufbau des Sicherheitsmanagementsystems (SMS) im Betriebsbereich zu bewerten?

Frage Nr. 4: Wie ist die Dokumentation des SMS im Betriebsbereich zu bewerten?

Frage Nr. 5: Wie wird Corporate Governance (Grundsätze der Unternehmensführung) für die Anlagensicherheit im Betriebsbereich eingeschätzt?

Frage Nr. 6: Wie werden die Regelungen zum finanziellen Rahmen für die Anlagensicherheit bewertet?

Frage Nr. 7: Wie wird die Überprüfung der Dokumentenlenkung des SMS im Betriebsbereich bewertet?

Frage Nr. 8: Wie ist die Regelung zur Bekanntgabe der Unternehmungspolitik bzw. Sicherheitspolitik im Unternehmen zu bewerten?

Frage Nr. 9: Wie wird die Einbeziehung der Beschäftigten in die Gestaltung und Umsetzung von Politiken und Regelungen bewertet?

Frage Nr. 10: Wie werden die Regelungen zur Überprüfung der Zielsetzung der Sicherheitspolitik bewertet?

Frage Nr. 11: Wie werden die Umsetzung der Sicherheitspolitik und der Regelungsumfang von betriebsinternen Sicherheitsvorschriften bewertet?

5.1.1 Frage Nr. 1: Wie ist die Qualität der Unternehmenspolitik des Unternehmens im Hinblick auf die Anlagensicherheit zu bewerten?

Bewertungshilfe:

Beim Vorliegen eines integrierten Managementsystems ist die Qualität der Unternehmenspolitik (Grundsatzerklärung, Vision, Leitlinien etc.) des Unternehmens sowie die Abdeckung des Punktes Anlagensicherheit im Sinne der Störfallverordnung in der Unternehmenspolitik zu bewerten. Sollte das Unternehmen ausschließlich über ein separates Sicherheitsmanagementsystem verfügen, so gelten die nachfolgenden Punkte für die Unternehmenspolitik zur Anlagensicherheit.

Die Unternehmenspolitik (Grundsatzerklärung, Vision, Leitlinien, etc.) sollte folgende Punkte ansprechen:

- Nennung von Firmenzielen, z. B. Kundenorientierung, Konkurrenzfähigkeit, Gesundheit-, Arbeits-, Umweltschutz, Anlagensicherheit, mit Hinweis auf eine Prioritätensetzung bei Angabe mehrerer Ziele.
- Schriftliche Festlegung mit verbindlicher Geltung für alle Beschäftigten, z. B. indem die Unternehmenspolitik durch den Vorstand, Firmeninhaber/in etc. unterschrieben ist.
- Nennung von Grundprinzipien zur Erreichung der o. g. Ziele.
- Regelmäßige Überprüfung, ob die o. g. Ziele erreicht werden.
- Bereitstellung notwendiger finanzieller und personeller Mittel zur Erreichung o. g. Ziele.
- Aus- und Weiterbildung der Beschäftigten im Bereich Anlagensicherheit und Umweltschutz.
- Informationsweitergabe (z. B. an Behörde, Öffentlichkeit).

Weiterhin sollte die Unternehmenspolitik klar und für jeden verständlich formuliert und ausreichend verfügbar sein.
Gegebenenfalls werden die Beschäftigten bei der Erstellung der Unternehmenspolitik eingebunden.

Bei den Firmenzielen muss die Verhinderung von Störfällen und die Begrenzung der Auswirkung von Störfällen im Ereignisfall Vorrang vor den anderen Zielen haben.

Die bereitgestellten finanziellen und personellen Mittel für die Anlagensicherheit müssen adäquat sein im Hinblick auf das Gefährdungspotential des Betriebsbereiches / der Anlage.
In der Unternehmenspolitik des integrierten Managementsystems ist die Priorität des Aspektes Anlagensicherheit erkennbar und innerhalb verschiedener Firmenzielen hoch eingestuft und hat im Ereignisfall Vorrang vor anderen Zielen. Weitere in der Unternehmenspolitik aufgeführte Punkte (z. B. Grundprinzipien, Überprüfungen) gelten auch für die Anlagensicherheit.

5.1.2 Frage Nr. 2: Wie wird das Konzept zur Verhinderung von Störfällen bewertet?

Bewertungshilfe:

Nach § 8 der Störfall-Verordnung müssen Betreiber von Betriebsbereichen (BB), die der Störfall-Verordnung unterliegen, über ein schriftliches Konzept zur Verhinderung von Störfällen verfügen. Der Betreiber hat die Umsetzung des Konzeptes durch angemessene Mittel und Strukturen sowie durch ein Sicherheitsmanagementsystem nach Anhang III sicherzustellen. Das Konzept zur Verhinderung von Störfällen ist vor Inbetriebnahme zu erstellen und muss folgende Anforderungen erfüllen:

- Es muss enthalten:
  - Die übergeordneten Ziele und Handlungsgrundsätze des Betreibers,
  - die Rolle und Verantwortung der Leitung des Betriebsbereiches,
  - die Verpflichtung, die Beherrschung der Gefahren von Störfällen ständig zu verbessern,
  - die Verpflichtung, ein hohes Schutzniveau zu gewährleisten.
- Es ist regelmäßig zu überprüfen und ggf. zu aktualisieren: (mindestens alle 5 Jahre) sowie anlassbezogen (wesentliche Änderung, Ereignis).

Auf die KAS-Leitfäden Nr. 19 "Leitfaden zum Konzept zur Verhinderung von Störfällen und zum Sicherheitsmanagementsystem“ und Nr. 29 "Besondere Anforderungen an Sicherheitstechnik und Sicherheitsorganisation zur Unterstützung von Anlagenpersonal in Notfallsituationen unter besonderer Berücksichtigung des Leitfadens KAS-20“ wird hingewiesen.

Im Rahmen einer Inspektion ist das Konzept zur Verhinderung von Störfällen eines BB einzusehen und zu bewerten, ob die oben genannten Anforderungen erfüllt werden.

Hierzu dienen auch die folgenden Hinweise.

BB der unteren Klasse:
Angelehnt an Ausführungen des KAS-Leitfadens Nr. 19:
Es gilt für Betriebsbereiche der unteren Klasse (alt: BB mit Grundpflichten), dass gemeinsam mit anderen zur Verfügung stehenden Dokumenten im Konzept zur Verhinderung von Störfällen die Erfüllung der Betreiberpflichten nach Störfall-Verordnung nachvollziehbar dargestellt werden muss.
Neben der Unternehmenspolitik bzw. Sicherheitspolitik und den daraus ggf. abgeleiteten Leitlinien soll in dem Konzept zur Verhinderung von Störfällen auch dargelegt werden,

A. welche Gefahren von Störfällen im Betriebsbereich vorliegen,
B. welche Maßnahmen zu ihrer Verhinderung und zur Begrenzung ihrer Folgen vorgesehen sind,
C. wie die ordnungsgemäße Umsetzung dieser Maßnahmen sichergestellt wird und
D. wie das Sicherheitsmanagementsystem aufgebaut und umgesetzt wird.

Die schriftliche Ausarbeitung sollte aus sich heraus verständlich sein, muss jedoch nicht so detaillierte Angaben enthalten wie ein Sicherheitsbericht nach § 9 der Störfall-Verordnung.

Das Konzept sollte über folgende Inhalte verfügen:

1. **Unternehmens- / Sicherheitspolitik und Leitlinien**
2. **Aufbau des Sicherheitsmanagementsystems (SMS)**
3. **Gefahrenpotenzial des Betriebsbereiches**
4. **Örtliche Lage**
5. **Stoffe**
6. **Art des Verfahrens bzw. der Tätigkeit**
7. **Technische und organisatorische Maßnahmen zur Verhinderung von Störfällen bzw. zur Begrenzung ihrer Folgen und ihre Einbindung im SMS**

Im Konzept kann auf an anderer Stelle im BB vorhandene Unterlagen verwiesen werden, z. B. auf die Anzeige nach § 7 der Störfall-Verordnung oder Sicherheitsbetrachtungen nach anderen Regelwerken.

Es wird jedoch nachdrücklich empfohlen, dass bei der Ausgestaltung des Konzeptes zur Verhinderung von Störfällen in nachvollziehbarer Weise hervorgeht, welche Schwerpunkte der Betreiber eines BB der unteren Klasse zur Erfüllung der Grundpflichten der Störfall-Verordnung, also zur Vermeidung von Störfällen und zur Begrenzung eventueller Auswirkungen, umgesetzt hat.

Zur Darstellung der Unternehmenspolitik und des SMS im Konzept wird auf die Bewertungshilfen der anderen Fragen dieses Prüfgebietes verwiesen.

Der Betreiber eines BB der unteren Klasse sollte im Konzept zur Verhinderung von Störfällen die Stoffe bzw. Stoffkategorien beschreiben, die das Gefahrenpotenzial des Betriebsbereiches prägen.
Neben der Menge und der Art des Umgangs spielen hier die physikalischen sowie sicherheits- und reaktionstechnischen Stoffdaten, die Wirkungsdaten sowie eventuelle Grenz- bzw. Beurteilungswerte eine besondere Rolle, wie sie sich auch aus den Sicherheitsdatenblättern ergeben können.

Im Hinblick auf die örtliche Lage sollte insbesondere auf benachbarte Wohnbebauung, schutzwürdige Objekte, Nachbaranlagen und Standortbesonderheiten (Gefährdung durch Erdbeben, Hochwasser etc.) eingegangen werden.

Es sollte dargelegt werden, welche Anlagen, Anlagenteile bzw. Tätigkeiten im Hinblick auf die Gefahr bzw. Verhinderung von Störfällen von Bedeutung sind, z. B.:

- technischer Zweck und Beschaffenheit der Betriebsbereiche/Anlagen mit Grundoperationen (eingehaust oder als Freianlage, physikalischen oder chemischen Umwandlungen, kontinuierlich oder diskontinuierlich, Zwischenlagerung von Edukten und Produkten, Handhabung von Reststoffen und Abgasen, manuelle Abfüllvorgänge),
- wesentliche Charakteristika der Reaktionen (z. B. Druck, exotherme Reaktion, besondere Stoffeigenschaften etc.). Zur sicherheitstechnischen Bewertung exothermer Reaktionen wird auf die Technische Regel Anlagensicherheit "Erkennen und Beherrschen exothermer Reaktionen" (TRAS 410) hingewiesen.

Der Betreiber sollte die im Rahmen einer systematischen Gefahrenanalyse identifizierten wesentlichen Gefahrenpotenziale und Gefährdungen, die vom Betriebsbereich ausgehen können, im Konzept beschreiben sowie die ermittelten sicherheitsrelevanten Anlagenteile aufführen.
Darauf aufbauend sollten die vom Betreiber vorgesehenen grundlegenden Maßnahmen zur Reduzierung bzw. Beherrschung der Gefahrenpotentiale sowie zur Begrenzung der Folgen eines eventuellen Störfalls dargestellt werden.

Solche Maßnahmen können technischer und organisatorischer Art sein und sind im SMS einzubinden.

Dies kann dargestellt werden durch eine Tabelle mit der Zuordnung der Regelungen / Anweisungen des Betriebsbereiches zu den Anforderungen der Störfallverordnung. *(Ergänzender Hinweis über SMVP hinaus: Eine aktuelle Fassung der Tabelle ist dem LANUV-Arbeitsblatt Nr. 41 „Darstellung des Sicherheitsmanagementsystems im Sicherheitsbericht“, Stand April 2019 /7/ zu entnehmen. Diese Tabelle steht auch als Worddokumentvorlage zum Download auf den Internetseiten des LANUV zur Verfügung.)*

BB der oberen Klasse:

Für Betriebsbereiche der oberen Klasse werden ausführliche Angaben, welche Gefahren von Störfällen im Betriebsbereich vorliegen und welche Maßnahmen zu ihrer Verhinderung und zur Begrenzung ihrer Folgen vorgesehen sind, im Sicherheitsbericht gemacht.

Bestandteil des Sicherheitsberichtes ist auch eine strukturierte, schriftliche Darlegung des SMS nach Anhang III der Störfallverordnung. Hierin kann das Konzept zur Verhinderung von Störfällen Bestandteil sein. Ein Beispiel bietet das Musterkapitel „Darstellung des Sicherheitsmanagementsystems im Sicherheitsbericht“ des LANUV NRW, Stand: Mai 2007. *(Im folgende die aktualisierte Fassung aus /7/ gegenüber SMVP als)* ein beispielhaftes Inhaltsverzeichnis:

Beispielinhaltsverzeichnis:	
1	***Allgemeines***
1.1	*Struktur des Unternehmens*
1.2	*Konzept zur Verhinderung von Störfällen*
1.3	*Unternehmenspolitik*
1.4	*Sicherheitskultur im Betriebsbereich*
1.5	*Berücksichtigung des Human Factors im Betriebsbereich*
2	***Das Sicherheitsmanagementsystem im Betriebsbereich***
2.1	*Aufbau und Struktur des Sicherheitsmanagementsystems*
2.2	*Organisation und Personal*
2.3	*Ermittlung und Bewertung der Gefahren von Störfällen*
2.4	*Überwachung des Betriebes*
2.5	*Sichere Durchführung von Änderungen*
2.6	*Planung für Notfälle*
2.7	*Überwachung der Leistungsfähigkeit des SMS*
2.8	*Systematische Überprüfung und Bewertung*
3	***Vorhandene Regelungen und Dokumente des Betriebsbereiches***
3.1	*Darstellung der Aufbauorganisation (Organigramme)*
3.2	*Inhaltsverzeichnis des Managementhandbuches*
3.3	*Liste aller vorhandenen Regelungen im Betriebsbereich (optional)*
3.4	*Zuordnung der Regelungen/Anweisungen des Betriebsbereiches zu den Anforderungen der StörfallV*
4	***Anhang***
	Kopien ausgewählter für das SMS relevante Regelungen/ Anweisungen des Betriebsbereiches (z.B. VA zur Ermittlung und Bewertung der Gefahren von Störfällen, VA Alarmmanagement etc.)

Abb. 23: Beispielinhaltsverzeichnis SMS im SB aus /7/

Nach dem KAS-Leitfaden Nr. 29 besteht auch die Möglichkeit, wesentliche Elemente des Konzeptes zur Verhinderung von Störfällen als generellen Prozess zur Erreichung, Aufrechterhaltung und Verbesserung der Anlagensicherheit aufzufassen. Ein solcher Prozess „Anlagensicherheit“ kann dem systematischen Managementkonzept des kontinuierlichen PLAN-DO-CHECK-ACT Kreisprozesses (PDCA-Zyklus) folgen und lässt sich aufgliedern in die Kreisschritte:

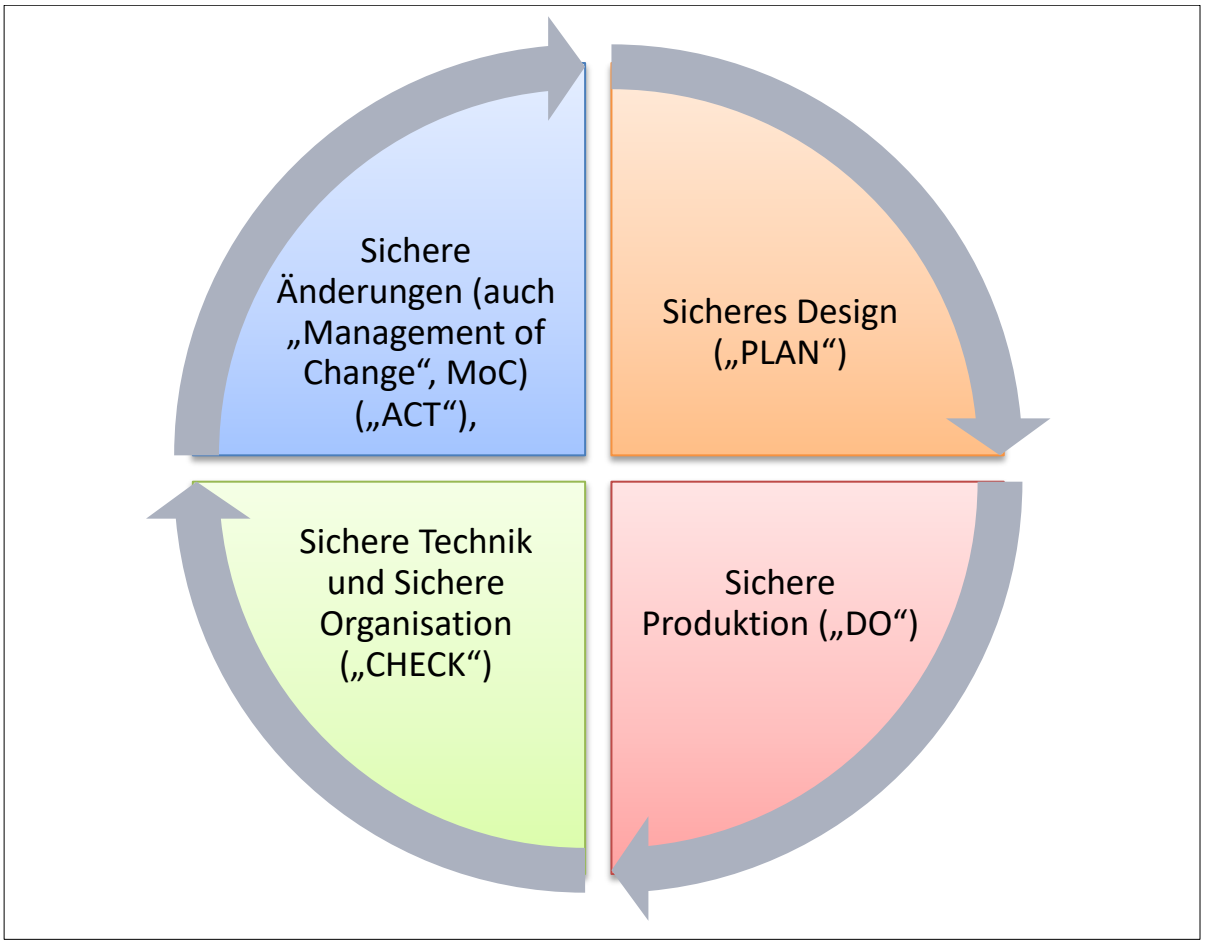

Abb. 24: Prozess „Anlagensicherheit“ dargestellt als PDCA-Zyklus

um in einem kontinuierlichen Verbesserungsprozess wieder mit Sicheres Design („PLAN“) zu beginnen.

Die Punkte des SMS nach Anhang III entsprechend der obigen Gliederung 2.2 bis 2.8 lassen sich diesen Schritten wie folgt zuordnen:

Sicheres Design („PLAN“):	2.3 und Teile von 2.2
Sichere Produktion („DO“):	2.4, 2.6 und Teile von 2.2
Sichere Technik und Sichere Organisation („CHECK“):	2.7, 2.8 und Teile von 2.4
Sichere Änderungen („ACT“):	2.5

5.1.3 Frage Nr. 3: Wie ist der Aufbau des Sicherheitsmanagementsystems (SMS) im Betriebsbereich zu bewerten?

Bewertungshilfe:

Ein Sicherheitsmanagementsystem (SMS) nach Störfallverordnung entspricht in seinen grundlegenden Anforderungen den generellen Anforderungen an Managementsysteme. D. h. es muss über einen prozessorientierten Ansatz, eine Struktur der Regelungen und Dokumentation und über Überprüfungszyklen, die kontinuierliche Verbesserungs- und Anpassungsprozesse gewährleisten, verfügen. Basieren muss das SMS auf einer Unternehmenspolitik zur Prozess- und Anlagensicherheit im Sinne der Störfall-Verordnung und es muss den Gefahren, Tätigkeiten und der Komplexität des Betriebsbereiches angemessen sein. Das SMS beruht daher auf einer Risikobeurteilung.
Das SMS muss mindestens folgende im Anhang III der Störfall-Verordnung aufgeführte zu regelnden Punkte umfassen und diese müssen bei den Prozessen des Betriebsbereiches Berücksichtigung finden:

a) Organisation und Personal
b) Ermittlung und Bewertung der Gefahren von Störfällen
c) Überwachung des Betriebes
d) Sichere Durchführung von Änderungen
e) Planung für Notfälle
f) Überwachung der Leistungsfähigkeit des SMS
g) Systematische Überprüfung und Bewertung

Bei Inspektionen können folgende Aspekte Berücksichtigung finden:
Es ist sinnvoll die obige Frage „Wie ist der Aufbau des Sicherheitsmanagementsystems (SMS) im Betriebsbereich zu bewerten?“ im Kontext mit der Frage „Wie ist die Dokumentation des SMS im Betriebsbereich zu bewerten?“ zu betrachten, da die Struktur der Regelungen und Dokumentation ein wesentlicher Bestandteil der generellen Anforderungen an SMS ist. Die Struktur der Regelungen und ihre Verknüpfungen untereinander sollten sich visuell darstellen lassen. Dies bildet in der Regel den Aufbau des SMS ab, lässt aber noch keine Aussage darüber zu, ob ein SMS im BB vorliegt.
Zur Beurteilung, ob ein SMS im BB vorliegt und nicht nur (einzelne) organisatorische Regelungen, müssen noch die folgenden zwei Aspekte betrachtet werden:

- Anlagensicherheit in der Unternehmenspolitik,
- Überprüfungszyklen.

Hierzu können die Antworten zu den folgenden Fragen hinzugezogen werden:

Prüfgebiet SMS: Konzept zur Verhinderung von Störfällen und Aufbau des SMS

- Wie ist die Qualität der Unternehmenspolitik des Unternehmens im Hinblick auf die Anlagensicherheit zu bewerten?
- Wie wird das Konzept zur Verhinderung von Störfällen bewertet?

Prüfgebiet SMS: Überwachung der Leistungsfähigkeit des Sicherheitsmanagementsystems

- Wie wird der Prozess zur Überprüfung der Zielsetzung und der Regelungen des Sicherheitsmanagementsystems bewertet?
- Wie wird der Prozess zum Auditsystem bewertet?

Prüfgebiet SMS: Systematische Überprüfung und Bewertung

- Wie wird die Vorgehensweise zur systematischen Überprüfung und Bewertung des Konzeptes zur Verhinderung von Störfällen bewertet?
- Wie wird die Vorgehensweise zur systematischen Überprüfung und Bewertung des SMS (Managementreview) bewertet?

Die adäquate Beteiligung der obersten Leitung ist eine wichtige Voraussetzung dafür, dass es sich um ein „gelebtes“ SMS handelt (siehe hierzu die Antwort zur Frage „Wie wird Corporate Governance (Grundsätze der Unternehmensführung) für die Anlagensicherheit im Betriebsbereich eingeschätzt?“ aus dem Prüfgebiet SMS: Konzept zur Verhinderung von Störfällen und Aufbau des SMS).
Liegen in einem BB Zertifikate (z. B. nach DIN EN ISO 9001 „Qualitätsmanagementsysteme-Anforderungen“ oder DIN EN ISO 14001 „Umweltmanagementsysteme-Anforderungen mit Anleitung zur Anwendung“) vor, so kann erwartet werden, dass dieser BB die grundlegenden Anforderungen an ein Managementsystem (Unternehmenspolitik, Struktur der Regelungen und Dokumentation (prozessorientiert) und Überprüfungszyklen) umgesetzt hat. Zu prüfen ist dann insbesondere, ob die Anforderungen der Störfall-Verordnung hierbei berücksichtigt sind.

Ob die nach Störfall-Verordnung geforderten relevanten Prozesse im SMS des BB vollständig vorhanden sind, wird durch die folgenden Prüfgebiete abgefragt:

SMS: Organisation und Personal

SMS: Ermittlung und Bewertung der Gefahren von Störfällen

SMS: Überwachung des Betriebes

SMS: Sichere Durchführung von Änderungen

SMS: Planung für Notfälle

SMS: Überwachung der Leistungsfähigkeit des SMS (hier die beiden Prozesse „Internes Berichtssystem“ und „Indikatoren/Kennzahlen“).

Das Prüfgebiet „SMS: Ermittlung und Bewertung der Gefahren von Störfällen“ stellt dabei das wichtigste Kernstück der Prozess- und Anlagensicherheit dar und ist die Basis, um angemessene Maßnahmen zur Verhinderung und Begrenzung von Störfällen zu bestimmen und umzusetzen.
Betriebsbereiche sollten eine Verweismatrix, die eine Zuordnung der Regelungen / Anweisungen des Betriebsbereiches zu den Anforderungen der Störfallverordnung enthält, erstellen und aktuell halten. Hiermit können die Betreiber von Betriebsbereichen auf den ersten Blick erkennen, ob das SMS Regelungen zu allen im Anhang III der Störfallverordnung aufgeführten Punkten enthält. Nähere Informationen hierzu können dem KAS-Leitfaden Nr. 19, Anlage 3

„Beispiel für die Darstellung der Zuordnung der Regelungen/Anweisungen des Betriebsbereiches zu den Anforderungen der Störfall-Verordnung“ entnommen werden. Die Anlage 3 stellt einen Auszug (Kapitel 3.4) aus der Veröffentlichung des Landesamtes für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen: „Musterkapitel, Darstellung des Sicherheitsmanagementsystems im Sicherheitsbericht“ dar.
Ergänzender Hinweis über SMVP hinaus: Eine aktuelle Fassung der Tabelle ist dem LANUV-Arbeitsblatt Nr. 41 „Darstellung des Sicherheitsmanagementsystems im Sicherheitsbericht“, Stand April 2019 /7/ zu entnehmen. Diese Tabelle steht auch als Worddokumentvorlage zum Download auf den Internetseiten des LANUV zur Verfügung.

Erläuterungen zu den generellen Anforderungen an Managementsystemen

Bei einem Managementsystem handelt es sich um ein festgelegtes und dokumentiertes System aller organisatorischen Strukturen, Abläufe, Vorkehrungen, Maßnahmen und Überprüfungen zur Erreichung von festgelegten (Unternehmens-) Zielen. Ein Managementsystem *beruht auf einer Risikobeurteilung und (Ergänzung zu /3/)* ist gekennzeichnet durch:

1. einen prozessorientierten Ansatz,
2. eine (hierarchische) Struktur der Regelungen und Dokumentation sowie
3. Überprüfungszyklen, die kontinuierliche Verbesserungs- und Anpassungsprozesse gewährleisten.

Erläuterungen zum Begriff Prozess sowie zum Verständnis eines strukturierten Aufbaus von Managementsystemen und Überprüfungszyklen:

Als Prozess werden ein System und eine Abfolge von Tätigkeiten verstanden, die Eingaben unter Verwendung von Mitteln in Ergebnisse umwandeln. Die Prozesse in einem Unternehmen müssen von diesem bestimmt werden und sind unternehmensspezifisch.

Es besteht die Möglichkeit, Unternehmensprozesse Prozessarten (z. B. Führungs-, Kern-, Unterstützungsprozessen) zuzuordnen. Ein Prozess selbst zieht sich durch alle Ebenen eines Managementsystems. Welche Aspekte eines Prozesses in Umfang und Tiefe in welcher Ebene eines Managementsystems behandelt werden, ist unternehmensspezifisch und auf das jeweilige Unternehmen zugeschnitten.“ /angelehnt an KAS-Leitfaden Nr. 8/

„Der strukturierte Aufbau eines Managementsystems findet seinen Ausdruck neben den Inhalten auch im entsprechenden Aufbau der Dokumentation des Managementsystems. Wie viele Dokumentationsebenen ein Managementsystem enthält und wie diese benannt sind, ist nicht festgelegt. Dies ist in der Praxis unterschiedlich und sollte dem jeweiligen Unternehmen entsprechen. Für einen strukturierten Aufbau müssen jedoch die Bezüge zwischen den Dokumentationsebenen vorhanden sein. /KAS-Leitfaden Nr. 8/“

Dieser Aufbau des SMS eines Betriebsbereiches sollte sich visuell veranschaulichen lassen.

Die Überprüfungszyklen ermöglichen kontinuierliche Verbesserungs- und Anpassungsprozesse. Veränderte Bedingungen werden durch die regelmäßigen Überprüfungen frühzeitig erkannt und es kann in einem sehr frühen Stadium effektiv reagiert werden. Zudem ermöglichen die Überprüfungszyklen ein frühzeitiges Identifizieren von Schwachstellen und ein effektives

Lernen aus Fehlern. Überprüfungszyklen von Managementsystemen werden oft als PDCA*-Regelkreis beschrieben und visuell dargestellt.

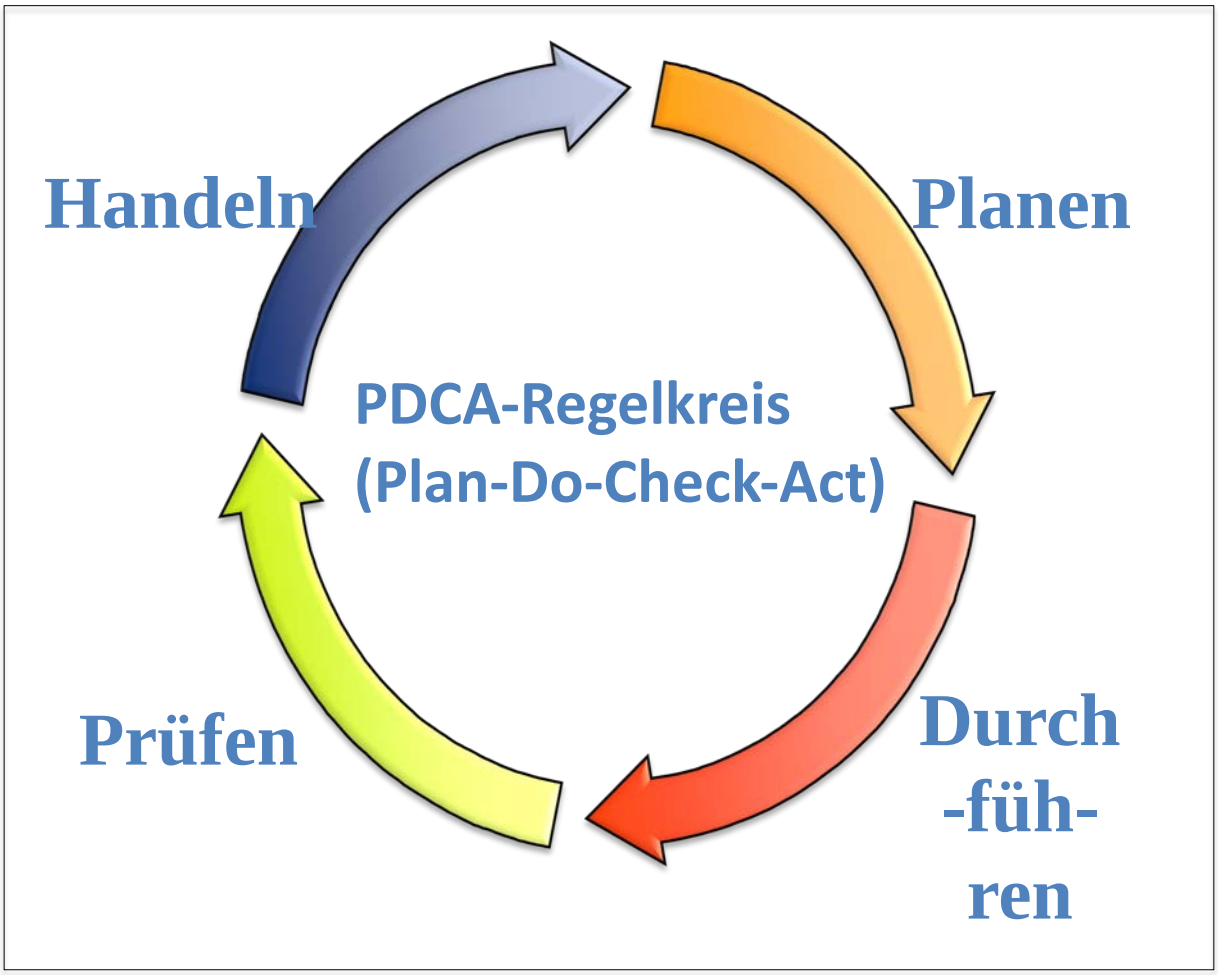

Abb.25: PDCA-Zyklus

*Plan(Planen)-Do(Handeln)-Check(Prüfen)-Act(Verbessern) -> *veraltet, seit 2015:*
Plan(Planen)-Do(Durchführen)-Check(Prüfen)-Act(Handeln)

Erläuterungen zu den Anforderungen an das Sicherheitsmanagementsystem nach Störfallverordnung

Das Sicherheitsmanagementsystem (SMS) im Sinne der Störfall-Verordnung muss in seinen Grundstrukturen den oben genannten Elementen eines Managementsystems entsprechen. Es zeichnet sich gegenüber anderen Managementsystemen dadurch aus, dass es die Umsetzung der Anlagensicherheit im Sinne der Störfall-Verordnung als Ziel vorgibt - ein Prozess „Anlagensicherheit“. Ziele sind, die Verhinderung von Störfällen sowie die Auswirkung eines Störfalls so gering wie möglich zu halten. Diese Ziele sind Bestandteil des Konzeptes zur Verhinderung von Störfällen. Ein SMS dient der Umsetzung des Konzeptes zur Verhinderung von Störfällen oder auch einer Sicherheitspolitik und ist eine strukturierte Umsetzung im Betriebsbereich, um diese Ziele zu erreichen. Bei einem integrierten Managementsystem muss die Anlagensicherheit in der Unternehmenspolitik des Betriebsbereiches verankert sein.

Das SMS muss den Gefahren, Tätigkeiten und der Komplexität des Betriebsbereiches angemessen sein und beruht insofern auf einer Risikobeurteilung.

Für das Management von Risiken in Unternehmen / Organisationen gibt es eine internationale Basisnorm, die ISO 31000 "Risk Management – Principles and guidelines". Der Begriff Risiko umfasst hier „Auswirkungen von Unsicherheit auf Ziele, Tätigkeiten und Anforderungen“ und beinhaltet sowohl Chancen als auch Bedrohungen *(Stand 2009).*

Aktualisierung aufgrund der DIN ISO 31000:2018-10 (nicht in /3/ enthalten):
*Der **Begriff Risiko** umfasst hier „Auswirkung von Unsicherheit auf Ziele.“*

Die ISO-31000 Vorgängerausgabe von 2009 wurde wegen von deutschen Normengremium kritisch bewerteter Aspekte nicht in eine deutschsprachige Norm überführt. Die ISO-31000:2018 ist gegenüber der Vorläuferversion inhaltlich gestrafft und kürzer gefasst, so gibt es jetzt z. B. acht statt elf Grundsätze. „Das Umgehen mit Risiken basiert auf den Grundsätzen, dem Rahmenwerk und dem Prozess.“, /DIN ISO 31000:2018-10, S. 6/.

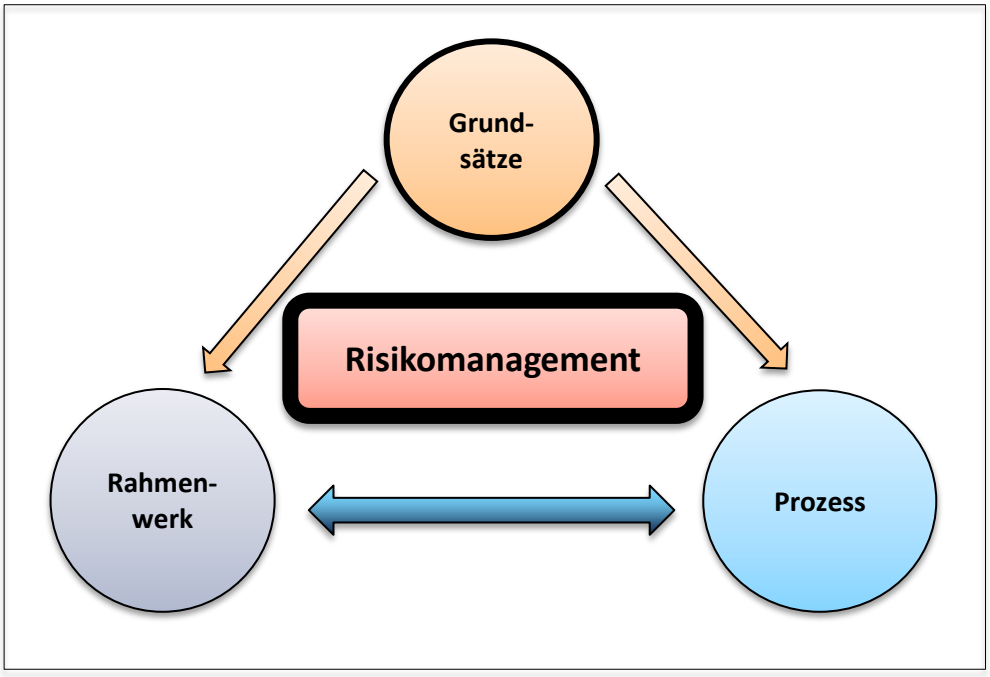

Abb. 26: Risikomanagement nach DIN ISO 31000:2018

Die Norm *beinhaltet* als *wichtige Elemente* für das Risikomanagement, u. a.

- Eingliederung in die Gesamtorganisation des Unternehmens,
- Top-down-Ansatz: Risikomanagement ist Aufgabe der obersten Leitung,
- die Berücksichtigung des PDCA-Regelkreis und
- den Risikomanagementprozess.

Der Risikomanagementprozess enthält die Schritte

- Kontext*, Anwendungsbereich und Kriterien bestimmen* (Bestimmung grundlegender Parameter, Einflussgrößen, Kriterien, die für die Organisation von Bedeutung sind),
- Risikobeurteilung bestehend aus *Risikoidentifikation* (*alt:* Risikoermittlung), Risikoanalyse und Risikobewertung,
- Risikobehandlung.

Die Aspekte Kommunikation *und* Konsultation*,* Überwachen *und* Überprüfen *sowie Aufzeichnen und Berichten* sind bei allen Schritten zu berücksichtigen.

„Der Risikomanagementprozess sollte integraler Bestandteil des Managements und der Entscheidungsfindung sein und in die Struktur, die Abläufe und die Prozesse der Organisation integriert werden.“ /DIN ISO 31000:2018-10, S. 17/

Die DIN EN 31010 „Risikomanagement – Verfahren zur Risikobeurteilung“ ist eine die ISO 31000 unterstützende Norm und leitet zur Auswahl und Anwendung systematischer Verfahren zur Risikobeurteilung an (ca. 30 Verfahren, z.B. Brainstorming, Prüflisten, Strukturiertes „Was-Wenn“-Verfahren, Fehlzustandsart- und auswirkungsanalyse (FMEA), Multi-Kriterien-Entscheidungsanalyse (MCDA)).
Beide Normen 31000 sowie 31010 geben an, nicht zur Zertifizierung vorgesehen zu sein.

Dies ist bei der DIN EN ISO 9001 „Qualitätsmanagementsysteme – Anforderungen“ anders; in der Fassung vom 2015 ist dort als neues Element der Ansatz „risikobasiertes Denken“ eingeführt worden, u. a. mit den Kapiteln 4.1. „Verstehen der Organisation und ihres Kontextes“ sowie 6.1 „Maßnahmen zum Umgang mit Risiken und Chancen“.
Das SMS muss mindestens die im Anhang III der Störfall-Verordnung aufgeführten Punkte umfassen und diese müssen bei den Prozessen des Betriebsbereiches Berücksichtigung finden:

a) Organisation und Personal
b) Ermittlung und Bewertung der Gefahren von Störfällen
c) Überwachung des Betriebes
d) Sichere Durchführung von Änderungen
e) Planung für Notfälle
f) Überwachung der Leistungsfähigkeit des SMS
g) Systematische Überprüfung und Bewertung

In der Praxis ist z. B. der Punkt b) „Ermittlung und Bewertung der Gefahren von Störfällen“ häufig ein eigenständiger Prozess, der bei Unternehmen, die nicht der Störfall-Verordnung unterliegen, nicht existiert. Demgegenüber existieren in Unternehmen z. B. bei den Punkten a) „Organisation und Personal“ oder c) „Überwachung des Betriebes“ schon vielfältige Prozesse mit zugehöriger Verfahrensdokumentation, z. B. zur Personalauswahl und Schulung oder zur Instandhaltung und Arbeitsanweisungen zu Betriebsabläufen.

In diese müssen dann bei Betriebsbereichen die spezifischen Elemente der Störfallverordnung integriert sein – neben den offensichtlichen Punkten aus Anhang III insbesondere auch die Anforderungen der §§ 3 – 6 der Störfallverordnung. Die oben genannten Elemente eines Sicherheitsmanagementsystems sind von jedem Betriebsbereich zu erfüllen. Abhängig von der Größe und Komplexität des Betriebsbereiches (KMU, Konzern) ergeben sich Unterschiede im SMS insbesondere im Hinblick auf den Dokumentationsaufbau und -umfang. Dies wird im nachfolgenden Prüfpunkt vertieft.
Bei Vorliegen eines integrierten Managementsystems (IMS) ist es wichtig, dass die Anlagensicherheit (Prozesssicherheit) angemessen umgesetzt wird, d.h. alle Elemente des SMS berücksichtigt sind – die reine Umsetzung von Arbeitsschutz- und Umweltschutz-Anforderungen decken die Anlagensicherheit im Sinne der Störfall-Verordnung nicht ausreichend ab (Beispiel: Störfall in der BP Raffinerie in Texas City, März 2005, siehe auch KAS-Bericht Nr. 7).

Die richtige Anwendung eines (Sicherheits-)Managementsystems führt zu Transparenz, Klarheit und Struktur der Regelungen im Unternehmen. Mittels einer umsichtigen Dokumentation trägt es dazu bei, das „Wissen“ im Unternehmen zu erhalten und fortzuschreiben. Notwendige Bedingung hierfür ist das richtige Maß bei der Festlegung von Regelungen und dem Ausmaß der Dokumentation. Werden zu viele Regelungen ohne vernünftige Struktur aufgestellt, so führt dies zu einer Überorganisation mit sich evt. widersprechenden Regelungen und einem zu hohen Zeitaufwand für eine sinnlose Bürokratie. Demgegenüber verursacht eine zu geringe Regelungsdichte chaotische Zustände. Prinzipiell sollten nur solche Regeln festgelegt werden, die von den Führungsebenen auch kontrolliert werden und im Hinblick auf die Vorbildfunktion von Vorgesetzten auch eingehalten werden. Voraussetzung für ein „gelebtes“ Managementsystem ist das Engagement der obersten Leitung eines Unternehmens hierfür. Ein „gelebtes“ Managementsystem ist ein Steuerungs- und Führungssystem, welches seine Wirkung auf das Verhalten von Beschäftigten bei allen Tätigkeiten und auf allen Hierarchie- und Organisationsebenen eines Betriebes entfaltet.

5.1.4 Frage Nr. 4: Wie ist die Dokumentation des SMS im Betriebsbereich zu bewerten?

Bewertungshilfe:

Wenn in einem Unternehmen ein Managementsystem aufgebaut werden soll, so beginnt dies sinnvoller Weise mit einer Bestandsaufnahme vorhandener schriftlich festgelegter Regelungen und Dokumentationen. Des Weiteren sind die im Unternehmen vorliegenden Abläufe und Prozesse zu erfassen. Dies ist notwendig, da sich der heutige Aufbau von Managementsystemen an den Prozessen orientieren soll – man spricht vom prozessorientierten Ansatz. Hierbei werden alle Anforderungen und Ziele, welche das Unternehmen umsetzen möchte, in den jeweiligen Prozessen berücksichtigt. Dementsprechend muss geklärt werden, was das Managementsystem erfüllen und umsetzen soll, d. h. im Hinblick auf die Störfallverordnung die Anlagensicherheit aber z. B. auch Qualität, Arbeitsschutz, Umweltschutz etc.
Im Weiteren muss bestimmt werden, wie die (Dokumenten-) Struktur des Managementsystems für das Unternehmen aussehen soll. Wenn in einem Unternehmen keine Parallelstrukturen aufgebaut werden, sondern „nur“ ein Managementsystem im Unternehmen existiert, welches alle Anforderungen abdeckt, so wird von einem integrierten Managementsystem (IMS) gesprochen.
Im Folgenden wird der Begriff Managementsystem verwendet; dabei kann es sich um ein integriertes Managementsystem, welches das Sicherheitsmanagementsystem (SMS) enthält, oder um ein separates SMS handeln.

Es existieren Regelungen zur Dokumentation des Sicherheitsmanagementsystems sowie zu deren regelmäßigen Überprüfungen. Der Dokumentenaufbau ist bestimmt und es ist festgelegt, was in welcher Form (z. B. schriftlich, EDV-mäßig, konzernweit, anlagenbezogen etc.) dokumentiert wird. Für alle genannten Punkte sind die Verantwortlichkeiten und Kompetenzen festzulegen.
Der Dokumentenaufbau besitzt eine nachvollziehbare Struktur, i. d. R. eine hierarchische, die einen durchgängig roten Faden aufweist. Dies spiegelt die Durchgängigkeit eines Prozesses durch die verschiedenen Ebenen eines Managementsystems. Welche Aspekte eines Prozesses in Umfang und Tiefe, in welcher Ebene des Dokumentenaufbaus eines Managementsystems behandelt werden, ist unternehmensspezifisch und auf das jeweilige Unternehmen zugeschnitten.
Bildlich lässt sich der Dokumentenaufbau z. B. als Pyramide visualisieren, welche in Ebenen eingeteilt ist, z. B.:

- Unternehmenspolitik,
- Managementhandbuch
- Verfahrensanweisungen
- Arbeitsanweisungen
- Mitgeltende Dokumente, z. B. Formblätter, Bedienungsanleitungen

/KAS-Leitfaden 8/: „An der Spitze des Dokumentenaufbaus steht die Unternehmenspolitik auch Vision, Grundsatzerklärung, Leitlinien etc. genannt. Die Unternehmenspolitik beschreibt die generellen Ziele und Grundlagen des Unternehmens und gilt für den gesamten Unternehmensbereich. Die nachfolgenden Dokumentationsebenen werden immer präziser und die Detailtiefe nimmt zu. Gleichzeitig kann der Geltungsbereich sich immer mehr einschränken, z. B.

kann eine Arbeitsanweisung für Befüllvorgänge nur für eine Abteilung relevant sein und nur dort gelten und nicht für das gesamte Unternehmen. Wie viele Dokumentationsebenen ein Managementsystem enthält und wie diese benannt sind, ist nicht festgelegt. Dies ist in der Praxis unterschiedlich und sollte dem jeweiligen Unternehmen entsprechen. Für einen strukturierten Aufbau müssen jedoch die Bezüge zwischen den Dokumentationsebenen vorhanden sein. Anhand des obigen Beispiels heißt dies z. B., dass mitgeltende Dokumente einer Arbeitsanweisung zugeordnet werden können, die Arbeitsanweisung einer Verfahrungsanweisung, diese einem Kapitel im Managementhandbuch, dieses wiederum einer Grundaussage in der Unternehmenspolitik. Umgekehrt müssen sich ebenso Bezüge herstellen lassen."

Bei der Ebene der Verfahrensanweisungen, auch als Prozessbeschreibungen oder Managementanweisungen etc. bezeichnet, handelt es sich um Durchführungsbestimmungen für Prozesse, d. h. diese beschreiben Zuständigkeiten und Verfahren zur Durchführung eines in der Regel umfangreichen Arbeitsablaufes, beispielsweise zur Verladung, Herstellung des Produktes XY, Instandhaltung etc.

Es ist sinnvoll, im Rahmen der Erstellung von Verfahrensanweisungen bei der Beschreibung der relevanten Dokumente für die Arbeitsabläufe eines Prozesses auf eine Unterscheidung zwischen Vorgabe- und Nachweisdokumente zurückzugreifen. Diese Unterscheidung trägt zur Klarheit bei. Vorgabedokumente sind z. B. Verfahrens- oder Arbeitsanweisungen oder ein Formblatt, z. B. Checkliste „Anlagenbegehung BE1". Bei den ausgefüllten Formblättern der Checkliste „Anlagenbegehung BE1" handelt es sich um ein Nachweisdokument. Weitere Nachweisdokumente sind z. B. Zeugnisse, Prüfbescheinigungen etc.

Umfang der Darstellung, Detaillierungsgrad und Sprache sind an die Größe und Komplexität des Unternehmens anzupassen.

Bei einem Kleinunternehmen kann der Dokumentationsaufbau zusätzlich zur Unternehmens- / Sicherheitspolitik beispielsweise nur aus zwei Ebenen „Verfahrensanweisungen" und „mit geltende Dokumente" bestehen. Sollte das Kleinunternehmen nur ein SMS implementiert haben, so kann es ggf. auch sinnvoll sein, dass die Dokumentation des SMS Bestandteil im Konzept zur Verhinderung von Störfällen ist. Das Konzept zur Verhinderung von Störfällen stellt dann quasi auch das Managementhandbuch dar.

Im Hinblick auf den angemessenen Umfang von Regelungen wird auf die Bewertungshilfe zur Frage „Wie wird die Resilienz des Betriebsbereiches eingeschätzt?" im Prüfgebiet „SMS: Systematische Überprüfung und Bewertung" verwiesen.

5.1.5 Frage Nr. 5: Wie wird Corporate Governance (Grundsätze der Unternehmensführung) für die Anlagensicherheit im Betriebsbereich eingeschätzt?

Bewertungshilfe:

Corporate Governance für die Anlagen- und Prozesssicherheit kann verstanden werden als die Beteiligung und das Engagement der obersten Leitung von Unternehmen im Hinblick auf die Anlagen- und Prozesssicherheit im Unternehmen. Hierzu gehört die Umsetzung von Anlagen- und Prozesssicherheit in der Unternehmenspolitik / -leitbild aber in auch Unternehmensrichtlinien etc. und in der Unternehmenskultur.

Bei der Bewertung dieser Frage kann auf Antworten zu den folgenden Fragen des SMS-Moduls zurückgegriffen werden (Auswahl):

Prüfgebiet SMS: Konzept zur Verhinderung von Störfällen und Aufbau des SMS

- Wie ist die Qualität der Unternehmenspolitik des Unternehmens im Hinblick auf die Anlagensicherheit zu bewerten?
- Wie wird das Konzept zur Verhinderung von Störfällen bewertet?
- Wie werden die Regelungen zur Überprüfung der Zielsetzung der Sicherheitspolitik bewertet?
- Wie werden die Regelungen zum finanziellen Rahmen für die Anlagensicherheit bewertet?
- Wie werden die Umsetzung der Sicherheitspolitik und der Regelungsumfang von betriebsinternen Sicherheitsvorschriften bewertet?

Prüfgebiet SMS: Systematische Überprüfung und Bewertung

- Wie wird die Vorgehensweise zur systematischen Überprüfung und Bewertung des Konzeptes zur Verhinderung von Störfällen bewertet?
- Wie wird die Vorgehensweise zur systematischen Überprüfung und Bewertung des SMS (Managementreview) bewertet?
- Wie wird die Sicherheitskultur des Betriebsbereiches eingeschätzt?
- Wie wird die Resilienz des Betriebsbereiches eingeschätzt?

Im Rahmen der Corporate Governance (CG) müssen sich die leitenden Führungskräfte über die mit den Aktivitäten ihres Unternehmens verbundenen Risiken im Klaren sein.

Laut dem OECD-Leitfaden „Corporate Governance für die Anlagen- und Prozesssicherheit“ müssen die leitenden Führungskräfte die Störfallrisiken zusammen mit den übrigen Unternehmensrisiken abwägen. Daher muss das Risikomanagement bezüglich der Anlagen- und Prozesssicherheit denselben Stellenwert haben wie andere Geschäftsprozesse einschließlich Finanzverwaltung, Märkte, Investitionsentscheidungen etc.
Bei einer Inspektion ist die oberste Leitung eines Betriebsbereiches (bzw. Mitglied der Geschäftsleitung / Geschäftsführung, welches die Anlagen- und Prozesssicherheit verantwortet) zu diesem Aspekt zu befragen.

Fragen der Inspektor/inn/en an die oberste Leitung des BB können hierbei sein:

- Wo sehen Sie die hauptsächlichen Störfallrisiken in ihrem Betriebsbereich (BB)?
  - Wie sehen Sie die Störfallrisiken im Kontext mit den anderen (welche) Unternehmensrisiken ihres BB?
- Welche Entscheidungen und Maßnahmen haben Sie in ihrem Betriebsbereich getroffen, um Störfälle zu verhindern?
- Wie würden Sie die Sicherheitskultur in Ihrem Betriebsbereich beschreiben?
  - Und im speziellen die Kommunikationskultur Ihres BB?
- Wann haben Sie das letzte Mal an einem Sicherheitsrundgang / Audit / Inspektion oder Ähnlichem in Ihrem Betriebsbereich teilgenommen und was ist Ihnen dabei aufgefallen?
- Wie würden Sie damit umgehen, wenn sich in Ihrem Betriebsbereich ein Störfall ereignet?

Weitere Fragen hierzu für eine vertiefte Bearbeitung finden sich im OECD-Leitfaden „Corporate Governance für die Anlagen- und Prozesssicherheit“ bzw. entsprechend für deutsche Verhältnisse modifiziert im Modul „Fragebogen Corporate Governance (Grundsätze der Unternehmensführung) zur Anlagen- und Prozesssicherheit (CG APS) der Bezirksregierung Arnsberg NRW“.

Bei einer Inspektion können Dokumente wie Geschäftsbericht / Lagebericht / Corporate Governance Bericht des BB eingesehen werden. Hieraus lässt sich ggf. ein Hinweis auf eine Berücksichtigung der Anlagen- und Prozesssicherheit im Rahmen des Corporate Governance entnehmen. Es werden dort Risikofelder und generelle Maßnahmen beschrieben, z. B. unter den Überschriften Unternehmensstruktur, Finanzen, Forschung und Entwicklung, Investitionen, Personal, Nachhaltigkeit, Sicherheit, Umweltschutz, IT-Sicherheit. Aussagen zur Anlagen- und Prozesssicherheit können sich z. B. in den Kapiteln zur Nachhaltigkeit, aber auch Sicherheit oder Umweltschutz finden.
Wenn Indikatoren oder Kennzahlen im Geschäftsbericht / Lagebericht / Corporate Governance Bericht oder ähnlichem aufgeführt werden, ist die Aufführung einer Kennzahl zur Anlagen- und Prozesssicherheit auch ein positiver Hinweis (zu Indikatoren / Kennzahlen siehe auch Bewertungshilfe zur Frage „Wie werden die Regelungen zur Verwendung von Kennzahlen bzw. (Leistungs-) Indikatoren zur Anlagensicherheit bewertet?“ im Kap. SMS: Überwachung der Leistungsfähigkeit des Sicherheitsmanagementsystems).

Weitere Erläuterungen:
Der OECD-Leitfaden „Corporate Governance für die Anlagen- und Prozesssicherheit“ (2013 übersetzte Version des „Corparate Governance for Process Safety, OECD Guidance for Senior Leaders in High Hazard Industries“, Juni 2012) nennt wesentliche Elemente einer Corporate Governance für die Anlagen- und Prozesssicherheit.
Er richtet sich an Leitende Führungskräfte in der (petro-) chemischen Industrie und anderen Industrieunternehmen mit hohem Gefahrenpotenzial, die Entscheidungen mit Einfluss auf die strategische Ausrichtung und Kultur eines Unternehmens treffen können, z. B. Chief Executive Officers (CEO), Präsident/inn/en, Mitglieder des Vorstands / Verwaltungsrats, Geschäftsführung, Direktor/inn/en.

Eine kurze, griffige Definition zum Corporate Governance für die Anlagen- und Prozesssicherheit lässt sich dem OECD-Leitfaden nicht entnehmen.

Corporate Governance wird ins Deutsche übersetzt mit „Grundsätze der Unternehmensführung“ und beinhaltet den Ordnungsrahmen für die Leitung und Überwachung eines Unternehmens. Seit 2002 gibt es in Deutschland den „Deutschen Corporate Governance Kodex“, welcher wesentliche gesetzliche Vorschriften zur Unternehmensführung benennt und anerkannte Standards guter und verantwortungsvoller Unternehmensführung enthält. U. a. sollen Vorstand und Aufsichtsrat eines Unternehmens in einem jährlich zu veröffentlichenden Corporate Governance Bericht über die Corporate Governance ihres Unternehmens berichten. Nach Angaben im „wirtschaftslexikon.gabler.de“ müssen sich aus Sicht von betriebswirtschaftlichen Anforderungen guter Unternehmensführung Regelungen zur Corporate Governance auf die folgenden vier Gestaltungsfelder erstrecken:

a) die Festlegung der übergeordneten Zielsetzung des Unternehmens, die dem Topmanagement eine Handlungsmaxime bietet, um Interessenkonflikte zwischen den Bezugsgruppen im Einzelfall zu bewältigen,
b) die Strukturen, Prozesse und Personen der Unternehmensführung, mit denen diese Zielsetzung erreicht werden soll,
c) die regelmäßige Evaluation der Führungsaktivitäten zur Bestandsaufnahme und kontinuierlichen Verbesserung der Modalitäten der Unternehmensführung sowie
d) die proaktive Unternehmenskommunikation, um durch Herstellung von Transparenz das Vertrauen und damit die letztlich existenznotwendige Unterstützung der relevanten Bezugsgruppen des Unternehmens zu gewinnen und zu festigen.

Der „Deutsche Corporate Governance Kodex“, *Stand 2015,* benennt im Kapitel 4 „Vorstand“ Unterkapitel 4.1 „Aufgaben und Zuständigkeiten“ u.a. folgendes:

> 4.1.3 Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance).
>
> 4.1.4 Der Vorstand sorgt für ein angemessenes Risikomanagement und Risikocontrolling im Unternehmen.

Für das Management von Risiken in Unternehmen / Organisationen gibt es eine internationale Basisnorm, die ISO 31000 "Risk Management – Principles and guidelines".

Der Begriff Risiko umfasst hier „Auswirkungen von Unsicherheit auf Ziele“ und beinhaltet sowohl Chancen als auch Bedrohungen.

Die Anwendung dieser Norm soll Unternehmen bei der Durchführung des Risikomanagements unterstützen, indem im Unternehmen Risiken systematisch identifiziert und bewertet werden und so die Ressourcen eines Unternehmens für den Umgang mit Risiken wirksam eingesetzt werden können. Ein adäquates Risikomanagement liefert einen wichtigen Beitrag, um Unternehmensziele zu erreichen und ist damit Bestandteil einer "guten" Corporate Governance. Die Anlagen- und Prozesssicherheit sollte als Ressource für das Risiko „Störfalle“ Berücksichtigung finden.

Hinweise/Ausführungen zum Begriff ‚Corporate Governance‘ aus dem „wirtschaftslexikon.gabler.de“:

Corporate Governance (CG) bezeichnet den rechtlichen und faktischen Ordnungsrahmen für die Leitung und Überwachung eines Unternehmens. Im Unterschied zur Unternehmensverfassung, die primär die Binnenordnung des Unternehmens betrifft, werden unter dem Stichwort CG auch Fragen der Einbindung des Unternehmens in sein Umfeld adressiert. Unternehmen bilden Orte der Bündelung von Beiträgen verschiedener Akteure bzw. Bezugsgruppen (z. B. Anteilseigner, Gläubiger, Arbeitnehmer und Lieferanten) zur arbeitsteiligen Wertschöpfung unter Leitung eines Topmanagements. Dabei werden die Beziehungen der Bezugsgruppen zum Unternehmen in expliziten oder impliziten Verträgen geregelt. Die Governanceproblematik des Unternehmens lässt sich im Kern darauf zurückführen, dass die geschlossenen Verträge zwangsläufig bis zu einem gewissen Grade unvollständig sind und die diversen Bezugsgruppen (Stakeholder) teils unterschiedliche Interessen verfolgen. Je nach ihren Einflussmöglichkeiten auf das Unternehmensgeschehen können die Akteure somit versuchen, die Unvollständigkeiten der Verträge zu ihren Gunsten - und damit meist zulasten anderer Bezugsgruppen - auszunutzen.

Verträge sind unvollständig, zum einen, da sie sich auf Transaktionen in der Zukunft beziehen und zum anderen nicht alle (komplexen und unvorhersehbaren) Entwicklungen im Austauschverhältnis zwischen den Vertragsparteien im Detail richtig und fair regeln können. Die gegenseitigen Rechte und Pflichten der Vertragsparteien lassen sich daher nur (mehr oder weniger) lückenhaft vertraglich vereinbaren. Alle Stakeholdergruppen können Risiken aus unvollständigen Verträgen ausgesetzt sein, aber sie verfügen jeweils grundsätzlich auch über Optionen, Unvollkommenheiten ihrer Verträge mit dem Unternehmen zu ihren Gunsten zu nutzen. Unvollständigkeit der Verträge und Unterschiedlichkeit der Interessenlagen bieten
den Stakeholdern nach den voranstehenden Überlegungen prinzipiell Gelegenheiten wie auch Motive zu dem opportunistischen Verhalten, im Eigeninteresse Vertragslücken zulasten anderer Bezugsgruppen auszunutzen. Hiermit korrespondierend unterliegen sie zugleich den Risiken des Opportunismus der übrigen Stakeholder. Das Unternehmensgeschehen stellt sich aus dieser Sicht somit als komplexes Geflecht von Austauschbeziehungen zahlreicher Akteure mit Opportunismusoptionen und Opportunismusrisiken dar.

Regelungen zur CG haben grundsätzlich die Aufgabe, durch geeignete rechtliche und faktische Arrangements die Spielräume und Motivationen der Akteure für opportunistisches Verhalten einzuschränken. Sie zielen darauf ab, unter Abwägung der Einbußen durch opportunistisches Verhalten (Opportunismuskosten) und der Aufwendungen für die Regelungen (Regulierungs- bzw. Governancekosten) möglichst günstige (Markt-)Bedingungen für eine produktive Wertschöpfung und faire Wertverteilung zu schaffen.
Regelungen der CG können Spielräume und Motivationen zu opportunistischem Verhalten zwar eindämmen, aber nicht alle denkbaren Konfliktfälle zwischen den Bezugsgruppen vorab lösen. Erforderlich ist daher eine übergeordnete Leitmaxime, die im Einzelfall eine Handlungsorientierung bietet.
Nach geltendem Recht sind Vorstand und Aufsichtsrat zur Wahrung des Unternehmensinteresses verpflichtet. Dabei ergibt sich das Unternehmensinteresse aus der angemessenen Berücksichtigung der diversen Einzelinteressen aller Bezugsgruppen.
Regelungen zur CG können auf drei verschiedenen Regulierungsebenen angesiedelt werden. Zunächst lassen sich gesetzliche Vorschriften und untergesetzliche Governancestandards unterscheiden. Gesetzliche Vorschriften sind das Ergebnis eines parlamentarischen Gesetzge-

bungsverfahrens und für alle Adressaten des betreffenden Gesetzes verbindlich. Untergesetzliche Governancestandards („soft law“) füllen die jeweils geltenden gesetzlichen Vorschriften aus und sollen qua (mehr oder weniger freiwilliger) Selbstbindung der Unternehmen wirksam werden. Innerhalb der Gruppe untergesetzlicher Governancestandards kann nach ihrer Geltungsreichweite zwischen generellen Regelwerken für eine bestimmte, größere Gruppe von Unternehmen (z. B. Kodizes wie der Deutsche Corporate Governance Kodex) und unternehmensindividuellen Leitlinien unterschieden werden.

5.1.6 Frage Nr. 6: Wie werden die Regelungen zum finanziellen Rahmen für die Anlagensicherheit bewertet?

Bewertungshilfe:

Es gibt ein Budget für den Bereich Anlagensicherheit, das ausreichend bemessen ist. Es werden sowohl regelmäßig anfallende Kosten als auch Sonderausgaben (z. B. spez. Investitionen, rasch verfügbare Mittel) berücksichtigt. Kriterien zur ausreichenden Bemessung sind vorhanden, ebenso Regelungen zur Mittelfreigabe. Bei den Regelungen zur Mittelfreigabe sollten nicht ausschließlich Kriterien wie z. B. finanzielle Gewinne vorhanden sein, sondern auch das Kriterium „Verbesserung der Anlagensicherheit“.

5.1.7 Frage Nr. 7: Wie wird die Überprüfung der Dokumentenlenkung des SMS im Betriebsbereich bewertet?

Bewertungshilfe:

Es müssen Regelungen zur Lenkung der Dokumente des (Sicherheits-)Managementsystems im Betriebsbereich vorliegen. Hierbei müssen die folgenden Punkte berücksichtigt werden: Erstellung, Änderung, turnusmäßige Überprüfung von Vorgabedokumenten auf Aktualität (z. B. alle 3 Jahre), Prüfung und Freigabe, Verteilen, Bereitstellen, Stilllegen und Archivieren. Die Verantwortlichkeiten, notwendigen Kompetenzen der beteiligten Beschäftigten und Befugnisse für die o. g. Punkte / Aufgaben sind klar und eindeutig zu regeln. Bei großen Firmen / Organisationen erfolgt dies in der Regel auf der Ebene von Verfahrensanweisungen / Prozessbeschreibungen etc. Bei Kleinstbetrieben kann dies z. B. auch ein Abschnitt im Managementhandbuch sein. Die regelmäßige Überprüfung der Regelungen zur Lenkung von Dokumenten muss sichergestellt sein. Dies kann z. B. im Rahmen des Auditsystems erfolgen.

5.1.8 Frage Nr. 8: Wie ist die Regelung zur Bekanntgabe der Unternehmungspolitik bzw. Sicherheitspolitik im Unternehmen zu bewerten?

Bewertungshilfe:

Die Beschäftigten kennen die Unternehmungspolitik bzw. Sicherheitspolitik. Dies wird durch verschiedene Formen der Weitergabe sichergestellt und auch überprüft. Die Beschäftigten haben jederzeit Zugang zur aktuellen Ausgabe der Grundsatzerklärung, z. B. durch einen Aushang am schwarzen Brett. Hierbei ist erkennbar, dass es sich um die aktuelle Fassung der Grundsatzerklärung handelt. Neue Mitarbeiter/innen bekommen ein Exemplar der Grundsatzerklärung ausgehändigt und Hinweise darauf, wo Sie sich informieren können.
Es gibt Regelungen, wie Fremdfirmenpersonal über die Grundsatzerklärung informiert wird.
Die Verantwortlichkeiten für die verschiedenen Aspekte der Bekanntmachung der Grundsatzerklärung sind festgelegt.

5.1.9 Frage Nr. 9: Wie wird die Einbeziehung der Beschäftigten in die Gestaltung und Umsetzung von Politiken und Regelungen bewertet?

Bewertungshilfe:

Dies ist ein Aspekt der Sicherheits- bzw. Kommunikationskultur (siehe auch Prüfgebiet „SMS: Systematische Überprüfung und Bewertung“). Die Unternehmens- / Sicherheitspolitik und die nachfolgenden Regelungen sind Thema bei regelmäßigen Betriebsbesprechungen, Mitarbeitergesprächen, Audits und dergleichen. Die Konsequenzen bei Nichtbeachtung der Grundsätze / nachfolgenden Regelungen sind festgelegt und es wird Abhilfe geschaffen. Dies ist auch über Hierarchieebenen hinweg möglich. Es gibt ein Vorschlagswesen mit Anreizen für erfolgte Vorschläge (immaterielle, finanzielle).

5.1.10 Frage Nr. 10: Wie werden die Regelungen zur Überprüfung der Zielsetzung der Sicherheitspolitik bewertet?

Bewertungshilfe:

Ziele lassen sich drei Zielebenen (Zielpyramide) zuordnen:

- **normative Ziele (globale Ziele, Leitziele):**

  Z. B. Unternehmenszweck, -politik, Vision oder Leitlinien eines Unternehmens / Organisation: grundsätzliche Ziele, welche Werte und grundlegende Einstellungen des Unternehmens (Unternehmensidentität) festlegen. Bei drei Zielebenen schließen die normativen Ziele Unternehmensziele mit ein. Bei Modellen mit 4 bzw. 5 Zielebenen werden die Unternehmensziele separat nach Vision / Leitbild aufgeführt.

  Langfristiger Zeithorizont, bei Unternehmenspolitik / -leitlinien z. B. 5-10 Jahre, bei Unternehmenszielen z. B. 3-5 Jahre

- **strategische Ziele:**

  Umsetzung der globalen Ziele in umsetzbare Ziele für die nächste Unternehmens- / Organisationsebene: z. B. Kompetenz des Personals im Konzern auf dem Gebiet der Anlagensicherheit erhöhen => in den Betriebsbereichen ein Programm zur Verbesserung der Meldekultur durchführen.

  Mittelfristiger Zeithorizont, 1-3 Jahre

- **operative Ziele (Handlungsziele):**

  Umsetzung der strategischen Ziele in Teilzielen für Funktionseinheiten des Unternehmens, die in der Regel messbar und terminbezogen sind (SMART-Kriterien erfüllen), z. B. Schulungen für die Meldung von Ereignissen durchführen.

  Kurzfristiger Zeithorizont, < 1 Jahr

Ziele sind gut zu überprüfen, wenn sie die SMART-Kriterien (Steuerungsrelevant, Messbar, Ambitioniert, Realistisch, Terminbezogen) erfüllen.

Ist dies aufgrund des vorliegenden Sachverhaltes (noch) nicht möglich, so können Indikatoren zum Einsatz kommen. Indikatoren sind Ersatzgrößen, die mit der relevanten Größe korrelieren und eine Größe / einen Tatbestand näherungsweise abbilden. Zum Thema Kennzahlen / Indikatoren siehe auch Bewertungshilfe zur Frage „Wie werden die Regelungen zur Verwendung von Kennzahlen bzw. (Leistungs-) Indikatoren zur Anlagensicherheit bewertet?“ im Prüfgebiet „SMS: Überwachung der Leistungsfähigkeit des Sicherheitsmanagementsystems“.

Es muss eine Regelung zur regelmäßigen Überprüfung der in der Unternehmenspolitik bzw. Sicherheitspolitik festgelegten Ziele geben, die auch für die Anlagensicherheit gilt.

Dies erfolgt in der Regel im Managementreview - siehe hierzu die Bewertungshilfe zur Frage „Wie wird die Vorgehensweise zur systematischen Überprüfung und Bewertung des SMS (Managementreview) bewertet?“ im Prüfgebiet „SMS: Systematische Überprüfung und Bewertung“.
Wichtig ist, dass der Betreiber des Betriebsbereichs (BB) die generellen Ziele der Anlagensicherheit durch entsprechende Teilziele auf allen Ebenen des BB bis in die Produktionsebene hinein umsetzt. Außerdem ist wichtig, dass der BB seine Ziele ausbalanciert, so dass nicht aufgrund von Produktionsdruck Sicherheit nebensächlich wird.
KAS-Leitfaden Nr. 29: „Es ist zu vermeiden, dass in Managementsystembeschreibungen die Bedeutung von Sicherheitszielen betont, im Alltag jedoch nur Indikatoren für wirtschaftliche Ziele erhoben werden. Auch in die Leistungsbewertung müssen beide Ziele einfließen, so dass die Ausbalancierung der Ziele ermöglicht wird.“

Es gibt festgelegte Zeitpunkte für die Überprüfungen (z. B. regelmäßig alle x Jahre, bei verschiedenen Anlässen) und die Verantwortlichkeiten hierfür sind eindeutig, lückenlos mit einer entsprechenden Entscheidungskompetenz festgelegt. Die Geschäftsführung / der Vorstand ist in das Überprüfungsprozedere eingebunden.

5.1.11 Frage Nr. 11: Wie werden die Umsetzung der Sicherheitspolitik und der Regelungsumfang von betriebsinternen Sicherheitsvorschriften bewertet?

Bewertungshilfe:

Für die Umsetzung existiert eine Systematik (z. B. Risikomanagement, -beurteilung, strukturierter Dokumentenaufbau des SMS) und es wird sichergestellt, dass alle Aspekte der Unternehmenspolitik (Grundsatzerklärung, Vision, Leitlinien etc.) im Hinblick auf die Anlagensicherheit umgesetzt werden. Die Beschäftigten sind mit eingebunden.

Es gibt Festlegungen, wie Änderungen der Grundsatzerklärung in die Sicherheitsrichtlinien einfließen.

Die Verantwortlichkeiten für die o. g. Punkte sind festgelegt.

Die Anlagensicherheit wird auch im Einkauf bzw. bei der Vergabe von Aufträgen an externe Firmen berücksichtigt. Beispielsweise wird der Auftrag an eine externe Firma vergeben, die sicherstellt, dass die Grundsatzerklärung / Sicherheitsrichtlinien des Auftraggebers eingehalten werden, auch wenn sie nicht das preiswerteste Angebot abgibt.

Der Regelungsumfang sollte so gestaltet sein, dass er

- alle Punkte der Grundsatzerklärung abdeckt,
- den Bereich Anlagensicherheit berücksichtigt,
- vom Umfang her für einzelne Beschäftigte handhabbar bleibt,
- für die Beschäftigten verständlich ist,
- vor Ort umsetzbar ist und
- immer auf dem aktuellen Stand ist.

Die Verantwortlichkeiten und Befugnisse für die o. g. Punkte sind klar und eindeutig zu regeln.

Im Hinblick auf den angemessenen Umfang von Regelungen wird auf die Bewertungshilfe zur Frage „Wie wird die Resilienz des Betriebsbereiches eingeschätzt?“ im Prüfgebiet „SMS: Systematische Überprüfung und Bewertung“ verwiesen.

5.2 SMS: Organisation und Personal

Dieses Prüfgebiet enthält die folgenden Fragen:

Frage Nr. 1: Wie sind die Regelungen zur Organisation des Betriebes zu bewerten?

Frage Nr. 2: Wie ist die Festlegung der Verantwortlichkeiten für die Anlagensicherheit zu bewerten?

Frage Nr. 3: Wie ist der Prozess zur Auswahl und Einsatz von geeignetem Personal zu bewerten?

Frage Nr. 4: Wie sind die Regelungen zur Gewährleistung einer ausreichenden personellen Besetzung zu bewerten?

Frage Nr. 5: Wie ist der Prozess zur Einarbeitung und Qualifizierung / Fortbildung von Mitarbeitern und Mitarbeiterinnen zu bewerten?

Frage Nr. 6: Wie wird der Prozess zum Wissensmanagement bewertet?

Frage Nr. 7: Wie werden die Regelungen zum Informationsfluss im Unternehmen bezüglich (sicherheitsrelevanter) Gesetze, Vorschriften, etc. bewertet?

Frage Nr. 8: Wie werden die Regelungen zum Einsatz von externen Firmen bewertet?

Frage Nr. 9: Wie werden die Regelungen zum Umgang mit externen Firmen bewertet?

Frage Nr. 10: Wie werden Maßnahmen zur Sensibilisierung der Beschäftigten für die Notwendigkeit ständiger Verbesserungen bewertet?

Frage Nr. 11: Wie ist die Präsenz der für Sicherheitsbelange Verantwortlichen vor Ort zu bewerten?

Frage Nr. 12: Wie werden die Regelungen zum Einsatz von Sicherheitsgremien bewertet?

5.2.1 Frage Nr. 1: Wie sind die Regelungen zur Organisation des Betriebes zu bewerten?

Bewertungshilfe:

Die Organisation eines Unternehmens hat die Aufgabe, einen Rahmen zu schaffen, innerhalb dessen Ziele erreicht werden, indem Anordnungen getroffen und Aufgaben arbeitsteilig erfüllt werden können. Das Ergebnis sind Organisationsstrukturen, die in Aufbau- und Ablauforganisation unterschieden werden können.

Die **Aufbauorganisation** eines Unternehmens stellt das hierarchische Gefüge von organisatorischen Einheiten (Abteilungen, Stellen) des Unternehmens mit deren Aufgaben und Kommunikationsbeziehungen dar. Grafisch kann die Aufbauorganisation als Organigramm dargestellt werden. Wichtig bei der Definition der Stellen ist es, dass eine adäquate Zuordnung zwischen Aufgaben und Verantwortung und hierfür notwendige Kompetenzen, Befugnisse und Rechten besteht.

Im Gegensatz zur **Aufbauorganisation**, die die organisatorischen Strukturen aufzeigt, regelt die Ablauforganisation die Gestaltung der betrieblichen Abläufe und Prozesse. Die Gestaltung der Arbeitsabläufe geschieht innerhalb der bestehenden Organisationsstruktur.

Es ist eine schriftliche Festlegung der Verantwortlichen, deren Rechte und Pflichten vorhanden, z. B. durch Organigramme, Stellen-, Funktionsbeschreibungen und es erfolgt eine eindeutige Zuordnung von Aufgaben, Funktionen, Zuständigkeiten und Befugnissen bis hinunter auf die Ebene des Anlagenpersonals.
Es liegen vor:

- Organigramme: Ja / Nein

  Bei Ja:
  - Welche?
  - Eindeutige Zuordnung?

Das Beauftragtenwesen (z. B. Immissionsschutz-, Störfallbeauftragte/r) oder werksinterne Einrichtungen (z. B. Werkschutz, Werkfeuerwehr) sind mitberücksichtigt und die Schnittstellen innerhalb der Gesamtorganisation definiert.

Interessenkonflikte aufgrund eines Aufgabenzuschnittes für eine/n Beschäftigte/n (z. B. Störfallbeauftragte und Betriebsleiter/in) sind zu vermeiden. Befugnisse und (zeitliche) Ressourcen werden so verteilt, dass die entsprechende Verantwortung auch wahrgenommen werden kann.
Es wird gewährleistet, dass die Kompetenzen bei den Beschäftigten zur Durchführung der festgelegten Aufgaben vorhanden sind. Es gibt ein System bzw. regelmäßige Überprüfungen mit dessen Hilfe Mängel in der Verantwortungs- und Kompetenzzuordnung erkannt und beseitigt werden.
Die Beschäftigten haben die Möglichkeit Kenntnisse über die festgelegten Verantwortlichkeiten aller Beschäftigten zu erlangen.

5.2.2 Frage Nr. 2: Wie ist die Festlegung der Verantwortlichkeiten für die Anlagensicherheit zu bewerten?

Bewertungshilfe:

Die Verantwortlichkeiten im Bereich Anlagensicherheit sind eindeutig geregelt (einschließlich Vertretung) und schriftlich festgehalten.

Die Aufgabenzuordnung bezogen auf die verantwortliche Person ist angemessen und es gibt Kriterien anhand derer diese bestimmt wird. Gegebenenfalls gibt es eine Pflichtenübertragung in der hierarchischen Linie bis auf die Ebene des Bedienpersonals.

Die Aufgaben sind schriftlich übertragen unter Angabe

- der übertragenden Pflichten
- der Befugnisse
- den Namen des/der Verpflichteten

sowie der Unterschrift des Arbeitgebenden und des/der Verpflichteten.

5.2.3 Frage Nr. 3: Wie ist der Prozess zur Auswahl und Einsatz von geeignetem Personal zu bewerten?

Bewertungshilfe:

Der Prozess zur Auswahl und Einsatz von geeignetem Personal (Personalplanung) ist schriftlich festgelegt. Hierin sind folgende Aspekte zu berücksichtigen:

- Verantwortliche für die Auswahl geeigneten Personals sind festgelegt und benannt (evt. Gremien),
- Ablauf des Prozesses unter besonderer Berücksichtigung der Schnittstellen zwischen Personal- und Fachabteilungen,
- es gibt festgelegte Kriterien, nach denen die Auswahl erfolgt, z. B. notwendige Ausbildung, Berufserfahrung, soziale Kompetenz im Hinblick auf die auszuübende Tätigkeit, Verantwortlichkeit. Für die auszuübende Tätigkeit, Verantwortlichkeit liegen z. B. Stellenbeschreibungen und/oder Funktionsbeschreibungen vor,
- die Kriterien berücksichtigen fachliche Anforderungen und auch Anforderungen im Hinblick auf die Sicherheitstechnik, Arbeitsschutz und Human Faktor („Human Factors“ beziehen sich auf Faktoren aus der Umwelt, der Organisation und der Arbeit wie auch auf menschliche oder individuelle Charakteristika, die einen sicherheits- und gesundheitsrelevanten Einfluss auf das Arbeitsverhalten haben (Health and Safety Executes (HSE), UK, 1999)).

Besonderes Augenmerk ist auf die Regelungen für den Einsatz geeigneten Personals, dass für Sicherheitsbelange tätig bzw. verantwortlich zu legen, insbesondere im Hinblick auf die Anforderungen der Tätigkeit/Verantwortlichkeit.

Der Prozess „Personalplanung“ ist in Form einer Verfahrensbeschreibung / Prozessbeschreibung / Managementanweisung etc. schriftlich festgelegt und dokumentiert, welche üblicherweise einen folgenden Aufbau aufweist:

- Ziele,
- Anwendungsbereich,
- Definition der Begrifflichkeiten,
- Beschreibung der Prozessschritte und Ablauf,
- Festlegung der Inhalte der Prozessschritte und Aufgaben,
- Festlegung von Zuständigkeiten und Verantwortlichkeiten zu den Aufgaben,
- Berücksichtigung zu den Schnittstellen anderer Prozesse,
- Festlegung von Dokumentationsinhalten bei den Prozessschritten.

Die obigen Gesichtspunkte gelten für mittelständische und Großunternehmen, die über eine Abteilung / Bereich für Personalangelegenheiten verfügen. Kleinunternehmen, mit z. B. drei Führungskräften bestehend aus Inhaber/in, Betriebsingenieur/in und Meister/innen müssen ihre Vorgehensweise und Kriterien schriftlich niedergelegt haben, z. B. in einem Kapitel des Managementhandbuchs unter Berücksichtigung der Anforderungen der Störfallverordnung.

Es müssen regelmäßige Überprüfungen erfolgen, ob die festgelegten Inhalte für den Prozess Personalplanung (u. a. Kriterien, Ablauf, Verantwortlichkeiten) angemessen sind, z. B. im Rahmen von Audits.

5.2.4 Frage Nr. 4: Wie sind die Regelungen zur Gewährleistung einer ausreichenden personellen Besetzung zu bewerten?

Bewertungshilfe:

Ausreichend viele Mitarbeiter und Mitarbeiterinnen sind entsprechend ihren Fähigkeiten im Einsatz, so dass die anstehenden Aufgaben problemlos bewältigt werden können. Besteht der Arbeitsbereich Anlagensicherheit z. B. aufgrund der Betriebsgröße nur aus einer Person, so sollte diese die Möglichkeit haben, auf entsprechend unterwiesene Beschäftigte aus anderen Bereichen des Betriebes oder auf Fremdfirmen zurückgreifen zu können. Kriterien (z. B. Arbeitsablaufzeiterfassung, gewachsene Personalstärke, Mindestpersonalstärkebesetzung) zur Personalstärkefestlegung existieren und werden berücksichtigt. Faktoren wie nicht bestimmungsgemäßer Betrieb, Übergabezeiten, Krankheit, Urlaub werden bei der Personalstärkefestlegung berücksichtigt. Es sind Folgeregelungen festgelegt für den Fall, dass eine Mindestpersonalstärkebesetzung nicht erreicht wird (Personalaustausch, Abfahren von Teilen des Betriebsbereiches).

5.2.5 Frage Nr. 5: Wie ist der Prozess zur Einarbeitung und Qualifizierung / Fortbildung von Mitarbeitern und Mitarbeiterinnen zu bewerten?

Bewertungshilfe:

Der Prozess zur Einarbeitung und / oder Qualifizierung / Fortbildung im Betriebsbereich ist schriftlich festgelegt. Hierin sind folgende Aspekte zu berücksichtigen:

1. **Ablauf und Zuständigkeiten im Rahmen von Einarbeitungen**
2. **Ablauf und Zuständigkeiten im Rahmen der Fortbildung und Qualifizierung**
3. **Schnittstellen zwischen Personal- und Fachabteilungen**

Ggf. kann die Einarbeitung als eine Form der Qualifizierung behandelt werden.

Die Fortbildung bzw. Qualifizierung von Beschäftigten eines Betriebsbereiches sollte im Rahmen eines Qualifizierungsprozesses erfolgen (KAS-Leitfaden Nr. 20). Angelehnt an den PDCA-Zyklus besteht dieser aus den folgenden Schritten:

➜ **Festlegung von Qualifizierungszielen**

Den Einstieg in den Qualifizierungsprozess bildet die Festlegung von Qualifizierungszielen. Grundlage hierfür ist die Bestimmung von notwendigen Kompetenzen für die Arbeitsstelle/Funktion/Aufgaben (Bedarfsanalyse). Wichtig ist eine genaue, aufgabenbezogene Beschreibung der Zielkompetenzen mit Hilfe überprüfbarer Kriterien (Soll-Feststellung).

➜ **Durchführung von Ist-Analysen**

Erfassung der vorhandenen Kompetenzen der Beschäftigten anhand der festgelegten Kriterien.

➜ **Durchführung von Soll-Ist-Analysen**

Ermittlung der Differenz zwischen den festgelegten Zielkompetenzen und den festgestellten vorhandenen Kompetenzen der Beschäftigten. Ergeben sich keine Defizite, sind keine weiteren Maßnahmen erforderlich.

➜ **Erstellung eines Qualifizierungsplans**

Defizite sind zu spezifizieren und dahingehend zu beurteilen, ob sie durch geeignete Qualifizierungsmaßnahmen ausgeglichen werden können und welche Qualifizierungsmaßnahmen dafür geeignet sind (z. B. Training on the job, Seminare zur Wissensvermittlung, Simulationen, praktische Übungen zur Vermittlung von Fertigkeiten).
Üblicherweise werden Lernzielkataloge erstellt (KAS-Leitfaden Nr. 20 enthält im Anhang II beispielhafte Lernzielkataloge zu den Themen „menschliche Fehler“, „Leistung und Leistungseinschränkungen“ und „Risikowahrnehmung und -einschätzung“). Aus der Gesamtheit aller Maßnahmen für alle betroffenen Beschäftigten ergibt sich der Qualifizierungsplan. Bevor die Qualifizierungsmaßnahmen durchgeführt werden können, müssen geeignete Seminare, Fortbildungsträger, Trainer/innen ausgewählt werden. Dies kann eine Schnittstelle zu einem anderen Prozess (z. B. Einkauf / Beschaffung) im Betriebsbereich sein. Hier ist es wichtig, dass die geeignete Qualität der Qualifizierungsmaßnahmen gewährleistet bleibt.

➜ Qualifizierungsdurchführung

Durchführung der ausgewählten Qualifizierungsmaßnahmen anhand des Qualifizierungsplans.

➜ Qualifizierungsergebnisse

Überprüfung der Effektivität und des Erfolges von Qualifizierungsmaßnahmen. Nach Abschluss der Qualifizierungsmaßnahmen ist erneut eine Erfassung der gegebenen Kompetenzen durchzuführen (diese sollte unabhängig von Trainer und Training erfolgen) – eine erneute Ist-Analyse bei den geschulten Beschäftigten. Abschließend erfolgt ein erneuter Soll – Ist Vergleich, um festzustellen, ob die Zielkompetenzen jetzt in der gewünschten Ausprägung vorhanden sind. Sind die Zielkompetenzen in der erforderlichen Ausprägung vorhanden (keine Soll - Ist Differenz), ist das Qualifizierungsziel erreicht, ansonsten erfolgt ein Rücksprung zur Ableitung besser geeigneter Qualifizierungsmaßnahmen.

➜ Qualifizierungsveränderung

Überprüfung der Qualifizierungsmaßnahmen mit den Qualifizierungsanforderungen. Die Qualifizierungsmaßnahmen sind als solche zu überprüfen: ob sie sich als geeignet erwiesen haben, die angestrebten Qualifizierungsziele zu erreichen. Wenn nicht, sind die Ursachen hierfür zu ermitteln und entsprechende Konsequenzen zu ziehen (z. B. Auswahl anderer Seminare). Sind die Kompetenzen nicht durch Qualifizierungsmaßnahmen herstellbar, sind arbeitsgestalterische (z. B. zur Veränderung der erforderlichen Kompetenzen) oder organisatorische Maßnahmen zur Problemlösung erforderlich. Der Zyklus soll regelmäßig durchlaufen werden, zusätzlich auch anlassbezogen z. B. nach sicherheitsrelevanten Änderungen, die veränderten Kompetenzbedarf nach sich ziehen können. Anlass können ebenfalls Ereignisse (z. B. Beinahe-Unfälle) sein.

Der Prozess „Qualifizierung“ ist in Form einer Verfahrensbeschreibung / Prozessbeschreibung / Managementanweisung etc. schriftlich festgelegt und dokumentiert, welche üblicherweise einen folgenden Aufbau aufweist:

- Ziele,
- Anwendungsbereich,
- Definition der Begrifflichkeiten,
- Beschreibung der Prozessschritte und Ablauf,
- Festlegung der Inhalte der Prozessschritte und Aufgaben,
- Festlegung von Zuständigkeiten und Verantwortlichkeiten zu den Aufgaben,
- Berücksichtigung zu den Schnittstellen anderer Prozesse,
- Festlegung von Dokumentationsinhalten bei den Prozessschritten.

Die obigen Gesichtspunkte gelten für mittelständische und Großunternehmen, die über eine Abteilung / Bereich für Personalangelegenheiten verfügen. Kleinunternehmen müssen ihre Vorgehensweise und Kriterien schriftlich niedergelegt haben, z. B. in einem Kapitel des Managementhandbuchs unter Berücksichtigung der Anforderungen der Störfallverordnung. Es müssen regelmäßige Überprüfungen erfolgen, ob die festgelegten Inhalte für den Prozess Qualifizierung (u. a. Kriterien, Ablauf, Verantwortlichkeiten) angemessen sind, z. B. im Rahmen von Audits.

Zu 1: Einarbeitung

Aspekte bei der Einarbeitung von neu eingestellten Beschäftigten

Zu Beginn erfolgt eine Unterrichtung über die (Unternehmens- und) Sicherheitspolitik bzw. das Konzept zur Verhinderung von Störfällen des Betriebes und es gibt eine Ansprechperson (Tutor/in) für einen definierten Zeitraum für die neu eingestellte Person zur Klärung auftretender Fragen. Der/die Tutor/in bekommt hierfür Zeit und wird von anderen Aufgaben entlastet. Er/Sie muss für diese Aufgabe geeignet sein, dies wird regelmäßig überprüft, z. B. anhand von Beurteilungen durch die Neueingestellten. Es gibt einen firmeninternen Einarbeitungsplan, evt. abgestuft nach den zu übernehmenden Aufgaben. Für den ordnungsgemäßen Ablauf der genannten Punkte gibt es eine verantwortliche Person und es existiert hierzu eine Dokumentation. Aspekte bei der Einarbeitung von Beschäftigten bei Beginn einer neuen Tätigkeit in dem Unternehmen Für die neue Tätigkeit aufgrund von Veränderungen im Aufgabenbereich, bei Einführung neuer Arbeitsmittel oder bei Einführung neuer Technologie existieren Einarbeitungs- oder Qualifizierungspläne entsprechend des obigen Qualifizierungsprozesses.

Zu 2: Fortbildung und Qualifizierung

Aspekte zu den Regelungen für die Weiterbildungen der Beschäftigten

Die finanziellen und zeitlichen Mittel werden bereitgestellt, so dass die Beschäftigten an Seminaren / Lehrgängen / firmeninterne Weiterbildungsangeboten etc. teilnehmen können. Es gibt für jeden Beschäftigten einen Weiterbildungsplan. Es gibt firmeninterne Kriterien (z. B. 1-2 Seminare pro Jahr und Beschäftigte; fachliche, fachübergreifende, soziale Kompetenz vermittelnde Angebote), die bei den Weiterbildungsplänen zugrunde gelegt werden. Es sind die finanziellen und zeitlichen Mittel gegeben, so dass die Beschäftigten für Sicherheitsbelange an auswärtigen Seminaren (VDI, VDE etc.) zum Thema Anlagensicherheit teilnehmen können. Die Teilnahme aller Beschäftigten an den regelmäßigen Weiterbildungen wird sichergestellt. In regelmäßigen Zeitabständen erfolgt eine Abfrage zum Weiterbildungsbedarf bei den Beschäftigten, deren Ergebnis in den Weiterbildungsplänen berücksichtigt wird. Es erfolgt eine Dokumentation der Weiterbildung. Bei Bedarf, z. B. nach Änderungen, Störungen, Unfällen o. ä. an der Anlage, gibt es zusätzliche Veranstaltungen. Die Verantwortlichkeiten und Zuständigkeiten für die o. g. Punkte sind klar und eindeutig geregelt.

5.2.6 Frage Nr. 6: Wie wird der Prozess zum Wissensmanagement bewertet?

Bewertungshilfe:

Wissensmanagement ist das bewusste, gezielte und steuernde Umgehen mit dem Wissen durch ein Unternehmen (Betriebsbereich). Wissen im und des Unternehmens soll transparent, (besser) nutzbar und bewertbar gemacht werden. Daten und Informationen sind Bestandteile von Wissen. Wissen entsteht durch die Verknüpfung von Informationen mit vorhandenem Wissen und beinhaltet Erfahrungen verbunden mit Gefühlen und Empfindungen (z. B. aufgrund gehörter Geräusche auf den Funktionszustand einer Maschine schließen zu können). Wissen benötigt die Fähigkeit, Verknüpfungen oder Ableitungen herstellen und Bewertungen vornehmen zu können. Es wird umgesetzt in Handlungen und dient so dem Erreichen von Zielen, der Bewältigung von Aufgaben und Situationen. Wissen ist an den Menschen gebunden und wird durch Organisation und Technik unterstützt.

Wissen:
Informationen + Erfahrungen + Ableitungen/Verknüpfungen und Bewertungen.

Für die Bewertung des Wissensmanagementprozesses eines Unternehmens / einer Organisation existieren verschiedene Reifegradmodelle.

Im Kontext der Störfallverordnung sollten Angaben im SMS eines Betriebsbereiches zum Wissensmanagement im Hinblick auf „sicherheitsrelevantes“ Wissen vorliegen.
Auf Antworten zu den folgenden Fragen kann dabei zurückgegriffen werden (Auswahl):

Prüfgebiet SMS: Konzept zur Verhinderung von Störfällen und Aufbau des SMS

- Wie wird die Einbeziehung der Beschäftigten in die Gestaltung und Umsetzung von Politiken und Regelungen bewertet?
- Wie ist der Aufbau des Sicherheitsmanagementsystems (SMS) im Betriebsbereich zu bewerten?
- Wie ist die Dokumentation des SMS im Betriebsbereich zu bewerten?
- Wie wird die Überprüfung der Dokumentenlenkung des SMS im Betriebsbereich bewertet?
- Wie werden die Umsetzung der Sicherheitspolitik und der Regelungsumfang von betriebsinternen Sicherheitsvorschriften bewertet?

Prüfgebiet SMS: Organisation und Personal

- Wie ist der Prozess zur Einarbeitung und Qualifizierung / Fortbildung von Mitarbeitern und Mitarbeiterinnen zu bewerten?
- Wie werden die Regelungen zum Informationsfluss im Unternehmen bezüglich (sicherheitsrelevanter) Gesetze, Vorschriften, etc. bewertet?

Prüfgebiet SMS: Überwachung des Betriebs

- Wie werden die Regelungen zum Umgang mit Anweisungen (Arbeits- / Betriebsanweisungen etc.) bewertet?
- Wie werden die Regelungen zur Durchführung von (Sicherheits-) Unterweisungen bewertet?

- Wie werden die Elemente der betrieblichen Kommunikation und ihre Dokumentation bewertet?

Prüfgebiet SMS: Sichere Durchführung von Änderungen und Anlagenneuplanungen

- Wie werden die Regelungen zur Kommunikation bei den verschiedenen Phasen eines Änderungsprozesses bewertet?
- Wie wird die Regelung zur Gewährleistung der Vollständigkeit und Aktualisierung der Betriebsdokumentationen bewertet?

Bei einem hohen Reifegrad für mittelständische und Großunternehmen ist der Prozess zum Wissensmanagement schriftlich festgelegt, z. B. in Verfahrensanweisungen.
Hierin sind folgende Aspekte zu berücksichtigen:

- Ziele, die mit dem Wissensmanagement erreicht werden sollen (strategisches Wissensmanagement),
- Ablauf und Zuständigkeiten des Wissensmanagementprozesses (z. B. Bereiche, beteiligte Personen, Dokumentation, Zusammenhang / Schnittstellen der Prozesse zu Informations-, Wissens-, Kompetenzmanagement),
- Beschreibung der Prozessschritte (Wissen identifizieren, erzeugen, entwickeln, erwerben, verteilen, anwenden, aufbewahren und verfügbar halten; operatives Wissensmanagement),
- Festlegung von Zuständigkeiten / Verantwortlichkeiten zu Aufgaben,
- Berücksichtigung zu den Schnittstellen anderer Prozesse (Aufbau des SMS – Regelungen und Dokumentation, Organisation und Personal - Qualifizierung von Personal, Auditsystem, internes Berichtsystem, Systematische Überprüfung und Bewertung),
- Festlegung von Dokumentationsinhalten bei den Prozessschritten.

Für kleine und mittelständische Unternehmen (KMU) wird auf die Veröffentlichung „Fit für den Wissenswettbewerb -Wissensmanagement in KMU erfolgreich einführen“ des Bundesministerium für Wirtschaft und Technologie hingewiesen.

Hinweise/Begriffe/Modelle im Rahmen des Wissensmanagements:

TOM-Modell:
Die drei Komponenten Technik, Organisation und Mensch bestimmen den Prozess des Wissensmanagements. Technik: Informations- und Kommunikationstechnologien, Organisation: Entwicklung und Umsetzung von Methoden für Wissenserwerb, -speicherung und -transfer, Mensch: Schaffung von Rahmenbedingungen für eine wissens- und lernfreundlichen Unternehmenskultur.

Die Wissenstreppe:
Zeichen (+Syntax =), Daten (+Bedeutung =), Informationen (+Vernetzung =), Wissen (+Anwendungsbezug =), Können (+Wollen =), Handeln (+richtig handeln=), Kompetenz (+Einzigartigkeit =), Wettbewerbsfähigkeit.

Entsprechend der Wissenstreppe können Reifegrade des Wissensmanagements definiert werden (nach Quelle North, 2002):

1. Reifegrad: „IT-Lösungen“: Zeichen, Daten
2. Reifegrad: „Spezielle Einzel-Lösungen“: Zeichen, Daten, Informationen
3. Reifegrad: „Professionelle Wissensorganisation“: Zeichen, Daten, Informationen, Wissen, Können
4. Reifegrad: „Wissensorientierte Unternehmensführung“: Zeichen, Daten, Informationen, Wissen, Können, Handeln, Kompetenz, Einzigartigkeit

Es wird unterschieden in explizites und implizites Wissen, internes und externes sowie individuelles und kollektives Wissen.

Implizites Wissen: unbewusstes (Erfahrungs-)Wissen
Individuelles Wissen: an einzelnen Personen gebundenes Wissen
Kollektives Wissen: Wissen des Betriebes /der Organisation

Ziele im Wissensmanagement sind z. B.
- Implizites in explizites Wissen, individuelles in kollektives Wissen zu überführen,
- Externes Wissen für den Betrieb/Organisation (zeitnah) verfügbar machen und integrieren,

=> Wissen für den Betrieb/Organisation besser nutzbar machen.

5.2.7 Frage Nr. 7: Wie werden die Regelungen zum Informationsfluss im Unternehmen bezüglich (sicherheitsrelevanter) Gesetze, Vorschriften, etc. bewertet?

Bewertungshilfe:

Es gibt eine Struktur innerhalb der geltenden Regelungen für das Unternehmen, z. B. im Hinblick auf ihre Verbindlichkeit. Die ständige Aktualität der Gesetze und Vorschriften sowie betriebsinterner Regelungen ist gewährleistet. Dies kann z. B. geschehen durch abonnierte Fachzeitschriften oder CD-Roms, wobei es sich um zuverlässige Quellen handeln muss. Für den Informationsfluss können Teilnahmen an einschlägigen Gremien und/oder Seminaren sinnvoll sein. Die Zuständigkeit für den Informationsfluss innerhalb des Unternehmens ist eindeutig geregelt, auch die Informationsweitergabe neuer Erkenntnisse auf dem Gebiet der Anlagensicherheit.
Es gibt definierte Elemente im Unternehmen (z. B. Besprechungen, Arbeitskreise, Zielvereinbarungsgespräche, Betriebsrundgänge), die den Informationsfluss im Unternehmen gewährleisten (siehe auch Bewertungshilfe zur Frage „Wie wird der Prozess zum Wissensmanagement bewertet?“ in diesem Prüfgebiet). Betriebsräte sind in den Informationsfluss eingebunden. Diese Elemente sind Bestandteil eines Prozesses zur formalen internen Kommunikation (siehe Bewertungshilfe zur Frage „Wie wird die Kommunikationskultur des Betriebsbereiches eingeschätzt?“ im Prüfgebiet „SMS: Systematische Überprüfung und Bewertung“).

5.2.8 Frage Nr. 8: Wie werden die Regelungen zum Einsatz von externen Firmen bewertet?

Bewertungshilfe:

Regelungen zur Auswahl und zum Einsatz von externen Firmen finden sich häufig in anderen Prozessen des Betriebsbereiches, z. B. „Beschaffung / Einkauf“, „Personalplanung“ etc.

Bei der Auswahl von externen Firmen ist die Berücksichtigung des Sicherheitsaspekts in hohem Maße zu gewährleisten. Hierfür kann es Kriterien geben (z. B. unterschiedliche Anforderungen an die von externen Firmen zu erfüllenden Sicherheitsaspekte bei der Wartung/Instandhaltung an sicherheitstechnisch relevanten Anlagenteilen, Spedition, Arbeiten an Außengebäuden etc.). Die Verantwortlichkeiten sind festzulegen und die Einhaltung von Sicherheitsaspekten ist zu überprüfen.
Kriterien für die Auswahl von Fremdfirmen sind festzulegen, z. B.:

- Ausreichende Qualifikationen (Ausbildung, Berufserfahrung, soziale Kompetenz der Beschäftigten)
- Nachweise (Zertifikate),
- Erfahrungen aus bisherigen Einsätzen,
- Ausstattung mit Arbeitsmitteln und
- Ausreichende personelle Besetzung.

Bei dem Auswahlverfahren von Fremdfirmen und in der Vertragsgestaltung mit Fremdfirmen sind die Belange der Anlagensicherheit in angemessener Weise zu berücksichtigen.

5.2.9 Frage Nr. 9: Wie werden die Regelungen zum Umgang mit externen Firmen bewertet?

Bewertungshilfe:

Regelungen zum Umgang mit externen Firmen finden sich häufig in verschiedenen anderen Prozessen des Betriebsbereiches, z. B. Schulung, Notfallplanung, Freigabe gefährlicher Arbeiten etc. Es ist wichtig, dass die Beschäftigten von externen Firmen jeweils angemessen in diesen Themenbereichen berücksichtigt werden.

Es sind folgende Aspekte zu berücksichtigen:

- **Es muss bekannt sein, welche Personen, einschließlich Beschäftigte von externen Firmen, sich wo im Betriebsbereich befinden. Dies kann z. B. durch ein Meldesystem erfolgen.**
  - **KAS-Leitfaden Nr. 19:**

  Beim Einsatz von Fremdfirmen und deren Subunternehmen ist darzulegen, wie auf Basis definierter Regelungen im SMS die erforderliche Qualifikation des Fremdpersonals sichergestellt wird und wie das Fremdpersonal in das System von Schulungen und Unterweisungen des Unternehmens eingebunden wird. Hierbei sind die Belange der Anlagensicherheit hinreichend zu beachten.
  Im SMS sind Verfahren festzulegen, die die Koordinierung zwischen dem Fremd- und Eigenpersonal (zum Beispiel Freigabeverfahren und Lenkung von Aufzeichnungen), die Verantwortungsbereiche sowie die Überwachung der Arbeiten regeln. Der Betreiber des Betriebsbereichs ist verantwortlich für die Koordination des Einsatzes verschiedener Fremdfirmen (vgl. § 8 ArbSchG, BetrSichV, TRBS 1112). Weiterhin ist anzugeben, wie beim betrieblichen Einsatz eine angemessene Kontrolle der Einhaltung der Sicherheitsvorgaben erfolgt. Es ist darzulegen, wie Beschäftigte von Fremdfirmen Vorschläge und Hinweise mit sicherheitstechnischer Bedeutung beim Auftraggeber einbringen können.

Es muss Regelungen zur Unterweisung von Beschäftigten von externen Firmen geben. So ist es z. B. nicht erforderlich, den Maler, der eine Gebäudewand neu streicht, genauso einzuweisen wie jemanden, der Instandhaltungsarbeiten an einer Anlage durchführt. Die Unterweisung sollte den tätigen Beschäftigten der externen Firmen erteilt werden und nur in Ausnahmefällen dem/der Chef/in der externen Firma allein. Für die Einhaltung der Regelungen sollten die Verantwortlichen der externen Firmen zuständig sein. Es haben Überprüfungen zu erfolgen, ob die Unterweisungen sachgemäß durchgeführt wurden, alle Beschäftigten der externen Firmen erfasst wurden und von ihnen auch verstanden wurden. Die Verantwortlichkeiten hierfür sind festzulegen.
Die Einhaltung von sicherheitsrelevanten Maßnahmen muss auf jeden Fall überprüft werden. Hierfür bietet sich ebenso wie für die Unterweisung ein System an, da Unterschiede (z. B. Maler- und Instandhaltungsarbeiten) bezüglich des Gefahrenpotentials der unterschiedlichen Arbeiten bestehen. Die Verantwortlichkeiten (insbesondere Schnittstellen zu den externen Firmen), Abläufe und Dokumentationen für die Überwachung müssen klar geregelt sein.

5.2.10 Frage Nr. 10: Wie werden Maßnahmen zur Sensibilisierung der Beschäftigten für die Notwendigkeit ständiger Verbesserungen bewertet?

Bewertungshilfe:

Es ist wichtig, dass die Beschäftigten eines Betriebsbereiches für die Notwendigkeit ständiger Verbesserungen sensibilisiert sind, d. h. Aspekte, die zur Verbesserung der Anlagensicherheit beitragen, erkennen, kommunizieren und entsprechend ihrer Befugnisse umsetzen. Dies ist auch Ausdruck einer guten Sicherheitskultur (siehe auch Prüfgebiet „SMS: Systematische Überprüfung und Bewertung“). Die ständigen Verbesserungen umfassen auch das Wahrnehmen von Veränderungen und eine frühzeitige Reaktion hierauf.
Der Betriebsbereich kann hierfür spezielle bewusstseinsfördernde Maßnahmen durchführen, z. B. in Form von Kampagnen zu bestimmten Themen, Mitarbeiterbefragungen o. ä..
Eine Förderung der Sensibilität für die Verbesserung der Anlagensicherheit erfolgt aber insbesondere auch durch die gute Umsetzung von z. B.

- Qualifizierungsmaßnahmen, insbesondere auch Umsetzung von Erkenntnissen aus durchgeführten (Notfall-) Übungen,
- guter betrieblicher Kommunikation,
- betrieblichem Vorschlagswesen,
- internen Berichtssystemen,
- Auditsystemen,
- Managementreviews.

Eine gute Umsetzung der oben genannten Elemente bedeutet, dass der PDCA-Zyklus kontinuierlich und regelmäßig durchlaufen wird.

5.2.11 Frage Nr. 11: Wie ist die Präsenz der für Sicherheitsbelange Verantwortlichen vor Ort zu bewerten?

Bewertungshilfe:

Den für Sicherheit Verantwortlichen steht für die Betreuung der Betriebe vor Ort genügend ihrer Arbeitszeit zur Verfügung (z. B. ca. 50%). Eine Zeitaufschlüsselung für die jeweiligen Aufgaben sollte vorhanden sein. Die für Sicherheit Verantwortlichen sollten eigeninitiativ Begehungen durchführen und nicht erst nach Aufforderung. Eine Präsenz vor Ort bei sicherheitsrelevanten Instandhaltungsarbeiten, Störungen, Reparaturen und dergleichen ist die Regel.

5.2.12 Frage Nr. 12: Wie werden die Regelungen zum Einsatz von Sicherheitsgremien bewertet?

Bewertungshilfe:

Liegt im BB ein dokumentierter Prozess zur formalen internen Kommunikation (siehe Bewertungshilfe zur Frage „Wie wird die Kommunikationskultur des Betriebsbereiches eingeschätzt?“ im Prüfgebiet „SMS: Systematische Überprüfung und Bewertung“) vor, so sollte hier auch der Einsatz von Sicherheitsgremien geregelt sein.

Es gibt Regelungen zur Einberufung von zeitlich begrenzten, übergreifenden Sicherheitsgremien. Hierzu kann sich z. B. eine betriebliche Richtlinie anbieten. Die Verantwortlichkeiten für diese Gremien müssen klar geregelt sein, ebenso Teilnahme an und Ablauf der Gremiensitzungen. Zuständige Verantwortliche kann z. B. die Betriebsleitung der betroffenen Betriebseinheit, jemand aus einer Stabsstelle für Sicherheit oder Beauftragte/r sein. Die Leitung des Gremiums sollte auch für die Einberufung der Mitglieder zuständig sein. Sicherheitsgremien werden in regelmäßigen Abständen, mindestens jedoch nachfolgenden Aktionen eingesetzt:

- Unfällen,
- Beinahe - Unfällen,
- Änderungen an der Anlage,
- Betriebsstörungen, etc.

Die Regelung zum Einsatz von Sicherheitsgremien umfasst auch den Aspekt „Umsetzung der von den Sicherheitsgremien beschlossenen Entscheidungen“. Für die Durchführung der Maßnahmen sollte die Betriebsleitung der betroffenen Betriebseinheit zuständig sein, auf jeden Fall muss die Zuständigkeit klar geregelt sein. Es muss eine Kontrolle der durchgeführten Maßnahmen erfolgen, z. B. durch den/die Betriebsingenieur/in oder durch die Sicherheitsfachkräfte. Zusätzlich sollten stichprobenartige Kontrollen durch an der Maßnahme nicht beteiligte Personen (z. B. Sicherheitsabteilung, Betriebs- oder Bereichsleitung, Mitglieder des Sicherheitsgremiums) erfolgen.

5.3 SMS: Ermittlung und Bewertung der Gefahren von Störfällen

Dieses Prüfgebiet enthält die folgenden Fragen:

Frage Nr. 1: Wie ist der Prozess zur Ermittlung und Bewertung der Gefahren von Störfällen zu bewerten?

Frage Nr. 2: Wie wird der Einsatz der zur Anwendung kommenden systematischen Methoden bewertet?

Frage Nr. 3: Wie wird die Vorgehensweise zur Ermittlung der sicherheitsrelevanten Teile des Betriebsbereiches bewertet?

Frage Nr. 4: Wie wird die Vorgehensweise zur Ermittlung der sicherheitsrelevanten Anlagenteile von den Anlagen des Betriebsbereiches bewertet?

5.3.1 Frage Nr. 1: Wie ist der Prozess zur Ermittlung und Bewertung der Gefahren von Störfällen zu bewerten?

Bewertungshilfe:

Der Prozess zur Ermittlung und Bewertung der Gefahren von Störfällen im Betriebsbereich ist schriftlich festgelegt, z. B. in Verfahrensanweisungen. Hierin sind folgende Aspekte zu berücksichtigen:

- Ziele des Prozesses zur Ermittlung und Bewertung der Gefahren von Störfällen,
- Anwendungsbereiche,
- Definition der Begrifflichkeiten,
- Ablauf und Zuständigkeiten des Prozesses zur Durchführung der Identifizierung und Bewertung von Gefahrenpotentialen (betreffend z. B. die Bereiche beteiligte Personen, Durchführungszeitpunkte, Methoden, Dokumentation, Schlussfolgerungen, Konsequenzen),
- Beschreibung der Prozessschritte,
- Festlegung von Zuständigkeiten/Verantwortlichkeiten zu Aufgaben,
- Berücksichtigung der Schnittstellen zu anderen Prozessen (insbesondere MoC, aber auch z. B. Überwachung des Betriebs (Alarmmanagement), IT-Sicherheit, Auditsystem, internes Berichtsystem),
- Festlegung von Dokumentationsinhalten bei den Prozessschritten.

Die obigen Gesichtspunkte gelten für mittelständische und Großunternehmen.

Kleinunternehmen müssen ihre Vorgehensweise und Kriterien unter Berücksichtigung der Anforderungen der Störfallverordnung schriftlich niederlegen. Aufgrund der anderen Organisationsstruktur kann dies z. B. in einem Kapitel des Managementhandbuchs erfolgen. Zu beschreibende Aspekte können hier insbesondere die Folgenden sein:

- o Zeitpunkte von Gefahrenanalysen und ihre Grundlage/Durchführung z. B.
  - eigene Durchführung durch den Inhaber mittels der Checkliste <Name, Datum, Quellenangabe> bei den Anlagenteilen <Auflistung>,
  - Erläuterung, wie gewährleistet wird, dass es sich um eine aktuelle Checkliste / Gefahrenanalysenmethode handelt

und/oder

- o Vergabe der Gefahrenanalyse an einen Dienstleister, prinzipiell oder bei Erfüllung bestimmter Kriterien, z. B.
  - einem Gefahrenpotential der Art <Nennung>, besonderer Fachthematik oder besonderes Anlagenteil (z. B. Brandschutzanlage, Kälteanlage), Beteiligung gefährliche Stoffe <Nennung der Namen> oder alle xx Jahre
  - Nennung der Kriterien, die der Dienstleiter erfüllen muss, damit eine angemessene Qualität der im Auftrag durchgeführten Gefahrenanalyse sichergestellt ist)
- o Inhalte der Dokumentation
- o Umgang mit den Ergebnissen aus der Gefahrenanalyse

- o Sicherstellung, dass die notwendigen Maßnahmen, die aus den Ergebnissen der Gefahrenanalysen abgeleitet worden, auch umgesetzt werden (z. B. Werkzeuge: To-Do-Liste mit Statusanzeigen, ausgefüllte Formblätter)

Für alle Betriebsbereiche gilt der Aspekt, dass regelmäßig eine Überprüfung erfolgt, ob der festgelegte Ablauf und die Verantwortlichkeiten für den Prozess zur Ermittlung und Bewertung der Gefahren von Störfällen angemessen sind, z. B. im Rahmen von Audits.

Hinweise zu den oben genannten Punkten z.B. einer Verfahrensanweisung:

Es ist festgelegt, wer für die Auswahl der zu beteiligenden Personen verantwortlich ist. Für die Auswahl der zu beteiligenden Personen stehen Kriterien zur Verfügung, z. B. nach Kenntnissen über

- die Anlage(ntechnik),
- das Verfahren,
- die Stoffe,
- die zur Anwendung kommende Methode,
- IT-Sicherheit,
- spezielle Schutzmaßnahmen (z. B. PLT, Brand-, Explosionsschutz).

Es gibt festgelegte Randbedingungen wann eine Identifizierung und Bewertung von Gefahrenpotentialen erfolgt. Beispielsweise bei

- Verfahrensentwicklung,
- Neuplanung,
- Änderungen an der Anlage (welche),
- Änderungen von Supportstrukturen (z. B. IT-Sicherheit, Werkfeuerwehr etc.) für die Anlage (welche),
- Kauf von Anlagenteilen,
- Betriebsstörungen (welche) / Störfälle,
- Instandhaltungsarbeiten,
- außergewöhnliche Betriebszustände,
- in regelmäßigen Abständen, z. B. alle 10 Jahre.

Die Verantwortlichkeit dafür, dass die Identifizierung und Bewertung von Gefahrenpotentialen zu den festgelegten Zeitpunkten erfolgt, ist festgelegt.

Es gibt festgelegte Kriterien, wann welche Methoden verwendet werden (siehe hierzu auch Antwort der Folgefrage).

Es ist festgelegt, wie mit den aus der Identifizierung und Bewertung von Gefahrenpotentialen abgeleiteten Maßnahmen umgegangen wird. Es sind die Verantwortlichkeiten bestimmt, wer über die Umsetzung der Maßnahmen und in welchem Zeitraum dies geschieht, entscheidet. Die Verantwortlichkeiten für die Durchführung der Maßnahmen sowie für die Überprüfung, ob die Maßnahmen ordnungsgemäß durchgeführt wurden, sind festgelegt.

Es ist geregelt, was von der Identifizierung und Bewertung von Gefahrenpotentialen wie dokumentiert wird. Dies kann z. B. sein:

- An der Identifizierung und Bewertung von Gefahrenpotentialen beteiligte Personen,
- Untersuchungsgegenstand,
- Ergebnisse,
- geschlussfolgerte Maßnahmen,
- Umsetzung der Maßnahmen,
- Überprüfung, ob die Maßnahmen umgesetzt wurden.

Es ist festgelegt, wie lange die Dokumentationen aufbewahrt werden und wer für die Dokumentation verantwortlich ist.

Die Ergebnisse aus den Untersuchungen werden entsprechend ihrer Relevanz veröffentlicht (auch über die Anlage oder den Betrieb hinaus, z. B. Beschäftigte des Betriebes, andere Betreiber, Behörden, Fachpublikum, Öffentlichkeit). Hierfür gibt es Kriterien. Es ist festgelegt, wer über eine Veröffentlichung entscheidet (Inhalt, Umfang, Zeitpunkt, etc.) und wer für die Durchführung der Veröffentlichung verantwortlich ist.

5.3.2 Frage Nr. 2: Wie wird der Einsatz der zur Anwendung kommenden systematischen Methoden bewertet?

Bewertungshilfe:

Es ist festgelegt, welche systematischen Methoden zur Anwendung kommen. Für Groß- und mittelständische Unternehmen ist dies im Rahmen des Prozesses zur Ermittlung und Bewertung der Gefahren von Störfällen schriftlich festgelegt, z. B. in Verfahrensanweisungen.

Systematische Methoden können z. B. sein:

- Checkliste
- PAAG/HAZOP –Verfahren
- Matrix-Methoden (z.B. Zürich-)
- Index-Methoden (z.B. Dow)

Ergänzender Hinweis zu /3/: Die DIN EN 31010 „Risikomanagement – Verfahren zur Risikobeurteilung“ leitet zur Auswahl und Anwendung systematischer Verfahren zur Risikobeurteilung an (ca. 30 Verfahren, z. B. Brainstorming, Prüflisten, HAZOP, Strukturiertes „Was-Wenn“-Verfahren, Fehlzustandsart- und -auswirkungsanalyse (FMEA), Multi-Kriterien-Entscheidungsanalyse (MCDA)).

Es sind Kriterien festgelegt,

- o unter welchen Bedingungen eine Methode zum Einsatz kommt, z. B.
  - verfahrensabhängig,
  - abhängig vom Gefährdungspotential (z. B. wird eine bestimmte Stoffmenge überschritten),
- o zur Bestimmung des Betrachtungsumfangs.

Bei der Untersuchung werden der bestimmungsgemäße und der nicht bestimmungsgemäße Betrieb berücksichtigt.

Es gibt Regelungen, die die Aktualität der zur Anwendung kommenden Methode sicherstellen.

5.3.3 Frage Nr. 3: Wie wird die Vorgehensweise zur Ermittlung der sicherheitsrelevanten Teile des Betriebsbereiches bewertet?

Bewertungshilfe:

Entsprechend der Definition im Bundesimmissionsschutzgesetz ist ein Betriebsbereich der gesamte unter der Aufsicht eines Betreibers stehende Bereich, sobald gefährliche Stoffe nach Anhang I der Störfallverordnung in entsprechender Menge in einer oder mehreren Anlagen des Bereichs einschließlich gemeinsamer oder verbundener Infrastrukturen und Lagerung vorhanden sein können.

Der Betreiber muss die sicherheitsrelevanten Teile seines Betriebsbereiches (SRB) bestimmen: Dies sind die Teile des Betriebsbereiches, die einen Störfall verursachen können, insbesondere auch jene Teile, in denen gefährliche Stoffe nach Anhang I Störfallverordnung vorkommen bzw. vorkommen können.
Wichtiges, aber nicht ausschließliches, Kriterium ist die Menge eines gefährlichen Stoffs. Daneben spielen die Eigenschaften der verwendeten gefährlichen Stoffe und die Bedingungen, unter denen sie gehandhabt oder gelagert werden, eine entscheidende Rolle.

Neben den Anlagen müssen aber auch die Tätigkeiten innerhalb eines Betriebsbereichs betrachtet werden, bei denen die Gefahr eines Störfalls bestehen kann. Diese beiden Systeme („Anlagen“) und Vorgänge („Tätigkeiten“) bilden die sicherheitsrelevanten Teile eines Betriebsbereichs (im Sinne von Anhang II Abschnitt III Nr. 1 der Störfallverordnung).

Tätigkeiten, bei denen die Gefahr eines Störfalls bestehen kann, sind beispielsweise

- innerbetrieblicher Transport,
- Bereitstellung,
- Lagern,
- Be- und Entladen,
- Herstellen von Stoffen durch chemische Umwandlung,
- Umgang mit Stoffen (Mahlen, Mischen, Umfüllen, Abpacken etc.)
- Synthese und Analytik von Stoffen, z. B. in Laboratorien,
- Lackieren,
- Betrieb von Kälteanlagen.

SRB beinhalten in der Regel ein oder mehrere sicherheitsrelevante Anlagenteile (SRA).

5.3.4 Frage Nr. 4: Wie wird die Vorgehensweise zur Ermittlung der sicherheitsrelevanten Anlagenteile von den Anlagen des Betriebsbereiches bewertet?

Bewertungshilfe:

Anlageteile sind sicherheitsrelevant, wenn bei deren Versagen oder Fehlen ein Störfall nicht auszuschließen ist. Dies bedeutet sicherheitsrelevante Anlagenteile (SRA) sind alle Apparate, Maschinen, Systeme, Ausrüstungsteile und Einrichtungen, von deren Auslegung, Beschaffenheit und Funktionsweise in besonderer Weise die Sicherheit der Anlage und die Begrenzung der Störfallauswirkungen abhängen.
Die sicherheitsrelevanten Anlagenteile sind ein Ergebnis einer Gefahrenanalyse.

Die Vorgehensweise zur Bestimmung der sicherheitsrelevanten Anlagenteile eines Betriebsbereiches muss dokumentiert sein und regelmäßig überprüft werden. Dies kann z. B. in einer Verfahrensanweisung „Prozess zur Ermittlung und Bewertung der Gefahren von Störfällen“ erfolgen.

Die sicherheitsrelevanten Anlagenteile werden in der Praxis in zwei Gruppen unterteilt:

a) sicherheitsrelevante Anlagenteile aufgrund ihres Stoffinhaltes

Dies sind Anlagenteile, in denen ein Stoff nach Anhang I Störfall-Verordnung in sicherheitstechnisch relevanter Menge vorhanden sein oder entstehen kann. Welche Menge im Einzelnen sicherheitsrelevant ist, ist abhängig von den Stoffeigenschaften (toxisch, brennbar, explosionsfähig, selbstentzündlich usw.) und von den Anlagen- und Umgebungsbedingungen (verdämmte / unverdämmte Explosion, Lachengröße usw.).

b) sicherheitsrelevante Anlagenteile aufgrund ihrer Schutzfunktion

Dies sind Anlagenteile, die eine Maßnahme zur Lösung einer Schutzaufgabe darstellen, beispielsweise

- Einrichtungen zur Gewährleistung eines sicherheitsrelevanten Massen- oder Energieflusses (z. B. Sicherheitsventile, Kühlsysteme, Stoppersysteme, Fackeln, Notstromaggregate),
- Einrichtungen zum Brand- und Explosionsschutz (z. B. Brandwände, Löschanlagen),
- PLT-Schutzeinrichtungen, *aktualisiert: PLT-Sicherheitseinrichtungen*
- Einrichtungen zur Detektion (z. B. Gaswarnanlage),
- Einrichtungen zur Ableitung, Beseitigung oder Rückhaltung (z. B. Auffangwannen) gefährlicher Stoffe.

Als pragmatisches Vorgehen erfolgt eine Einstufung von SRA aufgrund des Stoffinhaltes in der Praxis im ersten Ansatz anhand von Richtwerten.
Bei Erreichen oder Überschreiten eines Richtwerts liegt ein sicherheitsrelevantes Anlagenteil vor.
Bei Unterschreiten eines Richtwerts ist eine Einzelfallprüfung vorzunehmen.

In dem Bericht “Sicherheitsrelevante Teile eines Betriebsbereiches und Richtwerte für sicherheitsrelevante Anlagenteile (SRA)“ der KAS werden Richtwerte für SRA von 0,5 % und für einige Stoffe bzw. Stoffgruppierungen von 2 % von den in Anhang I Spalte 4 der Störfall-Verordnung aufgeführten Mengen empfohlen und in der Tabelle 1 aufgeführt.

Weitere Hinweise aus der Vollzugshilfe zur Störfall-Verordnung vom März 2004:
Zur Lösung einer Schutzaufgabe sind in der Regel mindestens zwei voneinander unabhängige Schutzmaßnahmen vorzusehen, damit auch bei einem Versagen einer Schutzmaßnahme wenigstens eine wirksame Schutzmaßnahme als Redundanz erhalten bleibt. Dabei sind passive Einrichtungen aktiven vorzuziehen, letztere wiederum organisatorischen Maßnahmen. Hinsichtlich der Klassifizierung von PLT-Einrichtungen, der Ausführung, des Betriebs und der Prüfung von PLT-Schutz- und Schadensbegrenzungseinrichtungen wird auf die VDI/VDE-Richtlinie 2180 verwiesen.

5.4 SMS: Überwachung des Betriebs

Dieses Prüfgebiet enthält die folgenden Fragen:

Frage Nr. 1: Wie werden die Regelungen zur Eintrittskontrolle und zum Schutz von Eingriffen Unbefugter im Betriebsbereich bewertet?

Frage Nr. 2: Wie wird der Prozess zur IT-Sicherheit im Rahmen der Anlagensicherheit bewertet?

Frage Nr. 3: Wie werden die Regelungen zur Kontrolle der betrieblichen Abläufe bewertet?

Frage Nr. 4: Wie werden die Regelungen zur Freigabe von Arbeiten, bei denen gefährliche Situationen entstehen können, bewertet?

Frage Nr. 5: Wie werden die Regelungen zum Umgang mit Anweisungen (Arbeits- / Betriebsanweisungen etc.) bewertet?

Frage Nr. 6: Wie werden die Regelungen zur Durchführung von (Sicherheits-) Unterweisungen bewertet?

Frage Nr. 7: Wie werden die Elemente der betrieblichen Kommunikation und ihre Dokumentation bewertet?

Frage Nr. 8: Wie werden die Regelungen für Schichtwechsel bewertet?

Frage Nr. 9: Wie wird der Prozess „Alarmmanagement“ bewertet?

Frage Nr. 10: Wie wird der Prozess zur Instandhaltung bewertet?

Frage Nr. 11: Wie wird der Prozess zur Gewährleistung der ordnungsgemäßen Durchführung von (wiederkehrenden) Prüfungen bewertet?

Frage Nr. 12: Wie werden Regelungen zur Berücksichtigung von Auswirkungen durch die Alterung von Anlagen und Anlagenteilen bewertet?

Frage Nr. 13: Wie werden die Regelungen zur Beschaffung von Betriebsmitteln und Geräten bewertet?

5.4.1 Frage Nr. 1: Wie werden die Regelungen zur Eintrittskontrolle und zum Schutz von Eingriffen Unbefugter im Betriebsbereich bewertet?

Bewertungshilfe:

Nach § 3 der Störfall-Verordnung hat der Betreiber die nach Art und Ausmaß der möglichen Gefahren erforderlichen Vorkehrungen zu treffen, um Störfälle durch Eingriffe Unbefugter zu verhindern.

Bei Regelungen zu den Maßnahmen gegen Eingriffe Unbefugter und der Eintrittskontrolle ist auf die Einbindung im Sicherheitsmanagementsystem und hier insbesondere auf die Gestaltung zu Schnittstellen, z. B. zu den Prozessen Gefahrenanalyse oder Fortbildung oder Umgang mit externen Firmen oder Planung für Notfälle, zu achten. Im Sicherheitsmanagementsystem muss festgelegt sein, dass die Einhaltung der Regelungen überwacht wird, z. B. von der Betriebsleitung, den Sicherheitsfachkräften, vom Anlagenpersonal. Abweichungen müssen untersucht werden und entsprechende Konsequenzen erfolgen. Die Verantwortlichkeit für die Zuständigkeit und die Überprüfung muss klar definiert sein.

Nach der Vollzugshilfe zur Störfall-Verordnung März 2004 ist ein Unbefugter im Sinne des § 3 der Störfall-Verordnung jede Person, die vorsätzlich Handlungen mit dem Ziel vornimmt, unmittelbar oder mittelbar einen Schaden zu verursachen. Hierbei ist es unerheblich, ob es sich um einen Beschäftigten des Betreibers, einen von ihm Beauftragten oder einen Dritten handelt. Empfehlungen zur Beurteilung, ob Gefahren durch Eingriffe Unbefugter vorliegen, und zur Auswahl geeigneter Schutzmaßnahmen enthält der Leitfaden SFK-GS-38.

Zusätzlicher Hinweis (nicht in /3/ enthalten): Der KAS-51 „Leitfaden Maßnahmen gegen Eingriffe Unbefugter“ (14. November 2019) ist eine grundlegende konzeptionelle und inhaltliche Überarbeitung des SFK-GS-38. Sowohl der KAS-51 als auch der SFK-GS-38 beinhalten das Thema Sicherungsanalyse. Ansonsten liegt der Fokus des KAS-51 auf der IT-Sicherheit. Ein weiteres Element des KAS-51 ist der Schutz vor Drohnenangriffen. Die folgenden Auszüge des SFK-GS-38 werden daher beibehalten.

Hinweis: Der kursive Text ist gegenüber /3/ aktualisiert worden)

Elemente aus dem Leitfaden SFK-GS-38:

Sicherungsrelevante Anlagen sind von den Betreibern unter Einbeziehung der für die innere Sicherheit zuständigen Behörden in besonderem Maße gegen Eingriffe Unbefugter zu sichern. Zur Erreichung dieser Sicherungsziele kommen insbesondere folgende Maßnahmen in Betracht:

- Die Grenzen von Betriebsbereichen (Werkszaun, Tore etc., bei Industrieparks ggf. die gemeinsame Grenze) sind durch technische und organisatorische Maßnahmen so zu sichern, dass Unbefugte ohne Anwendung von Gewalt (z. B. Beschädigung der Werkseinfriedung, *Drohnen,* Angriff auf Kontrollpersonal) oder arglistige Täuschung (z. B. Fälschung von Werksausweisen) nicht eindringen können und ein gewaltsames

Eindringen in angemessener Zeit erkannt wird (z. B. durch *Radar,* Alarmanlagen, Videoüberwachung, Streifengänge etc.).

- Betriebsfremde sollen identifizierbar sein, z. B. durch offenes Tragen von unterscheidbaren Werksausweisen. Besucher und Fremdfirmen sind angemessen zu überwachen. Auf die Schnittstellen zu den Prüfgebieten „SMS: Organisation und Personal“ (Einsatz und Umgang mit externen Firmen) sowie „SMS: Planung für Notfall“ (Bewertungshilfe zur Frage „Wie werden die Regelungen zum Prozess der Notfallplanung bewertet?“) wird hingewiesen.
- Die Anlagen selbst sind so zu sichern, dass ein Störfall ohne interne Kenntnisse und/oder technische Hilfsmittel durch Unbefugte nicht ausgelöst werden kann.

Der Nachweis ausreichender Vorkehrungen insbesondere des Betreibers (der oberen Klasse) gegen Eingriffe Unbefugter sollte im Rahmen einer Sicherungsanalyse erfolgen.

Kas-51 und SFK-GS-38:

Eine Sicherungsanalyse ist die Ermittlung und Bewertung von möglichen Eingriffen Unbefugter und der dadurch möglicherweise ausgelösten Gefahren unter Verwendung von systematischen Methoden. Ihre Erstellung setzt insbesondere Kenntnisse über mögliche Motivationen *(Bedrohungsanalyse)* und Handlungsmöglichkeiten Unbefugter *(Gefahrenanalyse)* voraus. *Im KAS-51 kommt die IT-Risikobeurteilung hinzu - aufgrund der raschen Änderungen im IT-Bereich sowohl im Hinblick auf die Gefährdungen als auch der Umsetzung von Schutzmaßnahmen.*

Dafür entfallen im KAS-51 die Begriffe Gefährdungsanalyse und Sicherungskonzept.

In der Sicherungsanalyse wird die Ermittlung und Beurteilung der spezifischen Gefährdungslage (Gefährdungsanalyse) mit den Ergebnissen der Ermittlung der Gefahrenstellen im Rahmen der im Sicherheitsbericht nach Störfallverordnung ohnehin erforderlichen Gefahrenanalyse zusammengeführt. Die Sicherungsanalyse kann Voraussetzung für die Ableitung von Sicherungszielen und der erforderlichen Sicherungsmaßnahmen im Rahmen der Erstellung eines Sicherungskonzeptes sein. Ihre Dokumentation, regelmäßige Überprüfung und Fortschreibung sowohl bei wesentlichen Änderungen als auch bei besonderem Anlass wird angeraten.

5.4.2 Frage Nr. 2: Wie wird der Prozess zur IT-Sicherheit im Rahmen der Anlagensicherheit bewertet?

Bewertungshilfe:

In Betriebsbereichen kommen zum Messen, Steuern und Regeln von Abläufen IT-Systeme und / oder industrielle Steuerungssysteme, z. B. Prozessleitsysteme zum Einsatz. In der Vergangenheit waren die industriellen Steuerungssysteme von anderen IT-Systemen und Netzen und auch dem Internet entkoppelt. Dies ändert sich zunehmend und damit werden die IT-Sicherheit (IT-Security, Informationssicherheit etc.) bzw. Teile hiervon auch wichtig für die Anlagensicherheit. Die IT-Sicherheitsmaßnahmen in einem Betriebsbereich sollten nicht dazu führen, dass wesentliche Dienste, Funktionen oder gar Notfallprozeduren nicht ausgeführt werden können. Da reine IT-Sicherheitsziele den Schutz der Informationen im Fokus haben, aber nicht unbedingt den von Betriebsmitteln / Anlagen, kann es im ungünstigen Fall ggf. zu Maßnahmen führen, die für die Anlagensicherheit kontraproduktiv sind.
Anderseits dürfen die IT-Sicherheitsmaßnahmen aber auch nicht auf einem so niedrigen Niveau ausgeführt werden, dass die Infrastruktur durch Cyberangriffe verwundbar ist oder gar ungeschützt mit dem Internet verbunden ist. Es ist daher auf eine Kompatibilität der verschiedenen Ziele im Betriebsbereich zu achten.
Die Anforderungen zur IT-Sicherheit sind momentan einem starken Entwicklungs- und Veränderungsprozess unterworfen.

Das IT-Sicherheitsgesetz (Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes - BSI-Gesetz – BSIG vom 14. August 2009) verlangt von Betreibern Kritischer Infrastrukturen die Erfüllung von gesetzlichen Anforderungen. Zu Kritischen Infrastrukturen gehören ab einer gewissen Größe z. B. Raffinerien oder Tankläger.

Im Rahmen einer Inspektion nach Störfallverordnung sind mögliche Schnittstellen zur Anlagensicherheit zu beachten, z.B. wie das PLS einer Anlage im Rahmen des Vorgehensmodells (hier nach VDI 2182 „Informationssicherheit in der industriellen Automatisierung“ Blatt 1) berücksichtigt wird, wie Einflüsse der IT-Sicherheit im Alarmmanagement berücksichtigt werden oder ob Sensoren und Aktoren über Remote Access Einrichtungen (spezifische Geräte-Zugänge, die in der Regel das Internet benutzen) verfügen.

Zusätzliche Hinweise (nicht in /3/ enthalten):
Der Fokus des KAS-51 „Leitfaden Maßnahmen gegen Eingriffe Unbefugter“ liegt auf der IT-Sicherheit und enthält hierzu Ausführungen einschließlich Kontrollfragen, die bei Inspektionen nach § 16 Störfall-Verordnung nachgefragt werden können bzw. den Einstieg in den Themenkomplex vereinfachen sollen.

Die im April 2019 überarbeitete VDI/VDE 2180 (Funktionale Sicherheit in der Prozessindustrie) enthält nun ein eigenes Kapitel zum Umgang mit Cyberphysikalischen Risiken bezogen auf die funktionale Sicherheit (Blatt 1, Kapitel 8). Demnach sind im Management der funktionalen Sicherheit IT-Sicherheitsaspekte in der Planung, der Beschaffung, der Validierung, im Betrieb, bei Änderungen und bei der Außerbetriebnahme zu berücksichtigen. Die Abschätzung der Gefährdungspotentiale soll hierfür durch eine IT-Risikobeurteilung (der PLT-Sicherheitseinrichtungen und PLT-Betriebseinrichtungen) erfolgen und befasst sich inhaltlich mit den Punkten: Hardware, Software, Daten, Verbindungen, Prozesse, Organisationen und Personen.

Definition „Asset“ im Sinne der Richtlinie VDI 2182 Blatt 1: alle materiellen und immateriellen Werte von Automatisierungsgeräten, Automatisierungssystemen, Maschinen oder Produktionsanlagen, die bedroht sein können und die schützenswert sind (z. B. SPS, Rezeptur, technische Schnittstellenfunktionen, Firmware).

Das Vorgehensmodell nach VDI 2182 beinhaltet die folgenden Schritte:

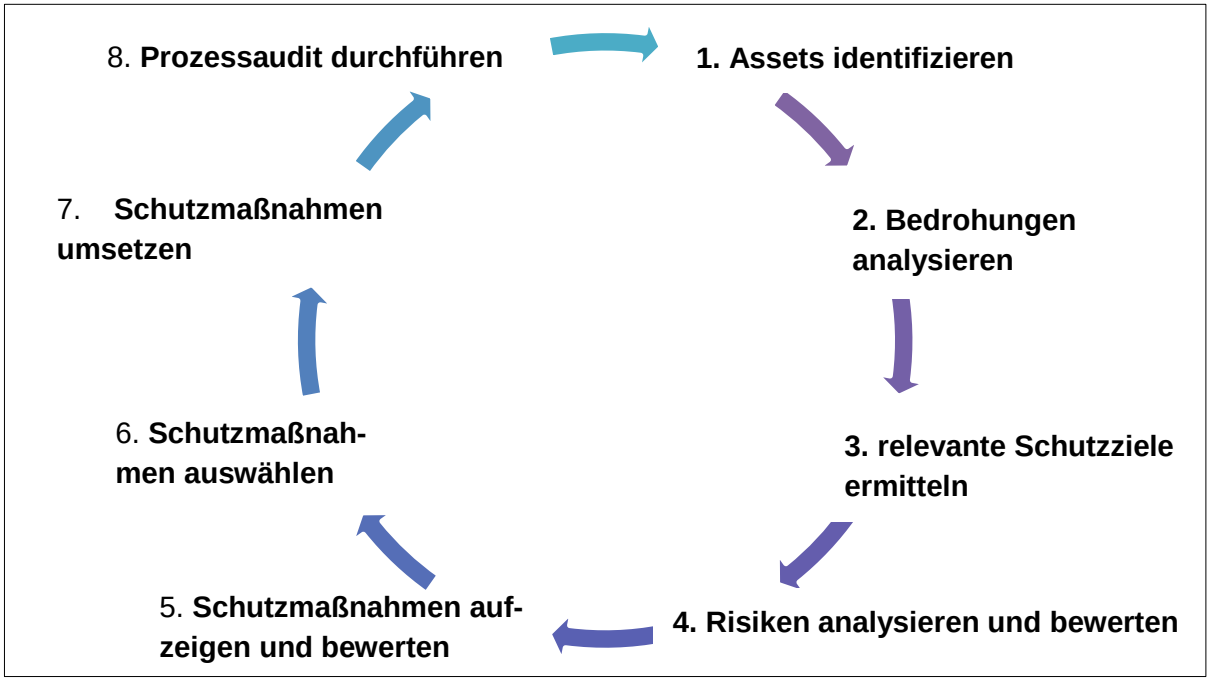

Abb. 27: Vorgehensmodell nach VDI 2182

Im Sinne des kontinuierlichen Verbesserungsprozesses (PDCA-Zyklus) wird nach dem 8. Schritt wieder mit dem Schritt 1 begonnen und der Kreislauf erneut (in regelmäßigen Abständen) durchlaufen.
Für mittelständische und Großunternehmen wird der Prozess zur IT-Sicherheit i. d. R. schriftlich festgelegt sein, z. B. in Verfahrensanweisungen, worin üblicherweise folgende Aspekte zu berücksichtigen sind:

1. Ziele des Prozesses zur IT-Sicherheit,
2. Anwendungsbereiche,
3. Definition der Begrifflichkeiten,
4. Ablauf und Zuständigkeiten des Prozesses zur IT-Sicherheit z. B. entsprechend des Vorgehensmodells nach VDI 2182 (beteiligte Personen, Durchführungszeitpunkte, Bereiche, Methoden, Dokumentation, Schlussfolgerungen, Konsequenzen),
5. Beschreibung der Prozessschritte,
6. Festlegung von Zuständigkeiten / Verantwortlichkeiten zu Aufgaben,
7. Berücksichtigung zu den Schnittstellen anderer Prozesse (z. B. Organisation und Personal (z. B. Fortbildung, Qualifizierung, Wissensmanagement), Überwachung des Betriebs (u. a. Instandhaltung, Alarmmanagement), MoC, Auditsystem, internes Berichtsystem, Notfallmanagement, Managementreview),
8. Festlegung von Dokumentationsinhalten bei den Prozessschritten.

Hinweis zum Vorgehensmodell bzw. den obigen Prozesspunkten Nr. 4 und 5: IT-gestützte Komponenten verfügen über einen sehr schnellen Lebenszyklus (z. B. Aktualität der Softwarekomponenten, für bestimmte Schritte innerhalb des Vorgehensmodells ist ein Zeitzyklus von 1-2 Jahre daher deutlich zu lang). Es sollten regelmäßige Überprüfungen erfolgen, ob der festgelegte Ablauf und die Verantwortlichkeiten für den Prozess IT-Sicherheit angemessen sind, z. B. im Rahmen von Audits.

Hinweis (nicht in /3/ enthalten):
Der KAS-51 „Leitfaden Maßnahmen gegen Eingriffe Unbefugter" enthält im Anhang 2 „IT-Sicherheit" 21 Kontrollfragen zu den folgenden sieben Leitsätzen, die bei Inspektionen zur IT-Sicherheit in Verbindung mit der Anlagensicherheit nachgefragt werden können:

1. *IT-Security ist Führungsaufgabe*
2. *Sensibilisierung und Unterweisung*
3. *Asset Register und Netzwerkarchitektur*
4. *IT-Sicherheit bei der Errichtung von Anlagen*
5. *Reaktion auf neue Schwachstellen und Bedrohungen (im KAS-44 Leitsätze der Kommission für Anlagensicherheit zum Schutz vor cyberphysischen Angriffen: Risikomanagement beim Betrieb von Anlagen)*
6. *Erkennung von IT-Sicherheitsvorfällen*
7. *Maßnahmen nach IT-Sicherheitsvorfällen*

Bei **Inspektionen** können z. B. folgende (kritische) Aspekte in der IT-Sicherheit in Verbindung mit der Anlagensicherheit nachgefragt werden:

- Welche Regelwerke / Richtlinien zur IT-Sicherheit sind dem Unternehmen bekannt?
  - Gibt es eine dokumentierte Vorgehensweise für einen Prozess IT-Sicherheit, z. B. in Form einer Verfahrensanweisung / Prozessbeschreibung?
- Wie ist Kommunikation zwischen Office IT (EDV-Abteilung) und Prozessleittechnik gestaltet?
  - Nehmen Fachleute der IT-Sicherheit an Gefahrenanalysen für die Anlagensicherheit teil?
- Wie ist die Sicherheit der Office IT im Hinblick auf den datentechnischen Austausch mit der Prozessleittechnik zu sehen?
  - Welche Angriffsszenarien sind betrachtet worden?
  - Wird Kryptographie (Verschlüsselung) eingesetzt und wobei?
  - Werden mobile Endgeräte eingesetzt?
- In welcher Form wird Authentication (Ausweisung), Authorization (Befugniserteilung, -management), Accounting (Verwaltung von Rechten bezogen auf die EDV) im Unternehmen / Betriebsbereich / Anlage umgesetzt?
  - Wie (sicher) erfolgt die Anmeldung (Passwörter / Passwortschutz)?
- Wie ist die Schnittstelle zwischen Management of Change (MOC) und IT-Sicherheit gestaltet)?
  - Werden Änderungen im Kontext der EDV (z. B. neue Software oder Updates) oder IT-Geräte vor Umsetzung in ihrer Auswirkung auf die Anlagensicherheit betrachtet?
  - Wie erfolgt die Aktivierung / Deaktivierung von Funktionen bei neuen Geräten?

- Im Hinblick auf die zu inspizierende Anlage:
  - Welche Netzwerke gibt es?
  - Wie sicher sind Firewall, Router und Ports?
  - Werden Virenscanner eingesetzt und wie sicher sind diese (Virenschutz)?
  - Welchen Datenaustausch gibt es?
- Ist bekannt, welche Geräte (auch Aktoren / Sensoren) in der Anlage über Remote-Access-Einrichtungen (spezifische Geräte-Zugänge, die in der Regel das Internet benutzen) verfügen?
  - Wie werden diese verwendet (z. B. zu Wartungszwecken) und wie sind sie (vor Eingriffen Unbefugter) abgesichert?
- Sind die Beschäftigten für die IT-Sicherheit sensibilisiert worden?
  - Gab/gibt es hierzu Fortbildungen / Kampagnen?

Weitere Hinweise/Informationen:

Bei der IT-Sicherheit geht es um die Datensicherheit, d. h. den Schutz der Daten im Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit sowie im Weiteren um die Echtheit (Authenzität), Nichtabstreitbarkeit und Zurechenbarkeit von Daten. Beim Datenschutz dagegen geht es um den Schutz personenbezogener Daten vor dem Missbrauch durch Dritte. Ziele und Methoden für den Datenschutz und der Datensicherheit können übereinstimmen, tun dies aber nicht zwangsläufig. Die IT-Sicherheit ist aber zumeist eine Voraussetzung für den Datenschutz, z. B. durch Zugriffskontrolle. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eine zentrale Stelle für Fragen zur IT-Sicherheit und veröffentlicht neben dem Grundschutz zur IT-Sicherheit auch Informationen, technische Richtlinien und Standards zur IT-Sicherheit.

Laut BSI sind die folgenden Elemente für den Prozess IT-Sicherheit in einer Organisation wichtig:

Die IT-Sicherheit ist in der Unternehmenspolitik verankert, d. h. es gibt ein Grundsatzdokument (z. B. Leitlinie zur Informationssicherheit, Sicherheitsleitlinie etc.) von der obersten Leitung zum Stellenwert, den grundsätzlichen Zielen und Strategien der IT-Sicherheit.

Die Umsetzung des Grundsatzdokuments zur IT-Sicherheit erfolgt durch ein Sicherheitskonzept mit dem Ziel wesentliche Informationen des Unternehmens zu schützen und einen Prozess IT-Sicherheit im Unternehmen.

Wichtige Elemente des Sicherheitskonzeptes nach BSI sind:

- **Strukturanalyse** dient dazu die zu schützenden Objekte (Assets) eines Unternehmens zu bestimmen mittels:
  1. Auflistung wichtiger Informationen, Geschäftsprozesse und Anwendungen,
  2. Netzplan mit eingesetzten IT-Systemen, Kommunikationsverbindungen und Schnittstellen,
  3. die vorhandenen IT-Systeme (Clients, Server, Netzkopplungselemente usw.),
  4. die räumlichen Gegebenheiten (Liegenschaften, Gebäude, Räume).
- **Schutzbedarfsfeststellung**: Bei welchen Objekten / Assets können die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit wie verletzt werden?

- Verletzung der Vertraulichkeit: Können vertrauliche Informationen unberechtigt zur Kenntnis genommen und / oder weitergegeben werden und wie kann dies geschehen (Szenarien)? Verletzung der Integrität: Kann die Korrektheit der Informationen und die Funktionsweise des Systems nicht mehr gegeben sein und wie kann dies geschehen (Szenarien)?
- Verletzung der Verfügbarkeit: Können autorisierte Benutzer/innen am Zugriff auf Informationen behindert werden und wie kann dies geschehen (Szenarien)?

o **Auswahl und Anpassung von Maßnahmen**

Aktualisierte Hinweise, Stand Feb. 2020
(in kursiver Schrift, nicht in /3/ enthalten):

anhand der Bausteine für den IT-Grundschutz sowie der elementaren Gefährdungen für die Informationssicherheit. Die Bausteine sind wie folgt gegliedert:

Bausteine des IT-Grundschutz-Kompendiums 2020	
Prozess-Bausteine	**System-Bausteine**
• *Sicherheitsmanagement (ISMS)*	• *Anwendungen (APP)*
• *Organisation und Personal (ORP)*	• *IT-Systeme (SYS)*
• *Konzepte und Vorgehensweisen (CON)*	• *Industrielle IT (IND)*
• *Betrieb (OPS)*	• *Netze und Kommunikation (NET)*
• *Detektion und Reaktion (DER)*	• *Infrastruktur (INF)*

Abb. 28: Bausteine des IT-Grundschutz-Kompendiums 2020

Die auszuwählenden Maßnahmen müssen den Anforderungen in den einzelnen Bausteinen genügen und werden in Abhängigkeit der im Einzelfall zu ermittelnden Gefährdungen ausgewählt. Die Anforderungen der Prozess- und System-Bausteine werden unterteilt in

- *Basis-Anforderungen, welche zwingend erfüllt werden müssen,*
- *Standard-Anforderungen, welche erfüllt werden sollen und*
- *darüberhinausgehenden Anforderungen bei einem erhöhten Schutzbedarf.*

Stand 2017
Es wird darauf hingewiesen, dass hier teilweise mehr materielle Details enthalten als die Version Stand Feb. 2020.

anhand der IT-Grundschutz-Bausteine – diese sind gegliedert nach Komponenten, Vorgehensweisen und IT-Systemen im Schichtenmodell:

B1: Übergreifende Aspekte
B2: Infrastruktur
B3: IT-Systeme
B4: Netze
B5: Anwendungen

sowie Gefährdungskataloge - diese enthalten die wesentlichen Gefährdungen für die Informationssicherheit z. B. gegliedert nach:

G1 Höhere Gewalt,
G2 Organisatorische Mängel,
G3 Menschliche Fehlhandlungen,
G4 Technisches Versagen,
G5 Vorsätzliche Handlungen
und Maßnahmenkataloge - enthalten Maßnahmen um den möglichen Gefährdungen für die Informationssicherheit zu begegnen, z. B. gegliedert nach:

M1 Infrastruktur,
M2 Organisation,
M3 Personal,
M4 Hard- und Software,
M5 Kommunikation,
M6 Notfallvorsorge.

- Ergänzende Sicherheitsanalyse mit Prüfung, ob ein zusätzlicher Analysebedarf besteht und dies ggf. durch eine Risikoanalyse abdecken, ggf. zusätzliche Maßnahmen vorsehen.
- Nochmalige Überprüfung aller ausgewählten vorgesehenen Maßnahmen und vorhandenen Maßnahmen (= konsolidierte Maßnahmen).

o **Maßnahmen umsetzen**

Die obigen Schritte des Sicherheitskonzeptes werden in regelmäßigen Abständen erneut durchlaufen, um die IT-Sicherheit aufrechtzuhalten. Damit wird auch die Umsetzung von Maßnahmen und deren Wirksamkeit überprüft.

Auf Basis des BSI IT-Grundschutz besteht die Möglichkeit ein Informationssicherheits-Managementsystem (IMIS) nach der ISO 27001 „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen“ zertifizieren zu lassen.

Für schnelle aktuell-sicherheitsgerichtete Informationen zur IT-Sicherheit stellt der BSI auf seinen Internet-Seiten Meldungen des CERT-Bundes zur Verfügung. Der CERT-BUND ermöglicht Unternehmen den Austausch von sicherheitsgerichteten Informationen und stellt einen Warn- und Informationsdienst zur IT-Sicherheit zur Verfügung.

Hinweise zu Regelwerke (Beispiele):

VDI 2182 „Informationssicherheit in der industriellen Automatisierung“:
Blatt 1 Allgemeines Vorgehensmodell
Blatt 2.1 Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Hersteller Speicherprogrammierbare Steuerung (SPS)
Blatt 3.1 Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Hersteller Prozessleitsystem einer LDPE-Anlage
Blatt 3.2 Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Integratoren LDPE-Reaktor
Blatt 3.3 Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Betreiber LDPE-Anlage

BSI (Bundesamt für Sicherheit in der Informationstechnik): IT-Sicherheit Grundschutz, Informationen, technische Richtlinien und Standards zur IT-Sicherheit (z. B. BSI-Standards – Methoden, Verfahren und Prozesse zur Informationssicherheit, IT-Grundschutz-Kompendium, IT-Grundschutz-Kataloge etc.).
Im Zusammenhang mit der Anlagensicherheit ist das ICS-Security-Kompendium hervorzuheben.

DIN ISO/IEC 27000 ff. Informationstechnik – IT-Sicherheitsverfahren –
27000: Informationssicherheits-Managementsysteme - Überblick und Terminologie
27001: Informationssicherheits-Managementsysteme – Anforderungen
27002: Leitfaden für Informationssicherheits-Maßnahmen
27003: Informationssicherheits-Managementsysteme – Leitfaden
27005: Informationssicherheit- Risikomanagement

DIN-IEC 62443 Industrielle Kommunikationsnetzte – IT-Sicherheit für Netze und Systeme ff. (ehemals ISA-IEC 62443 *bzw. ISA 95*)

5.4.3 Frage Nr. 3: Wie werden die Regelungen zur Kontrolle der betrieblichen Abläufe bewertet?

Bewertungshilfe:

Es gibt zwei Ebenen im Hinblick auf die Kontrolle der betrieblichen Abläufe. Zum einen durch die Beschäftigten, die an einem betrieblichen Ablauf beteiligt sind, zum anderen die Kontrolle durch Vorgesetzte oder Beauftragte z. B. im Rahmen von Stabsfunktionen.

Regelmäßige Rundgänge der Beschäftigten durch die Anlage dienen der Erfassung des Betriebszustandes von Anlagenkomponenten und ihres Umfeldes, oftmals dokumentiert in Checklisten oder Protokollen. Abweichungen vom Normalbetrieb sollten von Beschäftigten einschließlich von Fremdfirmen erkannt und gemeldet werden.

Die Kontrolle durch Vorgesetzte dient zur Überprüfung der korrekten Umsetzung von Anweisungen durch die Beschäftigten sowie der Information über den Betriebszustand der Anlage(n). Dies geschieht z. B. durch Rundgänge, das Einsehen von Schichtbüchern, Gespräche mit Mitarbeiter/innen, Kontrolle der Abarbeitung von Alarmmeldungen etc.

Die obigen Punkte können Teil einer Überprüfung sein, ob Inhalte von Unterweisungen durch die Beschäftigten verstanden wurden und eingehalten werden.

Es gibt Regelungen zum Vorgehen, wenn die Inhalte nicht eingehalten werden. Hinsichtlich des Vorgehens bei Verstößen ist es sinnvoll, klar angemessene Konsequenzen für Übertretungen aufzustellen und durchzuführen. Jedoch ist dies in einer angemessenen abgestuften Form zu praktizieren, die es erlaubt, dass ein offenes Betriebsklima herrscht und Vertuschungen nicht nötig sind (Fehlerkultur). Wichtig ist es, die jeweiligen Hintergründe der Verstöße zu betrachten und entsprechende Maßnahmen zu treffen (z. B. bei Sicherheitsmaßnahmen, die den Arbeitsablauf beeinträchtigen, an der Entwicklung von Sicherheitsmaßnahmen zu arbeiten, die den Arbeitsablauf nicht beinträchtigen).

5.4.4 Frage Nr. 4: Wie werden die Regelungen zur Freigabe von Arbeiten, bei denen gefährliche Situationen entstehen können, bewertet?

Bewertungshilfe:

In Betrieben sind Freigabeverfahren schon seit langem gängige Praxis, um Gefahren zu begegnen, die bei besonderen Tätigkeiten (z. B. feuergefährliche Arbeiten, Arbeiten in engen Räumen, Öffnen von Apparaten und Leitungen, Arbeiten in explosionsgefährdeten Bereichen) entstehen können. Folgende Punkte werden u. a. im Freigabeverfahren dargestellt bzw. geregelt:

- Verantwortlichkeiten, Zuständigkeiten, Befugnisse für die jeweiligen Punkte im Ablauf des Freigabeverfahrens,
- Durchzuführende Tätigkeiten (Umfang, Örtlichkeit, Zeitdauer),
- Gefahren (z. B. Körperverletzung, Brand, Freisetzung von gefährlichen Stoffen),
- Schutzmaßnahmen (z. B. Reinigung, Freiheit von gefährlichen Stoffen, besondere Werkzeuge, Persönliche Schutzausrüstung (PSA), Brandwache),
- Kontrolle der Durchführung (z. B. Vier-Augen-Prinzip),
- Abschluss und Abnahme der Arbeiten.

Bei der Regelung des Freigabeverfahrens ist auf die Einbindung im Sicherheitsmanagementsystem und hier insbesondere auf die Gestaltung von Schnittstellen, z. B. zu den Prozessen Gefahrenanalyse, Fortbildung, Umgang mit externen Firmen, MoC, zu achten. Im Sicherheitsmanagementsystem muss festgelegt sein, dass die Einhaltung der Freigaberegelungen überwacht wird, z. B. von der Betriebsleitung, den Sicherheitsfachkräften, vom Anlagenpersonal. Abweichungen müssen untersucht werden und entsprechende Konsequenzen erfolgen. Die Verantwortlichkeit für die Zuständigkeit und die Überprüfung muss klar definiert sein. Entsprechende Regelungen existieren auch für Fremdfirmen.

Eine Verwechslung zwischen gefahrenträchtigen und "normalen" Arbeiten sollte nicht möglich sein. Hier kann der Betreiber auf den Prozess zur Gefahrenanalyse und den Prozess zur Durchführung von Gefährdungsbeurteilungen nach dem Arbeitsschutzgesetz zurückgreifen.

5.4.5 Frage Nr. 5: Wie werden die Regelungen zum Umgang mit Anweisungen (Arbeits- / Betriebsanweisungen etc.) bewertet?

Bewertungshilfe:

Anweisungen sind ein wichtiges Element im SMS um den bestimmungsgemäßen Betrieb zu gewährleisten.
Bei der Erstellung der Anweisungen werden Aspekte der Arbeitssicherheit, des Umweltschutzes und der Anlagensicherheit berücksichtigt. Der Betreiber muss die Vorgehensweise zur Erstellung, Verteilung und Aktualisierung von Anweisungen schriftlich festlegen.

Bei **Kleinunternehmen** kann dies z. B. im Managementhandbuch erfolgen.

Für **mittelständische und Großunternehmen** sollte dies in Form einer Verfahrensbeschreibung / Prozessbeschreibung / Managementanweisung etc. schriftlich festgelegt und dokumentiert sein. Ggf. können sich die festgelegten Vorgehensweisen und Inhalte bei anderen Prozessen finden z. B. interne Kommunikation oder Lenkung von Dokumenten, auf jeden Fall sind Schnittstellen zu anderen Prozessen (z. B. auch Gefahrenanalyse, MoC, Auditsystem) zu berücksichtigen. Es müssen regelmäßige Überprüfungen erfolgen, ob die festgelegten Vorgehensweisen und Inhalte angemessen sind, z.B. im Rahmen von Audits.

Hinweise:
Auf die Betriebssicherheits- und Gefahrstoffverordnung und ihre technischen Regeln wird hingewiesen, z. B. TRGS 555 „Betriebsanweisung und Information der Beschäftigten“ ebenso als Erkenntnisquelle auf die Handlungshilfe zur Erstellung von Arbeitsunterlagen für die Prozessführung (2010, Lafrenz, Nickel, Nachreiner).

- Es ist zu definieren, wer bei der Erstellung von Anweisungen beteiligt ist, sinnvoll ist eine Beteiligung der betroffenen Beschäftigten.
- Die Anweisungen müssen zielführend, verständlich und einhaltbar sein.
- Relevante Ergebnisse aus dem Prozess Ermittlung und Bewertung der Gefahren von Störfällen sind zu berücksichtigen.
- Es erfolgt eine Kontrolle der Anweisungen, bevor diese in Kraft gesetzt werden.
- Die Aktualität der Anweisungen muss gewährleistet sein. Hierzu ist eine klare Verantwortungsregelung nötig. Es sind Kriterien festzulegen, anhand derer eine Aktualisierung erfolgt (turnusgemäß (z. B. halbjährlich), bei relevanten Änderungen von Prozess-, Betriebs- oder Arbeitsabläufen oder von Rechtsvorschriften und Regelwerk sowie durch das Lernen aus Ereignissen). Überprüfungen, ob die Aktualisierungen durchgeführt werden, sollten mit festgelegten Verantwortlichkeiten und Zeitabläufen gegeben sein – dies kann auch im Rahmen von Audits erfolgen. Regelungen zur Weitergabe der Aktualisierung an betroffene Beschäftigte sind wichtig.
- Die Bekanntheit der jeweils aktuellen Anweisungen muss gewährleistet sein. Dies kann z. B. durch Gespräche oder stichprobenartige Befragungen ermittelt werden.
- Die Anweisungen regeln nicht nur den Normalbetrieb, sondern enthalten auch Angaben über das Verhalten in besonderen Situationen (An- und Abfahren, Instandhaltungsbetrieb, Notsituationen, etc.) und weisen auf mögliche Gefahren und erforderliche Vorsichtsmaßnahmen hin.

- Anweisungen müssen allen unmittelbar und mittelbar betroffenen Beschäftigten zugänglich sein, sowie in ausreichender Zahl vorhanden sein. Anweisungen sollten einfach und verständlich geschrieben sein, zur besseren Verständlichkeit für ausländische Beschäftigte trägt auch die Existenz in verschiedenen Sprachen bei. Sinnvollerweise sind Anweisungen in den Sprachen verfügbar, wie es verschiedensprachige Beschäftigte im Unternehmen gibt.

Die Anweisungen können arbeitsplatz-, tätigkeits- und stoffbezogen sein und z. B. Zuständigkeiten und Verantwortlichkeiten benennen, Verfahrensabläufe und verschiedene Betriebsweisen, möglicherweise auftretende Störungen und den sicherheitsgerechten Umgang hiermit und Maßnahmen im Notfall beschreiben und regeln.

Die Anweisungen können folgende Punkte beinhalten / regeln:

- Anwendungsbereich: Arbeitsbereich / Tätigkeit,
- Gefahrstoffbezeichnung, Gefahren für Mensch und Umwelt (H-Sätze),
- Schutzmaßnahmen,
- Verhaltensregeln,
- hygienische Maßnahmen (P-Sätze),
- Verhalten bei Störungen / im Gefahrenfall,
- Erste Hilfe,
- Sachgerechte Entsorgung (bei Unfall, Leck, o. ä.),
- ggf. auch Instandhaltung,
- ggf. Folgen bei Nichtbeachtung.

5.4.6 Frage Nr. 6: Wie werden die Regelungen zur Durchführung von (Sicherheits-) Unterweisungen bewertet?

Bewertungshilfe:

Mit Unterweisungen wird z. B. die Kenntnis der Beschäftigten über Anweisungen (Arbeits- / Betriebsanweisungen regelmäßig aktualisiert und geprobt. Der Betreiber muss die Vorgehensweise zur Durchführung von Unterweisungen schriftlich festlegen. Dies kann z. B. im Prozess zur Einarbeitung und / oder Qualifizierung / Fortbildung erfolgen (siehe Prüfgebiet „SMS: Organisation und Personal“, Bewertungshilfe zur Frage “Wie ist der Prozess zur Einarbeitung und Qualifizierung / Fortbildung von Mitarbeitern und Mitarbeiterinnen zu bewerten?“).
Schnittstellen zu anderen Prozessen sind zu berücksichtigen. Es müssen regelmäßige Überprüfungen erfolgen, ob die festgelegten Vorgehensweisen und Inhalte angemessen sind, z. B. im Rahmen von Audits.
Auf die Unterweisungspflichten nach Arbeitsschutzgesetz und die technische Regel TRGS 555 „Betriebsanweisung und Information der Beschäftigten“ wird hingewiesen.

Hinweise:
Für die Unterweisungen und Trainings gibt es Regelungen, die folgende Punkte berücksichtigen:

- Verantwortlichkeiten (wer wofür)
- Zeitpunkte / -abstände von Unterweisungen (siehe 1)
- Kriterien für die Inhalte (siehe 2)
- welcher Personenkreis ist betroffen
- Sicherstellung der Teilnahme aller betroffenen Beschäftigten (Berücksichtigung z. B. von Schichtbetrieb, krankheits- / urlaubsbedingte Abwesenheit, Beschäftigte von Fremdfirmen)
- Überprüfung des Lernerfolgs (siehe 3)
- Dokumentation von Unterweisungen (Dokumentationsumfang, Aufbewahrungszeit, Verantwortlichkeiten)

Die Inhalte der Regelungen zu Unterweisungen und Trainings werden regelmäßig überprüft, z. B. im Rahmen von Audits.

1) Zeitpunkte / -abstände von Unterweisungen, z. B.:

- Turnusmäßig
- Vor
  - Aufnahme neuer Tätigkeiten
  - Inbetriebnahme neuer / geänderter Anlagen / Einrichtungen / Arbeitsmitteln
  - Änderungen von Prozess-, Betriebs-, Arbeitsabläufen
  - relevant geänderten Anweisungen
  - Einsatz neuer Stoffe / Betriebsmittel
  - Großabstellungen / Stilllegungen
- Nach
  - Unfällen, Ereignissen (Brand, Explosion, Stofffreisetzungen), Störfällen
  - Neue Erkenntnisse, z. B. durch Beinahe-Ereignisse

2) Zu Kriterien für die Inhalte

Bei den Unterweisungen soll auf die Gefahren, deren Ursachen und die entsprechenden Maßnahmen (technisch, organisatorisch, menschlich) eingegangen werden. Bestandteil von Unterweisungen sind auch die Inhalte von Anweisungen. Abweichungen vom Normalbetrieb sollen von den Beschäftigten einschließlich von Fremdfirmen erkannt und gemeldet werden. Zusätzlich zu Unterweisungen können auch Trainingsmaßnahmen erforderlich sein, um die Aneignung notwendiger Kompetenzen zu unterstützen.

3) Zur Überprüfung des Lernerfolgs

Für die Schulungen gilt, dass kleine Gruppen einen effizienteren Lernerfolg haben als große Gruppen. Der Lernerfolg wird überprüft, z. B. durch Inszenierung eines hypothetischen Störfalls, der dann von einer kleinen Gruppe "bearbeitet" werden kann. Es bieten sich aber auch Nachfragen oder schriftliche oder mündliche Tests an.

5.4.7 Frage Nr. 7: Wie werden die Elemente der betrieblichen Kommunikation und ihre Dokumentation bewertet?

Bewertungshilfe:

Ein wichtiges Element für den sicheren Betrieb ist die Kommunikation zwischen den Beschäftigten. Förderlich ist ein kooperativer Umgang der Beschäftigten miteinander, auf allen Hierarchieebenen und zwischen den Hierarchieebenen.

Wichtig ist eine Zusammenarbeit, die einen offenen und klaren Umgang mit Fehlern ermöglicht und zwar für Beschäftigte auf allen Hierarchieebenen. Die Beschäftigten werden ermutigt, aufgetretene Störungen, vermutete Gefährdungen, Beinaheunfälle etc. zu melden und Fehler als Chance für Verbesserungen, Lerneffekte und Weiterentwicklung zu verstehen werden. Es muss aber auch deutlich sein, dass bei mutwilligen Verstößen klare, angemessene Konsequenzen erfolgen.

Führung ist effizient, wenn Führungsverhalten, Führungserwartungen und Aufgabenerfordernis aneinander angepasst sind, d. h. Beziehungspflege, soziale Distanz, Entscheidungsautonomie, Verbindlichkeit von Planungen und Kommunikationsstil so ablaufen wie erwartet. Für eine gute betriebliche Kommunikation ist auch die Leitungs- oder Führungsspanne wichtig, d. h. die Zahl der einer Führungskraft untergeordneten Beschäftigten. Die Führungsspanne muss von der Organisation angemessen festgelegt werden und wird beispielsweise durch folgende Faktoren beeinflusst:

- Komplexität der Aufgaben,
- Interdependenz (wechselseitige Abhängigkeit) der Aufgaben,
- Gleichartigkeit der Aufgaben,
- Technologie,
- Kommunikationssystem,
- Qualifikation der Führungskräfte,
- Qualifikation der untergeordneten Beschäftigten,
- Komplexität und Hierarchieaufbau des Unternehmens.

Die Kommunikation zwischen den Beschäftigten unterscheidet sich in formellen Teil und in einen informellen Teil. Beide sind wichtig für die Leistung eines Betriebes.

Die **formelle Kommunikation** soll einen reibungslosen innerbetrieblichen Kommunikationsfluss gewährleisten, ist meist dauerhaft und personenunabhängig organisiert und in wesentlichen Teilen dokumentiert. Mittel der formellen internen Kommunikation können beispielsweise Rundschreiben (ggf. standardisierte Verteilerlisten), Veranstaltungen (z. B. Betriebsversammlung), Mitarbeiterzeitschrift, Management-Informationsbriefe, Mitarbeitergespräche, Schwarzes Brett etc. sein. Ergänzt oder auch abgelöst durch elektronische Kommunikationsmittel wie E-Mail, Intranet, Foren, Online-Newsletter etc.. Aber auch Dokumente von Managementsystemen sind teilweise Elemente der formellen Kommunikation. Neben dem allgemeinen Informationenfluss kann bei einer Überprüfung nach Störfallverordnung der Fokus auf Aspekte der Anlagensicherheit gelegt werden.

Im Folgenden eine beispielhafte Aufzählung von Elementen der Kommunikation in Betriebsbereichen:

- Informationsweitergabe in der Linienorganisation (Besprechungen, Protokolle),
- Dokumentation beim Schichtwechsel (Übergabeprotokolle, Betriebsbücher etc.),
- Meldungen von Ereignissen / Störungen / Abweichungen vom Normalbetrieb / Unsichere Zustände,
- Betriebs- / Arbeitsanweisungen,
- Unterweisungen (z. B. Inhalte, im Rahmen zu erwartenden Änderungen),
- Betriebliches Vorschlagswesen (Einreichung, Auswertung und Umsetzung von Verbesserungsvorschlägen),
- Gremien (Tagesordnungen, Protokolle).

Regelmäßige Überprüfungen des Informationsflusses und Vorgehensweisen der formellen Kommunikation sind sinnvoll. Dies kann im Rahmen des Auditsystems erfolgen.

Ergänzender Hinweis gegenüber /3/: Auf die Bewertungshilfe zur Frage Nr. 4 „Wie wird die Kommunikationskultur des Betriebsbereiches eingeschätzt?“ im Prüfgebiet „SMS: Systematische Überprüfung und Bewertung“ wird hingewiesen.

5.4.8 Frage Nr. 8: Wie werden die Regelungen für Schichtwechsel bewertet?

Bewertungshilfe:

Der Schichtwechsel stellt einen wichtigen Punkt innerhalb des sicheren Betriebes einer Anlage dar. Werden z. B. wichtige Informationen nicht weitergegeben oder befindet sich die Anlage während des Schichtwechsels sogar für einige Minuten unbeaufsichtigt, so kann dies weitreichende Folgen haben.

Der sichere Informationsfluss kann z. B. durch ein Übergabeprotokoll erreicht werden, in das alle wichtigen Daten und Änderungen die Anlage betreffend eingetragen werden sollten. Ein kurzes Gespräch zwischen dem Anlagenpersonal der verschiedenen Schichten ist ebenso von großem Vorteil und sollte für einen sicheren Betriebsablauf, genauso wie das Übergabeprotokoll, vorgeschrieben sein.

5.4.9 Frage Nr. 9: Wie wird der Prozess „Alarmmanagement“ bewertet?

Bewertungshilfe:

Als Alarmmanagement kann das systematische Management von Alarmen in einem Prozessleitsystem bezeichnet werden, um Zuverlässigkeit, Rentabilität und Sicherheit von produktionstechnischen Einrichtungen zu gewährleisten.

Ein Prozess „Alarmmanagement“ soll sicherstellen, dass das Alarmsystem richtig implementiert, eingeführt, betrieben, instandgehalten und überwacht wird.

Betriebsbereiche, die über keine Leitwarte verfügen und in denen nur singuläre Alarme, z. B. im Rahmen einer Gaswarn- oder Brandmeldeanlage, vorkommen können (z. B. Gefahrstofflager, Biogasanlage), sind von den folgenden Ausführungen zum Prozess „Alarmmanagement“ ausgenommen.

Der Prozess „Alarmmanagement“ sollte in Form einer Verfahrensbeschreibung / Prozessbeschreibung / Managementanweisung etc. schriftlich festgelegt und dokumentiert sein, in welcher die folgenden Punkte berücksichtigt werden:

- Ziele, die mit dem Prozess „Alarmmanagement“ umgesetzt und erreicht werden sollen (z. B. Hohe Funktionalität, Effektivität des Alarmsystems, Optimale Steuerung der Anlagen),
- Anwendungsbereich (z. B. Organisationseinheiten des Betriebsbereiches, Anlagen),
- Definition der Begrifflichkeiten (insbesondere die Begriffe Alarm / Meldung, Sicherheitsrelevante Alarme),
- Beschreibung der Prozessschritte und Ablauf des Alarmmanagements,
- Festlegung der Inhalte der Prozessschritte und Aufgaben,
- Festlegung von Zuständigkeiten und Verantwortlichkeiten zu den Aufgaben,
- Berücksichtigung zu den Schnittstellen anderer Prozesse (z. B. Gefahrenanalyse, MoC, internes Berichtsystem, Notfallplanung, Auditsystem),
- Festlegung von Dokumentationsinhalten bei den Prozessschritten.

Innerhalb des Prozesses „Alarmmanagement“ ist das Anlagen- / Leitwartenpersonal angemessen zu beteiligen, aber auch im Rahmen der Erstellung der VA „Alarmmanagement“.

Aus der VDI/VDE 3699 Blatt 5 „Prozessführung mit Bildschirmen Alarme / Meldungen“ vom September 2014 stammen die folgenden Ausführungen (in Anlehnung an EEMUA No 191 und NAMUR NE 102):

Ein Alarm ist eine Meldung, die eine unverzügliche Reaktion des/r Operator/s/in erfordert zur Abwendung von Gefahrensituationen (Frühwarnsystem zur Vermeidung von Notabschaltungen) und / oder ökonomischen Schäden (Produktqualität und / oder -quantität).

Die Reaktion auf einen Alarm kann z. B. sein:

- Bedieneingriff
- Erhöhte Aufmerksamkeit (bei der Prozessüberwachung)
- Veranlassen weiterer Untersuchungen

Ein Alarm muss folgende Eigenschaften besitzen:

- **relevant,**
- **eindeutig,**
- **zeitgerecht,**
- **priorisiert,**
- **verständlich,**
- **diagnostisch,**
- **hinweisend** (Ein Alarm hilft die notwendige Handlung zu finden),
- **fokussierend** (Ein Alarm lenkt die Aufmerksamkeit auf die wichtigen Punkte).

Bei den Prozessschritten sind auch folgende Punkte zu berücksichtigen:

- o Ergonomie,
- o Festlegung von Kriterien, die ein Alarmsystem erfüllen soll, z. B. Alarmraten
  - (Maximal ein Alarm / 10 min im Normalbetrieb,
  - Maximal zehn Alarme / 10 min im Störungsfall),
- o Alarmgestaltung,
- o Sicherheitsrelevante Alarme beinhalten insbesondere auch die Alarme der *aktualisiert: PLT-Sicherheitseinrichtungen (*PLT-Schutzeinrichtungen*)* im Sinne der VDI/VDE 2180,
- o Beteiligung von Leitwartenpersonal bei den einzelnen Prozessschritten, Umsetzung von Feedback,
- o Besonderheiten, wie An- und Abfahrvorgänge,
- o Auswertung der Historie, Abgleich Ist-Zustand mit den Kriterien,
- o Sicherstellung der Aktualität des zugrunde gelegten technischen Regelwerks.

Für alle Betriebsbereiche gilt der Aspekt, dass regelmäßige eine Überprüfung erfolgt, ob der festgelegte Ablauf und die Verantwortlichkeiten für den Prozess Alarmmanagement angemessen sind, z. B. im Rahmen von Audits.

Für eine vertiefte Bearbeitung des Alarmmanagements wird auf die Fragenliste „Alarmmanagement“ des LANUV NRW Stand April 2015 hingewiesen. Diese Fragenliste sowie weitere Informationen hierzu sind dem LANUV Arbeitsblatt 27 "Leitfaden Alarmmanagement" zu entnehmen.

5.4.10 Frage Nr. 10: Wie wird der Prozess zur Instandhaltung bewertet?

Bewertungshilfe:

Instandhaltung

Definition nach der TRBS 1112: *(nicht mehr aktuell:* **die** *Ausgabe: März 2019 der TRBS 1112 hat die u.s. Definition der BetrSichV übernommen)*

Kombination aller technischen und administrativen Maßnahmen sowie Maßnahmen des Managements während des Lebenszyklus eines Arbeitsmittels (technischen Einheit einer Anlage) zur Erhaltung des funktionsfähigen Zustandes oder der Rückführung in diesen, sodass es die geforderte Funktion erfüllen kann. Die Begriffe Wartung, Inspektion und Instandsetzung sind Bestandteil des Oberbegriffes Instandhaltung.

Definition nach der BetrSichV:

Instandhaltung ist die Gesamtheit aller Maßnahmen zur Erhaltung des sicheren Zustands oder der Rückführung in diesen. Instandhaltung umfasst insbesondere Inspektion, Wartung und Instandsetzung.

Im Hinblick auf Begriffsdefinitionen im Zusammenhang mit der Instandhaltung wird auf DIN EN 13306 Instandhaltung - Begriffe der Instandhaltung sowie die DIN 31051 Grundlagen der Instandhaltung hingewiesen.

Unter die Instandhaltung fallen auch Verbesserungen, die dazu dienen, die Zuverlässigkeit, Instandhaltbarkeit oder Sicherheit einer technischen Einheit zu erhöhen, z. B. durch die Beseitigung von Schwachstellen. Nicht unter Instandhaltung fällt eine Modifikation einer technischen Einheit dergestalt, dass diese eine geänderte Funktion erfüllen kann, z. B. eine höhere Leistungsfähigkeit etc..

Ein besonderer Bereich der Instandhaltung sind (wiederkehrende) Prüfungen. Ggf. gibt es für die Bereiche Instandhaltung und Prüfung spezifische Regelungen (siehe daher auch Bewertungshilfe zur Frage „Wie wird der Prozess zur Gewährleistung der ordnungsgemäßen Durchführung von wiederkehrenden Prüfungen bewertet?“).
Bei der (wiederkehrenden) Prüfung wird die Sicherheit und Leistungsfähigkeit einer technischen Einheit mittels festgelegter Prüfmethoden überprüft, ohne dass weitergehende Maßnahmen, wie z. B. Reparatur vorgesehen sind. Je nach Prüfmethode sind geeignete Messinstrumente Voraussetzung für die Überprüfung.

In Betrieben ist die Instandhaltung zur Erhaltung der Funktionsfähigkeit von Anlagenteilen schon lange geregelt. U. a. auch aufgrund gesetzlicher Vorgaben, z. B. der Betriebssicherheitsverordnung (BetrSichV) und den zugehörigen Technischen Regeln für Betriebssicherheit, hier insb. die TRBS 1112 Instandhaltung. Auch in der Störfall-Verordnung wird die Wartung und Reparatur explizit angesprochen (§ 6 Ergänzende Anforderungen und § 12 Sonstige Pflichten).

Auf die Einbindung der Regelungen zur Instandhaltung im Sicherheitsmanagementsystem und hier insbesondere auf die Gestaltung zu Schnittstellen, z. B. zu den Prozessen Gefahrenanalyse, Beschaffung, Qualifizierung, Umgang mit externen Firmen, Freigabe gefährlicher Arbeiten, Alarmmanagement, Notfallplanung, Auditsystem ist zu achten. Die bei den verschiedenen Instandhaltungsmaßnahmen zu beteiligenden Stellen und ihre Befugnisse sowie die verantwortlichen Personen sind klar festzulegen. Besondere Beachtung ist den Schnittstellen zu widmen, insbesondere auch bei der Beteiligung von externen Firmen.

Die Regelungen zur Instandhaltung muss der Betreiber schriftlich festlegen. Dies beinhaltet auch eine Bestimmung und Dokumentation der Anlagenteile im Betriebsbereich die der Instandhaltung unterliegen, verbunden mit einer Strategie und Methodik zur Überwachung und Prüfung des Zustands dieser Anlagenteile.

Bei **Kleinunternehmen** kann die Beschreibung des Ablaufes zur Instandhaltung und der Zuständigkeiten z. B. in einem Kapitel des Managementhandbuchs erfolgen.

Für **mittelständische und Großunternehmen** sollte der Prozess Instandhaltung in Form einer Verfahrensbeschreibung / Prozessbeschreibung / Managementanweisung etc. schriftlich festgelegt und dokumentiert sein, in welcher die folgenden Punkte berücksichtigt werden:

- Ziele, die mit dem Prozess umgesetzt und erreicht werden sollen,
- Anwendungsbereich,
- Definition der Begrifflichkeiten,
- Beschreibung der Prozessschritte und Ablauf der Instandhaltung (besonders zu berücksichtigen ist die Zusammenarbeit / Schnittstellen der verschiedenen Beteiligten, z. B. Fachabteilung, Instandhaltung, externe Firmen),
- Festlegung der Inhalte der Prozessschritte und Aufgaben,
- Festlegung von Zuständigkeiten und Verantwortlichkeiten zu den Aufgaben,
- Berücksichtigung zu den Schnittstellen anderer Prozesse (z. B. Beschaffung, Gefahrenanalyse, MoC, Auditsystem),
- Festlegung von Dokumentationsinhalten bei den Prozessschritten.

Es müssen regelmäßige Überprüfungen erfolgen, ob die festgelegten Vorgehensweisen und Inhalte für den Prozess Instandhaltung angemessen sind, z. B. im Rahmen von Audits.
Im Rahmen des Prozesses „Instandhaltung“ sollte insbesondere auf Inbetriebnahmeprozeduren und Abfahrvorgängen ein besonderes Augenmerk liegen.

Hinweise aus der Technische Regel TRBS 1112:

Die TRBS 1112 beschreibt die Vorgehensweise bei der Gefährdungsbeurteilung von Instandhaltungsarbeiten. Sie nennt beispielhafte Maßnahmen, die im Ergebnis der Gefährdungsbeurteilung bei der Durchführung der Instandhaltungsarbeiten zu berücksichtigen sind. Sie ist anzuwenden für

- die Planung und Ausführung von Instandhaltungstätigkeiten,
- Störungssuche,
- Erprobung nach Instandsetzung.

Vor Instandhaltungsmaßnahmen sind mindestens folgende Schritte durchzuführen:

- Art, Umfang und Abfolge der Instandhaltungsmaßnahmen festlegen,

- Gefährdungen ermitteln und beurteilen und die erforderlichen Maßnahmen festlegen,
- vor der Vergabe an Fremdfirmen die Sicherheitsanforderungen sowie Anforderungen an die Qualifikation des Instandhaltungspersonals festlegen.

Wird mit der Durchführung von Arbeiten in einem Betrieb eigenes Instandhaltungspersonal beauftragt, so hat der Arbeitgeber die betreffenden Beschäftigten über die relevanten Gefährdungen zu unterweisen.

Bei verschiedenen Arbeitgebern ist im Rahmen der Koordinationspflicht nach § 8 ArbSchG auch die Unterweisung der Arbeitnehmer zwischen den beteiligten Arbeitgebern erforderlich. Die Unterweisung muss insbesondere Informationen über örtliche Verhältnisse, weiterlaufende Arbeiten im Betrieb sowie damit einhergehende Gefährdungen beinhalten.

Im Umfeld der Instandhaltungsarbeiten tätige Beschäftigte sind über Zeit, Ort und Inhalt der vorgesehenen Instandhaltungsarbeiten sowie die dabei möglicherweise auftretenden Einschränkungen, Gefährdungen und die erforderliche Rücksichtnahme zu informieren.

Die Durchführung der Arbeiten darf nur unter Anwendung der festgelegten Maßnahmen erfolgen. Dabei sind die festgelegten Maßnahmen auf ihre Wirksamkeit zu überprüfen. Hierzu gehört insbesondere, dass die

- erforderlichen Arbeits- und Hilfsmittel bereitgestellt werden,
- organisatorischen Voraussetzungen bestehen und eingehalten werden,
- Verantwortlichkeiten festgelegt sind,
- Abstimmung über Art und Umfang der Arbeiten sowie Maßnahmen zur Gefahrenverhütung zwischen den Beteiligten erfolgt ist,
- Beschäftigten unterwiesen wurden und durch
- Begehung des Arbeitsplatzes festgestellt wurde, dass die Umgebungsbedingungen den Annahmen entsprechen.

Werden bei Instandhaltungsarbeiten von der Gefährdungsbeurteilung abweichende Gefährdungen festgestellt, so sind die Arbeiten unverzüglich, jedoch sicher, abzubrechen und der die Instandhaltung durchführende Arbeitgeber zu informieren. Diese haben die zusätzlichen erforderlichen Maßnahmen festzulegen, das Personal anzuweisen und die Gefährdungsbeurteilung anzupassen.
Während der Durchführung der Instandhaltungsarbeiten hat der die Instandhaltung durchführende Arbeitgeber die Umsetzung und Wirksamkeit der getroffenen Maßnahmen zu kontrollieren. Darüber hinaus hat er auf die Einhaltung der Vorschriften und Regeln des Arbeitsschutzes sowie auf die Befolgung der gegebenen Anweisungen zu achten und erforderlichenfalls ergänzende Anweisungen zu geben oder die Arbeiten zu unterbrechen.
Nach Abschluss der Arbeiten ist dafür Sorge zu tragen, dass sich das instandgesetzte Arbeitsmittel wieder in einem sicheren und funktionsfähigen Zustand befindet und alle Arbeits- und Hilfsmittel entfernt wurden. Ggf. ist eine Prüfung gemäß § 10 oder dem 3. Abschnitt der Betriebssicherheitsverordnung *(Stand 2019: gemäß §§ 14 oder 15 BetrSichV)* erforderlich.

Bei der Erprobung nach ausgeführter Instandhaltung muss die Sicherheit aller anwesenden Personen gewährleistet sein. Nicht unmittelbar an der Erprobung beteiligte Personen sind fernzuhalten (Absperren der Bereiche). Der Ablauf der Erprobung ist festzulegen. Vor Beginn der

Erprobung sind alle Beschäftigten über mögliche Gefahren und erforderliche Schutzmaßnahmen (z. B. das Einhalten von Sicherheitsabständen, die Benutzung von Schutzausrüstungen) sowie über Maßnahmen für mögliche Betriebsstörungen zu unterweisen.

Hinweise aus der VDI 2895 Richtlinie „Organisation der Instandhaltung“

Die Aufgaben der Instandhaltung können in strategische und operative Bereiche unterschieden werden.

Der **strategische Bereich** umfasst die Definition der Instandhaltungsziele (abgeleitet aus den Unternehmenszielen), gewählte Instandhaltungsstrategien und die Organisation der Instandhaltung.

Grundsätzliches Ziel der Instandhaltung ist die Gewährleistung der geforderten technischen Anlagenverfügbarkeit und -sicherheit. Daneben kann eine Vielzahl weiterer Ziele existieren, z. B.

- Systematisches Erkennen von Schwachstellen in Anlagen,
- Umsetzung und Dokumentation behördlicher Auflagen,
- Zusammenarbeit mit den Anlagenherstellern, um auf eine instandhaltungsgerechte Entwicklung neuer Anlagen hinzuwirken.

Die Instandhaltungsziele können mit Hilfe von Kennzahlen nachverfolgt werden (Beispiele für Kennzahlen in der Instandhaltung siehe VDI 2893 Richtlinie).

Eine Instandhaltungsstrategie gibt an, welche Instandhaltungsmaßnahmen an welchen Instandhaltungsobjekten zu welchen Zeitpunkten durchzuführen sind. Grundstrategien der Instandhaltung sind z. B. die geplante bzw. die ausfallbedingte Instandhaltung. Bei der geplanten/vorbeugende Instandhaltung lassen sich unterscheiden:

- vorausbestimmte Instandhaltung welche präventive Instandhaltungstätigkeiten nach Festlegung (z. B. anhand von Zeitabständen oder nach einer festgelegten Zahl von Nutzungseinheiten) ohne vorherige Zustandsermittlung der technischen Einheit durchführt,
- zustandsabhängige Instandhaltung mit vorheriger Zustandsermittlung der technischen Einheit z. B. mittels Inspektion, Messung etc., anhand deren Ergebnisse die notwendigen (präventiven) Instandhaltungstätigkeiten durchgeführt werden.

Die Kriterien für die Auswahl der anzuwendenden Instandhaltungsstrategie können z. B. technischer (z. B. Verschleißverhalten), wirtschaftlicher (z. B. Restlebensdauer), sicherheitstechnischer / gesetzlicher (z. B. Fristen), produktionsrelevanter (z. B. geforderte technische Verfügbarkeit) oder objektspezifischer Art (z. B. Wartungsfreundlichkeit, Vorhersehbarkeit des Ausfallverhaltens) sein.

Der **operative Bereich** der Instandhaltung beinhaltet die Instandhaltungsplanung, Instandhaltungssteuerung, Maßnahmendurchführung und Instandhaltungsanalyse.

Unter Instandhaltungsplanung versteht man die planmäßige Vorbereitung aller Instandhaltungsaktivitäten u.a. mit Budget-, Personal-, Betriebsmittel-, Werkstätten-, Material- und Ar-

beitsplanung. In der Arbeitsplanung werden Arbeitspläne zur Durchführung von meist geplanten (Wartungs-, Inspektionspläne), aber auch ungeplanten Instandhaltungsmaßnahmen (Instandsetzungspläne) erstellt.

Im Arbeitsplan werden für die einzelnen Instandhaltungstätigkeiten beispielsweise festgelegt:

- Personal-, Betriebsmittel- und Materialbedarf,
- Art und Reihenfolge der einzelnen Vorgänge, Planzeiten,
- Arbeitssicherheits- und Umweltschutzvorschriften,
- Schutzmaßnahmen,
- technische Pläne und Zeichnungen,
- Checklisten
- etc..

Auf die **VDI 2890 „Planmäßige Instandhaltung Anleitung zur Erstellung von Arbeits-, Wartungs- und Inspektionsplänen“** *(Gegenüber /3/ aktualisiert Stand März 2017: Inhalte sind noch gültig)* wird hingewiesen: Die Richtlinie soll ein Leitfaden für die Erstellung und Verwendung von Arbeits- / Wartungs- / Inspektionsplänen sein und benennt von den Instandhaltungsplanungs- und Steuerungssystemen (IPSS) bereitzustellende benötigte Funktionalitäten. Darüber hinaus werden Hinweise zur Überprüfung der Pläne im Lebenszyklus der instand zuhaltenden Betrachtungseinheit gegeben. Die von der Richtlinie vorgegebenen Standards bei der Erstellung von Arbeitsplänen sollen Verbesserungen bewirken bei der Kommunikation mit dem Hersteller, der Integration in Instandhaltungsplanungs- und Steuerungssysteme und der Übernahme von Herstellerunterlagen in die Betriebsinstandhaltung.

Die präventiven Instandhaltungsarbeiten werden terminiert um z. B. eine Minimierung instandhaltungsbedingter Produktionsausfälle, optimale Auslastung des Instandhaltungspersonals sowie eine anforderungsgerechte Koordination aller Instandhaltungsarbeiten zu erreichen. Im Rahmen der Auftragsüberwachung erfolgt ein ständiger Vergleich der vorliegenden Ist-Termine mit den Plan-Terminen der Aufträge und den Kapazitäten (Auslastung). Bei der Instandhaltungsanalyse erfolgt rückwirkend eine objekt- und maßnahmenbezogene Auswertung beispielsweise:

- Soll-Ist-Vergleiche (Kosten und Zeitaufwand)
- Auftragsabweichungsanalyse
- Schwachstellenanalyse
- Schadensursachenanalyse
- Ersatzteilverbrauchsanalyse

Diese Daten können auch für die Bildung anlagenspezifischer Kennzahlen herangezogen werden.

Total Productive Maintenance (TPM): Ein in Japan entwickeltes Konzept basierend auf ganzheitlichen Systemansatz in Verbindung mit der Strategie der ständigen Verbesserung, der die Eliminierung aller Produktionsverluste und aller Verschwendungen von Ressourcen zum Ziel hat, z. B. durch:

- instandhaltungsgerechte und -reduzierende Konstruktion
- präventive, zustandsabhängige Instandhaltung
- ➢ systematische Erfassung und Auswertung von Verlusten mit dem Ziel einer permanenten Systemverbesserung.

Hinweise:
Es gibt ein Instandhaltungskonzept oder Instandhaltungssystem, das auf einem bestimmten Prinzip z. B. Beauftragungsprinzip, eigenständiges Handeln der zuständigen Abteilung, Notwendigkeitsprinzip basieren kann. Sinnvoll ist eine geplante Instandhaltung, deren Instandhaltungskonzept (-plan, -handbuch o. ä.) zu folgenden Punkten Festlegungen enthalten kann: Instandhaltungsplanung (Strategie, Personal, Material etc.), Instandhaltungsobjekte (Anlage-, Ausrüstungsteile), Instandhaltungsmaßnahmen (Wartungen, Reinigungen, Inspektionen, Instandsetzungen).
Innerhalb des Instandhaltungssystems sind die Verantwortlichkeiten für alle Abläufe festgelegt.
Das Instandhaltungssystem kann EDV-gestützt sein und bei einer zentralen Organisationseinheit liegen.
Es können für unterschiedliche Anlagenkomponenten spezifische Wartungspläne geführt werden.
Regelungen zum Umgang mit Prüffristen im Instandhaltungskonzept müssen vorliegen (siehe hierzu Bewertungshilfe zur Frage „Wie wird der Prozess zur Gewährleistung der ordnungsgemäßen Durchführung von wiederkehrenden Prüfungen bewertet?“).

Es können Kriterienkataloge vorhanden sein, die bestimmen, welche Instandhaltungsarbeiten von den Beschäftigten der Anlage selbst durchgeführt werden dürfen.
Die Vorgehensweise für Beauftragungen ist geregelt und die jeweiligen Verantwortlichkeiten und der Umgang mit Fremdfirmen sind festgelegt.

Die Regelungen zur Durchführung von Instandhaltungsarbeiten können abhängig von Gefährdungspotential unterschiedlich sein, z. B. kann es für Tätigkeiten mit höherem Gefährdungspotential spezielle Erlaubnissysteme geben. Es gibt Festlegungen zu Überprüfungen der ordnungsgemäßen Durchführung von Instandhaltungsmaßnahmen. Es wird anhand von Überprüfungen festgestellt, ob die jeweiligen Instandhaltungsmaßnahmen ordnungsgemäß durchgeführt wurden. Die Vorgehensweise zur Behebung von bei der Überprüfung festgestellten Mängeln ist festgelegt. Die Verantwortlichen, Abläufe und Zeitpunkte für die Überprüfungen, die hieraus umzusetzenden Maßnahmen und die Überprüfung der Umsetzung sind festgelegt.

Es gibt Regelungen zur Dokumentation im Rahmen des Instandhaltungsprozesses (z. B. zu Inhalt, Beteiligte, Umfang, Aufbewahrungszeit, Zugang, Abzeichnung) und festgelegte Verantwortlichkeiten für die (abgestuften) Dokumentationen innerhalb des Instandhaltungssystems wie z. B. Dokumentation festgestellter Mängel, durchgeführter Überprüfungen.

5.4.11 Frage Nr. 11: Wie wird der Prozess zur Gewährleistung der ordnungsgemäßen Durchführung von (wiederkehrenden) Prüfungen bewertet?

Bewertungshilfe:

Ein besonderer Bereich der Instandhaltung sind (wiederkehrende) Prüfungen (siehe daher auch Bewertungshilfe zur Frage „Wie wird der Prozess zur Instandhaltung bewertet?“).
Bei der (wiederkehrenden) Prüfung wird die Sicherheit und Leistungsfähigkeit einer technischen Einheit mittels festgelegter Prüfmethoden überprüft, ohne dass weitergehende Maßnahmen, wie z. B. Reparatur vorgesehen sind. Je nach Prüfmethode sind geeignete Messinstrumente Voraussetzung für die Überprüfung. **Ziel bei der Festlegung von Fristen für die wiederkehrenden Prüfungen ist die sichere Verwendung und Leistungsfähigkeit einer technischen Einheit bis zur nächsten festgelegten Prüfung.**

Die (wiederkehrenden) Prüfungen sind gesetzlich geregelt in der Betriebssicherheitsverordnung (BetrSichV) und zugehörigen technischen Regeln, insbesondere der TRBS 1201 Prüfungen von Arbeitsmitteln und überwachungsbedürftigen Anlagen, aber auch TRBS 1201 Teil 1 Prüfung von Anlagen in explosionsgefährdeten Bereichen und TRBS 1201 Teil 2 Prüfungen bei Gefährdungen durch Dampf und Druck, etc.

Definition „Prüfung nach der BetrSichV bzw. TRBS 1201“:
Prüfung eines Prüfgegenstandes umfasst die Ermittlung des Istzustands, den Vergleich des Istzustands mit dem Sollzustand sowie die Bewertung der Abweichung des Istzustands vom Sollzustand.

Nach der **TRBS 1201** werden die zwei Prüfarten **Ordnungsprüfung** und **technische Prüfung** unterschieden.

Für die einzelnen Prüfungen sind Prüfart, Prüfumfang und Prüffristen festzulegen sowie die notwendige Qualifikation des Prüfpersonals zu bestimmen.

Die BetrSichV schreibt vor (Auszug aus § 3 (6)):
„Der Arbeitgeber hat Art und Umfang erforderlicher Prüfungen von Arbeitsmitteln sowie die Fristen von wiederkehrenden Prüfungen nach den §§ 14 und 16 zu ermitteln und festzulegen, soweit diese Verordnung nicht bereits entsprechende Vorgaben enthält.“ „Die Fristen für die wiederkehrenden Prüfungen sind so festzulegen, dass die Arbeitsmittel bis zur nächsten festgelegten Prüfung sicher verwendet werden können. “

Teilweise sind durch die BetrSichV Höchstfristen vorgegeben, die nicht überschritten werden dürfen.

Anlagen von denen spezielle Gefährdungen wie z. B. Absturz, Explosion, Brand, Druck, Zündquelle ausgehen, werden im **Produktsicherheitsgesetz** als **überwachungsbedürftige Anlagen** aufgeführt.

Für die überwachungsbedürftigen Anlagen sind nach der BetrSichV neben den gemeinsamen Vorschriften für Arbeitsmittel zusätzlich besondere Vorschriften zu beachten.

Insbesondere werden dort die **Prüfung vor Inbetriebnahme** sowie die **wiederkehrenden Prüfungen von bestimmten überwachungsbedürftigen Anlagen** gefordert. Diese dürfen nur verwendet werden, wenn die geforderten Prüfungen durchgeführt und dokumentiert wurden.
Für bestimmte überwachungsbedürftige Anlagen ist die Prüfung durch *Zugelassene Überwachungsstellen* vorzunehmen.
Bei den wiederkehrenden Prüfungen ist auch zu überprüfen, ob die Frist für die nächste wiederkehrende Prüfung zutreffend festgelegt wurde.

Der Prozess zur Gewährleistung der ordnungsgemäßen Durchführung von (wiederkehrenden) Prüfungen muss Bestandteil des SMS sein, entweder als eigenständiger Prozess oder integriert im Prozess „Instandhaltung“.
Im Prozessablauf ist sicherzustellen, dass alle sicherheitstechnisch relevanten Anlagenteile im Sinne der Anlagen- / Prozesssicherheit erfasst sind, für die wiederkehrenden Prüfungen notwendig sind, und hierfür Fristen ermittelt sind.

Prüffristen sind anhand von Kriterien (Vorschriften, Ausfallwerte etc.) festzulegen. Die Kriterien werden zu festgelegten Zeitpunkten hinterfragt (regelmäßige Überprüfung, Einfluss neuer Erkenntnisse, Ereignisse). Die Einhaltung der Prüffristen und die ordnungsgemäße Durchführung der Prüfungen sind sicherzustellen. Die Verantwortlichkeiten für alle Aufgaben im Prozessablauf müssen festgelegt sein, ebenso die erforderliche Dokumentation. Die Erfüllung der Anforderungen der BetrSichV muss sichergestellt sein.

5.4.12 Frage Nr. 12: Wie werden Regelungen zur Berücksichtigung von Auswirkungen durch die Alterung von Anlagen und Anlagenteilen bewertet?

Bewertungshilfe:

Der Alterung von Anlagen und Anlagenteilen wird durch eine gute Instandhaltung und wiederkehrende Prüfungen entgegengewirkt.

Die Instandhaltung dient der Erhaltung des sicheren Zustandes von Anlagen und Anlagenteilen und beinhaltet alle Maßnahmen hierzu, insbesondere Inspektion, Wartung und Instandsetzung sowie auch wiederkehrende Prüfungen.
Bei der wiederkehrenden Prüfung wird die Sicherheit und Leistungsfähigkeit einer Anlage oder eines Anlagenteils mittels festgelegter Prüfmethoden mit dem Ziel überprüft, ob eine sichere Verwendung und Leistungsfähigkeit bis zur nächsten wiederkehrenden Prüfung erfolgen kann. Ist dies nicht der Fall, werden weitergehende (Instandhaltungs-)Maßnahmen, wie z. B. Reparatur, Austausch etc. vorgenommen.

In Anlehnung an den **MAHBulletin Lessons Learned Nr. 7 „Major accidents related to ageing“** soll der vorsorgende Umgang mit der Alterung von Anlagen die folgenden Punkte berücksichtigen:

A. Physikalische werkstofftechnische Alterung der Anlagenkomponenten,
B. Alterung durch Weiterentwicklung der Technik,
C. Alterung durch Veränderungen in Organisation, Management und menschlichem Faktor,
D. Alterung durch konzeptionelle Weiterentwicklung von Sicherheitsphilosophie, Änderungen von Normen und sonstigen Regelwerken.

Die oben genannten Punkte zur Alterung werden zum Großteil durch Prozesse, die in anderen Prüfgebieten abgefragt werden, mit abgedeckt. Bei einer Inspektion ist dann der Schwerpunkt auf den Aspekt „Alterung“ zu legen. Bei den folgenden Fragen fließt dieser Aspekt mit ein:

Aus dem Prüfgebiet SMS: Systematische Überprüfung und Bewertung

- Wie wird die Vorgehensweise zur systematischen Überprüfung und Bewertung des SMS (Managementreview) bewertet?
- Wie wird die Sicherheitskultur des Betriebsbereiches eingeschätzt?

Aus dem Prüfgebiet SMS: Überwachung der Leistungsfähigkeit des Sicherheitsmanagementsystems

- Wie wird der Prozess zum Auditsystem bewertet?
- Wie wird der Prozess internes Berichtssystem bzw. die Regelungen zur Erfassung von und Umgang mit Ereignissen bewertet?
- Wie werden die Regelungen zur Verwendung von Kennzahlen bzw. (Leistungs-) Indikatoren zur Anlagensicherheit bewertet?

Weitere relevante Fragen sind:

ZU A) Physikalische werkstofftechnische Alterung der Anlagenkomponenten

Aus dem Prüfgebiet SMS: Überwachung des Betriebs:

- Wie wird der Prozess zur Instandhaltung bewertet?
- Wie wird der Prozess zur Gewährleistung der ordnungsgemäßen Durchführung von (wiederkehrenden) Prüfungen bewertet?“

Aus dem Prüfgebiet SMS: Ermittlung und Bewertung der Gefahren von Störfällen

- Wie ist der Prozess zur Ermittlung und Bewertung der Gefahren von Störfällen zu bewerten?
- Wie wird der Einsatz der zur Anwendung kommenden systematischen Methoden bewertet?
- Wie wird die Vorgehensweise zur Ermittlung der sicherheitsrelevanten Teile des Betriebsbereiches bewertet?
- Wie wird die Vorgehensweise zur Ermittlung der sicherheitsrelevanten Anlagenteile von den Anlagen des Betriebsbereiches bewertet?

ZU B /D) Alterung durch Weiterentwicklung der Technik

Aus dem Prüfgebiet SMS: Überwachung des Betriebs:

- Wie wird der Prozess zur Gewährleistung der ordnungsgemäßen Durchführung von (wiederkehrenden) Prüfungen bewertet?
- Aus dem Prüfgebiet SMS: Sichere Durchführung von Änderungen und Anlagenneuplanungen
- Wie wird der Prozess zur sicheren Durchführung von Änderungen (Management of Change: MoC) bewertet?

zu c) Alterung durch Veränderungen in Organisation, Management und menschlichem Faktor

Aus dem Prüfgebiet SMS: Organisation und Personal

- Wie wird der Prozess zum Wissensmanagement bewertet?

Aus dem Prüfgebiet SMS: Sichere Durchführung von Änderungen und Anlagenneuplanungen

- Wie wird der Prozess zur sicheren Durchführung von Änderungen (Management of Change: MoC) bewertet?
- Wie wird die Regelung zur Gewährleistung der Vollständigkeit und Aktualisierung der Betriebsdokumentationen bewertet?“

Von Relevanz für alle Punkte a) - d) ist die Bewertungshilfe zur Frage „Wie wird die Sicherheitskultur des Betriebsbereiches eingeschätzt?“, vor allem zum Aspekt „schleichende Veränderungen“. Sehr wichtig ist auch das regelmäßige und kontinuierliche Durchlaufen des PDCA-Zyklus einschließlich des Auditsystems.

Hinweise für Inspektoren/innen:

Mögliche Fragen zum Aspekt Alterung:

- Gibt es im BB Vorgaben dazu, wie die werkstofftechnische Alterung von Anlagenteilen berücksichtigt wird?
- Gibt es Indikatoren zur Bewertung der Alterung?
- Welche Indikatoren werden verwendet?
- Welche Vorgaben gibt es im Betriebsbereich, wenn sich der Stand der Technik ändert, insbesondere zur
- Ersatzteilbeschaffung von alter Technik?
- Kompatibilität von alter und neuer Technik?
- Wie wird der Wissenstransfer bei Änderungen von Personal in den Bereichen Management / Organisation sichergestellt?
- Welche Vorgaben gibt es im Betriebsbereich zur konzeptionellen Weiterentwicklung der Sicherheitsphilosophie oder zur Umsetzung von Änderungen bei Normen und sonstigen Regelwerken?

Folgende Unterlagen (Verfahrensbeschreibung / Prozessbeschreibung / Managementanweisung) sollten insbesondere eingesehen werden hinsichtlich:

- Instandhaltung und wiederkehrenden Prüfungen,
- MoC(Management of Change)-Prozess,
- Dokumentenlenkung und Betriebsdokumentation,
- Wissensmanagement,
- Qualifikation der Beschäftigten,
- Ermittlung und Bewertung der Gefahren von Störfällen.

Bei diesen Unterlagen ist der Fokus zum einen auf den Aspekt Alterung zu legen, d. h. inwiefern wird dieser berücksichtigt. Zum anderen muss die Umsetzung des PDCA-Zyklus im Blickpunkt stehen. D. h. es müssen regelmäßige Überprüfungen, z. B. im Rahmen von Audits erfolgen, ob die festgelegten Inhalte für den in der Verfahrensbeschreibung / Prozessbeschreibung /etc. dokumentierten Prozess (u. a. Ablauf, Verantwortlichkeiten) angemessen sind. Die Verwendung von Indikatoren zur Bewertung des Alterungszustandes von Anlagen /-teilen im Betriebsbereich ist positiv zu bewerten.

Weitere Hinweise/Erläuterungen:

Auf die OECD-Veröffentlichung „Ageing of Hazardous Installations“ von März 2017 wird hingewiesen.

Großbritannien hat im Jahr 2010 einen Schwerpunkt auf den Aspekt Alterung bei Inspektionen in Betriebsbereichen gelegt. Im Rahmen dessen wurden vom HSE (Health and Safety Executive) verschiedene Dokumente veröffentlicht, z. B.:

- Managing Ageing Plant – A Summary Guide
- Ageing Plant Operational Delivery Guide der COMAH Competent Authority

Beim letztgenannten handelt es sich um einen Behördenleitfaden zur Inspektion alternder Anlagen. Der zugehörige Anhang 5 enthält die folgenden 7 Prüfelemente mit Fragen:

- **Topic 1: Betreiberverantwortung** (Leadership)
- **Topic 2: Verzeichnis der Anlagen/-teile** (Plant and equipment on site – the Asset Register)
- **Topic 3: Maßnahmen zur Sicherstellung der technischen Dichtheit der Anlagen** (Assuring the integrity of the primary containment boundary)
- **Topic 4: Maßnahmen zur Sicherstellung der Funktionsfähigkeit sicherheitsrelevanter Ausrüstungsteile** (Assuring the integrity of safety-critical mechanical equipment)
- **Topic 5: Regelungen zur Überprüfung von Prozessleitsystemen** (EC&I Inspection and Test)
- **Topic 6: Management von überalterten (oder auslaufenden) Prozessleitsystemen und Ausrüstungsteilen** (EC&I management of Out-of-date or Obsolescent Equipment)
- **Topic 7: Ressourcen** (Resources)

In beiden HSE-Veröffentlichungen wird darauf hingewiesen, dass die Alterung bzw. der Alterungszustand einer Anlage nicht ausschließlich von der Anzahl der Jahre seit Bestehen abhängt, sondern insbesondere vom Zustand der Anlage, welchen Beanspruchungen und Lastwechseln die Anlage unterlag.

Der Zustand einer Anlage muss dergestalt sein, dass eine störungsfreie Produktion gewährleistet ist. Dies kann auch bei sehr alten Anlagen der Fall sein, während umgekehrt ggf. relativ „junge“ Anlagen schon starke Verschleißerscheinungen aufweisen können, die ein Versagen von Ausrüstungsteilen mit gravierenden Ausmaßen zur Folge haben können. Letzteres soll durch Maßnahmen verhindert werden – ein Fokus liegt hier auf Instandhaltungsmaßnahmen und wiederkehrenden Prüfungen.

Die HSE-Veröffentlichung „Managing Ageing Plant – A Summary Guide“ nennt als wichtige Elemente, die ein Betriebsbereich für einen sicheren Umgang mit der Alterung von Anlagen vorweisen muss:

- **Instandhaltungsprozess** (Maintenance Management Systems)
- **Prozesse zur Verwaltung von Anlagen / -teilen und Sicherstellung ihrer Lebensdauer** (Asset Management and Integrity Systems)
- **Audit und Überprüfungsprozesse** (Audit and Inspection regimes)
- **Prozesse zur Gefahrenanalyse und Risikobewertung** (Risk Assessment Management processes)
- **Sichere Durchführung von Änderungen** (Management of Change procedures)
- **Prozess zur Freigabe von gefährlichen Arbeiten** (Permit to Work)
- **Verantwortlichkeiten und Kommunikation** (Responsibilities and Communications)
- **Prozesse zur Durchführung von Qualifizierungen und Übungen** (Training and Competence development)

Als mögliche **Indikatoren zur Bewertung des Alterungszustandes von Anlagen /-teilen** nennt die HSE-Veröffentlichung:

Frühindikatoren (Leading Indicators)

- Anzahl geplanter Inspektionen / Prüfungen (Number of planned inspections)
- Anzahl und Frequenz wiederkehrender Prüfungen (Number and frequency of audits)
- Terminplan für den Austausch von Anlagen/-teilen (Planned replacement schedules for plant and equipment)
- Anzahl geplanter Notfallübungen (Number of Emergency Response exercises planned)
- Anzahl geplanter Überprüfungen sicherheitstechnisch relevanter Anlagenteile (Planned number of tests done on safety critical equipment)
- Anzahl der Teilnahmen von Anlagenpersonal an Fortbildungen (Training plans for identified staff and staff numbers attending)
- Anzahl der geplanten Überprüfungen von (Betriebs- / Arbeits-) Anweisungen (Planned procedure reviews)

Spätindikatoren (Lagging indicators)

- Anzahl von gravierenden Betriebsstörungen (Number of major failures of plant and equipment)
- Anzahl der Leckagen (Number of uncontrolled releases of product)
- Anzahl von Instandhaltungsarbeiten, die nachgebessert werden mussten (Number of reworks to maintenance activities)
- Anzahl nicht durchgeführter Maßnahmen aufgrund von Prüfungen / Inspektionen / Audits (Number of out-standing audit / Inspection action items)
- Anzahl der auftretenden Fehler der Prozessleittechnik bei Überprüfungen (Number of alarm/instrument failures during testing)
- Anzahl der Vorfälle (Ereignisse / Störfälle) bei gefährlichen Arbeiten, für die eine Freigabe notwendig ist (Number of incidents when working under a Permit to Work system)
- Anzahl der Vorfälle (Ereignisse / Störfälle) aufgrund menschlicher Fehlhandlungen (Number of incidents due to Human Error)

5.4.13 Frage Nr. 13: Wie werden die Regelungen zur Beschaffung von Betriebsmitteln und Geräten bewertet?

Bewertungshilfe:

Es ist sicherzustellen, dass der Aspekt Anlagensicherheit beim Einkauf genügend berücksichtigt wird. Regelungen und Kriterien, die dies sicherstellen sollten existieren und umgesetzt werden (z. B. Vorgaben hinsichtlich einer Lieferantenauswahl und -qualifikation, Überprüfung der (gefährlichen) Eigenschaften von Chemikalien vor ihrer Beschaffung und Einsatz, ausschließliche Verwendung von Chemikalien mit Sicherheitsdatenblättern, Einsatz von Betriebsmitteln und Betriebseinrichtungen mit Regelungen zu deren Überprüfung).

5.5 SMS: Sichere Durchführung von Änderungen und Anlagenneuplanungen

Dieses Prüfgebiet enthält die folgenden Fragen:

Frage Nr. 1: Wie wird der Prozess zur sicheren Durchführung von Änderungen (Management of Change: MoC) bewertet?

Frage Nr. 2: Wie werden die Regelungen zur Kommunikation bei den verschiedenen Phasen eines Änderungsprozesses bewertet?

Frage Nr. 3: Wie wird die Regelung zur Gewährleistung der Vollständigkeit und Aktualisierung der Betriebsdokumentationen bewertet?

Frage Nr. 4: Wie werden die Regelungen für einen zeitweisen Stillstand einer Anlage im Betriebsbereich bewertet?

Frage Nr. 5: Wie werden die Regelungen zur Inbetriebnahme einer Anlage im Betriebsbereich bewertet?

5.5.1 Frage Nr. 1: Wie wird der Prozess zur sicheren Durchführung von Änderungen (Management of Change: MoC) bewertet?

Bewertungshilfe:

Änderungen in einem Betriebsbereich können geplant sein oder schleichend entstehen und können technische, organisatorische oder managementrelevante Aspekte eines Betriebsbereiches betreffen. Für die Störfallvorsorge ist ein umfassendes Verständnis für die Bedeutung von Änderungen wichtig.

Sicherheitsrelevante Konsequenzen von schleichenden Änderungen sind schwierig zu erkennen und Mittel für einen positiven Umgang hiermit findet sich in der Überwachung der Leistungsfähigkeit des SMS und in einer guten Sicherheitskultur.

Sicherheitsrelevante Konsequenzen durch Änderungen gehen nicht nur von Änderungen der Technologie, Verfahrensabläufen oder vom Umgang mit Gefahrstoffen (= technische Änderungen) aus, sondern auch z. B. durch Managemententscheidungen oder organisatorische Änderungen. Als Beispiele hierfür können dienen: Die Festlegung der Sprache von Deutsch zu Englisch - auch bei der (internen) Kommunikation (Informationen werden falsch oder gar nicht weitergegeben, Formblätter falsch ausgefüllt etc.) oder Durchführung der Gefahrenanalyse von externen Dienstleistern oder Einführung Industrie 4.0 (Schnittstelle IT-Sicherheit / Anlagensicherheit).

Für die sichere Durchführung von geplanten Änderungen ist es wichtig, festzustellen, ob diese Auswirkungen auf das realisierte Sicherheitskonzept haben. Hierfür wird ein Überblick über die Konsequenzen der Änderung benötigt.
Daher erfolgen geplante technische Änderungen im Rahmen des Prozesses zur sicheren Durchführung von Änderungen **(Management of Change: MoC**). Dieser ist im Betriebsbereich schriftlich festgelegt, z. B. in Form einer Verfahrensbeschreibung / Prozessbeschreibung / Managementanweisung etc.. Hierin sind folgende Aspekte zu berücksichtigen:

1. Ziele, die mit dem Prozess MoC umgesetzt und erreicht werden sollen (z. B. sichere Umsetzung von geplanten Änderungen, Effektiver Einsatz von Investitionen),
2. Anwendungsbereich (z. B. Betriebsbereich, Arten von Änderungen, Organisationseinheiten des Betriebsbereiches, Anlagen),
3. Definition der Begrifflichkeiten (insbesondere sicherheitsrelevante Änderungen, Abstufung von Änderungen),
4. Beschreibung der Prozessschritte und Ablauf des MoC (abhängig von z. B. Art der Änderung, Informations- und Genehmigungsablauf)
5. Festlegung der Inhalte der Prozessschritte und Aufgaben (An- und Abfahrprozesse, Entleerung und Reinigung von Anlagenteilen, Stillstände, Auswirkungen der Bau- und Lagerungstätigkeiten (z. B. Zugänglichkeit für die Feuerwehr)
6. Festlegung von Zuständigkeiten und Verantwortlichkeiten zu den Prozessschritten und Aufgaben,
7. Berücksichtigung zu den Schnittstellen anderer Prozesse (z. B. Gefahrenanalyse, Genehmigungsbedürftigkeit, Dokumentation, IT-Sicherheit, Überwachung des Betriebs, Notfallplanung, Auditsystem),
8. Festlegung von Dokumentationsinhalten bei den Prozessschritten des MoC.

Es müssen regelmäßige Überprüfungen erfolgen, ob die festgelegten Inhalte für den Prozess MoC (u. a. Kriterien, Ablauf, Verantwortlichkeiten) angemessen sind, z. B. im Rahmen von Audits.

Die obigen Gesichtspunkte gelten für mittelständische und Großunternehmen.

Kleinunternehmen müssen ihre Vorgehensweise und Kriterien unter Berücksichtigung der Anforderungen der Störfall-Verordnung, schriftlich niedergelegen. Aufgrund der anderen Organisationsstruktur kann dies z. B. in einem Kapitel des Managementhandbuchs erfolgen.

Die Vorgehensweise bei Änderungen muss regelmäßig überprüft werden. Hierfür sind Kriterien festzulegen (z. B. Zeitabstände, Berücksichtigung besonderer Anlässe (z. B. (Beinahe-) Unfälle); was, wie, wann von wem geprüft wird, (z. B. Vollständigkeit aller sicherheitstechnisch relevanten Aspekte, Berücksichtigung neuer Erkenntnisse etc.). Die Zuständigkeiten hierfür müssen klar geregelt sein. Regelungen zur Dokumentation und zum Umgang mit den Ergebnissen aus den Überprüfungen müssen existieren.

Hinweise zu den oben genannten Punkten z. B. in einer Verfahrensanweisung:

Es gibt schriftlich festgelegte Vorgehensweisen, wie im Betriebsbereich Änderungen (Investitionen, Reparaturen, Änderungen des Stoffeinsatzes und Verfahrensablauf, Verhaltensänderung) gehandhabt werden. Änderungen von verfahrenstechnischen Abläufen mit Investitionsbedarf verlangen in der Regel die Bewertung und Genehmigung verschiedener Stellen im Betriebsbereich/Unternehmen.

Änderungen sollen eine frühzeitige Einbindung der Anlagensicherheit gewährleisten.

Die Vorgehensweisen können Elemente wie Beschreibung (z. B. Beantragung der Änderung, Gutachten und Freigabe durch Sachkundige, Inbetriebnahme), Begründung, erforderliche Mittel, Dokumentation, Überprüfungen enthalten. Alle Verantwortlichen für die jeweiligen Schritte bei einer Änderung sind schriftlich festzulegen. In der Regel wird es Untergliederungen bei den Änderungsverfahren geben, z. B.

- langfristig geplante Änderungen (Neuanlagen / Instandhaltung),
- kurzfristig erforderliche Änderungen aufgrund besonderer Umstände,
- Sicherheitsrelevanz,
- Planung, Außerbetriebnahme von Anlageteilen, Bau, Inbetriebnahme,
- Stilllegung, Demontage von Anlageteilen

Der unternehmensinterne Freigabeprozess eines Änderungsvorhabens sollte so angelegt sein, dass das Vorhaben selbst sowie die Entscheidung darüber transparent sind, also auch die Begründung für eine evt. Ablehnung aufweist.

Die Änderungsverfahren können im Hinblick des Aufwandes der verschiedenen Schritte, z. B.

- Vorbereitung,
- Freigabe,
- Durchführung der Änderung,
- Überprüfung der erfolgten Änderung,
- Dokumentation,

von der Sicherheitsrelevanz abhängig sein.

Zur Bestimmung der Sicherheitsrelevanz sollten Kriterien vorhanden sein, z. B.
Ausmaß der Änderungen,

- betroffene Anlagenteile (z.B. mit/ohne gefährlichen Stoffinhalte),
- Änderung von chemischen Reaktionen (beinhaltet z. B. auch die Änderung der Reihenfolge der Zugabe von Stoffen und sollte grundsätzlich nicht ohne Vorliegen der relevanten sicherheitstechnischen Kenndaten vorgenommen werden),
- Definition von Änderungsarbeiten unterschiedlicher Sicherheitsrelevanz (z. B. Gebäudeanstrich, Austausch eines Produktionsbehälters).

Auch Veränderungen, die auf sich selbst bezogen eine geringe Sicherheitsrelevanz haben, können Einfluss auf das Sicherheitskonzept der Anlage oder des Betriebsbereiches haben.

Wichtig ist auch eine Überprüfung der möglichen Auswirkungen auf übergreifende Systeme (wie z. B. Stickstoff-, Energieversorgung, Notfallschutzplanung, IT-Sicherheit, Transport).

Die Verknüpfung / Schnittstelle zum Prozess zur Ermittlung und Bewertung der Gefahren von Störfällen muss durch Kriterien klar definiert sein (z. B. stoffmengenbezogen oder Änderungen im Verfahrensablauf). Verantwortlichkeiten für die Einhaltung und Aktualisierung der Kriterien müssen festgelegt sein.

5.5.2 Frage Nr. 2: Wie werden die Regelungen zur Kommunikation bei den verschiedenen Phasen eines Änderungsprozesses bewertet?

Bewertungshilfe:

Es existieren Regelungen dazu, welche Fachbereiche bei Änderungen einzubinden sind (wie, wann, wer, wozu) und auch wie sichergestellt wird, dass alle sicherheitsrelevanten Daten während der Planungsphase den Einzelnen mit der Planung befassten Personen / Fachbereichen zur Verfügung stehen (z. B. Übergabeprotokolle, Übergabegespräche etc.).

Es sind Kriterien festgelegt, welche Informationen der Verfahrensentwickler oder externe Firmen vom Betrieb bekommen und umgekehrt. Die Ansprechpersonen auf beiden Seiten sind benannt. Die Informationswege sind nachvollziehbar, auch welcher informelle Informationsaustausch vorhanden ist.

Es wird sichergestellt, dass die zu erwartenden Änderungen den Beschäftigten rechtzeitig bekannt gegeben werden (Zeitpunkte können abhängen von Umfang, Art der Veränderungen oder Betroffenheit durch die Veränderungen). Kriterien zu Umfang, Inhalten und Form der Informationsweitergabe sollten festgelegt sein. Die Informationen können in schriftlicher, allgemeinverständlicher Form vorgenommen werden und neben Angabe der Änderungen auch die Auswirkungen auf die verschiedenen Betriebsarten (Prozess-, Instandhaltungs-, Reparaturbetrieb, IT-Sicherheit, etc.) enthalten. Ggf. können die Änderungen die Notwendigkeit von Schulungen und Fortbildungen erforderlich machen. Die Zuständigkeiten für die Informationsweitergabe müssen klar geregelt sein.

Regelmäßige Überprüfungen des Informationsflusses und Vorgehensweisen, wie mit den hieraus resultierenden Ergebnissen umgegangen wird, sind notwendig. Dies kann im Rahmen des Auditsystems erfolgen.

5.5.3 Frage Nr. 3: Wie wird die Regelung zur Gewährleistung der Vollständigkeit und Aktualisierung der Betriebsdokumentationen bewertet?

Bewertungshilfe:

Es muss Vorgehensweisen geben, die sicherstellen, dass die Aktualisierung der Betriebsdokumentation im Änderungsprozess gewährleistet ist (evt. in abgestufter Form).
Dies betrifft eine umfassende und vollständige Dokumentation der Veränderungen sowie eine Aktualisierung aller von der Änderung betroffener Unterlagen. Die Verantwortlichkeiten hierfür müssen klar geregelt sein. Eine regelmäßige Überprüfung der Vorgehensweisen ist durchzuführen.
Die relevanten Sicherheitsrichtlinien, (Betriebs- und Arbeits-) Anweisungen und Betriebsanleitungen sind jederzeit auf dem aktuellsten Stand zu halten, dies gilt auch für das Betriebshandbuch.
Anlagenveränderungen sind in die R&I-Fließbilder zu übertragen und die Anlagendokumentation wie auch der Sicherheitsbericht sind anzupassen. Auf die Berücksichtigung von Dokumentenänderungen im Rahmen erforderlicher Anzeige- und Genehmigungsverfahren wird hingewiesen.
Regelungen zum Überprüfungsprozess, ob die Aktualisierung der Dokumentation ordnungsgemäß und vollständig erfolgte, müssen existieren. Dies kann im Rahmen des Auditsystems erfolgen.

Eine Möglichkeit zur vollständigen Kompatibilitätsprüfung ist die Einführung eines Anlagen- oder Betriebshandbuches, das die Gesamtheit aller Dokumente (von der ersten Entwurfsplanung bis zur Genehmigungsurkunde, vom anlagenbezogenen Sicherheitsbericht bis zu den Protokollen über die Instandhaltung und die sicherheitstechnischen Veränderungen und Erweiterungen an der Anlage, etc.) enthält. Die Dokumente sollten sich immer auf dem aktuellen Stand befinden. Weiterhin dazu gehört die prozessbezogene Verfahrensakte, die alle Dokumente über den Prozess enthält und bereits in der Forschungsphase des Prozesses angelegt wird und ebenfalls laufend aktualisiert werden muss.
Der Vergleich der Angaben in beiden Dokumentationen ermöglicht eine sinnvolle Kompatibilitätsprüfung. Auch für diese Regelung muss die Zuständigkeit klar definiert sein.

5.5.4 Frage Nr. 4: Wie werden die Regelungen für einen zeitweisen Stillstand einer Anlage im Betriebsbereich bewertet?

Bewertungshilfe:

Festlegungen zur Vorgehensweise für einen zeitweisen Stillstand einer Anlage oder Anlagen oder Stilllegung derselben und der jeweiligen Verantwortlichen hierbei müssen vorhanden sein. Dies beinhaltet auch Regelungen zum Freimachen von Gefahrstoffen oder Drücken, Reinigung, Sicherung, Rückbau, Abnahme und Dokumentation.

Festlegungen zur Archivierung der Anlagendokumentation können erforderlich sein.

Regelungen zum Überprüfungsprozess, ob Stillstände ordnungsgemäß durchgeführt werden, müssen existieren. Dies kann im Rahmen des Auditsystems erfolgen.

5.5.5 Frage Nr. 5: Wie werden die Regelungen zur Inbetriebnahme einer Anlage im Betriebsbereich bewertet?

Bewertungshilfe:

Festlegungen zur Vorgehensweise bei der Inbetriebnahme und der jeweiligen Verantwortlichen hierbei müssen vorhanden sein.

Dies beinhaltet auch Regelungen zur Abnahme und Übergabe sowie zur Dokumentation.

Festlegungen, welche Personen / Fachabteilungen / externe Firmen bei der Inbetriebnahme einzubinden sind, können sinnvoll sein, ebenso welche Anlagendokumentation übergeben wird.

Bei Neuanlagen sollten Festlegungen vorhanden sein zur Gestaltung des Erfahrungsaustausches zwischen den vor der Übergabe einer Anlage beteiligten Personen und dem Betriebspersonal, das die Anlage fährt. Dieser Erfahrungsaustausch betrifft einen bestimmten Zeitraum, z. B. erstes Betriebsjahr.

Regelungen zum Überprüfungsprozess, ob die Inbetriebnahme ordnungsgemäß erfolgte, müssen existieren. Dies kann im Rahmen des Auditsystems erfolgen.

5.6 SMS: Planung für Notfälle

Dieses Prüfgebiet enthält die folgenden Fragen:

Frage Nr. 1: Wie sind die Regelungen zum Prozess Information der Öffentlichkeit zu bewerten?

Frage Nr. 2: Wie werden die Regelungen zum Prozess der Notfallplanung bewertet?

Frage Nr. 3: Wie werden die Regelungen zum Prozess der Erstellung und Überprüfung von Dokumenten zur Notfallplanung bewertet?

Frage Nr. 4: Wie werden die Regelungen zum Prozess der Unterweisung / Durchführung von Notfallübungen / Erprobung von AGAP bewertet?

Frage Nr. 5: Wie wird die Regelung der Entscheidungsbefugnisse im Betriebsbereich für den Notfall bewertet?

Frage Nr. 6: Wie sind die Regelungen der Meldepflichten zu bewerten?

Frage Nr. 7: Wie sind die Regelungen zum Krisenstab zu bewerten?

Frage Nr. 8: Wie wird die Zusammenarbeit mit den externen Notfall- und Rettungsdiensten bewertet?

Frage Nr. 9: Wie werden die Regelungen zur Ausstattung der betrieblichen Gefahrenabwehrkräfte bewertet?

Frage Nr. 10: Wie wird die Vorgehensweise zur Ausstattung des Betriebsbereiches mit den erforderlichen Warneinrichtungen bewertet?

5.6.1 Frage Nr. 1: Wie sind die Regelungen zum Prozess Information der Öffentlichkeit zu bewerten?

Bewertungshilfe:

Seit 2017 ist die Information der Öffentlichkeit durch Betreiber von Betriebsbereichen sowohl der unteren als der oberen Klasse verpflichtend. Dies ist für alle Betriebsbereiche im § 8a „Information der Öffentlichkeit“ der Störfall-Verordnung in Verbindung mit dem Anhang V Teil 1: „Informationen zu Betriebsbereichen der unteren und oberen Klasse“ geregelt.

Für Betriebsbereiche der oberen Klasse finden sich darüber hinaus weitergehende Anforderungen, aufgeführt in § 11 „Weitergehende Information der Öffentlichkeit“ der Störfall-Verordnung in Verbindung mit dem Anhang V Teil 2: „Weitergehende Informationen zu Betriebsbereichen der oberen Klasse, die von den Betreibern zu erfüllen sind“.

Der Betreiber muss die Vorgehensweise zur Erstellung, Verteilung und Aktualisierung der Unterlagen für die Information der Öffentlichkeit schriftlich festlegen.

Bei **Kleinunternehmen** kann dies z. B. in einem Kapitel des Managementhandbuchs erfolgen.

Für **mittelständische und Großunternehmen** sollte dieser Prozess Information der Öffentlichkeit in Form einer Verfahrensbeschreibung / Prozessbeschreibung / Managementanweisung etc. schriftlich festgelegt und dokumentiert sein, in welcher die folgenden Punkte berücksichtigt werden:

- Ziele, die mit dem Prozess umgesetzt und erreicht werden sollen,
- Anwendungsbereich,
- Definition der Begrifflichkeiten,
- Beschreibung der Prozessschritte und Ablauf der Information der Öffentlichkeit,
- Festlegung der Inhalte der Prozessschritte und Aufgaben,
- Festlegung von Zuständigkeiten und Verantwortlichkeiten zu den Aufgaben,
- Berücksichtigung zu den Schnittstellen anderer Prozesse (z. B. Gefahrenanalyse, MoC, Auditsystem),
- Festlegung von Dokumentationsinhalten bei den Prozessschritten.

Es müssen regelmäßige Überprüfungen erfolgen, ob die festgelegten Vorgehensweisen und Inhalte für den Prozess Information der Öffentlichkeit angemessen sind, z. B. im Rahmen von Audits.

Zu den Inhalten und weitere Hinweise:

Für die Erfüllung der Pflicht zur Information der Öffentlichkeit gilt:

- Die auf den neuesten Stand zu haltende Angaben sind der Öffentlichkeit ständig zugänglich zu machen, auch elektronisch,
- die Angaben müssen (erstmalig) einen Monat vor Inbetriebnahme eines Betriebsbereichs, sowie
- einen Monat vor störfallrelevanten Änderungen nach § 3 Absatz 5b des Bundes-Immissionsschutzgesetzes veröffentlicht werden.

Nach Anhang V Teil 1der Störfall-Verordnung müssen im Rahmen der Information zu Betriebsbereichen für die Öffentlichkeit die folgenden Angaben erfolgen:

1. Name oder Firma des Betreibers und vollständige Anschrift des Betriebsbereichs.

2. a. Bestätigung, dass es sich um einen Betriebsbereich der unteren bzw. oberen Klasse handelt, der unter die Störfall-Verordnung fällt und bei der zuständigen Überwachungsbehörde nach § 7 anzeigt wurde.

2. b. Der Sicherheitsbericht nach § 9 der zuständigen Überwachungsbehörde vorgelegt wurde, wenn es sich um einen Betriebsbereich der oberen Klasse handelt.

3. Eine verständlich abgefasste Erläuterung der Tätigkeiten im Betriebsbereich.

4. Nennung der im Betriebsbereich vorhandenen relevanten gefährlichen Stoffe, von denen ein Störfall ausgehen könnte in gebräuchlichen bzw. generischen Bezeichnungen oder Gefahreneinstufungen, sowie die Angabe ihrer wesentlichen Gefahreneigenschaften in einfachen Worten.

5. a. Allgemeine Informationen darüber, wie die betroffene Bevölkerung erforderlichenfalls gewarnt wird.

5. b. Angemessene Informationen über das Verhalten bei einem Störfall.

6. a. Datum der letzten Vor-Ort-Besichtigung im Rahmen einer Inspektion nach § 17 durch die zuständigen Überwachungsbehörden.

6. b. Unterrichtung darüber, wo ausführlichere Informationen zur Vor-Ort-Besichtigung und zum Überwachungsplan nach § 17 auf Anfrage eingeholt werden können.

7. Einzelheiten darüber, wo weitere Informationen eingeholt werden können.

Zu 5.b und 6.a.: alternativ kann auch ein Hinweis erfolgen, wo diese Informationen elektronisch zugänglich sind.

Es besteht die Möglichkeit, dass der Betreiber die Veröffentlichung von Informationen aus Gründen des Schutzes öffentlicher oder privater Belange einschränken kann. Dies bedarf der vorherigen Zustimmung der zuständigen Behörde nach den Bestimmungen des Bundes und der Länder über den Zugang zu Umweltinformationen.

Der Betreiber eines Betriebsbereichs der oberen Klasse hat der Öffentlichkeit auf Anfrage den Sicherheitsbericht nach § 9 unverzüglich zugänglich zu machen. Nach Zustimmung durch die zuständige Behörde kann der Betreiber einen geänderten Sicherheitsbericht, in dem nicht offen zu legenden Teile ausgespart sind, der Öffentlichkeit auf Anfrage zugänglich machen.

Betreiber von „Dominobetrieben“ nach § 15 Störfall-Verordnung müssen im Hinblick auf die Information der Öffentlichkeit zusammenarbeiten (§ 6 Absatz (2) der Störfall-Verordnung).

Die Informationen sind der Öffentlichkeit ständig zugänglich zu machen. Dies muss auf elektronischem Weg, z. B. im Rahmen des Internet, *aber auch vor Ort z. B. durch Schautafeln oder Informationsbroschüren, die an einer über einen angemessenen Zeitraum mit Personal besetzen Pforte hinterlegt werden,* erfolgen *(der kursive Text ist gegenüber /3/ aktualisiert worden)*.

Bei einer Verteilung von Informationsbroschüren an den betroffenen Bevölkerungskreis kann bei Betriebsbereichen der unteren Klasse als Anhaltspunkt der Achtungsabstand oder angemessene Abstand nach KAS-Leitfaden Nr. 18 für den Umkreis der Verteilung herangezogen werden.

Zusätzliche Anforderungen für Betriebsbereiche der oberen Klasse nach § 11und Anhang V Teil 2:

a. Die Informationen der Öffentlichkeit müssen zusätzlich Angaben nach Anhang V Teil 2 enthalten.
b. Der Betreiber eines Betriebsbereichs hat alle Personen und alle Einrichtungen mit Publikumsverkehr sowie Betriebsstätten oder benachbarte Betriebsbereiche, die von einem Störfall in diesem Betriebsbereich betroffen sein könnten, vor Inbetriebnahme über die Sicherheitsmaßnahmen und das richtige Verhalten im Fall eines Störfalls in einer auf die speziellen Bedürfnisse der jeweiligen Adressatengruppe abgestimmten Weise zu informieren. Dies kann durch Informationsbroschüren, die an die betroffenen Adressatengruppen im möglichen Einwirkbereich einer Anlage des Betriebsbereichs verteilt werden, geschehen. Der mögliche Einwirkbereich einer Anlage des Betriebsbereichs im Falle eines Störfalls ergibt sich aus den Ergebnissen einer Ausbreitungsberechnung für den Dennoch-Störfall. Die Informationsbroschüren enthalten zumindest die in Anhang V aufgeführten Angaben. Die Übermittelung dieser Informationen muss regelmäßig wiederholt werden müssen und darf in keinem Fall fünf Jahre überschreiten.
c. Die Informationen sind mit den Katastrophenschutz- und Gefahrenabwehrbehörden abzustimmen.
d. Der Betreiber hat die Informationen nach b. zu überprüfen, und zwar mindestens alle 3 Jahre und bei einer störfallrelevanten Änderung nach § 3 Absatz 5b des Bundes-Immissionsschutzgesetzes.
e. Soweit sich bei der Überprüfung Änderungen ergeben, die erhebliche Auswirkungen hinsichtlich der mit einem Störfall verbundenen Gefahren haben könnten, hat der Betreiber die Informationen unverzüglich zu aktualisieren und entsprechend b. zu wiederholen.

Der Teil 2 Weitergehende Informationen zu Betriebsbereichen der oberen Klasse des Anhangs V enthält die folgenden Anforderungen an die Inhalte der Informationen der Öffentlichkeit:

1. Allgemeine Informationen zu den Gefahren, die von einem Störfall ausgehen können, einschließlich ihrer möglichen Auswirkungen auf die menschliche Gesundheit und die Umwelt und zusammenfassende Darstellung der wesentlichen Störfallszenarien und der Maßnahmen, mit denen diese Szenarien verhindert werden oder ihre Auswirkungen begrenzt werden sollen.
2. Bestätigung, dass der Betreiber verpflichtet ist, auf dem Gelände des Betriebsbereichs – auch in Zusammenarbeit mit Notfall- und Rettungsdiensten – geeignete Maßnahmen zur Bekämpfung von Störfällen und zur größtmöglichen Begrenzung der Auswirkungen von Störfällen zu treffen.

3. Angemessene Informationen aus den externen Alarm- und Gefahrenabwehrplänen zur Bekämpfung der Auswirkungen von Ereignissen außerhalb des Betriebsgeländes mit der Aufforderung, allen Anordnungen von Notfall- oder Rettungsdiensten im Fall eines Ereignisses Folge zu leisten.
4. Gegebenenfalls Angabe, ob der Betriebsbereich in der Nähe des Hoheitsgebiets eines anderen Mitgliedstaats liegt und damit die Möglichkeit besteht, dass ein Störfall grenzüberschreitende Auswirkungen nach dem Übereinkommen über die grenzüberschreitenden Auswirkungen von Industrieunfällen der Wirtschaftskommission der Vereinten Nationen für Europa (UNECE) hat.

Eine ausreichende Information entsprechend der möglicherweise dennoch eintretenden Notsituation ist wichtig, um Fehlreaktionen der Bevölkerung zu vermeiden, bzw. eine eventuell nötige Evakuierung schnell durchführen zu können. Kriterien nach denen die Information der Öffentlichkeit erfolgt, müssen vorhanden sein.
Hierbei können zwei Aspekte unterschieden werden:

- Zum einen die Information der Öffentlichkeit im Vorfeld im Sinne des § 8a und 11 der Störfallverordnung und deren Anhang V.
- Zum anderen ist das Augenmerk zu richten auf die Informationswege zwischen Betreiber, Behörde und Bevölkerung im Ereignisfall. Dies wird in der Notfallplanung geregelt.

Die Verantwortlichkeiten für die jeweiligen Punkte müssen innerhalb des Betriebsbereichs klar geregelt sein, dies gilt auch für die Gestaltung der Schnittstellen zur externen Gefahrenabwehr. Überprüfungen zu allen o. g. Punkten müssen erfolgen. Wichtig ist auch eine regelmäßige Überprüfung der Information auf ihre Aktualität und wie die Information bei der Öffentlichkeit ankommt (werden alle Haushalte erreicht, sind die Informationen verständlich). Die Ausführung von Maßnahmen aufgrund der Ergebnisse aus den Überprüfungen ist zu überprüfen. Die Verantwortlichkeiten hierfür sind festzulegen.

5.6.2 Frage Nr. 2: Wie werden die Regelungen zum Prozess der Notfallplanung bewertet?

Bewertungshilfe:

Die Notfallplanung dient dazu, dass Betreiber von Betriebsbereichen bereits im Vorfeld Vorbereitungen treffen, wie im Notfall vorgegangen werden sollte, damit die Auswirkungen von Störfällen bzw. schweren Unfällen weitestgehend begrenzt werden können. Dazu muss systematisch untersucht werden, welche Notfälle denkbar sind, und wie eine angemessene Reaktion im Notfall aussehen sollte. Für den Notfall müssen Organisations- und Aufgabenverteilung eindeutig festgeschrieben und klare Regeln für Handlungen und Verhalten im Notfall gegeben werden. Dies gilt für alle Betriebsbereiche.
Bei mittelständischen und Großunternehmen sollte der Prozess „Notfallplanung“ in Form einer Verfahrensbeschreibung / Prozessbeschreibung / Managementanweisung etc. schriftlich festgelegt und dokumentiert sein, in welcher die folgenden Punkte berücksichtigt werden:

- Ziele,
- Anwendungsbereich (Betriebsbereich, ggf. abgestuft z. B. Organisationseinheiten des Betriebsbereiches, Anlagen),
- Definition der Begrifflichkeiten,
- Beschreibung der Prozessschritte und des Ablaufs:
  - Erstellung von (internen) Alarm- und Gefahrenabwehrplänen sowie weiteren Notfalldokumenten,
  - Schulungen,
  - Notfallübungen,
  - Meldepflichten,
  - Gefahrenabwehrkräfte,
  - Krisenstab,
  - Information, Abstimmung und Zusammenarbeit mit den externen Gefahrenabwehrorganisationen,
  - Information, Abstimmung und Zusammenarbeit mit weiteren Externen, z. B. Nachbarbetriebe,
  - Information der ggf. betroffenen Bevölkerung und sensibler Einrichtungen,
  - Identifizierung und Vorhaltung der notwendigen Sicherheitsausrüstungen / Einsatzmittel / Kommunikationseinrichtungen für Beschäftigte / Einsatzkräfte / Krisenstab.
- Festlegung der Inhalte der Prozessschritte und Aufgaben,
- Festlegung von Zuständigkeiten und Verantwortlichkeiten zu den Aufgaben,
- Berücksichtigung der Schnittstellen zu anderen Prozessen (z. B. Fortbildung, Ermittlung und Bewertung der Gefahren von Störfällen, internes Berichtsystem, Auditsystem),
- Festlegung von Dokumentationsinhalten bei den Prozessschritten.

Es müssen regelmäßige Überprüfungen erfolgen, ob die festgelegten Inhalte für den obigen Prozess (u. a. Ablauf, Verantwortlichkeiten, Inhalte, Schnittstellen) angemessen sind, dies kann z. B. im Rahmen von Audits erfolgen.

Die Betreiber von „Dominobetrieben“ nach § 15 Störfall-Verordnung müssen gemäß § 6 Störfall-Verordnung untereinander alle erforderlichen Informationen austauschen, damit sie in ihren internen Alarm- und Gefahrenabwehrplänen der Art und dem Ausmaß der Gesamtgefahr eines Störfalls Rechnung tragen können sowie bei der Übermittlung von Angaben zur Erstellung von externen Alarm- und Gefahrenabwehrplänen an die zuständige Behörde zusammenarbeiten. Die Zuständigkeiten für Zusammenarbeit, Austausch und Ermittlung, Zusammenstellung und Übermittlung dieser Informationen an die Behörden sind festzulegen. Eine regelmäßige Überprüfung und ggf. Aktualisierung dieser Punkte ist sicherzustellen.

Weitere Hinweise zu den Inhalten:

Ein sehr wichtiges Element in der Notfallplanung stellt die interne und externe Meldekette dar, welche die notwendigen Meldewege und ihre Auslösekriterien enthält. Die Meldewege müssen vorbereitet und festgelegt werden, z. B. in Form von Alarmierungsschemata, Telefon-, Melde- und Alarmierungslisten. Alle erstellten Unterlagen müssen einem festgelegten Überprüfungs- und Aktualisierungsverfahren unterliegen, insbesondere auf die Aktualität von Notfallrufnummern ist zu achten.
Ein Beispiel für die Ausgestaltung einer (externen) Meldekette ist das Vereinbaren eines Meldestufensystems für Vorabmeldungen an die Gefahrenabwehrbehörden, wie es im Anhang 3 der Vollzugshilfe zur Störfall-Verordnung dargestellt ist.

Eine Vorgehensweise zum Schutz von betriebsfremden Personen bei Notfällen muss existieren. Hierzu kann es ein abgestuftes Konzept geben (z. B. Besucher/innen werden durch Beschäftigte des Betriebsbereiches begleitet, ggf. erfolgt eine Unterweisung in die Sicherheitsvorkehrungen der besichtigten Betriebsteile, Unterweisungen für Mitarbeiter/innen von externen Firmen etc.). Es muss sichergestellt sein, dass eine einfache Kontrolle darüber gegeben ist, wie viele Personen sich in der Anlage / im Betriebsbereich befinden. Dies kann z. B. durch ein Meldekartensystem erfolgen.

Erläuterungen aus KAS-Leitfaden Nr. 29:

Zur Umsetzung der entsprechenden gesetzlichen Regelungen (u. a. Störfall-Verordnung) und zur Vorbereitung auf eventuelle Notfallsituationen wird empfohlen, folgenden Aufgaben spezifisch benannte Stellen in der Organisation zuzuweisen, präventiv zu üben und zu überprüfen. Diese sollten auch im Rahmen eines Notfallmanagements dokumentiert und im Ereignisfall abgearbeitet werden:

- Konzeptionelle und redaktionelle Bearbeitung von Alarm- und Gefahrenabwehrplänen (AGAP),
- Erstellen und Fortschreiben der für die Standortsituation notwendigen praktischen und juristischen Regelungen,
- Umsetzung geänderter gesetzlicher Rahmenbedingungen für den Standort,
- Organisation und Betreuung der Störungszentrale, Aufbau eines Krisenstabes,
- Organisation der bereichs- oder gesellschaftsübergreifenden Standortbereitschaften,
- Koordination des Vorgehens aller Beteiligten bei Schadensbewältigungen und Sicherstellung einer geordneten Kommunikation mit Behörden, Nachbarschaft und Presse,
- Aufarbeitung der Ereignisursachen.

Während einer Notfallsituation können Intransparenz, Dynamik und Unsicherheit der Situation ein Umschalten der Strategie erfordern, statt sich ggf. vorschnelles Handeln aufzwingen zu lassen. Wenn beispielsweise ein akuter Handlungsdruck besteht, ist zunächst eine Option zu wählen, die die Sicherheitslage verbessert und möglichst weitere Zeitreserven bringt (sogenannte no-regret-Entscheidung).
Dieses Umschalten kann am ehesten durch eine Person erfolgen, die sich gewissermaßen außerhalb des Geschehens und Handelns stellen kann (z. B. besondere/r Notfallmanager/in, Mitglied der Einsatzleitung, Betriebsleiter/in eines Nachbarbetriebes). **Insofern ist einer klugen Rollenzuweisung des Personals für die Notfallsituation besonderes Augenmerk zu schenken.** Günstig erweist sich auch, wenn sich die beteiligten Personen aus der Zusammenarbeit kennen, da sie nur so geteiltes Wissen (Wissen über die Gruppenmitglieder wie Kompetenzen, Aufgabenverteilung, Verantwortlichkeiten, entsteht nur aus der Erfahrung der Zusammenarbeit) entwickeln konnten.

Zur Vorbereitung auf Notfallsituationen sind die vorhandenen Ausrüstungsgegenstände und Hilfsmittel einer kritischen Betrachtung zu unterziehen. Da die Notfallsituation in der Regel von den Beteiligten als Stress erlebt wird, sollten alle Aspekte, die zusätzliche mentale Kapazitäten erfordern, minimiert werden, z. B. durch eine ergonomische Gestaltung von Anzeigen.

Weitere Hinweise

Regelungen zur Erstellung und Fortschreibung einer Notfallplanung müssen vorhanden sein.

Hierbei kann es Kriterien für Abstufungen (z. B. interne Alarm- und Gefahrenabwehrpläne (AGAP) nach § 10 der Störfall-Verordnung, Alarmpläne für Anlagen, Alarmordnungen für Verwaltungsgebäude, Kantinen etc.) geben, die z.B. Inhalt, Umfang (bevorzugt kurz, klar, knapp), Dokumentation, Fristen, Verteilung, Unterweisung betreffen.
Auf die Vollzugshilfe zur Störfallverordnung als Erkenntnisquelle wird hingewiesen.
Die Bereitstellung der erforderlichen Ressourcen und Hilfsmittel ist zu gewährleisten. Es sind zu beteiligende Personen und Stellen zu definieren. Es ist sinnvoll, Beschäftigte in die Notfallplanung mit einzubeziehen bzw. zwingend bei Anwendung des § 10 Störfall-Verordnung. Die Verantwortlichkeiten für die Erstellung und Fortschreibung der Notfallplanung sowie die Bereitstellung der Ressourcen müssen eindeutig geregelt sein. Definierte Kriterien für die zugrunde gelegten Szenarien können sinnvoll ein. Die Schnittstellen zur "Ermittlung und Bewertung der Gefahren von Störfällen" sind klar festzulegen. Regelungen und Verantwortlichkeiten zur regelmäßigen Überprüfung aller o. g. Punkte und Aktualisierung der Notfallplanung müssen existieren. Die Notfallplanung muss nach jeder Anlagenveränderung / -neuerung oder Veränderungen in Notdiensten überprüft und bei Bedarf entsprechend überarbeitet werden. Die Durchführung der ggf. erfolgten Aktualisierung ist zu überprüfen. Veränderungen sollten aufgrund besserer Reproduzierbarkeit entsprechend dokumentiert werden (Schnittstelle zu Lenkung von Dokumenten).

5.6.3 Frage Nr. 3: Wie werden die Regelungen zum Prozess der Erstellung und Überprüfung von Dokumenten zur Notfallplanung bewertet?

Bewertungshilfe:

Bei mittelständischen und Großunternehmen sollte der Prozess „Erstellung und Überprüfung von Dokumenten zur Notfallplanung“ in Form einer Verfahrensbeschreibung / Prozessbeschreibung / Managementanweisung etc. schriftlich festgelegt und dokumentiert sein (auf die mögliche Schnittstelle zum Prozess „Lenkung von Dokumenten“ wird hingewiesen) unter Berücksichtigung der folgenden Punkte:

- Ziele,
- Anwendungsbereich,
- Definition der Begrifflichkeiten,
- Beschreibung der Prozessschritte und Ablauf (Erstellung und Überprüfung von
  - Alarm- und Gefahrenabwehrplänen,
  - Alarmierungsschemata,
  - Telefon-, Melde- und Alarmierungslisten,
  - weitere Dokumente für Notfälle,
  - Informationen für die externe Gefahrenabwehr,
  - etc.)
- Festlegung der Inhalte der Prozessschritte und Aufgaben,
- Festlegung von Zuständigkeiten und Verantwortlichkeiten zu den Aufgaben,
- Berücksichtigung zu den Schnittstellen anderer Prozesse (z. B. Personal und Organisation, MoC, internes Berichtsystem, Auditsystem),
- Festlegung von Dokumentationsinhalten bei den Prozessschritten.

Es müssen regelmäßige Überprüfungen erfolgen, ob die festgelegten Inhalte für den obigen Prozess (u. a. Ablauf, Verantwortlichkeiten, Inhalte, Schnittstellen) angemessen sind, dies kann z.B. im Rahmen von Audits erfolgen.

Der Informationsfluss in Alarm- / Notfallsituationen im Rahmen der Notfallplanung muss klar festgelegt sein.

Hinweise zu den oben genannten Punkten z. B. einer Verfahrensanweisung:

Nach Anhang IV der Störfall-Verordnung müssen die Alarm- und Gefahrenabwehrpläne, welche Betreiber von Betriebsbereichen der oberen Klasse verpflichtend erstellen müssen, folgende Informationen beinhalten:

1. Namen oder betriebliche Stellung der Personen, die zur Einleitung von Sofortmaßnahmen ermächtigt sind, sowie der Person, die für die Durchführung und Koordinierung der Abhilfemaßnahmen auf dem Gelände des Betriebsbereichs verantwortlich ist.
2. Name oder betriebliche Stellung der Person, die für die Verbindung zu der für die externen Alarm- und Gefahrenabwehrpläne zuständigen Behörde verantwortlich ist.
3. Für vorhersehbare Umstände oder Vorfälle, die für das Auslösen eines Störfalls ausschlaggebend sein können, in jedem Einzelfall eine Beschreibung der Maßnahmen,

die zur Kontrolle dieser Umstände bzw. dieser Vorfälle sowie zur Begrenzung der Auswirkungen zu treffen sind, sowie eine Beschreibung der zur Verfügung stehenden Sicherheitsausrüstungen und Einsatzmittel.

4. Vorkehrungen zur Begrenzung der Risiken für Personen auf dem Gelände des Betriebsbereichs, einschließlich Angaben über die Art der Alarmierung sowie das von den Personen bei Alarm erwartete Verhalten.
5. Vorkehrungen zur frühzeitigen Warnung der für die Einleitung der in den externen Alarm- und Gefahrenabwehrplänen vorgesehenen Maßnahmen zuständigen Behörde, Art der Informationen, die bei der ersten Meldung mitzuteilen sind, sowie Vorkehrungen zur Übermittlung von detaillierteren Informationen, sobald diese verfügbar sind.
6. Vorkehrungen zur Ausbildung und Schulung des Personals in den Aufgaben, deren Wahrnehmung von ihm erwartet wird, sowie gegebenenfalls zur Koordinierung dieser Ausbildung und Schulung mit externen Notfall- und Rettungsdiensten.
7. Vorkehrungen zur Unterstützung von Abhilfemaßnahmen außerhalb des Geländes des Betriebsbereichs.

Nach § 10 der Störfall-Verordnung sind an der Erstellung der internen Alarm- und Gefahrenabwehrpläne die Beschäftigten zu beteiligen sowie die interne Alarm- und Gefahrenabwehrpläne zu überprüfen und zwar regelmäßig (mindestens alle drei Jahre) oder anlassbezogen und ggf. (unverzüglich) zu aktualisieren.
Kriterien für eine anlassbezogene Überprüfung können z. B. sein:

- Ereignisse,
- Erkenntnisse aus Notfallübungen,
- neue technische Erkenntnisse und Erkenntnisse darüber, wie bei Störfällen zu handeln ist,
- Änderungen im Betriebsbereich: organisatorische, technische, managementspezifischer Art:
- (sicherheitsrelevante) Anlagenänderungen,
- Änderungen der internen Gefahrenabwehr,
- geänderte Vorschriften,
- geänderte Anforderungen oder Ressourcen bei der externen Gefahrenabwehr,
- Hilfeleistungsorganisationen und Institutionen/Behörden,
- geänderte Adressen / Telefonnummern.

Erläuterungen aus dem KAS-Leitfaden Nr. 19:

Die Erstellung von Alarm- und Gefahrenabwehrplänen nach § 10 und Anhang IV Störfall-Verordnung ist nur für Betriebsbereiche der oberen Klasse verbindlich vorgeschrieben.
Für **Betriebsbereiche der unteren Klasse** gelten dennoch einige Mindeststandards nach anderen Regelwerken:

- Erstellung von Flucht- und Rettungsplänen,
- Erstellung von Feuerwehrplänen nach DIN 14095,
- Anwendung der BGV A1 (UVV Grundsätze der Prävention), z. B. Maßnahmen bei besonderen Gefahren, Erste Hilfe, Persönliche Schutzausrüstung,
- Betriebsanweisung nach § 14 GefStoffV, u. a. mit Informationen über Maßnahmen, die von den Beschäftigten, insbesondere von Rettungsmannschaften, bei Betriebsstörungen, Unfällen und Notfällen und zur Verhütung von diesen durchzuführen sind.

Sinnvoll sind die Bereithaltung von Notfallnummern und die Vorbereitung der Meldewege, ggf. auch die Einrichtung eines internen Bereitschaftsdienstes sowie die Regelung der Entscheidungsbefugnisse für den Notfall. Alle erstellten Unterlagen müssen einem festgelegten Überprüfungs- und Aktualisierungsverfahren unterliegen.

Im Hinblick auf Notfallsituation sollen Arbeitsanweisungen die folgenden Anforderungen erfüllen (KAS-Leitfaden Nr. 29):

- Informationen sollen nach ihrer Art wie Anforderungen, Arbeitsschritte etc. gruppiert werden.
- Die notwendigen Handlungsschritte sollen in kurzen, nummerierten Aufzählungen entsprechend ihres auszuführenden Ablaufs dargestellt sein, z. B.
    - Öffnen des Ventils xy,
    - Öffnen des Ventils yz
    - und nicht 1: Öffnen des Ventils yz nachdem Ventil xy geöffnet wurde.
- Ein Handlungsschritt soll mit einem Verb beginnen und es soll nur einer pro Schritt genannt werden. Handlungsschritte müssen präzise und eindeutig genannt werden, Formulierungen wie annähernd oder geeignet sollen vermieden werden.
- Das Personal soll keine mentalen Rechenoperationen wie Kopfrechnen oder wie schriftliches Addieren vollziehen müssen.
- Warnungen oder Sicherheitsanforderungen sollen hervorgehoben werden.
- Der Text soll durch klare Überschriften strukturiert werden.
- Die Verwendung von Passiv oder doppelten Verneinungen soll vermieden werden.
- Der Sprachgebrauch soll konsistent, an den Anwender angepasst sein. Wenn Abkürzungen oder spezifische technische Begriffe genannt werden, müssen sie erklärt und in allen Unterlagen konsistent verwendet werden.

Das Abarbeiten von Arbeitsschritten kann ggf. durch Checklisten erleichtert werden, die entsprechend vorbereitet werden sollen. Anweisungen für den Notfall sollten kurz, präzise und einfach verständlich sein sowie sich auf das Wesentliche beschränken. Hilfreich ist es, solche für typische Ausfallszenarien (u. a. von Strom und Kühlung) auch in Papierform griffbereit zu haben.
Bei der Planung ist auch zu berücksichtigen, ob in der Notfallsituation ggf. verschiedene Aufgaben von mehreren Personen gleichzeitig durchgeführt werden sollen. Ist dies der Fall, müssen die Arbeitsanweisungen mindestens in entsprechender Anzahl vorhanden sein.
Weiterhin ist zu prüfen, ob einzelne Handlungsschritte an entfernten Orten durchgeführt werden müssen, auch dort sollten dann Anweisungen vorhanden sein, bzw. die entsprechenden Seiten als „Mitnahmeexemplar“ gestaltet werden.
Sollen Hilfsmittel, Komponenten oder Anlagenteile verwendet werden, die nicht täglich gebraucht werden, sind Abbildungen in den Anweisungen eine geeignete Gedächtnisstütze für die Handelnden.

Als absolut notwendig hat sich das Vorhalten von aktuellen Telefonlisten, Melde- und Alarmierungslisten erwiesen.

5.6.4 Frage Nr. 4: Wie werden die Regelungen zum Prozess der Unterweisung / Durchführung von Notfallübungen / Erprobung von AGAP bewertet?

Bewertungshilfe:

Da sich die Notfallsituation grundlegend von der Normalsituation unterscheidet, sind Vorbereitungen in Form von regelmäßigen Unterweisungen, Schulungen und Übungen zwingend notwendig. Regelungen zum Prozess „Unterweisung / Schulung / Übung zu Notfallsituationen" betreffen Beschäftigte des Betriebsbereiches aber auch betriebsfremde Personen oder Organisationen (z. B. öffentliche Feuerwehr) und beinhalten auch die Durchführung von Notfallübungen, Erprobung von Alarm- und Gefahrenabwehrplänen oder Übungen zum Einsatz eines Krisenstabes.

Bei mittelständischen und Großunternehmen sollte der Prozess „Unterweisung / Schulung / Übung zu Notfallsituationen" in Form einer Verfahrensbeschreibung / Prozessbeschreibung / Managementanweisung etc. schriftlich festgelegt und dokumentiert sein - die Schnittstelle zum Prozess „Einarbeitung / Fortbildung / Qualifizierung von Beschäftigten" ist zu berücksichtigen. Die folgenden Punkte sollten im Prozess „Unterweisung / Schulung / Übung zu Notfallsituationen" berücksichtigt werden, wobei ggf. Teile davon auch durch den Prozess „Einarbeitung / Fortbildung / Qualifizierung von Beschäftigten" abdeckbar sind:

- Ziele, die mit dem Prozess „Unterweisung / Schulung / Übung zu Notfallsituationen" erreicht werden sollen (z. B. Effektives Handeln in Notfallsituationen, regelmäßige Teilnahme aller Beschäftigten im Betriebsbereich),
- Anwendungsbereich (z. B. Betriebsbereich, Organisationseinheiten des Betriebsbereiches, Anlagen, Schichten, Besucher/innen, Beschäftigte externer Firmen),
- Definition der Begrifflichkeiten,
- Beschreibung der Prozessschritte und Ablauf (Qualifizierungsmaßnahmen: Aufstellung von Unterweisungs- / Schulungs- und Übungsplänen und deren Inhalte, die Durchführung und die Auswertung der durchgeführten Qualifizierungsmaßnahmen, Zeitpunkte für die Durchführung von Qualifizierungsmaßnahmen (Intervalle (Unterweisung und Erprobung von Alarm- und Gefahrenabwehrplänen: mindestens alle drei Jahre), anlassbezogen etc.)),
- Festlegung der Inhalte der Prozessschritte und Aufgaben (Unterweisung und Erprobung von Alarm- und Gefahrenabwehrplänen, Art der Übung, einzubeziehender Personenkreis (Beschäftigte des Betriebsbereiches, von externen Firmen, externe Hilfeleistungsorganisationen und Gefahrenabwehrorganisationen),
- Auswertung der Erfahrungen bei den Qualifizierungsmaßnahmen, Umsetzung der Maßnahmen aus der Auswertung),
- Festlegung von Zuständigkeiten und Verantwortlichkeiten zu den Aufgaben,
- Berücksichtigung zu den Schnittstellen anderer Prozesse (z. B. Personal und Organisation, MoC, internes Berichtsystem, Auditsystem),
- Festlegung von Dokumentationsinhalten bei den Prozessschritten.

Es müssen regelmäßige Überprüfungen erfolgen, ob die festgelegten Inhalte für den obigen Prozess (u. a. Ablauf, Verantwortlichkeiten, Inhalte, Schnittstellen) angemessen sind, dies kann z. B. im Rahmen von Audits erfolgen.

Die Inhalte der Unterweisungen stellen insbesondere die vollständige Kenntnis über die notwendigen aktuellen Meldewege und ihre Auslösekriterien sicher.

Es haben Überprüfungen zu erfolgen, die auch untersuchen, ob die Unterweisungen über die relevanten Inhalte des Verhaltens in Notfällen sachgemäß vermittelt und von den unterwiesenen Personen verstanden wurden. Die Verantwortlichkeiten sind festzulegen.

Unterweisungen von neuen Mitarbeitern und Mitarbeiterinnen über die Inhalte der Notfallplanung sind zu Beginn der Aufnahme ihrer Tätigkeit zu gewährleisten. Bei Anwendung des § 10 (3) der Störfall-Verordnung muss dies vor der erstmaligen Beschäftigungsaufnahme erfolgen und gilt auch für nicht nur vorübergehend beschäftigtes Personal von Subunternehmen. Sinnvollerweise können diese Inhalte zur Notfallplanung im Rahmen der Regelungen zur Einarbeitung zu integriert werden (mögliche Schnittstelle zum Prüfgebiet Organisation und Personal).

Eine Vorgehensweise zum Schutz von betriebsfremden Personen bei Notfällen muss existieren. Hierzu kann es ein abgestuftes Konzept geben (z. B. Besucher/innen werden durch Beschäftigte des Betriebsbereiches begleitet, ggf. erfolgt eine Unterweisung in die Sicherheitsvorkehrungen der besichtigten Betriebsteile, Unterweisungen für Mitarbeiter/innen von externen Firmen etc.). Es muss sichergestellt sein, dass eine einfache Kontrolle darüber gegeben ist, wie viele Personen sich in der Anlage / im Betriebsbereich befinden. Dies kann z. B. durch ein Meldekartensystem erfolgen. Für die Unterweisung von Beschäftigten externer Firmen kann eine Schnittstelle zum Prüfgebiet Überwachung des Betriebs existieren bzw. die Unterweisung über das Verhalten bei Notfällen in die Sicherheitsunterweisung integriert sein.

Hinweise zu den oben genannten Punkten z. B. einer Verfahrensanweisung, Elemente aus dem KAS-Leitfaden 29:

Bei der Bewältigung von Notfallsituationen spielen nicht nur Kognitionen (z. B. Denken oder Wissen), sondern auch Emotionen (z. B. Angst) und Handlungsmotive (z. B. Eigenrettung) eine Rolle.

Die Vermittlung von erforderlichen Kompetenzen für Notfallsituationen soll in Trainingsmaßnahmen für die Beschäftigten erfolgen. Daher sollten Trainings für das Nicht-Planbare folgende Inhalte berücksichtigen:

- Teambildung und Aufrechterhalten der Funktionsfähigkeit des Teams auch bei starkem Handlungsdruck und Misserfolgen,
- Verfahren für Entscheidungen unter Unsicherheit und Zeitdruck (z. B. FORDEC),
- Führungsverhalten in der kritischen Situation, flexible Handhabung der Führungserfordernisse,
- Wissen um die typischen Fehler und Fallstricke beim Handeln unter Unbestimmtheit und Zeitnot wie eingeschränkte Hypothesenbildung, Vernachlässigen der Handlungskontrolle,
- Wissen um die Mechanismen (und Fehlertendenzen) bei der Lagebeurteilung unter der Bedingung unzureichender und unzuverlässiger Informationen und Methoden des konstruktiven Umgangs mit informationeller Überlastung,
- Einsicht in die persönlichen Reaktionsmuster bei Stress und emotionaler Belastung sowie Stressreduktion,
- Methoden für die Entwicklung eines gemeinsamen Situationsverständnisses.

Die in den Trainings vermittelten Inhalte sollten in Simulationen von Notfallsituationen verfestigt werden. Art von Übungen können sein:

- Alarmierungsübungen,
- Training zur Steigerung der Nachrichtenklarheit,
- Planbesprechung/Planübung,
- Stabsübungen,
- Krisenstabstraining,
- Stabsrahmenübungen,
- Strategische Krisenmanagementübungen,
- Übungen für Teilfunktionen,
- Vollübungen / Simulationen.

Möglich ist auch die Nutzung von virtueller Realität für Unfallsimulatoren, die in Verbindung mit dem Simulator des Prozessleitsystems auch für das Notfalltraining von Anlagenpersonal genutzt werden können. Außerdem hat es sich als äußerst hilfreich erwiesen, mit den Mitgliedern von Krisenstäben Medientrainings durchzuführen.

Auch kleinen und mittleren Betrieben wird empfohlen, mit örtlichen Feuerwehren, Behörden und Polizei Übungen durchzuführen.

5.6.5 Frage Nr. 5: Wie wird die Regelung der Entscheidungsbefugnisse im Betriebsbereich für den Notfall bewertet?

Bewertungshilfe:

Hingewiesen wird auch auf § 12 (1) Nr. 2 der Störfall-Verordnung, wonach Betreiber von Betriebsbereichen der oberen Klasse der zuständigen Behörde eine mit der Begrenzung der Auswirkung von Störfällen beauftragte Person oder Stelle benennen müssen.

Wer wann die Entscheidung trifft, ob die Planung für den Notfall aktiviert wird, sollte möglichst weit oben in der Firmenhierarchie liegen und in Zusammenarbeit mit den/der für die Sicherheit Verantwortlichen (z. B. Störfallbeauftragte/r, eine Sicherheitsabteilung, Anlagenleitung,) nach definierten Kriterien festgelegt werden.
Kriterien, die eine Rolle spielen können sind insbesondere der Zeitfaktor, aber auch entsprechende Befugnisse, Kompetenzen und der Position angemessene Übernahme von Verantwortung durch die Person, welche die Entscheidungen trifft bzw. umsetzt.

Positiv zu bewerten sind klare abgestufte angemessene Entscheidungsbefugnisse, die u. a. beginnen mit der Festlegung in einer Betriebsanweisung der Anlage bei welchem Alarmwert die Betriebsleitung zu informieren ist oder bei welchen Alarmwerten die Betriebsleitung über die einzuleitenden Maßnahmen entscheidet.
Die Aktualität diese Festlegungen ist sicherzustellen und muss regelmäßigen Überprüfungen unterliegen.

Elemente aus dem KAS-Leitfaden 29:

Bei der Bewältigung von Notfallsituationen müssen in der Regel Entscheidungen unter hoher Unsicherheit und mit Zeitdruck getroffen werden. Fehlentscheidungen können katastrophale Folgen haben. Für Piloten und Pilotinnen wurde die FORDEC-Methode zur strukturierten Entscheidungsfindung in kritischen Situationen entwickelt, die analog für Gefahrensituationen in technischen Anlagen angewandt werden kann. Entscheidungen sollen so robuster gegen vorschnelle – und damit gegebenenfalls unangemessene – Impulse und Gefühlseinflüsse werden und sind im Rahmen der Qualifizierungsmaßnahmen zu trainieren.

Auch während der Notfallsituation können Intransparenz, Dynamik und Unsicherheit der Situation ein Umschalten der Strategie erfordern, statt sich ggf. vorschnelles Handeln aufzwingen zu lassen. Wenn beispielsweise ein akuter Handlungsdruck besteht, ist zunächst eine Option zu wählen, die die Sicherheitslage verbessert und möglichst weitere Zeitreserven bringt (sogenannte no-regret-Entscheidung). Dieses Umschalten kann am ehesten durch eine Person erfolgen, die sich gewissermaßen außerhalb des Geschehens und Handelns stellen kann (z. B. besondere/r Notfallmanager/in, Mitglied der Einsatzleitung, Betriebsleiter/in eines Nachbarbetriebes).

Der Informationsfluss in Alarm- / Notfallsituationen im Rahmen der Notfallplanung muss klar festgelegt sein.

Die Einbindung der für die Sicherheit Verantwortlichen in Alarmsituationen ist klar zu festzulegen.
Die für die Sicherheit Verantwortlichen sollten umgehend und vollständig informiert werden. Eine vollständige Information kann z. B. durch einen Unfall/Störfallbogen erfüllt werden. Hier kann eine Schnittstelle zum Prüfgebiet „SMS: Überwachung der Leistungsfähigkeit des SMS vorliegen“. Inhalt des Bogens kann sein: Genauer Ort des Vorfalls, Angabe der Anzahl der Verletzten, Angabe der Schadensart, Angabe des Ausmaßes, Angabe der beteiligten Stoffe (mögliches Beispiel in der Vollzugshilfe zur Störfall-Verordnung). So kann verhindert werden, dass aufgrund von Stress wichtige Angaben vergessen oder erst zu spät gemacht werden. Allerdings ist der Umfang so zu gestalten, dass die Ausführung den Arbeitsablauf nicht unnötig behindert. Die Verantwortlichkeiten sind so festzulegen, dass der Informationsfluss sichergestellt ist.

5.6.6 Frage Nr. 6: Wie sind die Regelungen der Meldepflichten zu bewerten?

Bewertungshilfe:

Es müssen schriftliche Regelungen im Betriebsbereich zur Erfüllung der Meldepflichten nach Störfall-Verordnung vorhanden sein.

Bei großen Firmen / Organisationen kann dies auf der Ebene von Verfahrensanweisungen / Prozessbeschreibungen etc. erfolgen, ggf. jedoch auch Bestandteil im AGAP oder einer Verfahrensanweisung / Prozessbeschreibung zur externen Kommunikation sein.

Bei **Kleinstbetrieben** kann dies z. B. ein Abschnitt im Managementhandbuch sein.

Die Verantwortlichkeiten der beteiligten Beschäftigten und ihre Befugnisse für die Aufgaben im Rahmen der Meldepflichten sind klar und eindeutig zu regeln.

Auf die Schnittstelle zum internen Berichtssystem (siehe Prüfgebiet „SMS: Überwachung der Leistungsfähigkeit des Sicherheitsmanagementsystems“, Bewertungshilfe zur Frage „Wie wird der Prozess internes Berichtssystem bzw. die Regelungen zur Erfassung von und Umgang mit Ereignissen bewertet?“) ist zu achten, da meldepflichtige Ereignisse auch dort mit einfließen sollen.

Die regelmäßige Überprüfung der Regelungen muss sichergestellt sein. Dies kann z. B. im Rahmen des Auditsystems erfolgen.

Der Betreiber hat nach § 19 Meldeverfahren Störfall-Verordnung der zuständigen Behörde unverzüglich den Eintritt eines Ereignisses, das die Kriterien des Anhangs VI Teil 1 Störfall-Verordnung erfüllt, mitzuteilen. Er hat der zuständigen Behörde unverzüglich, spätestens innerhalb einer Woche nach Eintritt eines Ereignisses, eine ergänzende schriftliche Mitteilung vorzulegen, die mindestens die Angaben nach Anhang VI Teil 2 Störfall-Verordnung enthält. Er hat die Mitteilung bei Vorliegen neuer Erkenntnisse unverzüglich zu ergänzen oder zu berichtigen.

Für den Betreiber eines Betriebsbereichs können Meldepflichten nach anderen Rechtsvorschriften bestehen, z. B. nach Betriebssicherheitsverordnung oder nach Umwelt-Schadensanzeige.

5.6.7 Frage Nr. 7: Wie sind die Regelungen zum Krisenstab zu bewerten?

Bewertungshilfe:

Elemente aus dem KAS-Leitfaden 29, Kap. 6.3 Notfallmanagement – Technische Einsatzleitung, Krisenstab:

Im Folgenden werden verschiedene Aspekte und Besonderheiten der Notfallorganisation anhand von Beispielen aus größeren chemischen Betrieben beschrieben.

Für KMU gelten aber entsprechende Anforderungen und sollten in angemessener Weise umgesetzt werden. So erscheint es z. B. als gute Praxis, dass Betriebe, die nicht über entsprechende eigene Ressourcen verfügen, sich mit den entsprechenden externen Kräften (z. B. Behörden, Feuerwehren, Katastrophenschutzbehörden, usw.) zusammensetzen und für eventuelle Notfälle ein gemeinsames Vorgehen im Sinne des hier beschriebenen vereinbaren (siehe auch VCI-Leitfaden Notfallmanagement – Gefahrenabwehr 2010, Merkblätter Band 45: Musterkonzept für die Notfallplanung, LANUV NRW).
Dazu sind auf betrieblicher und behördlicher Seite **Organisationseinheiten (Stäbe)** einzurichten. Sie setzen sich i. d. R. aus einer **operativen („technischen") Einsatzleitung (TEL)** und einem **administrativ-organisatorischen Stab (Krisenstab)** zusammen.
Diese Stäbe sind eine besondere Organisationsform, die keine ständigen Einrichtungen sind und ereignisabhängig für einen begrenzten Zeitraum nach einem vorbestimmten Organisationsplan gebildet und besetzt werden.
Die **Technische Einsatzleitung** leitet und verantwortet die Maßnahmen der operativen Gefahrenabwehr und wird durch die Werk- oder die öffentliche Feuerwehr gestellt. Sie ist für die unmittelbaren Maßnahmen am Einsatzort und die Kommunikation zu externen Gefahrenabwehrorganisationen sowie zum Krisenstab verantwortlich.
Mitglieder der technischen Einsatzleitung sind Führungskräfte der internen Gefahrenabwehrorganisation, d. h. zum Beispiel der Werkfeuerwehr und der Werksicherheit.
In Betrieben, die nicht über eine Werkfeuerwehr verfügen, liegt die Führung der Technischen Einsatzleitung bei der für die Gefahrenabwehr zuständigen Behörde. In Katastrophenfällen gilt dies auch bei Unternehmen mit eigener Werkfeuerwehr.

Unabhängig von der Verfügbarkeit einer Werkfeuerwehr sollten Betrieb und Behörde jeweils einen **Krisenstab** einrichten. Den Krisenstäben des Betriebes obliegt die Koordination unterstützender Maßnahmen für die Gefahrenabwehr, sie verantworten die Kommunikation nach innen und außen und vertreten das Unternehmen gegenüber Behörden und Öffentlichkeit. Sie werden von Personen mit Schlüsselqualifikationen (siehe unten) besetzt, unter der Leitung einer verantwortlichen Person mit Führungserfahrung, um auch unter Druck schnelle Entscheidungen treffen zu können.
Ein typischer Stab setzt sich zusammen aus Werksleiter oder Werksleiterin, Ereignismanager oder Ereignismanagerin sowie Personen aus den Funktionsbereichen Kommunikations- und Öffentlichkeitsarbeit, Gesundheit, Sicherheit und Umwelt. Außerdem ist eine Vertretung des betroffenen Bereiches hinzuzuziehen, die Aussagen zu den Anlagen und Stoffen treffen kann.
Alle diese Funktionen sind in einer kontinuierlichen 24/7-Bereitschaft vorzuhalten.

Die Unternehmensleitung (zum Beispiel CEO (Chief Executive Officer: vergleichbar u. a.: Geschäftsführer/in)) sollte auf keinen Fall die Führung des Krisenstabes übernehmen. Ihre Aufgabe liegt eher in der Bewältigung der verschiedenen Schnittstellen zu den Stakeholdern (zum Beispiel Kunden, Öffentlichkeit).

Die **Befugnisse eines Krisenstabes im Ereignisfall** sind in einer Vereinbarung mit den produzierenden Bereichen zu regeln:

- Zutrittsrechte, „Schlüsselgewalt“ (wird zum Beispiel über den Werkschutz ausgeübt),
- Befugnis zur Lastveränderung / Abstellung von Produktionsanlagen,
- Recht, bei Ereignissen im Rahmen des Stoff- und Energieverbundes Kürzungen vorzunehmen,
- Weisungsbefugnis gegenüber Mitgliedern anderer Bereiche oder Gesellschaften,
- Erlaubnis, erste Sachverhalte über betroffene Bereiche möglichst abgestimmt im Rahmen der Gefahrenabwehr an Behörden und Öffentlichkeit weiterzugeben.

Typische **Aufgaben des Krisenstabs** sind:

- Operationsbasis schaffen (Zusammentreten, Kommunikationsschiene zur Technischen Einsatzleitung (TEL) und zu anderen Stellen aufbauen, Lage erfassen - Stand der Ereignisbekämpfung?, Welche Erstmaßnahmen sind erfolgt?, Ereignisbeschreibung, Lagefortbeschreibung),
- Informieren (betroffene Gesellschaft / Geschäftsbereich / Konzern, Behörden, Polizei, Öffentlichkeit (Pressegespräch, Pressemitteilung), Medieninformation, Bürgertelefon),
- Gefährdung ermitteln – Warnen (Beteiligung von gefährlichen Stoffen klären, Immissionsmessungen, Probenahmen, Beschäftigte warnen, Bevölkerung warnen (via Einsatzzentrale)),
- Ereignisbekämpfung unterstützen (Unterstützung der technischen Einsatzleitung (TEL), Schutzmaßnahmen für das Umfeld organisieren, technische Maßnahmen veranlassen: Energie(not)versorgung, Abstellen von Anlagen, Anlagenbereich sichern, absperren, Gebäude räumen, Lüftung etc. abschalten),
- Nachsorge (Pressekonferenz, Manöverkritik, weitere Maßnahmen einleiten: Freigabe / Sperrung des Anlagenbereichs, Entsorgung von Löschwasser, Ermittlung der Ursache, Ermittlung der Schadenshöhe etc.).

Der Krisenstab kann und soll *externe Unterstützung für folgende Aufgaben* einholen, falls diese notwendig sind und nicht im Unternehmen geleistet werden können:

- Psychologische Betreuung von Beteiligten und Betroffenen,
- Betrieb eines Call-Centers für die Öffentlichkeit,
- Daten-Management,
- Logistik,
- Transporte,
- Unterkunft,
- Kommunikation.

Es ist ein Krisenstabsraum einzurichten, der mit der geeigneten Technik für das Krisenmanagement ausgestattet ist. Hier ist zu überlegen, welche Technik, z. B. Kommunikationsmittel, redundant ausgelegt sein soll und für welche eine Notstromversorgung zu planen ist. Es ist dafür zu sorgen, dass die Technik regelmäßig geprüft und ggf. Instand gehalten wird. Die Verwendung der technischen Hilfsmittel sollte geschult werden.

Des Weiteren sind folgende Regeln für die Gestaltung von Krisenstäben einzuhalten:

Krisenstäbe agieren zurückgezogen, vorzugsweise in einer nicht öffentlich zugänglichen Einsatzzentrale, nicht aber vor Ort.
Der Krisenstab ist ein Beratungs- und Koordinierungsgremium, das im Fall einer Krise die Führung der Notfall- und Krisenorganisation übernimmt sowie Entscheidungen eines Funktionsträgers vorbereitet und unterstützt.
Die Schnittstellen zu anderen Organisationen / Stäben sind zu planen.
Der Krisenstab hat eine klar strukturierte und hierarchisch aufgebaute Organisationsform (ähnlich wie beim Militär). Allerdings müssen Führungskräfte für Notfallsituationen flexibel führen können, beispielsweise während einer sehr dynamischen Lage direktiv, aber in Vor- und Nachbereitung offen und integrativ.
Die Mitglieder des Krisenstabes sollen Funktionen übernehmen, die sie im Normalbetrieb haben, allerdings muss jedes Mitglied bereit sein, auch andere Aufgaben zu übernehmen. Im Krisenstab sollen auch Mitglieder vertreten sein, die erfahren im Umgang mit Behörden, Presse und der Öffentlichkeit sind.
Es sind schriftliche Funktionsbeschreibungen mit Aufgaben, Verantwortlichkeiten, Kompetenzen und Schnittstellen notwendig. Es ist darauf zu achten, dass konkurrierende Doppelaufgaben vermieden werden.

Mitglieder von Krisenstäben müssen über die folgenden individuellen Kompetenzen verfügen:

- Kommunikationskompetenz,
- Kritikfähigkeit, Kooperativität und Vertrauen,
- Entscheidungsfähigkeit,
- Problemlösekompetenz,
- Ressourcen und Grenzen der eigenen Person kennen,
- unter emotionaler Belastung arbeiten,

und über die folgenden organisatorisch strategischen Fähigkeiten verfügen:

- Informationsverarbeitung und -integration,
- Definition von Handlungsschwerpunkten,
- Strukturen und Mechanismen der Zusammenarbeit,
- Methoden der Entscheidungsfindung,
- flexible Anpassung an die Umstände, d. h. Mitglieder von Krisenstäben müssen über vertiefte Kompetenzen verfügen (vgl. Tabelle 1 des Leitfadens KAS-20 „Kompetenzen bezüglich menschlicher Faktoren im Rahmen der Anlagensicherheit“).

5.6.8 Frage Nr. 8: Wie wird die Zusammenarbeit mit den externen Notfall- und Rettungsdiensten bewertet?

Bewertungshilfe:

Die Zusammenarbeit der mit der betrieblichen Gefahrenabwehr beauftragten Stelle (z. B. Werkfeuerwehr) mit den externen Notfall- und Rettungsdiensten (z. B. öffentliche Feuerwehr) sollte klar definiert sein und regelmäßigen Überprüfungen unterliegen.
Sinnvoll ist es, regelmäßig einen Teil der Notfallübungen gemeinsam mit der öffentlichen Feuerwehr durchzuführen. Möglich ist es auch, dass zum Teil eine Ausbildung und technische Betreuung des externen Notfall- und Rettungsdienstes durch die mit der betrieblichen Gefahrenabwehr beauftragten Stelle erfolgt, so dass im Notfall nicht noch langwierige Unterweisungen (z. B. Beschreibung der Zufahrt, spezielle Gefahren etc.) erfolgen müssen.

Hingewiesen wird auf § 12 der Störfall-Verordnung nach dem der Betreiber eines Betriebsbereichs der oberen Klasse eine Person oder Stelle mit der Begrenzung der Auswirkungen von Störfällen zu beauftragen hat und diese der zuständigen Behörde benennen muss.

5.6.9 Frage Nr. 9: Wie werden die Regelungen zur Ausstattung der betrieblichen Gefahrenabwehrkräfte bewertet?

Bewertungshilfe:

Es existieren Kriterien zur personellen Besetzung der Gefahrenabwehrkräfte und ihrer Ausrüstung, die Verantwortlichkeiten hierfür sind festgelegt. Eine regelmäßige Überprüfung der Kriterien erfolgt.

Die personelle Besetzung und die Ausrüstung sollten im Einklang mit den aus den Gefahrenanalysen gemachten Erkenntnissen stehen, sodass eine klare Struktur gegeben ist, wie alle auf dem Werksgelände möglichen Unfälle beherrscht werden können.
Darüber hinaus werden Auswertungen von Einsätzen und Notfallübungen, sowie die Erfahrungen anderer Gefahrenabwehrstellen (regelmäßiger Erfahrungsaustausch) berücksichtigt.

Es existieren Regelungen, die sicherstellen, dass die Ausrüstung der mit der betrieblichen Gefahrenabwehr beauftragten Stelle mindestens den gesetzlichen Anforderungen entspricht. Zur Vorbereitung auf Notfallsituationen sind die vorhandenen Ausrüstungsgegenstände und Hilfsmittel einer kritischen Betrachtung zu unterziehen. Da die Notfallsituation in der Regel von den Beteiligten als Stress erlebt wird, sollten alle Aspekte, die zusätzliche mentale Kapazitäten erfordern, minimiert werden, z.B. durch eine ergonomische Gestaltung von Anzeigen (KAS-Leitfaden Nr. 29). Mehr Informationen und Beispiele hierzu finden sich im KAS-Leitfaden Nr. 29.
Wenn die Gefahrenabwehrkräfte durch Beschäftigte von Anlagen des Betriebsbereiches verstärkt werden, so ist sicherzustellen, dass hierdurch nicht an anderer Stelle Gefahren entstehen.
Das Personal einer zentralen Meldestelle kann ggf. im Einsatzfall als Leitstelle fungieren, da hier alle Informationen zusammenlaufen.
Die Verantwortlichkeiten für alle genannten Punkte und die Überprüfungszyklen sind festzulegen.

5.6.10 Frage Nr. 10: Wie wird die Vorgehensweise zur Ausstattung des Betriebsbereiches mit den erforderlichen Warneinrichtungen bewertet?

Bewertungshilfe:

Es existieren Regelungen nach denen die Festlegung erforderlicher Warneinrichtungen, sowie deren Umsetzung und Überprüfung erfolgt. Die jeweils Verantwortlichen hierfür müssen festgelegt sein. Es muss sichergestellt sein, dass die erforderlichen Einrichtungen im Ereignisfall funktionieren (z. B. Energieversorgung).

5.7 SMS: Überwachung der Leistungsfähigkeit des Sicherheitsmanagementsystems

Dieses Prüfgebiet enthält die folgenden Fragen:

Frage Nr. 1: Wie wird der Prozess zur Überprüfung der Zielsetzung und der Regelungen des Sicherheitsmanagementsystems bewertet?

Frage Nr. 2: Wie wird der Prozess zum Auditsystem bewertet?

Frage Nr. 3: Wie wird die Vorgehensweise zur Abstellung von Mängeln, die aus den durchgeführten Alarm-/Notfallübungen erkenntlich werden, bewertet?

Frage Nr. 4: Wie wird der Prozess internes Berichtssystem bzw. die Regelungen zur Erfassung von und Umgang mit Ereignissen bewertet?

Frage Nr. 5: Wie werden die Regelungen zur Verwendung von Kennzahlen bzw. (Leistungs-) Indikatoren zur Anlagensicherheit bewertet?

5.7.1 Frage Nr. 1: Wie wird der Prozess zur Überprüfung der Zielsetzung und der Regelungen des Sicherheitsmanagementsystems bewertet?

Bewertungshilfe:

Die Überprüfungen erfolgen regelmäßig anhand festgelegter Vorgehensweisen und beinhalten zum einen die Überprüfungen der Zielsetzungen des SMS, zum anderen die Überprüfungen der Regelungen des SMS, d. h. es wird überprüft, wie gut die Regelungen des SMS erfüllt werden. Die Zielsetzungen können im Rahmen von Managementreviews überprüft werden und werden im folgenden Prüfgebiet „SMS: Systematische Überprüfung und Bewertung“ behandelt.

Bei den meisten Betriebsbereichen werden die Überprüfungen der Regelungen des SMS durch ein Auditsystem erfolgen. Das Auditsystem des Sicherheitsmanagementsystems ist ein Führungselement von grundsätzlicher Bedeutung. Es dient dem Nachweis, dass in dem Unternehmen ein Sicherheitsmanagementsystem etabliert ist und effektiv funktioniert. Die im Rahmen des Auditsystems durchgeführten Audits liefern den unabhängigen Nachweis über vorhandene Defizite und Empfehlungen zu deren Behebung. Der Prozess zum Auditsystem wird in der nächsten Frage „Wie wird der Prozess zum Auditsystem bewertet?“ dieses Prüfgebietes behandelt.

Bei **Kleinunternehmen** können diese Überprüfungen auch andere Formen haben, z. B. Festlegung der Vorgehensweise zur Überprüfung im Konzept zur Verhinderung von Störfällen, Managementhandbuch oder ähnliches und Durchführung der Überprüfungen mittels Checkliste. Aber auch für Kleinunternehmen wird eine Auditierung empfohlen, dann als eine externe Dienstleistung in längeren Zeitabständen, z. B. alle 5 Jahre.
Bei der Festlegung der Vorgehensweise und Kriterien für die Überprüfungen z. B. in einem Kapitel des Managementhandbuchs können zu beschreibende Aspekte u. a. die Folgenden sein:

- Zeitpunkte zur Durchführung von Überprüfungen

und ihre Grundlage, Z. B.

- eigene Durchführung durch <Name>, z. B. Firmeninhaber/in mittels der generellen Checkliste <Name, Datum, Quellenangabe> (diese beinhaltet z. B. eine Auflistung aller Verfahrensanweisungen, Arbeits- und Betriebsanweisungen im Betriebsbereich) sowie speziellen Checklisten <Name, Datum, Quellenangabe> z. B. für Anlagenteile <Auflistung>,

und/oder

- Vergabe von Audits an einen Dienstleister: prinzipiell oder bei Erfüllung bestimmter Kriterien, z. B. alle xx Jahre, bei besonderer Fachthematik oder für bestimmte Anlagenteile,
  - Nennung der Kriterien, die der Dienstleiter erfüllen muss, damit eine angemessene Qualität des im Auftrag durchgeführten Audits sichergestellt ist (z. B. Qualifikation der externen Auditor/inn/en),

  - Durch die Vertragsgestaltung muss im Hinblick auf die Ergebnisse von Audits eine (partielle) Unabhängigkeit der Auditoren/innen sichergestellt sein,
- Inhalte der Dokumentation von Überprüfungen / Audits (z. B.: Die jährliche Überprüfung der Regelungen des SMS mittels der generellen Checkliste „Anweisungen im Betriebsbereich“ wird durch Aufbewahrung der ausgefüllten Checklisten dokumentiert.) und Aufbewahrungszeiträume,
- Umgang mit den Ergebnissen aus den Überprüfungen,
- Sicherstellung, dass die notwendigen Maßnahmen, die aus den Ergebnissen der Überprüfungen / Audits abgeleitet worden sind, auch umgesetzt werden (z. B. Werkzeuge: To-Do-Liste mit Statusanzeigen, ausgefüllte Formblätter), wer dies verantwortet und wie dies dokumentiert wird,
- Erläuterung, wie die für die Überprüfung zugrunde gelegte Vorgehensweise sowie die verwendeten Checklisten überprüft werden und wie die Aktualität der Checklisten gewährleistet wird.

Weitere Hinweise:

Die Checklisten können für verschiedene Anlagen- / Aufgabenbereiche unterschiedlich gestaltet sein, dies gilt auch für die Zeitabstände der Überprüfungen. Die Ergebnisse der Überprüfungen finden Eingang in der Beurteilung der Leistungsfähigkeit des Sicherheitsmanagementsystems. Sie können betriebsintern veröffentlicht werden. Die Veröffentlichung der Ergebnisse kann ein Anreiz für die Beschäftigten sein, Verbesserungen anzustreben. Die gewählte Ausführung der Überprüfung muss regelmäßig kontrolliert werden, z. B. ob die durchgeführten Überprüfungen ausreichend sind hinsichtlich ihrer Zeitabstände, der überprüften Bereiche / Anlagen etc.

5.7.2 Frage Nr. 2: Wie wird der Prozess zum Auditsystem bewertet?

Bewertungshilfe:

Wesentliches Kennzeichen eines (Sicherheits-)Managementsystems sind Überprüfungszyklen, die kontinuierliche Anpassungs- und Verbesserungsprozesse gewährleisten.
Ein wesentliches Werkzeug zur Sicherstellung von Überprüfungszyklen ist ein „Auditsystem“: die regelmäßige Durchführung von Audits unter festgelegten Randbedingungen.

Bei einem Audit erfolgt eine Überprüfung eines Prozesses (Handlungen und ihre Ergebnisse) im Hinblick auf vorgegebene Anforderungen (z. B. Verfahrensanweisungen, Normen, Gesetze). Ein Auditsystem ist Teil des Nachweises, dass in dem Unternehmen ein Sicherheitsmanagementsystem etabliert ist, effektiv funktioniert und für die Erreichung der im Rahmen der Sicherheitspolitik festgelegten Ziele geeignet ist.

Der Prozess „Auditsystem“ ist in Form einer Verfahrensbeschreibung / Prozessbeschreibung / Managementanweisung etc. schriftlich festzulegen, in welcher die folgenden Punkte berücksichtigt werden:

- Ziele, die mit dem Prozess „Auditsystem“ umgesetzt und erreicht werden sollen,
- Anwendungsbereich (z. B. Betriebsbereich, Organisationseinheiten des Betriebsbereiches),
- Definition der Begrifflichkeiten,
- Beschreibung der Prozessschritte und Ablauf im Rahmen des Auditsystems (Aufstellen von Auditplänen, Durchführung von internen und externen Audits, Benennung und Qualifikation der Auditor/inn/en, Maßnahmenverfolgung),
- Festlegung der Inhalte der Prozessschritte und Aufgaben,
- Festlegung von Zuständigkeiten und Verantwortlichkeiten zu den Aufgaben,
- Berücksichtigung zu den Schnittstellen anderer Prozesse (hier insb. Umsetzung von Folgemaßnahmen / Maßnahmenverfolgung, Managementreview),
- Umgang mit den Ergebnissen aus den Audits,
- Regelmäßige Überprüfung des Auditsystems,
- Festlegung von Dokumentationsinhalten (bei den Prozessschritten).

Die Auditpläne müssen die Punkte des SMS (Organisation und Personal, Ermittlung und Bewertung der Gefahren von Störfällen, Überwachung des Betriebs, Sichere Durchführung von Änderungen, Überwachung der Leistungsfähigkeit des SMS, Systematische Überprüfung und Bewertung) in angemessener Weise berücksichtigen.

In Anlehnung KAS-Leitfaden Nr. 19:

Es werden unterschiedliche Arten von Audits unterschieden, z. B.:

- **Interne Audits** (Auditoren/innen sind Beschäftigte des Unternehmens)
- **Externe Audits** (Auditoren/innen sind Beschäftigte einer externen Organisation)
- **Systemaudit** (Betrachtet die Aufbau- und Ablauforganisation, ob alle Elemente / Ziele des SMS berücksichtigt werden)

- **Complianceaudit** (Überprüfung der Übereinstimmung mit Genehmigungsbescheid / Auflagen, mit technischem Regelwerk, Werksnormen, Verfahrensanweisungen, etc.)
- **Prozessaudit** (Betrachtet einzelne Prozesse, z. B. Gefahrenanalyse, Überwachung des Betriebes, Instandhaltung, Änderungsmanagement, Meldung von Störfällen und Beinahestörfällen, Ausbildungs- und Schulungsmaßnahmen, Dokumentation)

Hinweise zu den Inhalten vom Prozess „Auditsystem“ (u. a. in Anlehnung an KAS-Leitfäden Nr. 7 und 19):

- Festlegung qualifizierter Auditleiter/in mit Befugnissen und Verantwortlichkeiten und Erfahrung in der Auditierung: Er/Sie vertritt (Vortragsrecht) das Auditteam bei der obersten Leitung des Unternehmens / Standorts bzw. der Hauptverwaltung / Unternehmensleitung je nach Unternehmensstruktur
- Aufstellung von Auditplänen (interne / externe Audits)
    - Einheiten (z. B. Abteilungen, Prozesse), die auditiert werden
    - Umfang der Audits
    - Tiefe der Audits
    - Audithäufigkeit (regelmäßig, anlass-, ereignisbezogen)
    - Arbeitsdokumente (Checklisten, Formulare zur Dokumentation der Auditfeststellungen und Schlussfolgerungen / empfohlenen Abhilfemaßnahmen)
    - Beteiligte Personen (Auditteams)
- Benennung von Auditoren/innen
    - Qualifikation der Auditoren/innen
    - Befugnisse der Auditoren/innen
    - Sicherstellung der (partiellen) Unabhängigkeit der Auditoren/innen
- Durchführung von Audits
    - Terminfestlegungen
    - Beteiligte Personen (bei den zu auditierenden Bereichen)
    - Dokumentation der Auditfeststellungen und Schlussfolgerungen mit Unterschriften
- Maßnahmenverfolgung
    - Einleitung von Korrektur- bzw. Vorbeugemaßnahmen
    - Vereinbarung von Maßnahmen mit der Fachabteilung
    - Aufnahme der Maßnahmen in den To-Do-Listen der Fachabteilung
    - Eingang der Defizite/Abhilfemaßnahmen in den nächsten Auditplan
    - Nachfolgeaudits
- Dokumentation/Berichte
    - Erstellung und Vorlage des (Jahres-)Berichts über die Ergebnisse der durchgeführten Audits einschließlich Vorlage bei der obersten Leitung mit folgenden Aussagen:
        - Anzahl durchgeführter Audits
        - Stand Zielerfüllung des Auditplans
        - Akkumulierte Auditfeststellungen und Schlussfolgerungen (Defizite / Best Practice)
        - Weiterführende Erkenntnisse und Vorschläge
        - Stand der Maßnahmenverfolgung

  - Dokumentation innerhalb des Auditsystems (Schnittstelle zur Lenkung von Dokumenten)
  - Verantwortlichkeiten
  - Aufbewahrungsfristen
- Regelmäßige Überprüfung des Auditsystems (erfolgt im Rahmen des Reviews bzw. durch externe Auditoren/innen: Anzahl, Umfang und Tiefe von durchgeführten Audits bestimmen die Auditintensität; diese ist so zu wählen, dass unter Berücksichtigung von betriebsbereichsspezifischen Bedingungen übergeordnete Ziele des Auditsystems erreicht werden können):
    - Erfassung aller relevanten Einheiten für die Audits
    - Qualifikation der Auditoren/innen
    - Eignung von Checklisten

Es gibt definierte Kriterien, nach denen das Auditsystem aufgebaut ist. Dies kann z. B. die folgenden Aspekte betreffen: Festlegungen, welche Bereiche zu welchen Zeitpunkten auditiert werden, Inhalte der Audits, beteiligte Personen, Umgang mit den Ergebnissen der Audits, Dokumentation der Audits, regelmäßige Überprüfung, ob die durchgeführten Audits ausreichend sind (Anzahl, Durchführungsform, auditierte Bereiche). Für alle Punkte sind die Verantwortlichkeiten festzulegen.

Es müssen Kriterien existieren, nach denen die Personen, die Audits durchführen festgelegt werden. Aspekte, die hierbei relevant sein können, sind z. B. Qualifikation (Aus- / Weiterbildung (technische, psychosoziale, organisatorische Bereiche), Erfahrung), persönliche Eignung, Befugnisse. Eine (partielle) Unabhängigkeit der Auditoren/innen muss sichergestellt sein. Die Kriterien sowie deren Beachtung und Umsetzung muss regelmäßig überprüft werden.

Festlegungen sind vorhanden nach welchen Kriterien (z. B. Umfang, Inhalte: Zustandsbeschreibung, Vereinbarungen, Abzeichnungen Verantwortliche / Teilnehmende, Termine, Maßnahmenverfolgung, Aufbewahrungszeiträume, Pflege) die Dokumentation der Audits erfolgt. Die Audit-Ergebnisse können in Checklisten und zusammenfassend durch die Audit-Teamleitung in einem Audit-Protokoll dokumentiert und von der auditierten Organisationseinheit unterschrieben werden. Dadurch wird die Anerkennung des Protokolls durch die auditierte Organisationseinheit gewährleistet. Das Audit-Protokoll kann unmittelbar danach an die auditierte Organisationseinheit und die Leitung der auditierten Organisationseinheit verteilt werden.

Es ist festzulegen, wie mit den Erkenntnissen aus den Audits umgegangen wird und welche Konsequenzen daraus gezogen werden. Hierzu kann es abgestufte Regelungen geben, z. B. im Hinblick auf die Zuständigkeiten für die Entscheidung, welche Maßnahmen getroffen werden müssen, Verantwortlichkeiten bei der Umsetzung von Maßnahmen, Zeiträume für die Umsetzung, Berichtspflichten, Veröffentlichungen. Dies braucht nicht nur Defizite oder Mängel zu betreffen, sondern kann auch die Weitergabe besonders gut entwickelter Lösungen beinhalten (best practice).

Die Verantwortlichkeiten für alle oben die genannten Punkte sind festzulegen.

Wenn im Rahmen eines Audits Abweichungen bzw. Schwachstellen gefunden werden, können diese durch den/die Audit-Teamleiter/in spezifiziert werden. Vorschläge zur Behebung der

Schwachstellen können im Rahmen des Audits erfolgen, ansonsten sollte die weitere Vorgehensweise definiert werden. Sinnvoll ist eine Abstimmung mit den Verantwortlichen am Audit teilnehmenden Personen der auditierten Organisationseinheit um möglichst eine Übereinstimmung im Hinblick auf das Ergebnis des Audits zu erreichen, z. B. hinsichtlich der Bewertung der gefundenen Schwachstellen, der durchzuführenden Korrekturmaßnahmen, der für ihre Durchführung verantwortlichen Personen und des einzuhaltenden Zeitrahmens.
Sollte keine Einigung erzielt werden können, so sollte dies im Audit-Protokoll entsprechend vermerkt werden.

Festlegungen, wie in diesem Fall weiter verfahren wird, sollten existieren. So kann im Falle eines Konfliktes mit dem jeweiligen Betrieb bei der Durchführung von Verbesserungsmaßnahmen ein Konfliktlösungsmodell dergestalt existieren, dass jeweils vorgesetzte Stellen zu informieren sind, wobei ggf. im Extremfall der Vorstand am Ende eine verbindliche Entscheidung zu treffen hat. Die Verantwortlichkeiten für die Umsetzung der beschlossenen Folgemaßnahmen aus den Audits müssen festgelegt sein. Entsprechende Kompetenzen und Mittel müssen zur Verfügung stehen, dies gilt auch für die Festlegung von Zeitrahmen für die Durchführung der Maßnahmen. Die Auswirkung der Folgemaßnahmen auf die Anlagensicherheit sollte überprüft werden (Schnittstelle zu Prüfgebiet „SMS: Sichere Durchführung von Änderungen). Die festgelegten Korrekturmaßnahmen sollten hinsichtlich ihrer Anwendung und Wirksamkeit nach einem festgelegten Zeitplan überprüft werden.

Die Verantwortlichen für die Durchführung von Kontrollen, ob die beschlossenen Folgemaßnahmen erfolgreich durchgeführt wurden müssen festgelegt sein. Dies gilt auch für die Konsequenzen, wenn Maßnahmen nicht ordnungsgemäß umgesetzt wurden oder nicht durchgeführt werden konnten. Die Kompetenzen der jeweils Verantwortlichen müssen dem Rechnung tragen. Es sollte zu den genannten Punkten eine entsprechende Dokumentation erfolgen.

5.7.3 Frage Nr. 3: Wie wird die Vorgehensweise zur Abstellung von Mängeln, die aus den durchgeführten Alarm- / Notfallübungen erkenntlich werden, bewertet?

Bewertungshilfe:

Es ist anhand von Kriterien festzulegen, wie die Vorgehensweise zur Abstellung von Mängeln, die aus den durchgeführten Alarm- / Notfallübungen erkannt werden, erfolgt. Bei den Kriterien kann es sich z. B. um Folgende handeln: Bewertung der Mängel, Einstufungen, in welchem Zeitraum die Abstellung der Mängel erfolgt, Durchführung der Arbeiten zur Abstellung der Mängel, Überprüfung der erfolgreichen Abstellung der Mängel. Es erfolgen regelmäßige Überprüfungen, sowohl, ob die festgelegte Vorgehensweise eingehalten wird, als auch ob die Vorgehensweise und die zugrunde gelegten Kriterien effektiv sind. Die Verantwortlichkeiten für alle genannten Punkte sind festzulegen.

5.7.4 Frage Nr. 4: Wie wird der Prozess internes Berichtssystem bzw. die Regelungen zur Erfassung von und Umgang mit Ereignissen bewertet?

Bewertungshilfe:

Die Erfassung und Verwertung von Störungen, Ereignissen, "Beinahe-Unfällen", Unfällen und Störfällen dient dem Lernen aus Ereignissen.

Dies kann in Betriebsbereichen von großen und ggf. mittelständischen Unternehmen durch die Umsetzung von internen Berichtssystemen erreicht werden, wie sie im Leitfaden KAS-8 „Empfehlungen für interne Berichtssysteme als Teil des Sicherheitsmanagementsystems gemäß Anhang III Störfall-Verordnung“ /siehe Kapitel Quellenangaben/ beschrieben werden.

Hierin werden unter **Ereignissen** insbesondere verstanden:

- Abweichungen von Vorgaben
- Handlungsunsicherheiten
- Auffälligkeiten von Technik, Organisation, menschliche Faktoren
- Potentielle oder latente kritische Situationen
- ungewöhnliche Zustände,
- jede Störung des bestimmungsgemäßen Betriebes, die eine Freisetzung von Gefahrstoffen bedingt,
- an Schutzsystemen festgestellte Defekte und Mängel,
- unmittelbare erhebliche Gefahren für die Sicherheit und Gesundheit,
- meldepflichtige Ereignisse im Sinne von Anhang VI Störfall-Verordnung.

Das interne Berichtssystem beinhaltet den Ablauf zur Erfassung und Analyse von Ereignissen, die Ableitung und Umsetzung von Maßnahmen sowie die Kommunikation und Verbreitung von Ergebnissen aus den Ereignisanalysen (Learning Lessons).

Die Ereignisanalyse muss mittels systematischer (ganzheitlicher) Analysemethoden erfolgen. Ganzheitlich bedeutet hier, dass die Analysemethode Aspekte von Mensch, Technik und Organisation (MTO) mit ihren Wechselbeziehungen untereinander berücksichtigt. Die Erkenntnisse aus den Ereignisanalysen werden abhängig z. B. von Übertragungspotential, Risikopotential und Tragweite intern und auch extern kommuniziert (Learning Lessons).

Der Prozess zum internen Berichtssystem ist im Betriebsbereich schriftlich festgelegt, z. B. in Form einer Verfahrensbeschreibung / Prozessbeschreibung / Managementanweisung etc.. Hierin sind folgende Aspekte zu berücksichtigen:

1. Ziele, die mit dem Prozess erreicht werden sollen,
2. Anwendungsbereich,
3. Definition der Begrifflichkeiten (z. B. Ereignis, (Arbeits-)Unfälle, Störfälle, Meldung, (ganzheitliche) Ereignisanalyse, Learning Lessons),
4. Beschreibung der Prozessschritte und Ablauf des internen Berichtssystems

5. Festlegung der Inhalte der Prozessschritte und Aufgaben (Meldungen erfassen und systematisieren; Auswahl der Meldungen, die einer vertieften Ereignisanalyse unterzogen werden; Ereignisanalyse durchführen (Analysemethoden, Fachkompetenz etc.), Ableitung von Maßnahmen und deren Umsetzung, Veröffentlichung von Ergebnissen aus den Ereignisanalysen und Trends aus den Meldungen, intern, extern)
6. Festlegung von Zuständigkeiten und Verantwortlichkeiten zu den Prozessschritten und Aufgaben,
7. Berücksichtigung zu den Schnittstellen anderer Prozesse (z. B. Personalfortbildung, Gefahrenanalyse, Überwachung des Betriebs, Notfallplanung, Sicherheitsindikatoren, Managementreview),
8. Festlegung von Dokumentationsinhalten bei den Prozessschritten (u. a. Bereitstellung von formalisierten Berichtsformen für Meldungen, Untersuchungsbericht der Ereignisanalysen, Kurzformbericht (Learning Lessons)).

Hinweise zu den obigen Punkten:

Es müssen regelmäßige Überprüfungen erfolgen, ob die festgelegten Inhalte für den Prozess internes Berichtssystem (u. a. Kriterien, Ablauf, Verantwortlichkeiten) angemessen sind, z. B. im Rahmen von Audits.

Detaillierte Informationen zu Aufbau, Umsetzung und Einbettung des internen Berichtssystems im SMS können dem Kapitel 2.5 des Leitfadens KAS-8 „Empfehlungen für interne Berichtssysteme als Teil des Sicherheitsmanagementsystems gemäß Anhang III Störfall-Verordnung“ entnommen werden.

Die obigen Gesichtspunkte gelten für Großunternehmen und ggf. mittelständische Unternehmen.

Voraussetzung für nutzbringende und gute Ergebnisse beim Prozess „Internes Berichtssystem“ ist eine konstruktive Fehlerkultur (siehe hierzu Kapitel „SMS: Systematischen Überprüfung und Bewertung“) und eine positiv entwickelte Meldekultur. Die Vorbildfunktion der Vorgesetzten im Umsetzen einer offenen Meldekultur ist wichtig, damit Beschäftigte angemessen Ereignisse mitteilen: „Was nicht gemeldet wird, kann nicht analysiert werden – was nicht analysiert wurde, kann nicht verbessert werden.“ (Leitfaden KAS-8)

Kleinunternehmen sind personell nur bedingt in der Lage den Prozess „Internes Berichtssystem“ vollständig umzusetzen und z. B. eine eigene, unabhängige Stelle für die Aufgaben des internen Berichtssystems einzurichten. Trotzdem bietet das Lernen aus Ereignissen auch hier eine wichtige Ressource um Verbesserungsmöglichkeiten einschließlich finanzieller Vorteile im Betrieb zu erkennen und umzusetzen. Beispielweise kann der/die Störfallbeauftragte die Meldungen von Ereignissen entgegennehmen, de-personalisieren und erfassen während die vertieften Analysen, regelmäßigen Systembetrachtungen und die Kommunikation verallgemeinerbare Erkenntnisse und Empfehlungen („Learning Lessons“) als externe Dienstleistung vergeben wird. Möglichkeiten bestimmte Teile / Aufgaben des Prozesses „Internes Berichtssystem“ für mehrere Kleinunternehmen zu übernehmen bieten eventuell auch Verbände etc.

Wie im Kleinunternehmen die Erfassung von und der Umgang mit Ereignissen erfolgt muss festgelegt und dokumentiert sein, z. B. im Konzept zur Verhinderung von Störfällen, Managementhandbuch oder ähnliches, zu beschreibende Aspekte können u. a. die Folgenden sein:

- Meldung von Ereignissen (Definition) durch die Beschäftigten an eine benannte Person, z. B. Störfallbeauftragte,
- Durchführung von Gesprächsrunden zum Thema Lernen aus Ereignissen / Meldekultur mit den Beschäftigten des Betriebs, z. B. halbjährlich,
- Zeitpunkte zur Durchführung von Ereignisanalysen und ihre Grundlage, Z. B.
- eigene Durchführung von Analysen für Ereignisse der Art z. B. durch <Name>, z. B. Firmeninhaber/in mittels der Methode(n: ggf. abgestuft nach Art des Ereignisses: <Name, Quellenangabe> (Eine Möglichkeit ein Unfallgeschehen ganzheitlich zu untersuchen bietet der Leitfaden „Ganzheitliche Unfallanalyse – Leitfaden zur Ermittlung grundlegender Ursachen von Arbeitsunfällen in kleinen und mittleren Unternehmen“ von B. Fahlbruch, I. Meyer /kostenlose pdf-Datei siehe Kapitel Quellenangaben/; hierin sind auch weitere Methoden kurz beschrieben und hinsichtlich einer KMU-Tauglichkeit bewertet),

und/oder

- Vergabe von Ereignisanalysen als externe Dienstleistung: prinzipiell oder bei Erfüllung bestimmter Kriterien, z. B. bei Ereignissen der Art ….,
- Umgang mit den Ergebnissen aus den Ereignisanalysen einschließlich der Kommunikation nach innen und außen,
- Sicherstellung, dass die notwendigen Maßnahmen, die aus den Ergebnissen der Ereignisanalysen abgeleitet worden sind, auch umgesetzt werden (z. B. Werkzeuge: To-Do-Liste mit Statusanzeigen, ausgefüllte Formblätter), wer dies verantwortet und wie dies dokumentiert wird,
- Erläuterung, welche Aspekte zur Erfassung von und Umgang mit Ereignissen (z. B. Anzahl von Meldungen, Ereignisanalysen, durchgeführte Maßnahmen, Kommunikation, Inhalte aus den Gesprächsrunden) in das Managementreview einfließen,
- Regelmäßige Überprüfung der Regelungen zur Erfassung von und Umgang mit Ereignissen.

Zusätzliche Erläuterungen:

Die Erfassung von Unfällen und "Beinahe-Unfällen" muss systematisch nach definierten Kriterien geregelt werden, z. B. durch die Festlegung von Meldepflichten, wie und an wen diese erfolgen, was gemeldet und dokumentiert wird. Hierfür kann es ein abgestuftes Konzept geben.
Die Untersuchung der Unfallursachen ist durch eine Richtlinie oder Festlegung nach definierten Kriterien geregelt. Dabei sollten als mögliche Ursachenbereiche vielfältige Aspekte berücksichtigt werden, wie z. B. stoffliche, technische, organisatorische, managementspezifische, physische, psychische, soziale.
Es kann eine abgestufte Vorgehensweise zur Untersuchung der Unfallursachen geben, nach Kriterien wie z. B. Verantwortliche für die Durchführung der Untersuchung, Personen, die an der Untersuchung zu beteiligen sind, interne Untersuchung, externe Vergabe.

Das Betriebsklima ist möglichst so zu gestalten, dass verantwortungsvoll und offen mit Fehlern umgegangen wird, so dass die Anreize zur Vertuschung möglichst gering gehalten werden.

Aus der Ermittlung der Unfallursachen sind entsprechende Maßnahmen abzuleiten. Wie mit den Ergebnissen aus den Untersuchungen der Unfälle oder Beinaheunfälle umgegangen wird, muss nach definierten Kriterien geregelt sein. Betroffen sind beispielweise die Umsetzung von Maßnahmen im Betriebsbereich, die Verantwortlichkeiten für die Entscheidung, welche Maßnahmen, in welchem Zeitraum umgesetzt werden, die Veröffentlichung der Untersuchungsergebnisse intern und extern.

Die Inhalte und die Einhaltung der obigen Regelung werden regelmäßig überprüft. Die Überprüfung beinhaltet auch, ob die Regelungen zur Erfassung der Unfälle und "Beinahe-Unfälle" geeignet sind, alle relevanten Ereignisse zu erfassen. Der Umgang mit den Ergebnissen aus diesen Überprüfungen ist festzulegen. Die Verantwortlichkeiten sind für alle genannten Punkte festzulegen.

5.7.5 Frage Nr. 5: Wie werden die Regelungen zur Verwendung von Kennzahlen bzw. (Leistungs-) Indikatoren zur Anlagensicherheit bewertet?

Bewertungshilfe:

Um in kurzer, knapper Form den Leistungsstand von Prozessen innerhalb von Unternehmen oder Organisationen darzustellen, können (Leistungs-) Kennzahlen oder Indikatoren bestimmt und nachverfolgt werden.

Kennzahlen enthalten in konzentrierter kompakter Form Informationen, quantitativ und qualitativ erfassbare, indem sie Sachverhalte und Zusammenhänge mathematisch beschreiben und auf messbaren Daten / Fakten beruhen.

Auch die Prozesssicherheit von Betriebsbereichen und ihren Anlagen einschließlich der Leistungsfähigkeit des Sicherheitsmanagementsystems (SMS) können durch Kennzahlen bzw. Indikatoren beschrieben werden.

Prinzipiell können Kennzahlen in zwei Arten eingeteilt werden:

- Es ist bereits ein (negatives) Ereignis eingetreten, dann ist die Rede von **Spätindikatoren, Lagging Indicators, reaktiven Kennzahlen,** oder **Ergebniskennzahlen** etc.,
- Es ist noch kein (negatives) Ereignis eingetreten, dann wird gesprochen von **Frühindikatoren, Leading Indicators, proaktiven Kennzahlen**, oder **Aktivitätskennzahlen** etc..

Für die Prozesssicherheit können folgende Kennzahlen von Bedeutung sein, z. B.:

Spätindikatoren (absolut):

- Anzahl der Stofffreisetzungen (nach Menge und Gefährlichkeitsmerkmal des Stoffes klassifiziert),
- Anzahl der Brände,
- Anzahl der Explosionen,
- Anzahl der Anlagenabstellungen durch automatischen oder manuellen Notaus.

Anzahl der Stofffreisetzungen als **Loss of Primary Containment (LoPC)** nach **VCI-Leitfaden zur Erfassung von Performance-Indikatoren für die Prozesssicherheit (Januar 2015)** oberhalb folgender Mengenschwellen:

- **> 5 kg** bei Vorliegen einer der GHS Kategorien Akute Toxizität der Kat. 1 und 2 sowie Muta. 1A, Carc. 1A, Repr. 1A, STOT SE 1,
- **> 100 kg** bei allen sonstigen nach GHS eingestuften gefährlichen Stoffen,
- **> 2.000 kg** bei alle anderen, nicht nach GHS eingestuften Stoffe.

Abb. 29: Loss of Primary Containment (LoPC) nach VCI-Leitfaden

Frühindikatoren (relativ):

- Anteil der erledigten durchzuführenden sicherheitsrelevanten Prüfungen,
- Anteil der nicht termingerecht (wiederkehrend) durchgeführten Gefahrenanalysen,
- Anteil der termingerecht fertig gestellten Maßnahmen von Auditfeststellungen (Follow-up).

Weitere in Kennzahlen erfassbare Aspekte können beispielsweise die Qualifikation, die Unterweisung oder die Durchführung von anderen sicherheitsrelevanten organisatorischen Maßnahmen sein.

Meist werden die Begriffe Indikatoren und Kennzahlen synonym verwendet.

Es gibt aber auch die Möglichkeit der **Unterscheidung von Kennzahlen und Indikatoren** dergestalt, dass es sich bei **Indikatoren** um Ersatzgrößen handelt, die mit der relevanten Größe korrelieren und eine Größe/einen Tatbestand näherungsweise abbilden (Darstellung von „weichen" Faktoren). *In diesem Sinne kommen dann Indikatoren zum Einsatz bei nicht direkt messbaren bzw. nicht direkt beobachtbaren Tatbeständen.*

Bei einer Inspektion können folgenden Fragen an den Betreiber des BB gestellt werden:

- o Werden Kennzahlen / Indikatoren zur Prozesssicherheit / Anlagensicherheit erfasst?
  - Welche?
  - Wie erfolgt die Erfassung?
- o Wofür werden diese Kennzahlen / Indikatoren Betreiber benutzt / eingesetzt?
- o Welche Trends sind im Betriebsbereich erkennbar?

Zur besseren Bewertung dieser Thematik sollte von den Inspektor/innen auch die beim Betreiber vorliegende Dokumentation hierzu eingesehen werden.

Bedeutung von Kennzahlen

Die Erfassung von Kennzahlen zur Prozesssicherheit dient dazu, im Abgleich mit aufgestellten Zielen zur Anlagensicherheit eine ergebnisorientierte Steuerung zu ermöglichen. Dazu ist auch eine angemessene Kommunikation und Beteiligung der obersten Leitung wichtig.
Die regelmäßige Erhebung von Kennzahlen ermöglichen Vergleiche, z. B. über die Zeit, mit anderen Organisationseinheiten (Benchmarking) oder zwischen Soll und Ist.
Damit können Antworten gegeben werden zu Fragen der Art:

- Gibt es auffällige Veränderungen zum Vorjahr?, Wie ist der Trend?
- Wie gut sind wir im Vergleich zu anderen Unternehmen bzw. Einheiten unserer Organisation?
- In welchem Ausmaß haben wir unsere Ziele erreicht?

Bei Abweichungen von den Zielen sind die Gründe zu analysieren und Verbesserungsansätze herauszufinden und in konkrete Maßnahmen für das Unternehmen oder einzelnen organisatorischen Einheiten umzusetzen.

Insbesondere für Groß- und mittelständische Unternehmen sollte dem Aufbau, der Entwicklung, Pflege und Nutzung von Kennzahlen in der Prozesssicherheit ein systematischer Prozess zugrunde liegen.
Auf den Leitfaden zur Erfassung von Performance-Indikatoren für die Prozesssicherheit (Januar 2015) des VCI wird hingewiesen.

Der OECD Leitfaden Guidance on Developing Safety Performance Indicators empfiehlt einen 7-stufigen Prozess zur Entwicklung eines Kennzahlenprogramms:

1. Ein Kennzahl-Team gründen,
2. Die maßgeblichen Kriterien definieren,
3. Spätindikatoren und relevante Maßstäbe definieren,
4. Frühindikatoren und relevante Maßstäbe definieren,
5. Daten erfassen und Ergebnisse der Kennzahlen berichten,
6. Maßnahmen aufgrund der Ergebnisse der Kennzahlen ergreifen,
7. Kennzahlensystem bewerten und verbessern.

Dieser Prozess stellt einen geschlossenen Kreislauf dar, wobei die Schritte (3) und (4) iterativ sein können, bis eine geeignete Kombination an Spät- und Frühindikatoren gefunden ist.

Weitere Hinweise aus Leitfaden zur Erfassung von Performance-Indikatoren für die Prozesssicherheit (Januar 2015) des VCI (nur Auszug, geringfügig modifiziert / gekürzt):

Die Sicherheitsperformance von Anlagen und Verfahren lässt sich anhand von Kennzahlen, den Key Performance Indikatoren (KPI), bewerten. Zu den KPI‘s zählen auch die Prozess-Sicherheitsereignisse, die so genannten Process Safety Incidents (PSI), die in den Unternehmen regelmäßig eingesetzt werden. Sie lassen sich auch branchenweit anwenden.
Die Kennzahl PSI erfasst Ereignisse mit eher geringen oder gar keinen Auswirkungen auf Menschen und Umwelt, die aber durch eine Stofffreisetzung gekennzeichnet ist bzw. dadurch, dass die erste Schutzhülle ihre Wirkung verloren hat.

Dieser Leitfaden dient der Definition von Kennzahlen zur Verfahrens- und Anlagensicherheit und insbesondere dazu, für PSI‘s die Basis eines einheitlichen Berichtsystems festzulegen. Er definiert Einschränkungen und Voraussetzungen für ein effektives internes System zur Erfassung der Ereignisse sowie einheitliche Kriterien, nach denen sich Ereignisse als Prozess-Sicherheitsereignisse, so genannte Process Safety Incidents (PSI’s) einstufen lassen. Methoden für die Entwicklung und Verwendung von Prozess-Sicherheitsindikatoren werden erläutert.

Ziel ist es, ein Berichtssystem vorzulegen, das globale, regionale und nationale Daten zur Sicherheitsperformance liefert, mit denen die Unternehmensleitung die tatsächliche Performance und Trends erkennen kann, um unvorhergesehene und unerwünschte sicherheitsrelevante Prozessereignisse zu vermeiden, zu verringern oder zu korrigieren.

Dieser Leitfaden befasst sich hauptsächlich mit der Definition und Erfassung des PSI für die Prozess-Sicherheitsperformance. Dieser hebt auf ein stattgefundenes Ereignis ab mit Auswirkungen wie z. B. Brand, Verletzungen mit der Folge mindestens eines Ausfalltages oder Ereignisse mit Stoffaustritt oberhalb definierter (s. u.) Freisetzungsvolumen. Der PSI eignet sich bei vergleichbaren Produktionsstandorten für ein Benchmarking und eine Trendanalyse und

gibt dem Management die Möglichkeit, Schlussfolgerungen zu ziehen und eine kontinuierliche Verbesserung voranzutreiben.

Indikatoren, die dagegen der Überwachung der Prävention und der Kontrollsysteme dienen, lassen erkennen, inwieweit das Unternehmen auf Ereignisse vorbereitet ist. Dazu zählen z. B. Beinaheunfälle oder die Anzahl rechtzeitig durchgeführter Inspektionen. Sie sind – auch wenn sie wichtige Managementwerkzeuge darstellen – nicht Gegenstand dieses Leitfadens.

Es liegt in der Verantwortung des Unternehmens, solche Indikatoren angemessen zu berücksichtigen, um für ein effektives Prozesssicherheitsmanagement zu sorgen.

Die erfolgreiche Einführung eines PSI-Berichtssystems zur Bewertung der Sicherheitsperformance innerhalb eines Unternehmens sollte folgendes berücksichtigen:
Das Berichtssystem wird top down von der Vorstandsebene bis hinunter zum einzelnen Mitarbeiter umgesetzt.
Die Vorteile eines solchen Berichtssystems werden dem verantwortlichen Management bis hinunter zur Betriebsleitung klar vermittelt. Ein Missbrauch der PSIR (Process Safety Incident Rate) ist zu vermeiden.
Ein kleines Werk innerhalb eines Unternehmens mit nur einem PSI kann eine deutlich höhere PSIR aufweisen als der Mittelwert des gesamten Unternehmens. Das ist aber nicht automatisch gleichbedeutend mit einer schlechten Sicherheitsperformance des kleinen Werks.
Die Unternehmensleitung sollte dazu ermutigt werden, die PSI zu kommunizieren, deshalb sollte die Meldung von Ereignissen keinen Einfluss auf die Leistungsbewertung der Führungskräfte oder das Bonussystem haben. Prozess-Sicherheitsereignisse und Arbeitsunfälle werden meistens durch menschliches Versagen oder Organisationsmängel verursacht.

Ein offenes Klima, in dem Management und Mitarbeiter ermutigt werden, Abweichungen zu melden, kann helfen, das System zu verbessern.

5.8 SMS: Systematische Überprüfung und Bewertung

Dieses Prüfgebiet enthält die folgenden Fragen:

Frage Nr. 1: Wie wird die Vorgehensweise zur systematischen Überprüfung und Bewertung des Konzeptes zur Verhinderung von Störfällen bewertet?

Frage Nr. 2: Wie wird die Vorgehensweise zur systematischen Überprüfung und Bewertung des SMS (Managementreview) bewertet?

Frage Nr. 3: Wie wird die Sicherheitskultur des Betriebsbereiches eingeschätzt?

Frage Nr. 4: Wie wird die Kommunikationskultur des Betriebsbereiches eingeschätzt?

Frage Nr. 5: Wie wird die Fehlerkultur des Betriebsbereiches eingeschätzt?

Frage Nr. 6: Wie wird die Resilienz des Betriebsbereiches eingeschätzt?

5.8.1 Frage Nr. 1: Wie wird die Vorgehensweise zur systematischen Überprüfung und Bewertung des Konzeptes zur Verhinderung von Störfällen bewertet?

Bewertungshilfe:

Es gibt schriftlich festgelegte Regelungen, wie die systematische Überprüfung und Bewertung des Konzeptes zur Verhinderung von Störfällen erfolgt.

Nach § 8 der Störfallverordnung hat der Betreiber das Konzept zu überprüfen und soweit erforderlich zu aktualisieren, und zwar

1. mindestens alle fünf Jahre nach erstmaliger Erstellung oder Änderung,
2. vor einer Änderung nach § 7 Absatz 3 (störfallrelevante Änderungen nach § 3 Absatz 5b BImschG) und
3. unverzüglich nach einem Ereignis nach Anhang VI Teil 1.

Das Konzept muss die übergeordneten Ziele und Handlungsgrundsätze des Betreibers, die Rolle und die Verantwortung der Leitung des Betriebsbereichs umfassen sowie die Verpflichtung beinhalten, die Beherrschung der Gefahren von Störfällen ständig zu verbessern und ein hohes Schutzniveau zu gewährleisten.

Im Rahmen der systematischen Überprüfung ist durch die oberste Leitung zu bewerten, ob diese Inhalte im Konzept noch richtig und angemessen sind oder ob Anpassungen vorzunehmen sind. Ist letzteres der Fall so ist das Konzept zu überarbeiten. Die Verantwortlichkeiten mit den entsprechenden Kompetenzen für die Durchführung der Überprüfung des Konzeptes zur Verhinderung von Störfällen anhand festgelegter Kriterien und der Einhaltung der Regelungen müssen festgelegt sein. Die Überprüfung des Konzeptes muss dokumentiert sein.

Bei **Betriebsbereichen der unteren Klasse bzw. Kleinstunternehmen** wird dies in der Regel durch die oberste Leitung des Betriebsbereiches erfolgen und die Vorgehensweise zur Überprüfung des Konzeptes kann im Konzept selbst beschrieben sein. Zu nennen sind

- Verantwortliche Person(en),
- Zeitpunkte bzw. -abstände und
- Kriterien, die zur Überprüfung herangezogen werden, beispielsweise
  - Unfallzahlen,
  - Ergebnisse aus den Audits und Überprüfungen (Schnittstelle zu Prüfgebiet "SMS: Überwachung der Leistungsfähigkeit des SMS"),
  - Umsetzung von Maßnahmen,
  - Ergebnisse aus durchgeführten Übungen,
  - Zufriedenheit der Beschäftigten (z. B. aus Mitarbeiter/innen - Gesprächen, Umfragen),
  - neue Erkenntnisse.

Bei **Betriebsbereichen der oberen Klasse** kann das Konzept Bestandteil des Sicherheitsberichtes sein. Hier kann die Überprüfung des Konzeptes in die Überprüfungsregeln des Sicherheitsberichtes und / oder Managementreviews eingebunden sein. Die übergeordneten Ziele zur Anlagensicherheit und Störfallvorsorge des Betreibers eines Betriebsbereiches der oberen Klasse finden sich dann in der Unternehmens- und / oder Sicherheitspolitik des Betreibers und sind in diesem Rahmen durch die oberste Leitung zu prüfen und zu bewerten (siehe hierzu auch Bewertungshilfen zu den Fragen „Wie werden die Regelungen zur Überprüfung der Zielsetzung der Sicherheitspolitik bewertet?“ sowie „Wie wird Corporate Governance (Grundsätze der Unternehmensführung) für die Anlagensicherheit in dem Betriebsbereich eingeschätzt?“ im Prüfgebiet „SMS: Konzept zur Verhinderung von Störfällen und Aufbau des SMS“).

5.8.2 Frage Nr. 2: Wie wird die Vorgehensweise zur systematischen Überprüfung und Bewertung des SMS (Managementreview) bewertet?

Bewertungshilfe:

Im Betriebsbereich müssen festgelegte Kriterien existieren, wie die systematische Überprüfung und Bewertung des Sicherheitsmanagementsystems im Hinblick auf seine Wirksamkeit und Angemessenheit Störfälle zu verhindern und Störfallauswirkungen zu begrenzen, erfolgt. Die abschließende Bewertung einer Überprüfung des Sicherheitsmanagementsystems muss durch die oberste Leitung des Betriebsbereiches erfolgen.

Nach § 8 der Störfall-VO hat der Betreiber das Sicherheitsmanagementsystem nach Anhang III sowie die Verfahren zu dessen Umsetzung zu überprüfen und soweit erforderlich zu aktualisieren, und zwar

1. mindestens alle fünf Jahre nach erstmaliger Erstellung oder Änderung,
2. vor einer Änderung nach § 7 Absatz 3 (störfallrelevante Änderungen nach § 3 Absatz 5b BImschG) und
3. unverzüglich nach einem Ereignis nach Anhang VI Teil 1.

Die folgenden Ausführungen gelten überwiegend für Konzerne und größere mittelständische Unternehmen:

Gängige Praxis zur Überprüfung von Managementsystemen durch die oberste Leitung ist die jährliche Durchführung von Managementreviews.
Dies ist ein angemessener Zeitraum, damit die Ziele eines Managementsystems erreicht werden können. Ein geplanter Zeitabstand von 5 Jahren ist hier nicht zielführend. Der Zeitabstand von 5 Jahren zur regelmäßigen Überprüfung der Unternehmenspolitik ist demgegenüber angemessen (siehe hierzu auch Bewertungshilfe zur Frage "Wie werden die Regelungen zur Überprüfung der Zielsetzung der Sicherheitspolitik bewertet?" im Prüfgebiet „SMS: Konzept zur Verhinderung von Störfällen und Aufbau des SMS“).
Bei einer Inspektion kann die Dokumentation der letzten zwei durchgeführten Managementreviews eingesehen werden und die untenstehenden Fragen aus dem KAS-Leitfaden Nr. 19 an den Betreiber des BB gestellt werden.

Definition „Managementreview“

Das Managementreview stellt eine regelmäßige Bewertung des Managementsystems und der zugrundeliegenden Unternehmenspolitik einer Organisation durch die oberste Leitung dar. Dabei wird die Eignung, Angemessenheit, Wirksamkeit und Aktualität des Managementsystems, der Unternehmensziele und -politik überprüft. Die Ergebnisse des Managementreviews beinhalten Entscheidungen und Maßnahmen zur Verbesserung des Managementsystems, Bereitstellung von Ressourcen und Benennung von Zielen.

Quelle: KAS-Leitfaden Nr. 8:

Abb. 30: Definition „Managementreview“ (laut KAS-Leitfaden Nr. 8)

Die folgenden Ausführungen zum Managementreview enthalten Elemente aus dem KAS-Leitfaden Nr. 19:

Bezogen auf das Sicherheitsmanagementsystem werden im Rahmen des Managementreviews die Eignung, Angemessenheit, Wirksamkeit und Aktualität des Sicherheitsmanagementsystems, das Konzept zur Verhinderung von Störfällen und die Sicherheitspolitik bzw. die Unternehmenspolitik im Hinblick auf die Anlagensicherheit überprüft.

Bei einem Integrierten Managementsystem wird dabei die Eignung, Angemessenheit, Wirksamkeit und Aktualität des Managementsystems im Hinblick auf die sieben durch das SMS zu regelnde Punkte im Anhang III der Störfallverordnung, das Konzept zur Verhinderung von Störfällen und die Unternehmenspolitik im Hinblick auf die Anlagensicherheit überprüft.

Darüber hinaus müssen auch die Ziele des Betriebsbereiches bzw. Unternehmensziele zur Anlagensicherheit überprüft werden (siehe auch Bewertungshilfe zur Frage „Wie werden die Regelungen zur Überprüfung der Zielsetzung der Sicherheitspolitik bewertet?“ im Prüfgebiet „SMS: Konzept zur Verhinderung von Störfällen und Aufbau des SMS“).
Im Hinblick auf die generellen Ziele zur Anlagensicherheit sollten beim Managementreview folgende Fragen beantwortet werden:

- Wurden die vorgegebenen Ziele zur Anlagensicherheit erreicht?
- Sind neue Ziele zur Anlagensicherheit erforderlich?
- War das SMS geeignet diese Ziele zu unterstützen?
- Gibt es neue Anforderungen, die durch das SMS umgesetzt werden müssen?
- Welche Verbesserungen sind möglich?

Die oberste Leitung trifft aufgrund der Ergebnisse des Managementreviews die erforderlichen Entscheidungen für Maßnahmen zur Verbesserung des Sicherheitsmanagementsystems bzw. des integrierten Managementsystems, Bereitstellung von Ressourcen für die Anlagensicherheit und Benennung von Zielen zur Anlagensicherheit.

Der Verfahrensablauf des Managementreviews einschließlich zugehöriger Zuständigkeiten mit Zeitpunkten und Anforderungen an die Dokumentation des Managementreviews muss schriftlich festgelegt (z. B. im Managementhandbuch) sein. Hierin sollten sich folgende Festlegungen finden:

- Zeitpunkte zur Durchführung der Managementreviews (Zeitzyklus, z. B. einmal jährlich, alle zwei Jahre; nach einem Störfall / größerem Ereignis),
- Verantwortung / Bewertung durch die oberste Leitung, Geschäftsführung,
- Unterlagen, aufgrund derer die oberste Leitung das Managementreview durchführt,
- Nachverfolgung / Durchführung der veranlassten Maßnahmen (wer, wann, Überprüfung der Durchführung),
- Dokumentation des Managementreviews (was, wer).

Anhand von Unterlagen nimmt die oberste Leitung des Betriebsbereiches die Bewertung des SMS vor. Kriterien, die zur Überprüfung herangezogen werden können, sind z. B.

- Erkenntnisse aus der Ermittlung und Bewertung der Gefahren von Störfällen oder des internen Berichtssystems (Erfassung und Untersuchung von Störfällen, Beinahestörfällen und Betriebsstörungen),

- Unfallzahlen,
- Auswertung der durchgeführten Audits (Abweichungen, Mängel, Verbesserungsvorschläge, Best Practice) und
- Ergebnisse aus der Überprüfungen der Leistungsfähigkeit des SMS – z. B. in Form von Kennzahlen,
- bereitgestellte Mittel,
- Stand zur Umsetzung von Maßnahmen,
- Auswertung von Personalmaßnahmen (Schulungen, Qualifizierungen, Mitarbeiterbefragungen),
- Ergebnisse aus durchgeführten Übungen,
- Einhaltung von Gesetzen (Änderungen, Genehmigungsstand, Überschreitungen, eingehaltene Prüffristen),
- neue Erkenntnisse zum Stand der Sicherheitstechnik (Auswirkungen auf den Betriebsbereich).

Überprüft werden sollte auch, ob die aus dem vorherigen Managementreview resultierenden Maßnahmen Erfolg hatten.

Folgende Unterlagen können z. B. einem Managementreview zugrunde gelegt werden, d. h. der obersten Leitung zur Bewertung dienen:

- Berichte des/der Störfallbeauftragten,
- Störfälle / Einzelereignisse größeren Ausmaßes,
- Berichte über die durchgeführten Audits und ihre Ergebnisse,
- Status zur Durchführung von Maßnahmen (in Arbeit, erledigt),
- Durchgeführte herausragende Maßnahmen zur Anlagensicherheit,
- Zeitliche Entwicklung von relevanten Kennzahlen zur Anlagensicherheit,
- Kennzahlen aus dem internen Berichtssystem (siehe hierzu auch Bewertungshilfe zur Frage „Wie werden der Prozess internes Berichtssystem bzw. die Regelungen zur Erfassung von und Umgang mit Ereignissen bewertet?“ im Prüfgebiet „SMS: Überwachung der Leistungsfähigkeit des Sicherheitsmanagementsystems“), z. B.:
    - Anzahl der Meldungen gesamt,
    - Anzahl der durchgeführten vertieften Analysen,
    - Anzahl Informationsweitergabe als „Learning Lessons“,
    - Angaben zu empfohlenen Maßnahmen, evt. nach Technik, Mensch, Organisation aufgeschlüsselt.

Mögliche weitere Information für das Managementreview:

- o Besondere Einzelereignisse, aufgefundene Ursachen
- o Ergebnisse aus der Systembetrachtung und Trendanalyse.

Hinweis: „In Unternehmen mit einem hohen Risikopotential sieht die KAS die Beurteilung der persönlichen und professionellen Kompetenz von Beschäftigten aller Hierarchieebenen als ein wichtiges Element des Management Reviews an.“ (Anhang 4 in KAS-7)

5.8.3 Frage Nr. 3: Wie wird die Sicherheitskultur des Betriebsbereiches eingeschätzt?

Bewertungshilfe:

Definition „Sicherheitskultur“

Sicherheitskultur kann als Teil einer Unternehmens- oder Organisationskultur verstanden werden, welcher den Aspekt der Sicherheit in Normen, Werten, Einstellungen und Verhalten der Beschäftigten widerspiegelt.

Unter dem Begriff “Sicherheitskultur“ ist eine sicherheitsgerichtete Grundhaltung auf allen Hierarchiestufen zu verstehen. Alle Unternehmensangehörigen sollen sich ihrer Verantwortung für die Sicherheit bewusst sein und die Fähigkeit, Mittel und Kompetenzen haben, die Verantwortung auch wahrzunehmen.

Die Sicherheitskultur umfasst zwei Hauptkomponenten. Die erste betrifft die übergeordnete Verantwortung des Managements zur Formulierung und konsequenten Umsetzung einer sicherheitsgerichteten Unternehmensphilosophie, zur Schaffung einer geeigneten Organisationsstruktur sowie zur Bereitstellung der notwendigen personellen und technischen Mittel. Die zweite Komponente beinhaltet die Einstellung und das Verhalten des Personals aller Hierarchiestufen sowie die Kommunikation zwischen diesen.

Der kontinuierliche Verbesserungsprozess ist Bestandteil einer gut entwickelten Sicherheitskultur. Dies führt zu einer kontinuierlichen Steigerung des Sicherheitsniveaus unabhängig vom Niveau rechtlicher Vorgaben.

Quelle: KAS-Leitfaden Nr. 7 bzw. Nr. 8

Abb. 31: Definition „Sicherheitskultur“ aus KAS-Leitfaden Nr. 8 (äquivalent auch im KAS-Bericht Nr. 7)

Hinweise zur Qualität der Sicherheitskultur des Betriebsbereiches können folgende Aspekte geben:

Den Beschäftigten werden Zeit, Mittel und Ressourcen für die Anlagensicherheit in ihrem Betriebsalltag zur Verfügung gestellt. Je selbstverständlicher dies in den alltäglichen Betriebsabläufen berücksichtigt wird, desto höher ist der Nutzen.

Dies beinhaltet auch, dass Vorgesetzte, bis hin zur obersten Leitung, von der Relevanz der Anlagensicherheit überzeugt sind und auch danach handeln (Vorbildfunktion).

Es gibt eine **Wechselbeziehung von Sicherheitsmanagementsystem (SMS) und Sicherheitskultur**: Ein gut gelebtes SMS kann als Beleg für eine positive Sicherheitskultur betrachtet werden.

Bei einer schlecht ausgeprägten Sicherheitskultur wird das SMS viele Mängel aufweisen, allerdings kann durch die Einführung oder Verbesserung eines SMS auch die Sicherheitskultur verbessert werden.

Spezifische Aspekte zur Sicherheitskultur finden sich auch bei der Corporate Governance, Sicherheitspolitik, Fehler- und Kommunikationskultur und Resilienz. Die Kommunikation der Erkenntnisse aus Betriebserfahrungen und Ereignissen über die Betriebsgrenzen hinaus (s. a. internes Berichtssystem) kann auch ein Indikator für eine positiv entwickelte Sicherheitskultur /KAS Bericht Nr. 7/ sein.

Zur **Bewertung von Sicherheitskulturen** gibt es Einteilung in Reifegrade oder Entwicklungsstufen von Sicherheitskulturen, z. B. in

Entwicklungsstufen / Reifegrade von Sicherheitskulturen nach Hudson

Stufe 1: Pathologisch,

Stufe 2: Reaktiv,

Stufe 3: Kalkulativ,

Stufe 4: Proaktiv),

Stufe 5: Generativ.

Abb. 32: Entwicklungsstufen / Reifegrade von Sicherheitskulturen nach Hudson

oder

Entwicklungsstufen / Reifegrade von Sicherheitskulturen nach Keil Zentrum

Stufe 1: Emerging (Aufkeimend),

Stufe 2: Managing (Organisiert),

Stufe 3: Involving (Einbeziehend),

Stufe 4: Cooperating (Kooperativ),

Stufe 5: Continuous improvement (Kontinuierliche Verbesserung)

Abb. 33: Entwicklungsstufen / Reifegrade von Sicherheitskulturen nach Keil Zentrum

oder

Phasen von Sicherheitskulturen nach K. Weißenborn, abgeleitet nach Bradly-Kurve

Phase 1: Instinkt,

Phase 2: Kontrolle,

Phase 3: Verständnis,

Phase 4: Kooperation.

Abb. 34: Phasen von Sicherheitskulturen nach K. Weißenborn, abgeleitet nach Bradly-Kurve

Abhängig von dem zugrunde gelegten Modell zur Sicherheitskultur gibt es vielfältige analytische Instrumente um diese zu bewerten.
Eine wesentliche Unterteilung stellt die Durchführung der Analyse durch externe Expert/inn/en oder als Selbstbeurteilung im Betriebsbereich dar.

Zur Veranschaulichung folgt ein Auszug von Statements zur Selbstbewertung der Sicherheitskultur (aus UBA-Texte 22/08 Einfluss menschlicher Faktoren auf Unfälle in der verfahrenstechnischen Industrie), die mit „stimmt gar nicht“, „stimmt wenig“, „stimmt teils teils“, „stimmt ziemlich“, „stimmt völlig“ und „für mich nicht zutreffend“ beantwortet werden können:

- Ich finde es wichtig, auf unerwartete Ereignisse vorbereitet zu sein.
- Es ist mir leicht möglich auf Erfahrungen von ehemaligen Kolleg/inn/en oder Vorgänger/inne/n zurückzugreifen.
- Meine Arbeit wird geschätzt.
- Ich sage es den Vorgesetzten, wenn sie sich irren.
- In meiner Abteilung werden technische Komponenten regelmäßig durch Unabhängige auf ihre Sicherheit überprüft.
- Mir ist bewusst, dass Routine gefährlich sein kann.
- Ich beteilige mich an der Überarbeitung von Prozeduren, mit denen ich arbeite.
- Wenn sich jemand gefährdend verhält schreite ich sofort ein.
- In Sicherheitsfragen gehen meine Vorgesetzten mit gutem Beispiel voran.
- Ich achte auf potentielle Gefahren für andere.
- usw.

Die Phasen der Sicherheitskultur bauen aufeinander auf.

Daher ist es sinnvoll, die Entwicklungsstufe / den Reifegrad zu bestimmen und darauf aufbauend die angemessenen Maßnahmen zur Weiterentwicklung der Sicherheitskultur zu ergreifen.

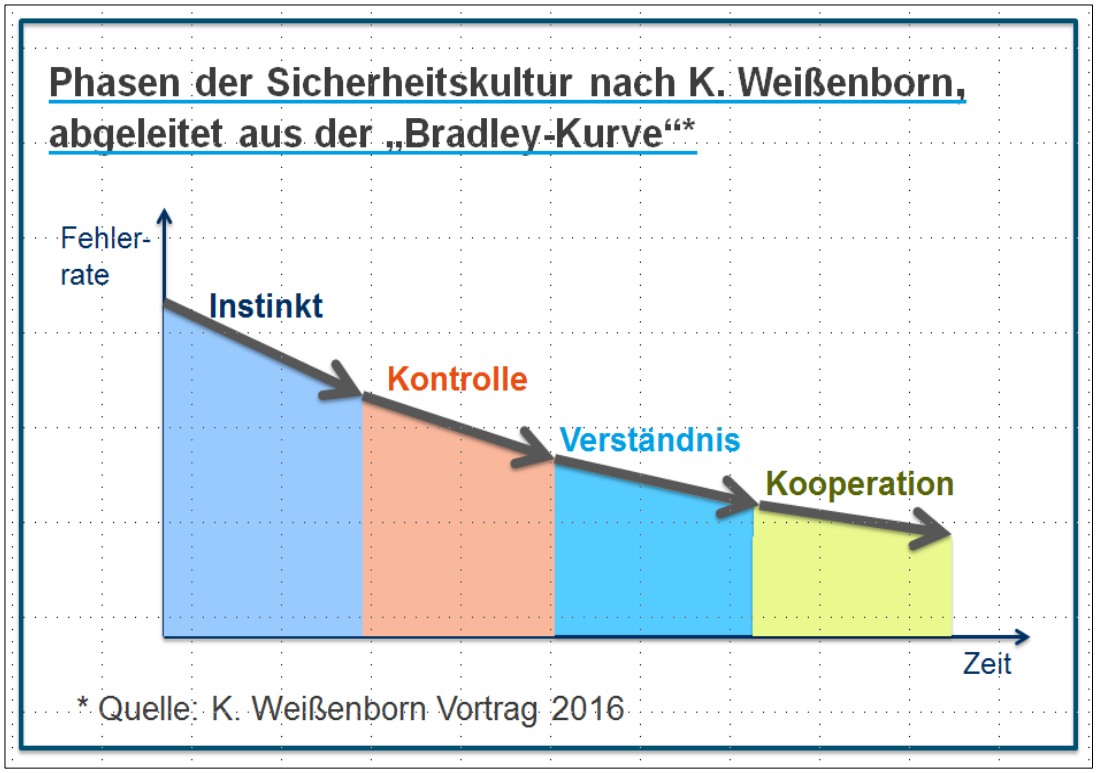

Abb. 35: Phasen der Sicherheitskultur

Beispiele (nach K. Weißenborn):
Phase „Instinkt“ u.a. mit Ausprägungen der Art „Einhaltung von gesetzlichen Bestimmungen“, „Sicherheit spielt nur eine geringe Rolle für die Beschäftigten“, „Sicherheitsverantwortung liegt (nur) beim Beauftragten für Arbeitsschutz und Anlagensicherheit“
– die Sicherheitskultur kann verbessert werden, indem die oberste Leitung sich für Sicherheit engagiert und Führungskräfte durch Maßnahmen und Handlungen zeigen, dass Sicherheit eine hohe Bedeutung hat.
Phase „Kontrolle“ u.a. mit Ausprägungen der Art „Management zeigt Engagement für Sicherheit“, „Disziplin und Regeln zur Sicherheit sind wichtig und werden überwacht und kontrolliert“, „Starker Fokus auf Schulungen“
– die Sicherheitskultur kann verbessert werden, durch die konsequente Umsetzung des SMS, Durchführung von Ereignis- und Gefahrenanalysen, Führung so gestalten, dass sie wird als gerecht wahrgenommen wird (angemessener Umgang mit Fehlern).
Phase „Verständnis“ u.a. mit Ausprägungen der Art „Persönliches Wissen und Engagement der Beschäftigten für Sicherheit“, „Prinzipien zur Sicherheit sind bekannt und verinnerlicht“, „Individualität wird anerkannt“ „Fürsorge für die eigene Person“, „Es liegt Übung und Routine zum sicherheitsgerechten Umgang vor“,
– die Sicherheitskultur kann verbessert werden, durch Fokus auf Teams und Teamtrainings, Partnerfirmenmanagement, kooperativen Führungsstil.
Phase „Kooperation“ u.a. mit Ausprägungen der Art „Anderen helfen mitzumachen“, „Eigenen Beitrag zur Sicherheit leisten“, „Sorge für Andere tragen“, „Stolz auf den Betriebsbereich sein“
– die Sicherheitskultur kann verbessert werden, durch Maßnahmen zur Förderung von Co-Kreativität, zur Verinnerlichung des Prinzips Gesamtoptimum vor Einzeloptimum, Teams führen sich selbst.

Zum Aspekt schleichende Veränderungen:

Schleichende Veränderungen sind (sehr) langsame eher kontinuierliche Veränderungen in (sehr) kleinen Schritten.
Diese nehmen Menschen häufig nicht bewusst war und verpassen damit die Chance Fehlentwicklungen in einem frühzeitigen unkritischen Stadium entgegenzusteuern.

Beispiele für schleichende Veränderungen im Rahmen der Anlagensicherheit:

- Gefahrenanalysen werden von Beschäftigten des BB mit Unterstützung externer Dienstleister durchgeführt. Im Laufe der Zeit verschiebt sich der Anteil der Unterstützung externer Dienstleister dahingehend, dass dieser die Gefahrenanalysen durchführt mit nur geringfügiger Beteiligung von Beschäftigten des BB (z. B. aufgrund sich verändernder Aufgaben und/oder Aufgabendichte bei den Beschäftigten des BB). Die Auswirkungen dieser schleichenden Veränderung können durchaus gravierend sein: Know How des BB geht verloren, Schnittstellenproblematik nimmt zu (Maßgebliche Informationen kommen nicht angemessen bei Beschäftigten an, Maßnahmen werden nicht oder unvollständig getroffen / umgesetzt etc.).
- Entnahme aus einem Stickstoff-Druckbehälter sinkt (von mehrmals wöchentlich zu 1 x im Monat). Dies führt zu einer Druckerhöhung. Gemeinsam mit weiteren Bedingungen führt dies schließlich zum Zerknall mit erheblichen Schäden (Trümmerwurf bis ca. 150 m).

Bei einer höheren Entwicklungsstufe der Sicherheitskultur wird durch die erhöhte Aufmerksamkeit und Achtsamkeit zur Anlagensicherheit die Wahrnehmung für schleichende Veränderungen erhöht. Verbunden mit frühzeitigen Reaktionen können Fehlentwicklungen durch schleichende Veränderungen eher unterbunden werden.

Hinweise für Inspektoren/innen:

Die Sicherheitskultur muss der BB selber erschaffen und leben. Von den Inspektoren/innen können daher Impulse kommen im Sinne, wie die Sicherheitskultur des BB auf „Fremde“ erscheint, wie das Fremdbild aussieht. Dies kann durchaus erheblich vom „Selbstbild“ der Beschäftigten des BB abweichen. Eine Diskussion mit dem Betreiber im Hinblick auf was ist „richtig“ und was ist „falsch“ führt hier ins Leere. Inspektoren/innen sollten darauf hinwirken, dass der Betreiber bereit ist, sich mit dem Fremdbild auseinander zu setzten und Fragen wie „Warum wirke ich so? Sind Korrekturen für die Sicherheitskultur erforderlich? etc.“ durchdenkt. Dies gilt analog für die nachfolgend abgefragten Einschätzungen zur Kommunikations- und Fehlerkultur und Resilienz.

Mögliche (Einstiegs-)Fragen zur Sicherheitskultur für Inspektoren/innen*:*

- Wie schätzt der Betreiber des BB seine Sicherheitskultur an? Anhand welche Indikatoren / Maßnahmen?
- Sind Modelle zur Sicherheitskultur / analytische Instrumente zur Bewertung der Sicherheitskultur bekannt?
- Welche Maßnahmen des Betreibers, die getroffen / umgesetzt / vorgesehen sind, dienen auch der Förderung einer guten Sicherheitskultur?
- Werden im BB Arbeitsplatz-Gefährdungsbeurteilungen für Psychische Belastungen durchgeführt? Lassen sich hieraus Erkenntnisse zur Bewertung der Sicherheitskultur ableiten?

5.8.4 Frage Nr. 4: Wie wird die Kommunikationskultur des Betriebsbereiches eingeschätzt?

Bewertungshilfe:

Bei der Kommunikationskultur liegt der Fokus auf Inhalt, Art und Weise der Verständigung innerhalb einer (großen) Gruppe von Menschen.

Die Kommunikationskultur ist ein wichtiger Bestandteil der Sicherheitskultur und spielt eine große Rolle beim Wissensmanagement und bei der Meldekultur im Rahmen des internen Berichtswesens.

Die Kommunikation eines Betriebsbereiches (BB) lässt sich unterteilen in eine **interne Kommunikation** – der Kommunikation zwischen den Beschäftigten und der **Kommunikation nach außen** (siehe hierzu auch Prüfgebiet „SMS: Planung für Notfälle“).

Die interne Kommunikation beinhaltet sowohl die Weitergabe von Informationen als auch den Dialog und Austausch zwischen der Geschäftsführung, den einzelnen Managementebenen und ihren Beschäftigten im BB und **lässt sich unterscheiden in die formelle und informelle Kommunikation.**

Die Gestaltung der formalen internen Kommunikation ist Aufgabe der Führungskräfte.

Bei großen Betrieben kann es sinnvoll sein, die interne Kommunikation als einen eigenständigen Prozess zu behandeln.

Nach Führmann und Schmidbauer gibt es ein **Drei-Stufenkonzept der internen Kommunikation** mit den Stufen:

- **Analytisch** (beinhaltet: Aufgabenstellung, Recherche und Faktenspiegel, Statusanalyse),
- **Strategisch** (beinhaltet: Ziele, Bezugsgruppen, Positionierung, Botschaften und Themen, Konkretisierung),
- **Operativ** (beinhaltet Instrumente, Zeitplanung, Budgetierung, Erfolgskontrolle).

Die Kommunikationsstruktur lässt sich unterscheiden in etablierte und anlassbezogene Elemente sowie in die inhaltlichen Elemente Information und Dialog / Austausch.

Kommunikationsinstrumente sind z. B. Mitarbeiterzeitschrift, Kummerkasten, Regelbesprechungen, Betriebsversammlungen, Mitarbeitergespräche, Intranet, Broschüren, Plakate, Kick-off-Veranstaltung etc.

Im Gegensatz zur informellen internen Kommunikation soll die formelle interne Kommunikation eine gleichberechtigte Information aller Beschäftigten herstellen mit dem Ziel diese angemessen in das Unternehmensgeschehen einzubinden und die Aufgabenerledigung zu fördern.

Die interne Kommunikation beinhaltet daher z. B.:

- Weitergabe notwendiger Informationen,
- Vermittlung betriebsinterner Werte und Ziele,
- Verdeutlichung unternehmensinterne Zusammenhänge,
- Stärkung der Zusammenarbeit der verschiedenen Unternehmensbereiche,
- Sicherung von Motivation und Leistungsbereitschaft der Beschäftigten.

Zu einer guten Kommunikationskultur gehört ein effektiver Informationsfluss, ein intensiver Austausch zwischen Führungskräften und den Mitarbeiter/innen und funktionierende Kommunikationswege der Mitarbeiter/innen untereinander.

Eine gute Kommunikationskultur wird gefördert durch eine gute Organisation der internen Kommunikation, benötigt aber auch ein entsprechend positives persönliches Kommunikationsverhalten jedes Beschäftigten im BB. Dies kann z. B. durch Fortbildungen gefördert werden.

Kommunikation ist mehr als nur Informationsweitergabe.

Wichtig sind drei Elemente der Kommunikation:

- Übertragung,
- Aufnahme und
- Bestätigung.

Eine Nachricht ist übermittelt worden, dann muss überprüft werden, ob sie erhalten und verstanden wurde und dann auch in die entsprechende Handlung umgesetzt wurde.

Positiv zu bewerten ist eine transparente, offene und klare Kommunikation.

Sinnvoll ist die Einbeziehung des Wissens der Beschäftigten (z. B. Vorschlagswesen) sowie z. B. in regelmäßigen Abständen eine Bewertung der Führungsqualitäten von Vorgesetzten durch untergebene Beschäftigte. Diese sollte in anonymer Form erfolgen und als Grundlage dazu dienen, relevantes Veränderungspotential in diesem Bereich zu erkennen und dann Maßnahmen hierzu umzusetzen.

Eine handhabbare, nutzbare Dokumentation ist ein wichtiger Bestandteil der Kommunikationskultur.

Zur Transparenz trägt eine entsprechende Weitergabe der Ergebnisse aus Überprüfungen und Audits, auch die Überprüfung und Bewertung des Konzeptes zur Verhinderung von Störfällen und des Sicherheitsmanagementsystems, durch die Leitungsebenen an die Beschäftigten bei.

Ergänzender Hinweis gegenüber /3/: Auf die Bewertungshilfe zur Frage Nr. 7 „: Wie werden die Elemente der betrieblichen Kommunikation und ihre Dokumentation bewertet?“ im Prüfgebiet „SMS: Überwachung des Betriebs“ wird hingewiesen.

5.8.5 Frage Nr. 5: Wie wird die Fehlerkultur des Betriebsbereiches eingeschätzt?

Bewertungshilfe:

Fehlerkultur ist der Teil der Sicherheitskultur, der den Umgang mit Fehlern im Unternehmen / Betriebsbereich (in einer Organisation) bestimmt.

Sie bestimmt, wie der/die einzelne Mitarbeiter/in und die Gesamtheit der Mitarbeiter/innen in allen Hierarchieebenen eines Unternehmens / Betriebsbereichs mit Fehlern umgehen. Eine konstruktive Fehlerkultur kann sich nur in einer Atmosphäre gegenseitigen Vertrauens entwickeln und dauerhaft gelebt werden.

(Ein menschlicher) Fehler bedeutet, dass eine geplante Folge von Aktivitäten nicht zu dem vorgesehenen Ergebnis führen und dies nicht einem zufälligen oder unvorhergesehenen Ereignis zugeschrieben werden kann. Ein Fehler kann nur im Nachhinein als solcher bezeichnet werden.

Definitionen zu „Fehler“ und „Latente Fehler“ aus dem KAS-Leitfaden Nr. 8:

Ein **Fehler** innerhalb des Mensch-Maschine-Systems (MMS) liegt vor, wenn das Ergebnis der Ausführung der Aufgabe eine vorgegebene bzw. situationsbezogene zugelassene Abweichung von der Aufgabe überschreitet, d.h. wenn die Arbeitsqualität außerhalb einer geforderten bzw. situationsbedingten Grenze liegt („out-of-tolerance-action“).

Bei **latenten Fehlern** handelt es sich um Fehler, die vor dem unerwünschten Ereignis unentdeckt blieben und die unter Umständen räumlich / zeitlich weit von dem aktiven Fehler getrennt sein mögen, aber dennoch für das Entstehen der Auslösehandlung maßgeblich mitbedingend sind. Latente Fehler stellen in komplexen Systemen wegen ihrer prinzipiellen Verborgenheit eine erhebliche Sicherheitsbedrohung dar. (Indikatoren: Maßnahmenverfolgungen / To-do-listen bei Ergebnissen aus Audits / Notfallübungen o. ä.: zeitnahe Umsetzung?)

Abb. 36: Definition „Fehler“ und „Latente Fehler“ gemäß KAS-Leitfaden Nr. 8

Bei einer konstruktiven Fehlerkultur erfolgt der Umgang mit Fehlern nicht im Sinne der Suche nach Schuldigen (wie bei einem strafrechtlichen Vorgehen), sondern im Sinne einer raschen und optimalen Behebung von Fehlern sowie dem Lernen aus Fehlern durch eine angemessene Ursachenklärung.

Förderlich ist ein kooperativer Umgang der Beschäftigten miteinander, auf allen Hierarchieebenen und zwischen den Hierarchieebenen.

Die Vorgesetzten, bis hin zur obersten Leitung, sind sich ihrer Vorbildfunktion bewusst und handeln auch danach. Die Beschäftigten werden ermutigt, aufgetretene Störungen, vermutete Gefährdungen, Beinaheunfälle etc. zu melden und Fehler als Chance für Verbesserungen, Lerneffekte und Weiterentwicklung zu verstehen.

Es muss aber auch deutlich sein, dass bei mutwilligen Verstößen klare angemessene Konsequenzen erfolgen.

Die konstruktive Fehlerkultur ist geprägt von dem Bewusstsein, dass Fehler zum menschlichen Handeln gehören und fehlerhaftes Verhalten in der Regel nicht auf Inkompetenz oder Schädigungsabsichten zurückzuführen ist. Ist diese grundlegende Akzeptanz gegeben werden Fehler als Lernchance begriffen, das Verhalten zu verbessern.

5.8.6 Frage Nr. 6: Wie wird die Resilienz des Betriebsbereiches eingeschätzt?

Bewertungshilfe:

Resilienz angelehnt nach Vortrag von Dr. Babette Fahlbruch:

Resilienz ist die Fähigkeit eines (organisationalen) Systems (Betriebsbereiches), Risiken vorherzusehen und mit ihnen effektiv umzugehen. Dazu passt es seine Handlungen, Teilsysteme und Prozesse so an, dass seine Kernfunktionen stabil und effektiv in der bestehenden Umwelt ausgeführt werden können. Diese Eigenschaft wird besonders wichtig, wenn die Umwelt nicht stabil ist und diese Instabilität zur Zerstörung des Systems (Betriebsbereiches) führen kann.
Resiliente Organisationen erreichen verschiedene Unternehmensziele simultan und flexibel. Resilienz ist auch die Fähigkeit nach einem Unfall / einer Krise schnell zum Normalbetrieb zurückzukehren. Resilienz ist ein dynamischer Prozess.

Merkmale resilienter Organisationen:

- **Durchsetzungsvermögen: Schnelle und effektive Reaktion auf erkannte Gefahren (Indikatoren: Maßnahmenverfolgungen / To-do-listen bei Ergebnissen aus Audits / Notfallübungen o. ä.: zeitnahe Umsetzung?),**
- **konservative Entscheidungen in Sicherheitsfragen: Ausbalancieren bzw. Abfedern des Produktionsdruckes und der Sicherheitserfordernisse,**
- **Flexibilität,**
- **Ressourcen,**
- **Die Wahrnehmung für die (möglichen) Gefahren aufrecht erhalten (statt sich durch Routine in einer falschen Sicherheit zu wiegen).**

nach B. Fahlbruch

Abb. 37: Merkmale resilienter Organisationen nach B. Fahlbruch

Resilienz angelehnt nach Vortrag von Prof. Dr. Toni Wäfler:

Resilienz ist eine erweiterte Sichtweise auf die Sicherheit, eine Erweiterung bestehender SMS. **Der Mensch wird** bei dieser Sichtweise (Safety II nach Hollnagel**) als Sicherheitsfaktor angesehen und ist die Ressource für Anpassungsfähigkeit (Resilienz). Die Resilienz beinhaltet insbesondere die Fähigkeit einer Organisation unter dynamischen Bedingungen die Kontrolle aufrecht zu erhalten.**

Resilienz bedeutet die Fähigkeit einer Organisation

- **sich effizient an wechselnde gefährdende Einflüsse anzupassen (nicht: gefährdende Einflüsse vermeiden oder ihnen widerstehen) und**
- **einen dynamisch stabilen Zustand zu erreichen, auch und gerade nach Zwischenfällen.**

Prämisse ist hierbei:

- **Unsichere Zustände entstehen durch unzureichende Anpassung und nicht: weil ein Fehler geschah,**
- **Sicherheit entsteht durch proaktive adaptive Prozesse und nicht durch reaktive Barrieren.**

nach T. Wäfler

Abb. 38: Fähigkeiten resilienter Organisationen nach T. Wäfler

Bei der früheren Sichtweise (**Safety I nach Hollnagel**) wird der *Mensch als Risikofaktor* gesehen: Er macht potenziell Fehler, Fehlerquellen müssen gefunden und über die Sicherstellung einer vorschriftsgemäßen Arbeitsausführung vermieden werden. Wird unter dieser Sichtweise eine Ereignisanalyse durchgeführt, so unterliegt man schnell einem **Rückschaufehler (Hindsight-Bias)**: Eine rückblickende Vereinfachung und Überschätzung der Vorhersehbarkeit des Ergebnisses. Eigentlich alltägliche Handlungen werden rückblickend als Fehler bezeichnet – allerdings nur, wenn sie negative Folgen hatten. Es kann viele Gründe für das Abweichen von Vorschriften geben:

- Zu viele Vorschriften,
- Vorschriften nicht gekannt / nicht verstanden,
- Widersprüche zwischen den Vorschriften,
- Vorschriften nicht geeignet für Nicht-Standard-Situationen,
- Notwendigkeit sich an Situationen anzupassen.

Bei Forschungen zur Resilienz wird der Fokus nicht auf Fehler gelegt (was ist falsch gelaufen), sondern es wird untersucht, wie kommt es zum Erfolg (warum laufen Dinge richtig).

Nach Hollnagel gilt das **Efficiency-Thoroughness Trade-Off (ETTO) Prinzip:**

Menschen und Organisationen müssen (i. d. R.) bei der Aufgabenerfüllung eine Balance finden zwischen (Handlungs-)Effizienz (Efficiency) und Gründlichkeit (Thoroughness).

Das Prinzip ETTO ist nicht gleichzusetzen mit Produktivität und / oder Sicherheit. Es führt zu Variabilität in der Arbeitsausführung:

- Diese Variabilität ist eine Stärke des Menschen, weil sie es ihm erlaubt, sich anzupassen.
- Dieselbe Variabilität trägt aber auch zu negativen Ereignissen bei. Dann nennen wir sie „Fehler“.

Bei der Standardisierung lassen sich drei Arten bestimmen:

a. Handlungsvorgaben (Detaillierte Vorschrift für eine konkrete operative Handlungsweise)
b. Prozessvorgaben (Leitlinien / Checklisten zur Vorgehensweise)
c. Zielvorgaben (Vorgabe des Ziels, ohne Aussage, wie das Ziel erreicht werden soll)

Von a. nach c. nimmt dabei der operative Handlungsspielraum aber auch die Effektivität bei zunehmender Unsicherheit zu.

Um Safety I und Safety II zueinander in Beziehung zu setzen, kann ein Unternehmen (Betriebsbereich) Bereiche mit einer geringen Bandbreite von Schwankungen und Störungen bzw. einer guten Vorhersehbarkeit der Schwankungen und Störungen mittels Stabilität, d. h. Standards (klare Handlungsvorgaben z. B. in Form von Arbeitsanweisungen) handhaben, während Bereiche mit einer großen Bandbreite von Schwankungen und Störungen bzw. einer schlechten Vorhersehbarkeit der Schwankungen und Störungen durch Flexibilität / Anpassung, z. B. durch die Orientierung an Zielvorgaben bewältigt werden müssen.

Bei der Gestaltung der Regelungen im Betriebsbereich ist es wichtig den obigen Aspekt zu berücksichtigen. Dies kann gut erfolgen, wenn der Dokumentenaufbau des MS oder SMS eine nachvollziehbare Struktur mit einem roten Faden bzw. Prozessorientierung aufweist, wie dies in der Bewertungshilfe zur Frage „Wie ist die Dokumentation des SMS im Betriebsbereich zu bewerten?“ beschrieben ist. Eine weitere Voraussetzung wird i. d. R. ein entsprechender Reifegrad / Phase der Sicherheitskultur sein.

Im Rahmen von Inspektionen können zur Einschätzung der Resilienz Gespräche mit Beschäftigten verschiedener Hierarchiestufen geführt werden. Hierbei können Antworten zu folgenden Fragen hilfreich sein:

- Gab es in der Vergangenheit unvorhergesehene kritische Situationen, die Sie gut bewältigt haben?
  - Welche Faktoren haben zur erfolgreichen Bewältigung beigetragen?
- Welche Gefahren sehen Sie bei Ihrer Tätigkeit / dem Betriebsbereich?
- Gibt es Handlungsvorgaben zum Umgang mit Gefahren?
  - (Sind Abweichungen davon möglich?)

6 Quellenangaben zu den Prüfgebieten SMS (Sicherheitsmanagementsystem)

6.1 Aufbau der Quellenangaben

Die Quellenangaben werden in die zwei Kapitel „Übergeordnete Quellenangaben“ und „Kapitelbezogene Quellenangaben“ aufgeteilt. Quellenangaben aus den Kapitel „Übergeordnete Quellenangaben“ stehen in Bezug zu mehreren SMS-Kapiteln. *Der kursive Text ist gegenüber /3/ aktualisiert worden.*

6.2 Übergeordnete Quellenangaben

Zwölften Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes - Störfallverordnung -12.BImSchV, Stand 14. Januar 2017

Directive 2012/18/EU of the European Parliament and oft the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC

Die Kommission für Anlagensicherheit (KAS) ist eine nach § 51a Bundes-Immissionsschutzgesetz beim Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit gebildete Kommission (vormals Störfallkommission (SFK)).
Auf der Homepage der Kommission für Anlagensicherheit (KAS) sind die folgenden Publikationen kostenfrei als Download erhältlich (http://www.kas-bmu.de/ -> Publikationen):

KAS-51 „Leitfaden Maßnahmen gegen Eingriffe Unbefugter“ (14. November 2019), (der kursive Text ist gegenüber /3/ aktualisiert worden)

KAS-29 „Leitfaden Besondere Anforderungen an Sicherheitstechnik und Sicherheitsorganisation zur Unterstützung von Anlagenpersonal in Notfallsituationen unter besonderer Berücksichtigung des Leitfadens KAS-20“ (Februar 2014)

KAS-20 „Leitfaden Kompetenzen bezüglich menschlicher Faktoren im Rahmen der Anlagensicherheit (Betreiber, Behörden und Sachverständige)“ erarbeitet vom Arbeitskreis „Menschliche Faktoren“ (06/2011)

KAS-19 „Leitfaden zum Konzept zur Verhinderung von Störfällen und zum Sicherheitsmanagementsystem“ erarbeitet vom Arbeitskreis „Überarbeitung und Zusammenführung der Leitfäden SFK-GS-23 und –24 überarbeitet von dem Ausschuss „Seveso-Richtlinie“, 3. überarbeitete Fassung“ (November 2018), (der kursive Text ist gegenüber /3/ aktualisiert worden)

KAS-19 „Leitfaden zum Konzept zur Verhinderung von Störfällen und zum Sicherheitsmanagementsystem“ erarbeitet vom Arbeitskreis „Überarbeitung und Zusammenführung der Leitfäden SFK-GS-23 und –24“ (06/2011)

KAS-13 Abschlussbericht des Arbeitskreises Tanklager „Bewertung des Tanklagerbrands von Buncefield / GB vom 11.12.2005 und daraus für deutsche Großtanklager für Ottokraftstoff abgeleitete Empfehlungen“ (11/2009)

KAS-8 „Leitfaden Empfehlungen für interne Berichtssysteme als Teil des Sicherheitsmanagementsystems gemäß Anhang III der Störfallverordnung“ des Arbeitskreises „Menschliche Faktoren“ (10/2008)

KAS-7 Bericht des Arbeitskreises „Texas City“: „Empfehlungen der KAS für eine Weiterentwicklung der Sicherheitskultur - Lehren nach Texas City 2005“ (10/2008)

KAS-5 Bericht des Arbeitskreises „Risikokommunikation“: „Risikokommunikation - Anforderungen nach Störfall-Verordnung, Praxis und Empfehlungen“ (06/2008)

KAS-1 Bericht “Sicherheitsrelevante Teile eines Betriebsbereiches und Richtwerte für sicherheitsrelevante Anlagenteile (SRA)“ (02.06.2015, redaktionell angepasst am 05.10.2017), (der kursive Text ist gegenüber /3/ aktualisiert worden)

KAS-1 Abschlussbericht „Richtwerte für sicherheitsrelevante Anlagenteile (SRA) und sicherheitsrelevante Teile eines Betriebsbereiches (SRB)“
Hinweis: Der Bericht KAS-1 A basiert auf der geltenden Störfall-Verordnung 2005 (11/2006). Der Bericht KAS-1 B basiert auf der Seveso-III-Richtlinie (06/2015).

SFK-GS-45 „Leitfaden Schnittstelle Notfallplanung“ des Arbeitskreises „Schnittstelle Notfallplanung“ (10/2005)

Hinweise zur Berücksichtigung von Human-Factor-Aspekten bei der proaktiven Notfallvorsorge des Arbeitskreises „Human Factor“ (05/2003)

SFK-GS-38 „Leitfaden Maßnahmen gegen Eingriffe Unbefugter“ der ad hoc-Arbeitsgruppe Eingriffe Unbefugter (10/2002)

SFK-GS-32 „Human-Factor-Aspekte für Betriebsbereiche und Anlagen nach der Störfallverordnung (12. BImSchV)“ des Arbeitskreises „Human Factor“ (09/2001)

OECD /CCA Workshop Mai 2007 in Potsdam: „Einfluss menschlicher Faktoren auf Chemieunfälle“
Zusammenfassung der Präsentationen und Ergebnisse im UBA Forschungsbericht 206 48 300 „Einfluss menschlicher Faktoren auf Unfälle in der verfahrenstechnischen Industrie“, Texte 22/08, ISSN 1862-4804
Download auf den Internetseiten des Umweltbundesamtes: http://www.umweltbundesamt.de (UBA-Texte 22/08 Einfluss menschlicher Faktoren auf Unfälle in der verfahrenstechnischen Industrie)

„Anlagensicherheit“, Hrsg. B. Richter, Hüthig Verlag, Heidelberg, 2007, ISBN: 978-3-7785-4007-7

6.3 Quellenangaben zu SMS: Konzept zur Verhinderung von Störfällen und Aufbau des SMS

LANUV-Arbeitsblatt 41 „Darstellung des Sicherheitsmanagementsystems im Sicherheitsbericht“, Stand April 2019, (der kursive Text ist gegenüber /3/ aktualisiert worden)

Musterkapitel „Darstellung des Sicherheitsmanagementsystems im Sicherheitsbericht“ des LANUV NRW, Stand: Mai 2007

Technische Regel Anlagensicherheit
TRAS 410 „Erkennen und Beherrschen exothermer chemischer Reaktionen“ - Fassung 10/2012
Download TRAS 410 kostenfrei erhältlich auf der Homepage der Kommission für Anlagensicherheit (KAS) (http://www.kas-bmu.de/)
Die TRAS 410 wurde am 20.12.2012 im Bundesanzeiger veröffentlicht.
Hinweis: Die von der KAS am 14.11.2019 verabschiedete, aber noch nicht bekanntgegebene Neufassung der TRAS 410 (Entwurf) steht als Download auf der Homepage der KAS zur Verfügung)

OECD-Leitfaden „Corporate Governance für die Anlagen- und Prozesssicherheit“ (Juni 2012)

Modul „Fragebogen Corporate Governance (Grundsätze der Unternehmensführung) zur Anlagen- und Prozesssicherheit (CG APS) der Bezirksregierung Arnsberg NRW“: Für deutsche Verhältnisse modifizierte Fragen des OECD-Leitfadens „Corporate Governance für die Anlagen- und Prozesssicherheit“.

„Deutscher Corporate Governance Kodex“ in der Fassung vom 5. Mai 2015 mit Beschlüssen aus der Plenarsitzung vom 5. Mai 2015 von der Regierungskommision Deutscher Corporate Governance Kodex*; Hinweis: Letzte Fassung vom 16. Dezember 2019*

ISO 31000 "Risk Management – Principles and guidelines", November 2009
Hinweis: DIN ISO 31000:2018-10 Risikomanagement - Leitlinien (ISO 31000:2018)

Begriff Corporate Governance aus dem wirtschaftslexikon.gabler.de

DIN EN 31010 (VDE 0050-1) „Risikomanagement – Verfahren zur Risikobeurteilung“, November 2010

DIN EN ISO 9000 „Qualitätsmanagementsysteme – Grundlagen und Begriffe“, November 2015

DIN EN ISO 9001 „Qualitätsmanagementsysteme – Anforderungen“, November 2015

6.4 Quellenangaben zu SMS: Organisation und Personal

Veröffentlichung „Fit für den Wissenswettbewerb -Wissensmanagement in KMU erfolgreich einführen“ des Bundesministerium für Wirtschaft und Technologie

Gesetz über die Durchführung von Maßnahmen des Arbeitsschutzes zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Beschäftigten bei der Arbeit - Arbeitsschutzgesetz – ArbSchG vom 7. August 1996 (Stand 01.01.2016)

Gesetz über die Bereitstellung von Produkten auf dem Markt - Produktsicherheitsgesetz – ProdSG vom 8. November 2011 (Stand 08.09.2015)

Verordnung über Sicherheit und Gesundheitsschutz bei der Verwendung von Arbeitsmitteln - Betriebssicherheitsverordnung – BetrSichV vom 3. Februar 2015 (Stand 05.04.2017) und den zugehörigen Technischen Regeln für Betriebssicherheit (TRBS), insb. TRBS 1112 Instandhaltung, Ausgabe: Oktober 2010 GMBl. Nr. 60 vom 14. Oktober 2010 S. 1219

Vollzugshilfe zur Störfall-Verordnung vom März 2004,

VDI 4006 Richtlinie Blatt 1 „Menschliche Zuverlässigkeit – Ergonomische Forderungen und Methoden der Bewertung“, März 2015

6.5 Quellenangaben zu SMS: Ermittlung und Bewertung der Gefahren von Störfällen

VDI 4006 Richtlinie Blatt 2 „Menschliche Zuverlässigkeit – Methoden zur quantitativen Bewertung menschlicher Zuverlässigkeit“, Februar 2003; aktualisierte Fassung: November 2017

Risikobeurteilung in der Anlagensicherheit
Das PAAG- / HAZOP – Verfahren und weitere praxisbewährte Methoden,
Hrsg. IVSS Sektion Chemie, 5. Ausgabe 3/2020, ISBN 92-843-7037-X
https://ww1.issa.int/de/prevention-chemistry
(der kursive Text ist gegenüber /3/ ergänzt worden)

6.6 Quellenangaben zu SMS: Überwachung des Betriebs

VDI/VDE 2180 Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT):
Blatt 1: Einführung, Begriffe, Konzeption, April 2007
Blatt 2: Managementsystem, April 2007
Blatt 3: Anlagenplanung, -errichtung und -betrieb, April 2007
Blatt 4: Nachweis der Hardwaresicherheitsintegrität einer PLT-Schutzeinrichtung, Juli 2010
Blatt 5: Empfehlungen zur Umsetzung in die Praxis, Mai 2010
Blatt 6: Anwendung der funktionalen Sicherheit im Rahmen von Explosionsschutzmaßnahmen, Juni 2013

Hinweis (der kursive Text ist gegenüber /3/ aktualisiert worden): Die VDI/VDE 2180 ist grundlegend überarbeitet worden bzw. befindet sich im Überarbeitungsprozess. Der Titel der Richtlinienreihe VDI/VDE 2180 lautet nun „Funktionale Sicherheit in der Prozessindustrie“ und enthält folgende Blätter:

Herausgabe	***VDI/VDE 2180 „Funktionale Sicherheit in der Prozessindustrie“, Untertitel:***	***Änderung gegenüber Vorausgabe***
April 2019	*Blatt 1 Einführung, Begriffe, Konzeption*	*Enthält Inhalte der Blätter 1, 2 und 5 der Vorausgabe.*
September 2019	*Blatt 2 Planung, Errichtung und Betrieb von PLT-Sicherheitsfunktionen*	*Enthält Inhalte des Blattes 3 der Vorausgabe.*
September 2019	*Blatt 3 Nachweis der Ausfallwahrscheinlichkeit im Anforderungsfall (PFD)*	*Enthält Inhalte des Blattes 4 der Vorausgabe.*
Gründruck Februar 2020	*Blatt 4 Mechanische Komponenten in PLT-Sicherheitsfunktionen*	*Die Inhalte sind neu, Inhalte des Blattes 6 der Vorausgabe entfallen.*

Abb. 39: Blätter des Richtlinienreihe VDI/VDE 2180 „Funktionale Sicherheit in der Prozess-industrie“

VDI/VDE 2180 Ausgabe April 2019	*VDI/VDE 2180 Ausgabe April 2007*
PLT-Betriebseinrichtung (PLT-B) (Messen, Steuern, Regeln, Alarmieren, Melden, Schalten)	*PLT-Betriebseinrichtung (Messen, Steuern, Regeln) PLT-Überwachungseinrichtung (Alarmieren, Melden, Schalten)*
PLT-Betriebseinrichtung mit Sicherheitsfunktion (PLT-BS) (Risikominderung um maximal Faktor 10)	*Hochverfügbare PLT-Überwachungseinrichtung*
PLT-Sicherheitseinrichtung (PLT-S) (Risikominderung >10: SIL 1 bis SIL 4)	*PLT-Schutzeinrichtungen*

Abb. 40: Einteilung der PLT-Einrichtungen nach VDI/VDE 2180 „neu“ gegenüber „alt“

TRGS 555 „Betriebsanweisung und Information der Beschäftigten“

Handlungshilfe zur Erstellung von Arbeitsunterlagen für die Prozessführung (2010, Lafrenz, Nickel, Nachreiner)

VDI/VDE 3699 Blatt 5 „Prozessführung mit Bildschirmen Alarme / Meldungen“, September 2014

IT-Sicherheitsgesetz (Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes - BSI-Gesetz – BSIG vom 14. August 2009)

Hinweise zu Regelwerke (Beispiele):
VDI 2182 „Informationssicherheit in der industriellen Automatisierung“:
Blatt 1 Allgemeines Vorgehensmodell
Blatt 2.1 Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Hersteller Speicherprogrammierbare Steuerung (SPS)
Blatt 3.1 Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Hersteller Prozessleitsystem einer LDPE-Anlage
Blatt 3.2 Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Integratoren LDPE-Reaktor
Blatt 3.3 Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Betreiber LDPE-Anlage

BSI (Bundesamt für Sicherheit in der Informationstechnik): IT-Sicherheit Grundschutz, Informationen, technische Richtlinien und Standards zur IT-Sicherheit (z. B. BSI-Standards – Methoden, Verfahren und Prozesse zur Informationssicherheit, IT-Grundschutz-Kompendium, IT-Grundschutz-Kataloge etc.). Im Zusammenhang mit der Anlagensicherheit ist das ICS-Security-Kompendium hervorzuheben.
DIN ISO/IEC 27000 ff. Informationstechnik – IT-Sicherheitsverfahren –
27000: Informationssicherheits-Managementsysteme - Überblick und Terminologie
27001: Informationssicherheits-Managementsysteme – Anforderungen
27002: Leitfaden für Informationssicherheits-Maßnahmen
27003: Informationssicherheits-Managementsysteme – Leitfaden
27005: Informationssicherheit- Risikomanagement

DIN-IEC 62443 Industrielle Kommunikationsnetzte – IT-Sicherheit für Netze und Systeme ff. (ehemals ISA-IEC 62443)
DIN EN 13306 Instandhaltung – Begriffe der Instandhaltung, Dezember 2010
DIN 31051 Grundlagen der Instandhaltung, September 2012*, Stand 2019-06*

VDI 2890 „Planmäßige Instandhaltung Anleitung zur Erstellung von Arbeits-, Wartungs- und Inspektionsplänen“, Entwurf Stand April 2015*, Stand 2017-03*
VDI 2893 Richtlinie *Stand 2019-11*
VDI 2895 Richtlinie „Organisation der Instandhaltung - Instandhalten als Unternehmensaufgabe“, Dezember 2012

ISSA Prevention Series No. 2054 (G), 2007
Instandhaltung und Änderungen - Besondere Gefährdungen und Risiken bei Prozessanlagen Hinweise für die Praxis
Herausgeber: Internationale Sektion der IVSS für die Verhütung von Arbeitsunfällen und Berufskrankheiten in der chemischen Industrie, Kurfürsten-Anlage 62, 69115 Heidelberg, Deutschland. ISSN 1015-8022, ISBN 92-843-7177-5

MAHBulletin Lessons Learned Nr. 7 „Major accidents related to ageing“

HSE (Health and Safety Executive) verschiedene Dokumente veröffentlicht
- Manageing Ageing Plant – A Summary Guide
- Ageing Plant Operational Delivery Guide der COMAH Competent Authority

TRBS 1201 Prüfungen von Arbeitsmitteln und überwachungsbedürftigen Anlagen
TRBS 1201 Teil 1 Prüfung von Anlagen in explosionsgefährdeten Bereichen und Überprüfung von Arbeitsplätzen in explosionsgefährdeten Bereichen
TRBS 1201 Teil 2 Prüfungen bei Gefährdungen durch Dampf und Druck

6.7 Quellenangaben zu SMS: Planung für Notfälle

Ordnungsbehördliche Verordnung über die unverzügliche Anzeige von umweltrelevanten Ereignissen beim Betrieb von Anlagen - Umwelt-Schadensanzeige-Verordnung vom 21. Februar 1995, Stand 08.11.2014

VCI-Leitfaden Notfallmanagement – Gefahrenabwehr 2010,

Merkblätter Band 45: Musterkonzept für die Notfallplanung, LANUV NRW

6.8 Quellenangaben zu SMS: Überwachung der Leistungsfähigkeit des Sicherheitsmanagementsystems

VDI 4006 Richtlinie Blatt 3 „Menschliche Zuverlässigkeit – Methoden zur Ereignisanalyse“, August 2013

Leitfaden „Ganzheitliche Unfallanalyse – Leitfaden zur Ermittlung grundlegender Ursachen von Arbeitsunfällen in kleinen und mittleren Unternehmen“ von B. Fahlbruch, I. Meyer (https://www.baua.de/ unter Publikationen)

Leitfaden zur Erfassung von Performance-Indikatoren für die Prozesssicherheit (Januar 2015) des VCI

OECD Leitfaden Guidance on Developing Safety Performance Indicators

6.9 Quellenangaben zu SMS: Systematische Überprüfung und Bewertung

Vortrag K. Weißenborn Sicherheitskultur

Führmann und Schmidbauer Drei-Stufenkonzept der internen Kommunikation

Resilienz angelehnt nach Vortrag von Dr. Babette Fahlbruch

Resilienz angelehnt nach Vortrag von Prof. Dr. Toni Wäfler

Literatur zum Thema Kommunikation / Betriebs-psychologie

SCHULZ VON THUN, F.:Miteinander reden, Rowohlt Taschenbuchverlag

GROS, E., 1994: Anwendungsbezogene Arbeits-, Betriebs- und Organisationspsychologie, Verlag für Angewandte Psychologie Göttingen

BIRD (JR), F. E., GERMAIN, G.L.: Verlustkontrolle als Führungsaufgabe

ROGERS, C.R.: Die nicht-direktive Beratung, Fischer Taschenbuchverlag

WEINBERGER, S.: Klientenzentrierte Gesprächsführung, Beltz Verlag

STAHL, E.: Dynamik in Gruppen, 2002: Dynamik in Gruppen, Beltz-Verlag

RECHTIEN, W., 1999: Angewandte Gruppendynamik, Beltz Verlag

LANG, R.W.: Schlüsselqualifikationen, Deutscher Taschenbuch Verlag

KASTNER, M., 1999: Erfolgreich mit sozialer Kompetenz, Herder Verlag

7 Literatur

[1] Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen:
Zur Inspektion von Sicherheitsmanagementsystemen, Essen, Stand Januar 2006

[2] Überwachungsplan der Abteilung für Umwelt und Arbeitsschutz der Bezirksregierung Köln, 5. Auflage, Stand: 7/2017

[3] Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen:
Auflistung der Fragen mit Bewertungshilfen zur Unterstützung der Beurteilung von Sicherheitsmanagementsystemen nach Anhang III der Störfallverordnung 2017, Stand August 2017 https://www.lanuv.nrw.de/fileadmin/lanuv/anlagen/pdf/SMS_Fragen_mit_Bewertungshilfen_2017.08.28.pdf

[4] Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen: Musterkapitel, Darstellung des Sicherheitsmanagementsystems im Sicherheitsbericht, Essen, Stand Mai 2007 https://www.lanuv.nrw.de/fileadmin/lanuv/anlagen/pdf/SB_Musterkapitel_SMS.pdf

[5] Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen:
SMVP zum Download
(https://www.lanuv.nrw.de/umwelt/industrieanlagen/anlagensicherheit/ueberwachung-von-betriebsbereichen/smvp-zum-download)

[6] Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen:
Hilfetext deutsch: Safety-Management-Valuation-Program Bedienungsanleitung
(https://www.lanuv.nrw.de/fileadmin/lanuv/umwelt/pdf/SMVP_de.pdf)

[7] Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen,LANUV-Arbeitsblatt 41, Stand 04/2019: Darstellung des Sicherheitsmanagementsystems im Sicherheitsbericht, https://www.lanuv.nrw.de/umwelt/industrieanlagen/anlagensicherheit/sicherheitsmanagement-system-sms/sms-im-sicherheitsbericht

8 Abbildungsverzeichnis

9 Abkürzungsverzeichnis

Abkürzung	Definition
AA	Arbeitsanweisungen
AGAP	Alarm- und Gefahrenabwehrpläne
ArbSchG	Arbeitsschutzgesetz
BA	Betriebsanweisungen
BB	Betriebsbereich
BetrSichV	Betriebssicherheitsverordnung
BGV	Berufsgenossenschaftliche Vorschriften (von den deutschen Berufsgenossenschaften erlassenen Unfallverhütungsvorschriften bis 1.05.2014, danach DGUV)
BGV A1	Grundsätze der Prävention, seit 1.05.2014 DGUV Vorschrift 1
BGW	Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege
BImSchV	Bundes-Immissionsschutz-Verordnung
BR	Bezirksregierungen
BSI	Bundesamt für Sicherheit in der Informationstechnik
CD	Compact Disc
CEO	Chief Executive Officers (geschäftsführendes Vorstandsmitglied)
CERT	Computer Emergency Response Team
CG	Corporate Governance (deutsch: Grundsätze der Unternehmensführung)
CG APS	Corporate Governance (Grundsätze der Unternehmensführung) zur Anlagen- und Prozesssicherheit
CLP	Classification, Labelling and Packaging, (deutsch: Einstufung, Kennzeichnung und Verpackung von Stoffen und Gemischen). Die europäische CLP-Verordnung setzt die internationale GHS um.
COMAH	Control of Major Accident Hazards (England)
DGUV	Vorschriften- und Regelwerk der gesetzlichen Unfallversicherung
DIN	Deutsche Institut für Normung e. V.
EC&I	Electrical, Control & Instrumentation
EDV	Elektronische Datenverarbeitung
EEMUA	Engineering Equipment and Materials Users Association
EN	Europäische Norm
ETTO	Efficiency-Thoroughness Trade-Off
EU	Europäische Union
FMEA	Fehler- Möglichkeiten- und Einfluss-Analyse (englisch: Failure Mode and Effects Analysis)
FORDEC	Methode zur strukturierten Entscheidungsfindung (Facts, Options, Risks & Benefits, Decision, Execution, Check: Schritte, die zur Entscheidungsfindung führen)
GDV	Gesamtverband der Deutschen Versicherungswirtschaft e. V.
GefStoffV	Gefahrstoffverordnung
GHS	Globally Harmonized System of Classification, Labelling and Packaging of Chemicals
HAZOP	Hazard and Operability Study

H-Sätze	H-Sätze (Hazard Statements) nach GHS bzw. CLP-VO beschreiben Gefährdungen, die von den chemischen Stoffen oder Zubereitungen ausgehen
HSE	Health and Safety Executive (britische Arbeitsschutzbehörde)
ICS	Industrial Control Systems (deutsch: industrielle Steuerungssysteme, Automatisierungssysteme)
IEC	Internationale Elektrotechnische Kommission
IMIS	Informationssicherheits-Managementsystem
IMS	Integriertes Managementsystem
IPSC	Institute for the Protektion and Security of the Citizen (EU)
IPSS	Instandhaltungsplanungs- und Steuerungssystemen
IRAM	Integreted Risk Assessment Method
ISA	Instrument Society of Automation; vorher Instrumentation, Systems, and Automation Society, ursprünglich Instrument Society of America: ein Gremium für Standards in den USA
ISO	International Organization for Standardization (Internationale Organisation für Normung)
IVSS	Internationalen Vereinigung für Soziale Sicherheit
IT	Informationstechnik
KAS	Kommission für Anlagensicherheit
KMU	Kleine und mittlere Unternehmen
KPI	Key Performance Indicator
LANUV	Landesamt für Natur, Umwelt und Verbraucherschutz
LoPC	Loss of Primary Containment (Stofffreisetzung)
LPDE	Low-Density-Polyethylen
MAHB	Major Accidents Hazards Bureau (EU)
MCDA	Multi-Kriterien-Entscheidungsanalyse (englisch: Multi Criteria Decision Analysis)
MKULNV	Ministerium für Klimaschutz, Umwelt, Landwirtschaft, Natur- und Verbraucherschutz
MULNV	Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz
MMS	Mensch-Maschine-System
MoC	Management of Change (Änderungsmanagement)
MS	Managementsystem
MTO	Mensch, Technik, Organisation
NAMUR	Normenarbeitsgemeinschaft für Meß- und Regeltechnik in der chemischen Industrie (1949); seit 2005: Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V
NAMUR NE	NAMUR-Empfehlungen
NRW	Nordrhein-Westfalen
OECD	Organisation for Economic Co-operation and Development (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)

PAAG	Prognose, Auffinden der Ursache, Abschätzen der Auswirkungen, Gegenmaßnahmen
PDCA	Plan-Do-Check-Act (Planen-Handeln-Prüfen-Verbessern)
PFD	Ausfallwahrscheinlichkeit bei Anforderung (Probability of Dangerous Failure on Demand)
PLS	Prozessleitsystem
PLT	Prozessleittechnik
PSA	Persönliche Schutzausrüstung
P-Sätze	P-Sätze (Precautionary Statements) nach GHS bzw. CLP-VO geben Sicherheitshinweise im Umgang mit chemischen Stoffen oder Zubereitungen, die mit H-Sätzen eingestuft sind.
PSI	Process Safety Incidents (Prozess-Sicherheitsereignisse)
PSIR	Process Safety Incident Rate
R&I-Fließ-schemata	Rohrleitungs- und Instrumentenfließschema
SB	Sicherheitsbericht
SFK	Störfallkommission
SMART	Steuerungsrelevant, Messbar, Ambitioniert, Realistisch, Terminbezogen
SMS	Sicherheitsmanagementsystem
SMVP	Safety-Management-Valuation-Program
SPS	Speicherprogrammierbare Steuerung
SRA	sicherheitsrelevantes Anlagenteil
SRB	sicherheitsrelevantes Teil eines Betriebsbereiches
TEL	Technische Einsatzleitung
TPM	Total Productive Maintenance
TRAS	Technische Regel Anlagensicherheit
TRBS	Technische Regeln für Betriebssicherheit
TRGS	Technische Regeln für Gefahrstoffe
UK	United Kingdom (Vereinigtes Königreich Großbritannien und Nordirland)
UNECE	Wirtschaftskommission für Europa der Vereinten Nationen
UVV	Unfallverhütungsvorschriften (2000 bis 1.05.2014 BGV, seitdem DGUV)
VA	Verfahrensanweisung
VCI	Verband der chemischen Industrie e.V.
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e. V.
VDI	Verein Deutscher Ingenieure
VdS	Verband der Sachversicherer
VO	Verordnung

Landesamt für Natur, Umwelt und
Verbraucherschutz Nordrhein-Westfalen

Leibnizstraße 10
45659 Recklinghausen
Telefon 02361 305-0
poststelle@lanuv.nrw.de

www.lanuv.nrw.de