TÜV AUSTRIA

PROCESS SAFETY INDICATORS

Empfehlungen für die praktische Anwendbarkeit von Sicherheitsindikatoren bei Prozessanlagen

ISBN 978-3-200-05198-0

Inhaltsverzeichnis

1 Vorwort

Obgleich die langjährige Unfallstatistik in Österreich keine gravierenden Vorfälle mit gefährlichen Stoffen[1] ausweist, ist die Möglichkeit derartiger Ereignisse unbestritten. Wegen des Schadenspotentials von Unfällen mit gefährlichen Stoffen ist es erforderlich, alle Maßnahmen zu deren Vermeidung und Begrenzung möglicher Folgen zu ergreifen. Die Verantwortung für die Sicherheit gefährlicher Anlagen obliegt in erster Linie den Betreibern dieser Anlagen, sodass sich der Inhalt der gegenständlichen Publikation auch primär an die Betreiber richtet.

Der Hauptzweck der vorliegenden Publikation besteht darin, einerseits einen Nachweis zu ermöglichen, dass die Arbeitnehmer in Anlagen mit hohem Gefahrenpotential als Sicherheitsfaktoren in ihrer Verantwortung für Sicherheit gefördert werden, andererseits auch Potentiale für diese Förderung zu identifizieren. Dies deshalb, da die Sicherheit einer Anlage mit gefährlichen Stoffen nicht nur von einer ausgereiften Sicherheitstechnik und durchdachten organisatorischen Vorkehrungen abhängt, sondern auch von der Kompetenz und Selbstsicherheit der Arbeitnehmer. Mit dem Begriff der „Sicherheitskultur“ wird diese Aufgabe umschrieben.

Sicherheit - speziell bei Anlagen mit hohem Gefahrenpotential - muss als Erfolg eines Gesamtsystems angesehen werden. Daraus ergibt sich die Notwendigkeit der Festlegung von Indikatoren, die diesen Erfolg dokumentieren. Hier zeigt sich der Paradigmenwechsel von der reinen Fehler- und Unfallvermeidung zur gesamthaften proaktiven Betrachtung. Unfallzahlen geben nicht ausreichend Aufschluss über den Zustand der Sicherheitskultur. Unfälle können stets erst im Nachhinein einer Ursache zugeordnet werden; bei Anlagen mit hohem Gefahrenpotential reicht überdies das Fehlen von konkreten Unfällen nicht aus, um als Nachweis für ausreichende Sicherheit zu dienen, da auch sehr unwahrscheinliche Ereignisse maßgebend sein können.

Mit der vorliegenden Publikation wird versucht, Empfehlungen für die Festlegung von aussagekräftigen Indikatoren zu geben, die einerseits ein sicheres System beschreiben, aber andererseits auch erlauben, Verbesserungen rechtzeitig in die Wege zu leiten. Die Empfehlung richtet sich an die Betreiber von Anlagen und ist nicht als behördliches Nachweisinstrument zu verstehen; für die Behörden soll durch die vorliegende Publikation hauptsächlich der gegenwärtige Informationsstand hinsichtlich des Themas der Sicherheitskultur, seiner Zielsetzung und Belegbarkeit dargestellt werden.

Die Empfehlung wurde von einer Arbeitsgruppe erstellt, die in nahezu gleicher Zusammensetzung bereits zwei Publikationen[2] zu ähnlichen Themen vorbereitet hat. In der Gruppe haben Vertreter von Firmen, die Anlagen mit hohem Gefahrenpotential besitzen, einschlägig befasste Konsulenten und Behörden zusammengearbeitet.

Die Arbeitsgruppe war von 2015 - 2017 tätig.

---

[1] Gefährliche Stoffe: Stoffe, Polymere, Verbindungen, Mischungen oder Zubereitungen, die aufgrund ihrer chemischen, physikalischen oder (öko-)toxikologischen Eigenschaften eine Gefahr darstellen. Darin eingeschlossen sind auch Stoffe, die normalerweise nicht als gefährlich gelten, unter bestimmten Umständen (z.B. Feuer, durchgehende Reaktionen) mit anderen Stoffen oder bei anderen Betriebsbedingungen (Temperatur, Druck) reagieren und dabei gefährliche Stoffe bilden können.

[2] *Layer of Protection Analyse (LOPA) zur risikobasierenden Bewertung von Szenarien - Guideline zur Anwendung für prozessbedingte Störungen bei der Sicherheitsanalyse von technischen Anlagen (2012)* und
Technische Risikoanalysen für Anlagen mit hohem Gefahrenpotenzial - Empfehlung für eine Methodenstruktur (2014), jeweils erschienen bei Edition TÜV Austria

Arbeitsgruppe PSI

Teilnehmer:

DI Dr. Martin Doktor, Leiter Competence Center Anlagensicherheit, TÜV Austria
DI Hans-Jürgen Essl, Process Safety, Borealis Agrolinz Melamin, Linz
DI Dr. Friedrich Fröschl, Process Safety, VTU Engineering GmbH
DI Dr. Marian Goriup, Process Safety, Borealis Polyolefine GmbH, Schwechat
DI (FH) Helmut Lengerer, Head Technical Safety, Sandoz GmbH
DI Alfred Moser, Planung-Technik und Umwelt, Magistrat Linz
DI Erhard Peitbuchner, Process Safety, VTU Engineering GmbH
Ing. Georg Sagerer, Process Safety, Lenzing AG
DI Dr. Dieter Schiefer, Seveso-Beauftragter, Amt der OÖ Landesregierung
DI Ernst Simon, Abteilung 15, Stmk. Landesregierung
DI Dr. Michael Struckl, Leiter der Abt. Gewerbetechnik, BMWFW
DI Dr. Ulrike Weingerl, Process Safety, OMV AG
DI Helmut Weißböck, Process Safety, Lenzing AG
DI (FH) Rupert Wieser, Technical Safety, Sandoz GmbH

2 Einleitung

2.1 Sicherheitsmanagement und Sicherheitskultur

Der Begriff „Management“ geht auf das lateinische „Manus“ (Hand) zurück, aus dem das italienische „maneggiare“ entstand, das so viel wie „handhaben“ bedeutet und aus diesem wiederum das englische „manage“ mit den Bedeutungen „verwalten, führen, schaffen, handhaben, bewältigen“ usw. Der Begriff „Management“ erlangte durch das Buch „The Managerial Revolution“, 1941 von James Burnham geschrieben, weitreichende Bekanntheit.

Es existieren verschiedenste Deutungen und Überlegungen zum Inhalt des Begriffs „Management“; eine Beschreibung lautet wie folgt:

„Management ist durch das Vorhandensein von drei Elementen gekennzeichnet, nämlich

- *Gestaltung*
- *Lenkung und*
- *Entwicklung“* (Dyllich, Probst & Ulrich, 1982, S. 114)

Aufbauend auf dem Managementbegriff entstand der Begriff des „Managementsystems“. Darunter kann die Gesamtheit aller (real existierenden) organisatorischen Maßnahmen verstanden werden, die geeignet sind, die Erreichung festgelegter Unternehmensziele sicherzustellen; dies können aufbauorganisatorische Maßnahmen (Hierarchie, Verantwortung, Zuständigkeit) als auch ablauforganisatorische Maßnahmen (Berichtswesen, Informationswege, Entscheidungswege, Arbeitsverfahren) sein.

Sicherheit in Industriebetrieben mit hohem Gefährdungspotential ist vor allem auch eine Managementaufgabe. Der Rahmen staatlicher Normen allein reicht nicht aus, sämtliche Einflussfaktoren und Gefahrenquellen ausreichend zu berücksichtigen. Deshalb müssen innerhalb der Strukturen staatlicher Anforderungen zusätzliche Systeme geschaffen werden, die diese Anforderungen umsetzen, interpretieren und ergänzen. Dies geschieht auf Grund einer Reihe von Impulsen oder Überlegungen:

- Wahrnehmung der ethischen Unternehmensverantwortung,
- Vermeidung materiellen Schadens, auch durch die öffentliche Meinung,
- Vermeidung staatlicher Eingriffe,
- Wahrnehmung des Freiraums staatlicher Anforderungen und
- Positives Unternehmensimage.

Um die Managementaufgabe der Gewährleistung von Sicherheit umsetzen zu können, bedarf es der Einbettung diesbezüglicher Systeme in eine adäquate Sicherheitskultur.

Der Ursprung dieses Begriffes wird meist im Untersuchungsbericht der IAEA[3] im Jahr 1992 über den Tschernobyl-Unfall gesehen; die diesbezügliche Anmerkung lautet (IAEA, 1992, S.23f):

„The accident can be said to have flowed from deficient safety culture, not only at the Chernobyl plant but throughout the Soviet design, operating and regulatory organizations for nuclear power that existed at the time“.

Aus dieser Erwähnung entstand 1993 die am häufigsten verwendete Definition von Sicherheitskultur in einem Dokument des Advisory Committee on Safety of Nuclear Installations (ACSNI, 1993):

„The product of individual and group values, attitudes , perceptions, competencies and patterns of behaviour that determine the commitment to and the style and proficiency of an organization's health and safety management.“

[3] International Atomic Energy Agency

Wichtig ist ferner, dass die Sicherheitskultur zwei Wesensmerkmale besitzt:

1) Einerseits die Rahmenbedingung innerhalb des Unternehmens und die Verantwortlichkeit innerhalb der Managementstruktur und
2) andererseits die Haltung des Personals auf allen Ebenen, mit der auf diese Rahmenbedingungen reagiert und von diesen profitiert wird.

Sicherheitskultur und Sicherheitsmanagementsystem sind also in vielfältiger Weise miteinander verwoben. Der grundlegende Unterschied zwischen einem dokumentierbaren (Sicherheits-) Managementsystem und der übergeordneten Sicherheitskultur liegt in der Rolle der schwer zugänglichen Einflussfaktoren der Sicherheitskultur. Im Sicherheitsmanagementsystem können reale physische Details (z.B. die technische Ausrüstung), Verhaltensweisen, Ziele und Bewertungsmaßstäbe beschrieben und beurteilt werden. Wie allerdings das Thema „Sicherheit“ gelebt wird, ist auch von unbewussten Zielen und Wertmaßstäben abhängig, die weder leicht erfasst noch eindeutig beurteilt werden können.

Es liegt an der Unternehmensführung, für die Rahmenbedingungen zu sorgen, wobei es sich um Faktoren handelt, die jedenfalls nicht dem Bereich staatlicher Vorschriften zuzuordnen sind. Die Sicherheitskultur kann als zentraler Wert bzw. zentrales Element der betrieblichen Organisation verstanden werden, Sicherheitskultur kann dabei auch als notwendige Ergänzung des Managementsystems verstanden werden, um dessen Elemente zu einem „wohlgeformten Ganzen“ zu verbinden (s. Künzler, 2002, S.86).

Abbildung 1:Anforderungen an die Unternehmensführung (s. Daniel, 2008, S.3)

2.2 Unfallursachen

Der Einfluss menschlicher Faktoren auf sicherheitskritische Vorfälle ist nicht generell eindeutig darstellbar. Schätzungen besagen, dass bei 80 % der untersuchten Vorfälle menschliche Faktoren eine kausale oder beitragende Rolle spielen können (UBA, 2008, S.9). Dabei handelt es sich nicht nur um eindeutige Fehlerursachen wie Fehlbedienung oder Fehlverhalten, sondern auch um Ursachen in Zusammenhang mit Managemententscheidungen oder dergleichen.

Eine Beschreibung der Thematik stammt von James Reason[4] (Reason, 1993, S.8): *„The major residual safety problems do not belong exclusively to either the technical or the human domain; rather they emerge from as yet little understood interactions between technical and social aspects of systems.“* Von Reason stammt auch die Aussage, dass menschliches oder technisches Versagen oft nur das letzte Glied einer Kette von Fehlentscheidungen oder riskanten Systembedingungen ist.

[4] Begründer des „Schweizer Käse - Modells“; siehe auch Kapitel 4.3

Die vorherrschende Betrachtungsweise, wonach sicherheitsrelevante Erkenntnisse durch Unfallanalysen und Rekonstruktion der Ursachen gewonnen werden, ist zwangsläufig generalisierend und lässt Begleitfaktoren, die dem Bereich der Sicherheitskultur zuzurechnen sind, außer Acht.

Das Konzept der Sicherheitskultur geht dagegen davon aus, dass sich potentielle Unfallursachen durch Merkmale manifestieren, welche Trends und Begleitumstände erkennen lassen und solcherart eine Vermeidung der Unfallursachen ermöglichen. Die Problematik liegt dabei in der objektiven Bewertung der Einflussgröße „Mensch“ (Zuverlässigkeit, psychologische Randbedingungen, Klassifikation von Verhalten, Beurteilung von Entscheidungsabläufen usw.) für die Unfallvermeidung.

Die Schätzungen über den Anteil von menschlichen Fehlern als Unfallursache variieren sehr, reichen aber bis zu 80% (siehe oben). Menschliche Einflussgrößen können bei

- Entwurf und Bau einer Anlage,
- beim Betrieb und
- bei der Instandhaltung

relevant sein. Dabei sind auftretende Fehler entweder von der Leistungsfähigkeit und Zuverlässigkeit des Individuums oder vom Umfeld abhängig; Letzteres ist das Resultat des Managementsystems und der Sicherheitskultur. Daraus ergibt sich die Notwendigkeit einer ganzheitlichen Betrachtung.

3 Allgemeines

Sicherheitskultur, Sicherheitsmanagementsysteme und Sicherheitsindikatoren sind als Begriffe und Praktiken bei Unternehmen der Prozessindustrie gebräuchlich. Die gesetzlichen Vorgaben hierzu beschränken sich in Österreich auf die EU - Richtlinie 2012/18/EG (Seveso III) und deren nationale Umsetzung.

Nach Artikel 8 der Seveso III - Richtlinie haben die der Richtlinie unterliegenden Betriebe ein Sicherheitskonzept zu erstellen, aus dem die übergeordneten Gesamtziele und Handlungsgrundsätze in Bezug auf die Verhütung schwerer Unfälle hervorgehen. Die Umsetzung des Konzepts ist bei den so genannten Betrieben der „oberen Klasse“ (das sind jene, bei welchen die entsprechende Mengenschwelle der Spalte 3 des Anhangs der Richtlinie an gefährlichen Stoffen überschritten ist) durch ein Sicherheitsmanagementsystem (SMS) nachzuweisen.

Die inhaltlichen Vorgaben für ein SMS sind in Anhang III der Richtlinie enthalten. Diese Vorgaben sind in sieben Untergruppen aufgeteilt, nämlich

1) Organisation und Personal,
2) Ermittlung und Bewertung der Gefahren schwerer Unfälle,
3) Betriebskontrolle,
4) sichere Durchführung von Änderungen,
5) Planung für Notfälle,
6) Leistungsüberwachung und
7) Audit und Überprüfung.

Unter Leistungsüberwachung ist als Anforderung angeführt:

„Festlegung und Durchführung von Verfahren zur kontinuierlichen Beurteilung der Einhaltung der Ziele, die in dem Konzept des Betreibers und im Sicherheitsmanagement festgelegt sind, sowie von Mechanismen zur Prüfung und Einleitung von Abhilfemaßnahmen bei Nichteinhaltung. Die Verfahren umfassen das System des Betreibers für die Meldung schwerer Unfälle oder „Beinaheunfälle“, insbesondere solcher, bei denen die Schutzmaßnahmen versagt haben, sowie die entsprechenden Untersuchungen und Folgemaßnahmen auf Grundlage der gesammelten Erfahrungen. Die Verfahren könnten auch Leistungsindikatoren wie sicherheitsbezogene Leistungsindikatoren und/oder andere relevante Indikatoren beinhalten“.

Hier kommen die Begriffe „Beinaheunfall“ (Near Miss) und „sicherheitsbezogener Leistungsindikator“ vor.

In Österreich ist die Seveso III - Richtlinie durch die Gewerbeordnung[5] 1994 und die Industrieunfallverordnung[6] 2015 umgesetzt (die meisten der Betriebe, die der Seveso - Richtlinie unterliegen, sind gewerbliche Betriebsanlagen). Da die Verpflichtung in ähnlicher Weise schon nach der seit 1997 geltenden Seveso II - Richtlinie bestand, wurde von den mit der Inspektion von Seveso - Betrieben befassten Landesbehörden ein Fragebogen zur Beurteilung von SMS erstellt[7]. Als Punkt zur Erfassung der Effizienz des SMS ist dort u.a. aufgeführt: *„Sind konkrete und messbare Kriterien für die Leistungsfähigkeit des SMS festgelegt (z.B. Unfallzahlen, Anzahl meldepflichtiger Störungen)?“*.

Weitere verbindliche Vorgaben für SMS für ortsfeste Anlagen[8] und damit in Zusammenhang stehende Themenkomplexe gibt es in Österreich nicht.

[5] BGBl. I Nr. 81/2015 idF BGBl. I Nr. 155/2015

[6] BGBl. II Nr. 229/2015

[7] „Empfehlung Nr. 3 des Bundesländer-Arbeitskreises Seveso - Seveso-Inspektionskatalog für Sicherheitsmanagementsysteme“, verfügbar über http://www.umwelt.steiermark.at/cms/dokumente/10899190_28322874/9588e547/BLAK-Empfehlung%20Nr.%203%20-%20Inspektionskatalog%20SMS-Nov%202007_Stand%202011-04-20.pdf

[8] Einige Bestimmungen mit gleichartigen Begriffen sind im Eisenbahnrecht vorhanden.

Im Zusammenhang mit der Thematik von SMS sind folgende gebräuchliche Grundlagen zu nennen:

- ISO/IEC 31000:2009 Risk Management - Guidelines for principles and implementation of risk management
- ISO/IEC 31010:2009 Risk management - Risk assessment techniques
- ONR 49000:2014 ff. Risikomanagement für Organisationen und Systeme - Begriffe und Grundlagen - Umsetzung von ISO 31000 in die Praxis
- IEC Guide 73:2009 Risk Management–Vocabulary - Guidelines for use in standards

4 Theoretische Grundlagen

4.1 Der Ursprung: Das Heinrich - Konzept

Die Annahme eines Zusammenhanges zwischen bestimmten Daten, menschlichen Einflussfaktoren und dem Auftreten schwerer Unfälle wurde in neuerer Zeit erstmals durch W.H. Heinrich (1931) beschrieben. Heinrich postulierte drei Grundsätze:

- Es gibt eine Beziehung zwischen der Zahl bestimmter gleichartiger Unfallarten und dem jeweiligen Schweregrad,
- die häufigste Unfallursache ist die menschliche Fehlhandlung und
- die Verminderung von jedweden Arbeitsunfällen führt auch zu einer Verminderung der Zahl der schweren Unfälle.

Heinrich analysierte diverse Datensammlungen über aufgetretene Unfälle und zog daraus den Schluss, dass sich eine quantitative Beziehung aufstellen lässt, die als „Heinrich - Pyramide“ bekannt geworden ist.

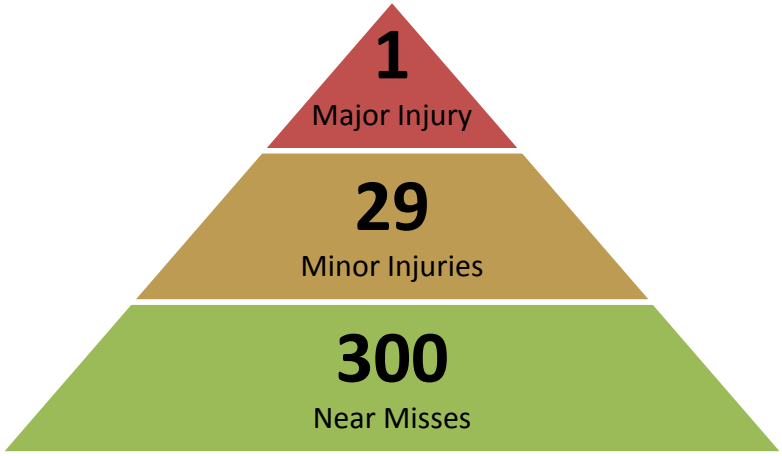

Abbildung 2: Das Heinrich Modell (Heinrich, 1931)

Die Klassifizierung in der originalen Heinrich-Pyramide unterschied sich von heutigen Modellen. Als Major Injury wird ein Unfall bezeichnet, der entweder berichtspflichtig oder „versicherungsrelevant“ ist, Minor Injury ist ein Unfall mit einer medizinischen Versorgung ohne Krankenhausaufenthalt und ein Near Miss ein Ereignis ohne Verletzung.

In seinem Buch kommt Heinrich auch zu Schlussfolgerungen, die viel später in modernen Konzepten des Sicherheitsmanagements zu finden sind. Zusammenfassend hat er bereits damals die Ansicht vertreten, dass

- 88 % aller Unfälle Bedienungsfehler oder dergleichen durch das Personal zur Ursache haben,
- 10 % auf technische Ursachen (Ausstattung, Arbeitsumgebung) zurückzuführen sind und
- 2 % der Unfälle unvermeidlich sind.

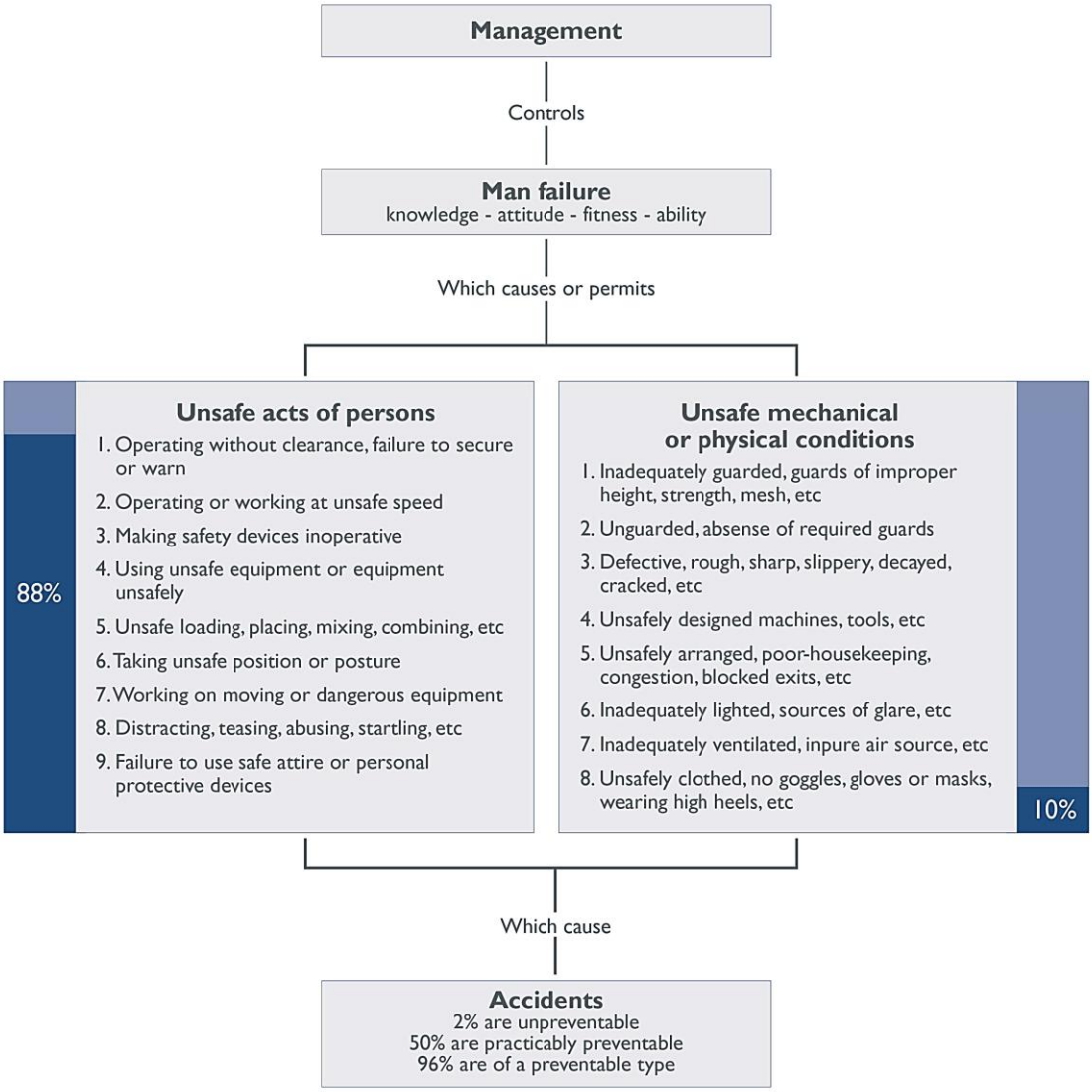

Abbildung 3: Direkte und unmittelbare Unfallursachen nach Heinrich, Bild aus (OHS, 2012, S.6)[9]

4.2 Weiterentwicklung des Heinrich - Konzepts

1969 beschäftigte sich Frank Bird (1996) mit den Grundlagen des Heinrich-Konzepts, das bis dahin eine Leitbildfunktion in der Unfallverhütung hatte. Er analysierte ca. 1,7 Millionen Vorfälle in 297 Unternehmen aus 21 Branchen und kam zum Schluss, dass sich dadurch ein Verhältnis 1:10:30:600 ergibt (Tödlicher Unfall - Schwerer Unfall - Unfall - Vorfall). Der „Vorfall“ in der „Bird - Pyramide“ wird als „Near Miss“ bezeichnet, was bis heute zu Kritik an diesem Konzept geführt hat, da die Zahl von 600 Near Miss - Ereignissen als zu hoch angesehen wird, wenn einem solchen Ereignis tatsächlich das Potential für einen schweren oder tödlichen Unfall zugerechnet wird.

[9] Das Bild enthält einen Schreibfehler, da es in der letzten Zeile 96 % an Stelle von 98 % als Summe der tatsächlich vermeidbaren Unfälle angibt.

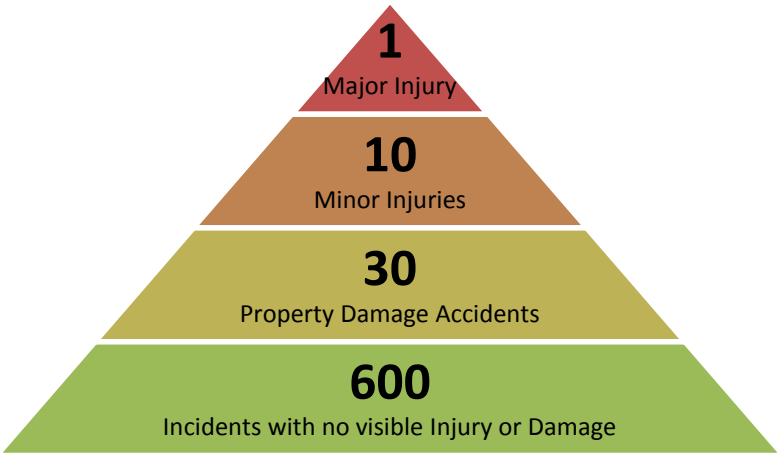

Abbildung 4: „Bird-Pyramide“ (s. Bird, 1996)

Ein weiteres, vielfach zitiertes Verhältnis stammt von DuPont (Käfer, 1999, S.17) und nennt eine Beziehung von

1	Unfall mit Todesfolge
30	Unfall mit Krankenhausaufenthalt
300	Unfall mit Versorgung im Krankenhaus ohne Aufenthalt
3.000	Unfall mit örtlicher Versorgung durch Erste Hilfe oder dergleichen
30.000	unsichere Handlungen

Es lag nahe, dass man sich sehr bald mit der untersten Ebene, der „unsicheren Handlungen“ befasste und deren Rolle untersuchte. Die Ursache hierfür war nicht zuletzt die Unschärfe der Datensammlungen im Bereich der „unsafe conditions“ oder „minor injuries“ und selbst bei üblicherweise gut dokumentierten Vorfällen mit gravierenden Folgen sind ebendiese Folgen zwar ausreichend beschrieben, oft jedoch nicht der Verlauf, der zum Unfall geführt hat.

Aus dieser Problematik entstand das Konzept einer ganzheitlichen Betrachtung und der vorausschauenden Festlegung von Randbedingungen der Unfallvermeidung.

4.3 Die Systemfehlertheorie von James Reason

Die verschiedenen Unfallpyramiden sind Modelle, die eine lineare Beziehung zwischen einer Unfallursache und dem angenommenen „unerwünschten Ereignis“ unterstellen; wie in Kapitel 4.1 auch gezeigt, wird in einzelne Ursachenkategorien unterschieden. James Reason (Reason, 1990) entwickelte diese Überlegung weiter und wies nach der Untersuchung von diversen Unfallberichten auf die notwendige Unterscheidung zwischen aktivem und latentem Versagen bzw. aktive oder latente Fehler hin.

- Aktive Fehler sind Fehlhandlungen, die direkt im Arbeits- bzw. Produktionsprozess an der Mensch-Maschine-Schnittstelle begangen werden; z.B. Versehen, Irrtümer etc. im Sinne sicherheitskritischer Verhaltensweisen.
- Latente Fehler werden hingegen zeitlich und räumlich weit entfernt von der Unfallentstehung begangen; z.B. werden Wartungs- oder Instandhaltungsprozeduren fehlerhaft ausgeführt oder bereits bei der Entwicklung des Systems haben sich Konstruktionsfehler eingeschlichen.

Nach Reason ist zudem die Unterscheidung zwischen Personen- und Systemfehlern relevant:

- Personenfehler sind direkt Personen zuordenbare Fehler, wie z.B. Unachtsamkeit, moralisch begründete Fehlhandlungen oder Vergesslichkeit.
- Systemfehler sind solche, die auf die Bedingungen einwirken, welche die Arbeitsverhältnisse bzw. die Mensch/Maschine-Schnittstellen bestimmen oder solche, die für Barrieren gegen menschliche Fehler sorgen sollen (auch für die Begrenzung der Folgen menschlicher Fehler).

Reason postuliert daher, dass es vier Ebenen[10] gibt, welche als Ursachen für latente oder aktive Personen- und Systemfehler auftreten können. Bei einer sehr ungünstigen Kombination von Ereignissen in jeder dieser Ebenen kann es zu einem Unfall kommen[11].

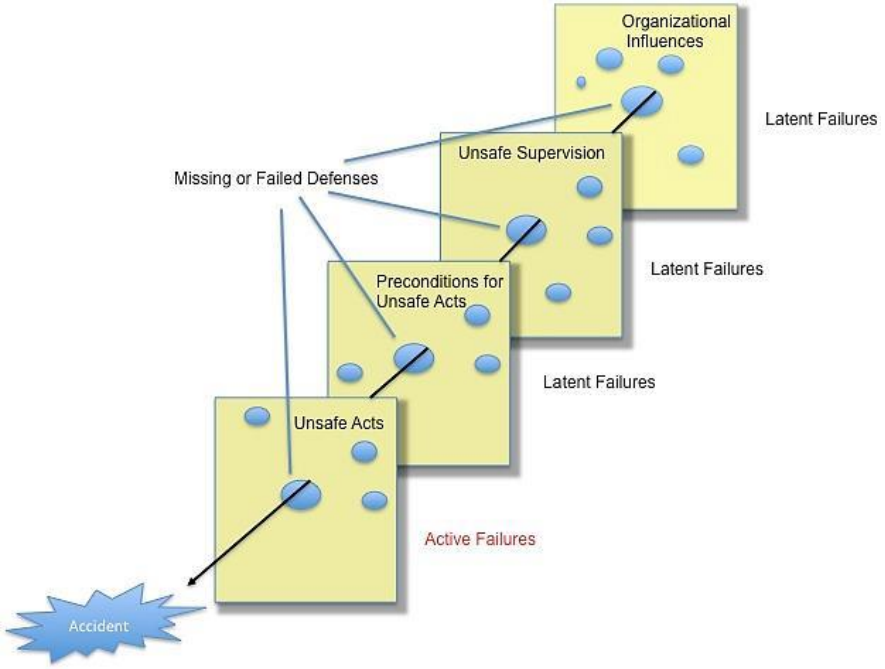

Abbildung 5: Unfallursachen nach Reason

Aufbauend auf dieses theoretische Grundgerüst nannte Reason (Reason, 1997) fünf Merkmale einer effektiven Sicherheitskultur:

- Vorhandensein eines Informationssystems, das Daten und Einzelheiten zu Vorfällen, Near Misses oder Ergebnissen proaktiver Überprüfungen sammelt, analysiert und die Erkenntnisse weiter leitet.
- Vorhandensein einer „Reportingkultur“ welche in der Lage ist, das Personal über eigene Fehler berichten zu lassen.
- Vorhandensein einer Atmosphäre des Vertrauens[12], die das Personal zu Berichten über sicherheitsrelevante Informationen ermutigt, in der aber auch die Grenze zwischen akzeptablem und unakzeptablem Verhalten klar geregelt ist.
- Vorhandensein eines flexiblen Systems, welches fähig ist, die betriebliche Organisationsstruktur einer dynamischen Umgebung anzupassen.
- Fähigkeit und Entschlossenheit, die richtigen Entscheidungen für das betriebliche Sicherheitssystem zu treffen und diese Entscheidungen umzusetzen, wenn Änderungen erforderlich sind.

[10] In früheren Publikationen fünf Ebenen.

[11] Es gibt zahlreiche ähnliche Darstellungen, welche die Schutzebenen als Abfolge technischer und organisatorischer Art enthalten und einen Unfall ebenfalls als „ungünstige Versagenskombination“ definieren

[12] Dies kann auch als „Fehlerkultur“ umschrieben werden.

4.4 Schlussfolgerungen der Arbeitsgruppe zum theoretischen Grundgerüst

Die Arbeitsgruppe setzte sich mit dem zuvor beschriebenen theoretischen Rahmen auseinander und berücksichtige dabei praktische Erfahrungen. Insgesamt kam man zu dem Schluss, dass sich damit ein grundsätzlich schlüssiges Konzept einer Sicherheitskultur entwickeln lässt, dass jedoch einige ergänzende Aussagen getroffen werden sollten; diese sind für die weiteren Ausführungen in der gegenständlichen Empfehlung von Relevanz:

- Eine Unterscheidung nach Fehlerkategorien ist jedenfalls sinnvoll.
- Die Annahme einer pyramidenförmigen Beziehung zwischen den verschiedenen Kategorien von Vorfällen und Unfällen ist grundsätzlich gerechtfertigt. Allerdings wäre es nicht korrekt, zwingend eine zahlenmäßige Proportionalität in Form tatsächlich eintretender Ereignisse zwischen den Pyramidenebenen anzunehmen. Es ist davon auszugehen, dass eine Verringerung von als negativ bewerteten Ereignissen an der Pyramidenbasis auch eine Reduzierung von schweren Unfällen an der Pyramidenspitze bewirken kann, allerdings nur ausgedrückt als Ereigniswahrscheinlichkeit.
- Absolute Zahlen haben bei der Pyramidendarstellung keinen „Alleinstellungswert“, da zu viele Unsicherheiten vorhanden sind (z.B. Zuordnung zu bestimmten potentiellen Schweregraden). Offensichtliche Fakten bzw. Ereignisse mit einfacher Zuordnung reichen für eine umfassende Darstellung nicht aus, da weniger sichtbare oder feststellbare Ereignisse mit hohem Gefahrenpotential vielfach wichtiger wären.
- Es ist zu beachten, dass schon bei der Datensammlung und -darstellung auf eine Unterscheidung geachtet wird: Ereignisse und Fakten, die auf verhaltensbasierte Fehler schließen lassen, sind für die Frage der Sicherheitskultur wichtiger als rein technische Fehler.
- Die Konzeption einer Sicherheitskultur muss jedenfalls darauf abstellen, dass nicht ein zahlenmäßiges Ergebnis als alleiniger Erfolg bewertet wird, sondern die konkreten Schlussfolgerungen (Plan-Do-Check-Act).
- Die Schaffung einer Fehlerkultur bzw. einer Atmosphäre des Vertrauens ist überwiegend von den jeweiligen betrieblichen Verhältnissen abhängig und wird maßgeblich von den Führungskräften geprägt und kultiviert. Die Entwicklung einer Reportingkultur ist ein langwieriger Prozess, für den die Auswahl der erwünschten Indikatoren entscheidend ist. Unter Umständen wird die Reportingkultur ein evolutionärer Prozess sein, der am Beginn zu viele Daten liefert. Dabei soll jedoch jedenfalls darauf geachtet werden, dass der Begriff „Fehler“ nicht negativ besetzt ist, um zu einem „Lessons Learned“-Ergebnis zu kommen.

5 Sicherheitsindikatoren Allgemeines

5.1 Allgemeines

Ein Indikator (lateinisch „indicare“, also „anzeigen“) bezeichnet allgemein umgangssprachlich einen Hinweis auf einen bestimmten Sachverhalt oder für ein Ereignis[13]. Idealerweise ist ein Indikator als Kennzahl gestaltet; eine Kennzahl ist eine Maßzahl, die zur Quantifizierung dient und der eine Vorschrift zur quantitativen reproduzierbaren Messung einer Größe oder eines Zustandes oder Vorgangs zugrunde liegt.

Sicherheitsindikatoren sind direkt beobachtbare oder aus Beobachtungen indirekt ableitbare Parameter, die es erlauben, Rückschlüsse zu ziehen, inwieweit ein System sicherheitsgerichtet ist oder sein wird (s. Herczeg, 2014, S.263).

Leading indicators

sind Indikatoren, die die Wahrscheinlichkeit bzw. das Risiko zukünftiger (unerwünschter) Ereignisse anzeigen und es ermöglichen einzugreifen, ehe das (unerwünschte) Ereignis eintritt (vorausschauend)[14].

Lagging indicators

sind Indikatoren, die nach einem (unerwünschten) Ereignis feststellbar sind und das Ereignis dokumentieren (rückblickend).

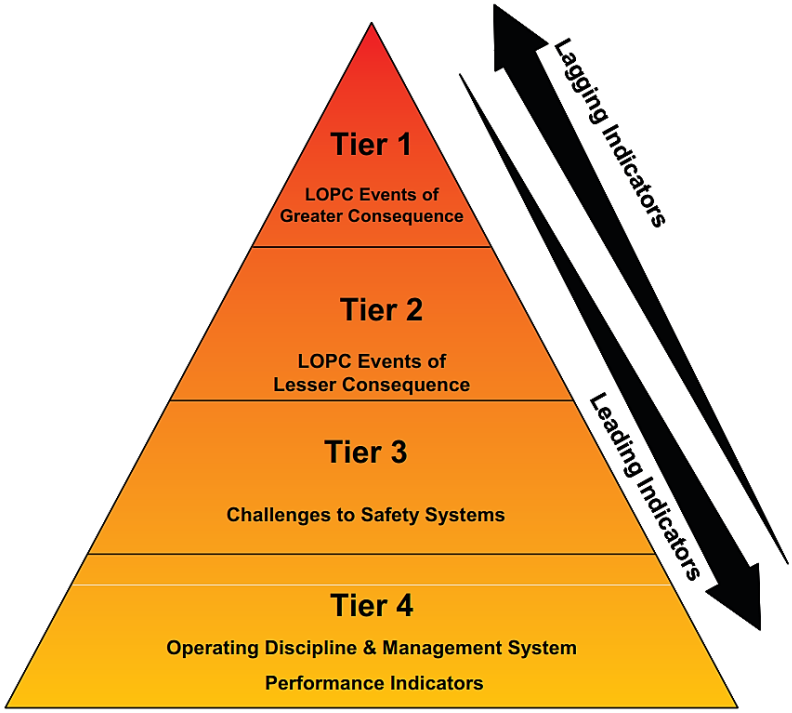

Abbildung 6: Prozesssicherheitsindikatoren Pyramide nach API RP 754[15] (API, 2010, S.8)

Die Arbeitsgruppe kam - als Grundlage für die weiteren Ausführungen - zu folgenden Bemerkungen bzw. Schlussfolgerungen:

- In Zusammenhang mit der gegenständlichen Empfehlung ist festzuhalten, dass eine exakte Trennung zwischen den beiden Kategorien „lagging“ und „leading“ nicht möglich ist; je nach Schutzziel und Verwendungszweck wird jedoch ein Merkmal mehr hervortreten.
- Es ist möglich, dass der gleiche Indikator für mehrere Bereiche verwendet werden kann.

[13] Begriffsdefinition Wikipedia

[14] Als einzelner Wert oder als Trend

[15] LOPC = Loss of Primary Containment (Stofffreisetzung)

- Nach Möglichkeit sind Indikatoren quantitativ zu bestimmen, qualitative Indikatoren können jedoch zum Verständnis eines Problems oder zur Bewertung einer Sachfrage beitragen.
- Grundlegende Auswahlkriterien für Indikatoren sind:
    - Aktualität
    - Aussagekraft
    - Verhältnis Zeitaufwand/Anzahl erhältlicher Indikatoren
    - Relevanz für einen konkreten Prozess
    - Überleitung von Trends, d.h. noch nicht exakt quantitativ ausgewertete Informationen, zu definierten Indikatoren
    - Messbarkeit
    - Belastbare/verifizierbare Daten (möglichst nicht manipulierbar)
- Für die vorliegende Empfehlung (und die Auswahl der Indikatoren) ist die Unterscheidung zwischen Arbeitssicherheit und Anlagensicherheit wesentlich. Es kann als gesicherte Erkenntnis gelten[16], dass niedrige Unfallzahlen bei der Arbeitssicherheit nicht automatisch das Vorhandensein einer „sicheren Anlage“ bedeuten.
- *„If you can't measure it you can't improve it“* (Peter Drucker)
- *„Measure what you value and do not value what you measure“* (Andy Hargreaves)

5.2 Sicherheitsindikatoren und Berichtswesen

Zwischen Sicherheitsindikatoren und dem Berichtswesen über Vorfälle besteht ein Zusammenhang. Es ist allerdings sehr von den spezifischen Rahmenbedingungen abhängig, in welcher Form das Berichtswesen in die Gestaltung der betrieblich gewählten Sicherheitsindikatoren einfließt. Typischerweise tauchen die Begriffe „Near Miss“ und „Process Safety Incident“ im gegebenen Zusammenhang auf.

Für die folgenden Empfehlungen ist die Unterscheidung der folgenden Begriffe relevant:

Vorfall (Incident)[17,18]:

Ein ungeplantes, unerwünschtes (identifizierbares) Ereignis, welches eine Gesundheitsgefährdung oder einen Umweltschaden auslösen könnte, mit Abstufung von vernachlässigbar bis katastrophal; unten auch mit „sonstiger Vorfall mit Gefahrenpotential“ bezeichnet.

Beinaheunfälle (Near Miss)[19]:

Vorfälle, bei denen es zu keiner Schädigung bzw. Gesundheitsgefährdung kam, dies hätte jedoch bei einer geringfügig geänderten Abfolge der Ereignisse oder des zeitlichen Ablaufes eintreten können.

Eine andere Definition lautet: „Near Miss“ sind unsichere Zustände, unsichere Handlungen, versteckte Gefahren, Risikopotenziale, Schwachstellen, sicherheits-widriges Verhalten, die rechtzeitig erkannt wurden und ohne größere Folgen blieben. Die Auslegung, welche Vorfälle oder Ereignisse als „Near Miss“ einzustufen sind, ist vielfach schwierig und erfordert immer eine genauere Analyse (siehe auch nachstehendes Kapitel).

Process Safety Incident (PSI)[20, 21]:

Dabei handelt es sich um Vorfälle, die ausschließlich bei einem verfahrenstechnischen Prozess auftreten und die einen definierten Schweregrad überschreiten (CCPS-Tabelle). Nach der definierten Abstufung sind

[16] http://www.en-s.de/systematik%20der%20anlagensicherheit.html

[17] http://safety.blr.com/workplace-safety-news/safety-administration/workplace-accidents/11zll01-Incident-vs.-Accident-Whats-the-Difference/

[18] Manche Quellen ergänzen den Begriff mit der Beschreibung „dangerous occurence“

[19] „Near misses describe incidents where no property was damaged and no personal injury sustained, but where, given a slight shift in time or position, damage and/or injury easily could have occurred” (U.S. OSHA definition).

[20] Die Abkürzung „PSI“ wird entweder für „Process Safety Indicator“ oder für „Process Safety Incident“ verwendet

[21] „Reportable PSI“ entstammen dem CEFIC Guidance Document und sind von den Mitgliedsunternehmen als solche zu behandeln

Process Safety Incidents gravierender als „Near Misses“ (mit oder ohne tatsächliche Schäden); siehe nachstehende Abbildung 7.

Unfall (Accident)[22]:

Plötzliches, zeitlich und örtlich bestimmbares und von außen einwirkendes Ereignis, bei dem eine natürliche Person unfreiwillig einen Körperschaden erleidet oder ein erheblicher Umweltschaden auftritt[23].

Schwerer Unfall (Major Accident):

Ein Begriff aus der Seveso III – Richtlinie; ein schwerer Unfall ist ein Ereignis - z.B. eine Emission, einen Brand oder eine Explosion größeren Ausmaßes -, das sich aus unkontrollierten Vorgängen in einem unter diese Richtlinie fallenden Betrieb ergibt, das unmittelbar oder später innerhalb oder außerhalb des Betriebs zu einer ernsten Gefahr für die menschliche Gesundheit oder die Umwelt führt und bei dem ein oder mehrere gefährliche Stoffe beteiligt sind (Artikel 3 Z 13).

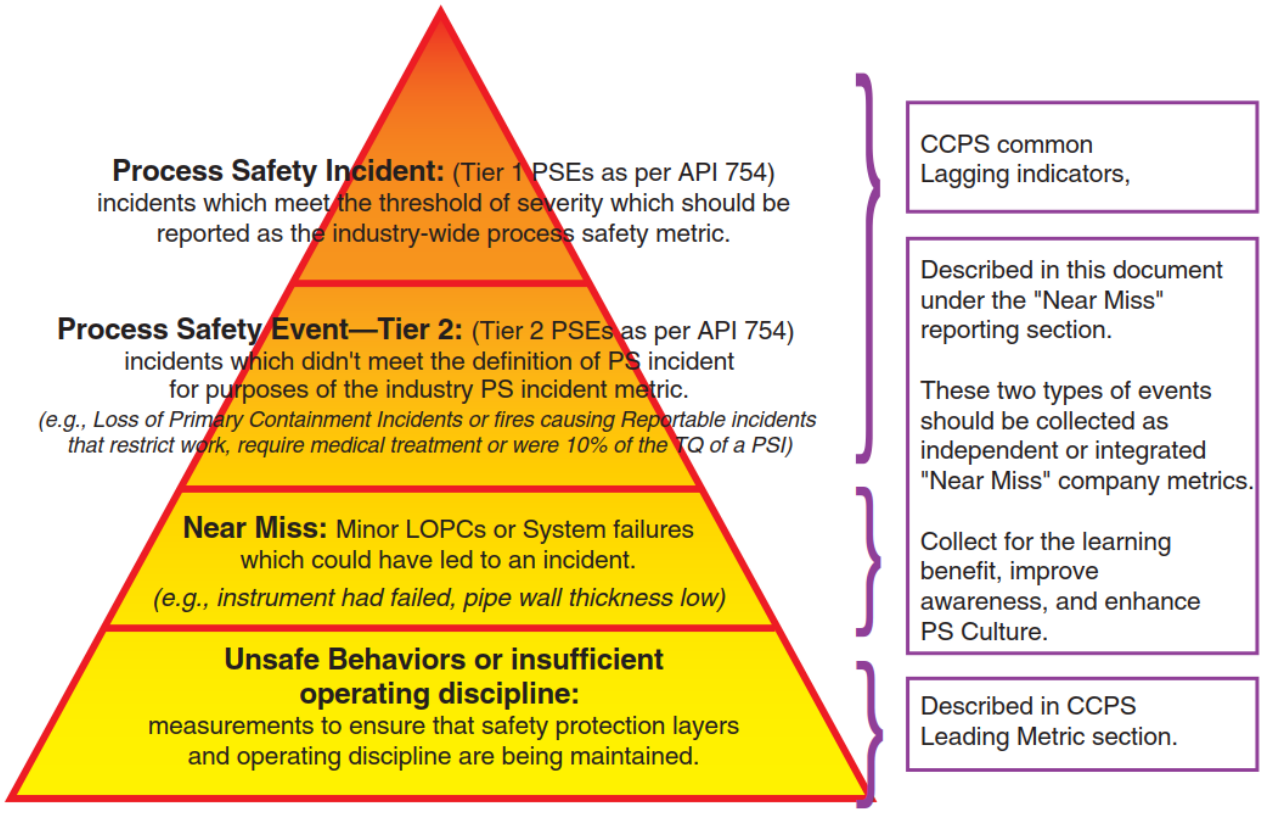

Abbildung 7: Pyramide der Prozesssicherheits-Messgrößen (CCPS, 2011, S.4)

Wie aus dem vorherigen Kapitel ersichtlich, enthält die einschlägige Literatur Unterscheidungen hinsichtlich der Schwere eines berichteten Vorfalls. Grundsätzlich kann (absteigend nach Schweregrad) zwischen

- Process Safety Incidents,
- Near Misses und
- sonstigen Vorfällen mit Gefahrenpotential

unterschieden werden.

[22] In manchen Quellen existiert auch der Begriff „Adverse Event“

[23] Definition Wikipedia

Die Arbeitsgruppe hat basierend auf einem Entscheidungsbaum der Cefic (Cefic, 2011, S.3) versucht klar Abzugrenzen was als Process Safety Incident gilt (siehe Abbildung 8).

Es ist jedoch nicht eindeutig geregelt, was als Beinaheunfall (Near Miss) einzustufen ist. Eine Abgrenzung zum „sonstigen" Vorfall mit Gefahrenpotential ist vage, da die Begriffsbestimmung nur allgemein gehalten ist. Beispielhaft lässt sich dazu ausführen, dass folgende Ereignisse typische Beinaheunfälle/Near Misses sind:

- Verlassen des sicheren Betriebsfensters
- Ansprechen von EMSR Abschaltungen
- Ansprechen von Sicherheitsventilen
- LOPCs die unter den CEFIC Mengenschwellen sind.

Störungen[24], bei welchen eine dafür vorgesehene präventive Sicherheitseinrichtung anspricht, gelten nicht als Beinaheunfälle (z.B. Ansprechen von Temperatur-Hoch-Abschaltung), solche Vorfälle können aber als Hinweis auf ein Fehlverhalten des Prozesses dienen und sind als Leading Indicator gut geeignet.

Process Safety Incidents sind konkret bestimmbar und daher ist ihre Anzahl als (Lagging) Indikator geeignet. Ziel wäre demnach, diese Anzahl zu reduzieren („Zero Repeat") oder die Auswirkungen einzuschränken; für jeden gemeldeten Process Safety Incident werden die Ursachen ermittelt und Gegenmaßnahmen getroffen.

Hinsichtlich der Beinaheunfälle ist dies nicht in dieser Deutlichkeit möglich. Die Anzahl an gemeldeten Beinaheunfällen ist nicht vorrangig als Indikator zu sehen, da diese stark von der Meldekultur abhängen. Zwar sollte zuerst auch Beachtung auf die Quantität von gemeldeten Beinaheunfällen gelegt werden, aber erst wenn eine Meldekultur etabliert ist die Qualität der gemeldeten Vorfälle gesteigert werden; danach kann über eine Verwertbarkeit der gemeldeten Anzahl als Indikator entschieden werden. Um dies bestmöglich vorzunehmen, erfolgt bei Near Misses eine risikobasierende Priorisierung (potentielle Schwere bzw. Häufung von gleichartigen Vorfällen) bevor die Ursachen ermittelt und Gegenmaßnahmen getroffen werden. Für diese risikobasierende Priorisierung ist es hilfreich, dies z.B. mittels Bow-Tie oder Ereignisbaum zu betrachten und Schwere und Eintrittswahrscheinlichkeit zu bewerten. Relevant sind jene Near Misses welche das „Potential" zu einer schwerwiegenderen Konsequenz gehabt hätten. Ohne Priorisierung können gemeldete Beinaheunfälle lediglich für generelle Trendaussagen herangezogen werden (Hinze, 2013,S.27).

Ein Indikator „Near Miss" kann folgende Zielsetzungen erfüllen:

- Betrieb gegenüber Anlagensicherheit sensibilisieren
- Anhäufungen zu erkennen und Gegenmaßnahmen einleiten
- Ermöglicht Priorisierung von zukünftigen Schwerpunkten
- Lernen aus Ereignissen

5.3 Literaturempfehlungen

- EPSC - Process Safety Performance Indicators
- CEFIC „Guidance on Process Safety Performance Indicators"
- UK HSE „Developing process safety indicators"
- API RP 754 „Process Safety Performance Indicators for the Refining and Petrochemical Industries"
- OECD Guidance on Safety Performance Indicators

[24] Eine Störung im Sinne einer „Betriebsstörung" ist ein Ereignis, das unerwartet eintritt und eine Unterbrechung oder zumindest eine Verzögerung der Aufgabendurchführung zur Folge hat (Definition Wikipedia)

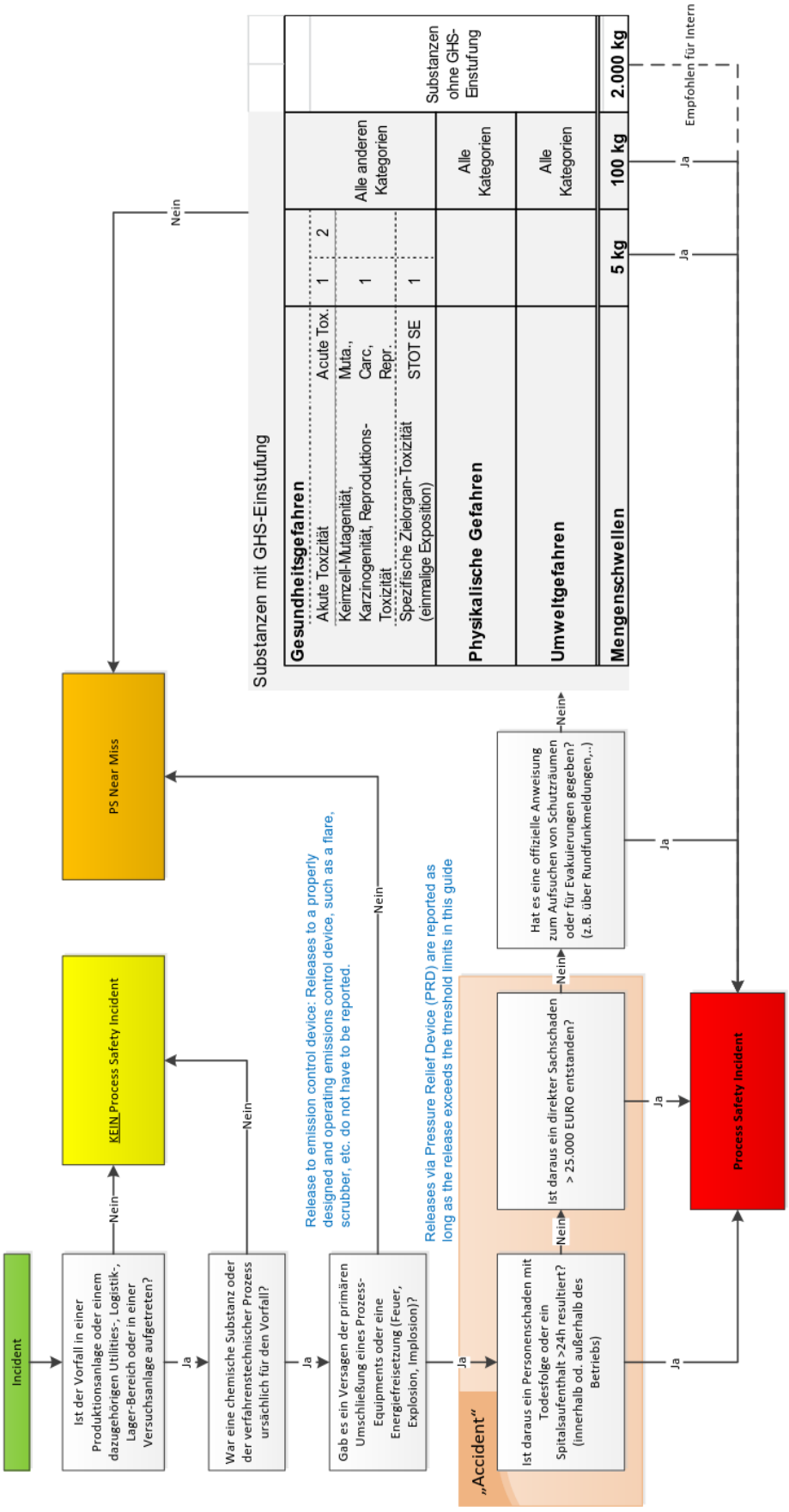

Abbildung 8: Entscheidungsbaum für Process Safety Incident

6 Empfehlungen und praktische Überlegungen für Sicherheitsindikatoren

Primäres Ziel der vorliegenden Empfehlung ist eine Strategie zur Entwicklung bzw. Verbesserung der betrieblichen Sicherheitskultur. Dafür sind in erster Linie Indikatoren dienlich, die als „leading" einzustufen sind, also eine Entwicklung oder einen Status im Betrieb erkennen lassen, der am Anfang einer möglichen Gefahrensituation steht oder demonstriert, dass derartige Situationen effektiv vermieden werden. Wie aus Kapitel 2.1 zu entnehmen ist, sind die Sicherheitskultur und das Sicherheitsmanagementsystem miteinander verwoben. Die Arbeitsgruppe postulierte für die Definition von Indikatoren, die primär verhaltensbasierte Trends anzeigen, dass diese mit einem umrissenen sicherheitstechnisch relevanten Bereich verknüpft sein sollten. In den „Process Safety Guidelines" des Centre for Chemical Process Safety (CCPS, 2007) des „American Institute of Chemical Engineers (AIChE)" sind 20 Elemente genannt, die für ein effektives Process Safety Management relevant sind. Diese 20 Elemente gruppieren sich in vier Themenblöcke, nämlich

- Bekenntnis zur Prozesssicherheit (Commit to Process Safety),
- Kenntnis der Gefahren und Risiken (Understand Hazards and Risks),
- Beherrschen der Risiken (Manage Risk) und
- aus Erfahrung lernen (Learn from Experience).

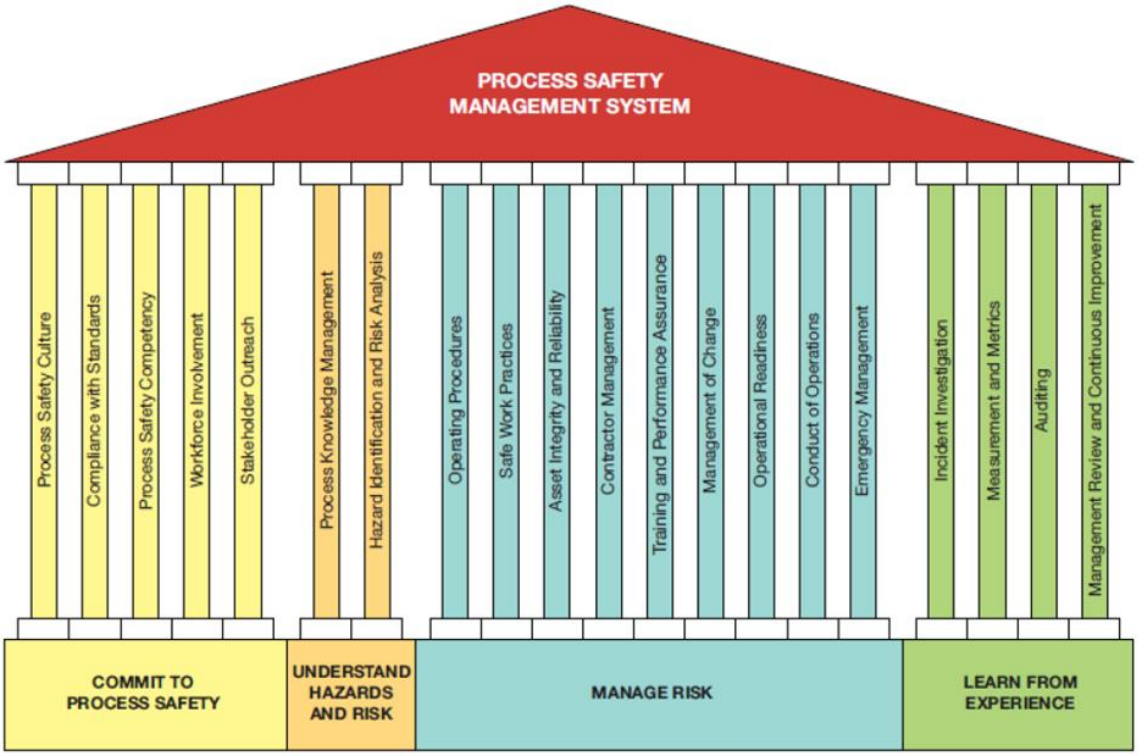

Abbildung 9: Die 20 Säulen der Prozesssicherheit (CCPS, 2007)

Diese 20 Elemente aus den vier obigen Themenblöcken repräsentieren jene Bereiche, die eine Gesamtaussage zur Anlagensicherheit erlauben und jeweils einen dafür relevanten Teilbereich darstellen.

Im Einzelnen sind die 20 Elemente folgende:

1) Sicherheitskultur (Process Safety Culture)
2) Einhaltung von Standards (Compliance with Standards)
3) Fachkompetenz für Sicherheit (Process Safety Competency)
4) Einbeziehung der Mitarbeiter (Workforce Involvement)
5) Einbindung sämtlicher Interessenten (Stakeholder Outreach)

6) Wissensmanagement (Process Knowledge Management)
7) Gefahrenermittlung und Risikoanalyse (Hazard Identification and Risk Analysis)
8) Betriebsabläufe (Operating Procedures)
9) Sichere Arbeitsverfahren (Safe Work Practices)
10) Anlagenintegrität und -zuverlässigkeit (Asset Integrity and Reliability)
11) Fremdfirmenmanagement (Contractor Management)
12) Schulungs- und Leistungssicherung (Training and Performance Assurance)
13) Änderungsmanagement (Management of Change)
14) Betriebsbereitschaft (Operational Readiness)
15) Betriebsablaufdisziplin (Conduct of Operations)
16) Notfallmanagement (Emergency Management)
17) Untersuchung von Vorfällen (Incident Investigation)
18) Indikatoren (Measurement and Metrics)
19) Prüfung und Kontrolle (Auditing)
20) Managementbewertung und laufende Verbesserung (Management Review and Continuous Improvement)

Die Arbeitsgruppe stufte die Elemente 3, 6, 7, 9, 10, 11, 13, 14, 17 und 19 als relevant und geeignet für die Bestimmung eines Indikators ein, der auf einen Rückschluss auf die bestehende Sicherheitskultur erlaubt. Zusätzlich wurde ein Element „sicherer Betriebsbereich“ als notwendig für eine Aussage angesehen. Die jeweiligen Inhalte des CCPS-Guides waren jedoch nur allgemeine Anleitung für die Beschreibung der Indikatoren, eine komplette Orientierung ist nicht erfolgt.

Bei den nachstehenden Empfehlungen handelt es sich um Vorschläge, die erforderlichenfalls an die Umstände des Einzelfalles angepasst werden müssen.

Im Folgenden werden diese Themen näher erläutert.

6.1 Fachkompetenz für Prozesssicherheit (Process Safety Competency)

Ziel:

Die Definition und das Herstellen der notwendigen Kompetenzen in Bezug auf Sicherheit. In der Psychologie wird Kompetenz häufig definiert als *„die bei Individuen verfügbaren oder durch sie erlernbaren kognitiven Fähigkeiten und Fertigkeiten, um bestimmte Probleme zu lösen, sowie die damit verbundenen motivationalen, volitionalen (durch den Willen bestimmt; Anm.) und sozialen Bereitschaften und Fähigkeiten, um die Problemlösungen in variablen Situationen erfolgreich und verantwortungsvoll nutzen können“* (Weinert, 2001, S.27f, zit. Nach Wikipedia). Als Resultat der Kompetenzherstellung bzw. -förderung soll sich ein Verständnis für sicherheitsrelevantes Verhalten ergeben, wodurch die Wahrscheinlichkeit gesteigert wird, dass Mitarbeiter in abnormalen Situationen die richtigen Maßnahmen ergreifen. Konkret betrifft dies u.a. Beherrschung der Kerntätigkeiten des Arbeitsplatzes, Wissen über die Gefahren der Tätigkeiten und der Schutzeinrichtungen, Verständnis für den Prozess, Beherrschen der sicherheitsrelevanten Prozeduren (z.B. Schichtübergabe, Betriebsanweisungen - insbesondere Sicherheitsschaltungen, Arbeitsfreigabe), Maßnahmen bei Stör- und Notfällen oder Regelungen über die „Kompetenzhierarchie“ (Zuständigkeit für Problemlösungen).

Kriterien:

- Stellen-/Tätigkeits-/Funktionsbeschreibung
- Beschreibung von Kernkompetenzen
- Kompetenzmanagement
- Nachweis von Kompetenzen
- Vorhandensein spezifischer Schulungen und Trainings

Mögliche Indikatoren:

- Prozentsatz der Arbeitsplätze mit gültiger bzw. vorhandener Funktionsbeschreibung

- Prozentsatz der Arbeitsplätze mit konkreten Kompetenzanforderungen
- Erfüllungsgrad der Schulungs- und / oder Trainingspläne
- Periodische Überprüfung der Kompetenzen
- Verhältnis Schulungen Prozesssicherheit/Arbeitssicherheit

6.2 Wissensmanagement zur Prozesssicherheit (Process Knowledge Management)

Ziel:

Die Erstellung und Verfügbarkeit von technischer Dokumenten der Anlage d.h. als Dokumentation der Anlage und Engineering - Basis für die Anlagenplanung (Rohrklassen, Berechnungscodes, Rezepturen, Prozessbeschreibung, Massenbilanzen, Wärmetönungen; Safe Operating Envelope – Betriebsfenster für alle betrieblich relevanten Parameter wie z.B. Druck, Temperatur, Zusammensetzung, Phasentrennung, Nebenprodukte, ….). Weitere Bestandteile: Berechnungen, Rohrleitungs- und Instrumentierungspläne, Verriegelungsmatrix, Engineering Basis und Standards, Revisionszyklen von technischen Dokumenten. Die Dokumente sollen möglichst kurzfristig (elektronisch) verfügbar sein und den aktuellen Anlagenzustand wiedergeben.

Kriterien:

- Vollständigkeit der Unterlagen
- Aktueller Zustand (as built)
- tatsächlich nachgewiesene Verwendung der Dokumente
- Festlegung der Verantwortlichkeit der Aktualisierung
- Festlegung, welche Dokumente für wen relevant sind

Indikatoren:

- Nachgewiesene Überprüfung der Anlagendokumentation auf Grund der Aktionspunkte in einer Prozessgefahrenanalyse mit nachfolgender Aktualisierung der Unterlagen (Anzahl)
- Verhältnis zwischen fehlender Dokumentation bzw. Spezifikation von Equipment und Apparaten bei Wiederbestellung zur Gesamtanzahl Equipment / Apparatebestellungen
- Anzahl fehlerhafter Spezifikationen die auf Grund von Lieferantenrückmeldungen geändert werden müssen; z.B.: veraltete Normen, Korrektur der Materialwahl, entspricht nicht dem Stand der Technik… .
- Vollständigkeit der Zuordnung von personellen Zuständigkeiten für Dokumente

6.3 Gefahrenermittlung und Risikoanalyse (Hazard Identification and Risk Analysis)

Ziel:

Gefahrenquellen vollständig ermitteln, verstehen, die Risiken bewerten um mit angemessenen Maßnahmen entsprechend abzusichern. Im Detail soll dies folgende Bestandteile umfassen:

- Richtlinien und Vorgaben für die Planung und die Durchführung von Studien
- Dokumentation, dass die relevanten Risiken erkannt und verstanden wurden
- Festlegung von Kriterien für das zulässige/tolerierbare Risikoausmaß
- Bestimmung möglicher Risikokontrollmaßnahmen, technischer Lösungen und damit verbundener Aktivitäten
- Bestimmung und Nachweis des verbleibenden Restrisikos
- Vollständige, berichtsfähige Risikoanalyse.

Kriterien:

- Konkret durchgeführte Risikoanalysen
- Interdisziplinäre und adäquate (adäquat in Bezug auf notwendige Fachkompetenzen) Teamzusammensetzungen für eine Risikoanalyse inkl. Risikoeigner (Risk Owner)[25] bzw. von ihm befugte Person,
- Aktualität und Qualität der Risikoanalysen,
- Teamdisziplin,
- Nachverfolgung von Empfehlungen und Zuständigkeit / Priorisierung,
- Auswahl geeigneter Methoden für die Gefahrenidentifizierung (SWIFT, Checkliste, HAZOP…), Risikobewertung (Risikograph, LOPA, FMECA, QRA…) und Maßnahmenfestlegung (Stand der Technik),
- Dringlichkeitsreihung für Maßnahmen

Indikatoren:

- Summe Empfehlungen / Summe betrachteter Szenarien;
- Anzahl der offenen, überfälligen Maßnahmen (Zeitbezug);
- Anzahl/Prozentsatz der fristgerecht umgesetzten Maßnahmen
- Gegenüberstellung der Anzahl von berichteten „Incidents, Near Misses…“ mit den Arten der (vorab) identifizierten Gefahrenquellen;
- Anzahl von Teilanlagen ohne Risikoanalysen
- Anzahl von geplanten / Anzahl von durchgeführten Risikoanalysen (Zeitbezug);
- Anzahl HAZOP Tage Risk Owner anwesend / Anzahl HAZOP Tage

6.4 Sichere Arbeitsverfahren (Safe Work Practices) [26]

Ziel:

Festlegung eines integrierten Systems von Abläufen und Freigaben sowie von sicheren Arbeitsweisen um daraus resultierende Vorfälle zu vermeiden. Dabei sollen primär Vorfälle bei Nicht-Routine-Tätigkeiten wie die Freisetzung von gefährlichen Stoffen und Energie berücksichtigt werden. Tätigkeiten und Abläufe sollen nach ihrer Gefährdung bewertet und Maßnahmen darauf abgestimmt sein.

Kriterien:

- Fokus liegt auf Nicht-Routine-Tätigkeiten.
- Beschreibung von Methoden zur Bestimmung der Schutzmaßnahmen, die für die sichere Durchführung von Tätigkeiten mit erhöhtem Gefahrenpotential notwendig sind (z.B. Lock out/Tag out; Einstieg in Behälter; Vorgehen bei Arbeiten in Ex-Bereichen; Arbeitsfreigabewesen; Zutrittsberechtigungen, Heißarbeiten…)
- Für jeden Einzelfall ist eine Gefahrenevaluierung erforderlich
- Freigabe für die Durchführung der Tätigkeit hat durch eine verantwortliche/autorisierte Person zu erfolgen (keine Standard Operating Procedure)

Indikatoren:

- Anzahl vollständig ausgefüllter Arbeitsfreigabeprotokolle im Verhältnis zur Gesamtzahl an Arbeitsfreigaben
- Anzahl der ausgegebenen Arbeitsfreigaben pro Zeiteinheit
- Anzahl berichteter Near Miss, die in Verbindung mit Arbeitsfreigaben stehen, im Verhältnis zur Gesamtanzahl an Arbeitsfreigaben

---

[25] Im Sinne ISO 27001 ist ein Risk Owner *„a person or entity with the accountability and authority to manage a risk. Basically, this is a person who is both interested in resolving a risk, and positioned highly enough in the organization to do something about it.”*

[26] Element „Standard Operating Procedures“ wird nicht betrachtet weil die für die Empfehlung wesentlichen Punkte vornehmlich in „Safe Work Practices“ behandelt werden.

- Prozentsatz der vollständig abgeschlossenen Arbeitsfreigaben inklusive Rückgabe und Rücknahme
- Anzahl der verantwortlichen/autorisierten Personen pro Schicht
- Werden die Prozeduren für Safe Work Practices regelmäßig aktualisiert?

6.5 Anlagenintegrität und -zuverlässigkeit (Asset Integrity and Reliability)

Ziel:

System von Aktivitäten wie Wartung, Tests oder Abnahmeprüfungen, durch die sichergestellt wird, dass relevante Einrichtungen und Komponenten während der gesamten Nutzungszeit verfügbar und zuverlässig sind. Dadurch sollen zwei Anforderungen erfüllt werden:

- Einerseits die Vermeidung von Loss of Containment - Ereignissen mit großer Schadenswirkung und
- andererseits die Sicherstellung hoher Verfügbarkeit und Zuverlässigkeit von Systemen und Einrichtungen zur Vermeidung von Loss of Containment - Ereignissen sowie zur Begrenzung von Schadensfolgen

Kriterien:

- Abnahmeprüfungen
- Instandhaltung, bestehend aus
    - Wartung[27] (Maßnahmen zur Verzögerung des Abbaus des vorhandenen Abnutzungsvorrates der Betrachtungseinheit während der Nutzung eines Objekts; wird nach technischen Regeln oder einer Herstellervorschrift durchgeführt, zum Beispiel nach einer bestimmten Laufleistung oder Zeitdauer, dem Wartungsintervall)
    - Inspektion (prüfende Tätigkeit im Sinne einer Kontrolle durch einen Inspizienten, bzw. Inspektor; dient dabei der Feststellung des ordnungsgemäßen Zustandes eines Gegenstandes, eines Sachverhaltes oder einer Einrichtung) und
    - Reparatur (von lateinisch reparare „wiederherstellen“) bzw. Instandsetzung (Vorgang, bei dem ein defektes Objekt in den ursprünglichen, funktionsfähigen Zustand zurückversetzt wird).
- Durchführung der Instandhaltung durch geeignetes Personal
- Kontrollsystem für die Instandhaltungsmaßnahmen
- Qualitätskontrolle

Indikatoren:

- Ausmaß der zeitlichen Abstände zu vorgesehenen oder vorgeschriebenen Wartungs- oder Inspektionsintervallen (z.B. durch DGÜW-V oder Herstellerangaben vorgegeben); in Maximum-, Minimum- und Durchschnittszeiten.
- Erfüllung von Wartungsplänen nach $\text{Indikator}_{\text{Wartungsplan}} = \left(\frac{N_{\text{gewartet}}}{N_{\text{geplant}}}\right) * 100\%$
    - N_{gewartet}…Anzahl der gewarteten Komponenten
    - N_{geplant}…Anzahl der Komponenten, die laut Plan gewartet werden sollten
- Indikator für die Integrität nach $\text{Indikator}_{\text{Integrität}} = \left(1 - \frac{N_{\text{fehlerhaft}}}{N_{\text{Gesamt}}}\right) * 100\%$
    - $N_{\text{fehlerhaft}}$…Anzahl der entdeckten gefährlichen Fehler bei der Prüfung
    - N_{Gesamt}…Anzahl der durchgeführten Überprüfungen
    - Sinnvollerweise sollte N nach gleichartigen Komponenten/Einrichtungen unterteilt werden, z.B. Sicherheitsventile, Schütze, analoge Messungen, Auffangwannen,…
- Anzahl der ungeplanten Reparaturen

[27] DIN 31051 beschreibt den Komplex Instandhaltung mit den Teilen Wartung, Inspektion, Reparatur und Verbesserung; siehe auch EN 13306:2010.

6.6 Fremdfirmenmanagement (Contractor Management)

Ziel:

Sicherer Anlagenbetrieb auch bei Beschäftigung von Fremdfirmen (Kontraktoren)[28]; dies kann unter anderem auch enthalten:

- Liste von zuverlässigen Fremdfirmen mit gutem eigenem Sicherheitsmanagement,
- Vorbereitung und Training der Bediensteten der Fremdfirmen,
- sicherheitsgerichtete Beschreibung des Auswahlverfahrens.

Kriterien:

- Vertragliche Regelungen, die sicherstellen, dass auch bei Arbeiten mit Kontraktoren alle Sicherheitsanforderungen eingehalten werden.
- Es darf nicht zu Situationen kommen, wo sich keiner für die Sicherheit verantwortlich fühlt.
- Abgestufte Vorkehrungen je nach Gefährdungsgrad der ausgeführten Arbeiten
- Kontrollsysteme zur Überprüfung der Anforderungen an Kontraktoren

Indikatoren:

- Werden Kontraktoren - Audits gemacht?
- Gibt es ein Kontraktoren - Management mit definierten Zuständigkeiten und Schnittstellen?
- Werden im Auswahlverfahren von Kontraktoren auch Prozesssicherheitsqualifikationen abgefragt/geschult?

6.7 Änderungsmanagement (Management of Change)

Ziel:

Das Management of Change - MoC stellt sicher dass bei Änderungen keine neuen Risiken entstehen; dies umfasst das Vorhandensein von Risikokontrollmechanismen proportional zu den geplanten Änderungen und entsprechende Maßnahmen (Kommunikation, Schulung usw.).

Kriterien:

- Information der am MoC beteiligten Personen und Änderung bzw. Aktualisierung der betroffenen Dokumente
- Risiko bei Änderungen (Prozess, Produkt, organisatorisch…) strukturiert hinterfragen und bewerten, bevor die Änderungen implementiert werden.
- Definition vom Umfang des MoC (z.B.: HSE, Qualität)
- Vorhandensein von auf das MoC abgestimmten Freigabeprozessen
- Abstimmung auf andere Elemente (Process Safety Knowledge usw.)

Indikatoren:

- Anzahl der MoC´s (ausgelöst durch Änderung Anlagenlayout, Änderung Prozessleitsystem, Änderung von Lieferanten, Änderung von Einsatzstoffen usw.)
- MoC-Dauer (d.h. Vorlaufzeit/Dauer des Vorbereitungsvorgangs)
- Verhältnis MoC´s / Arbeitsfreigaben (Arbeitsaufträge)
- Verhältnis Aktionspunkte aus der Risikoanalyse / Anzahl MoC´s

[28] Fremdfirmen können in folgender Konstellation auftreten:

1. Leihpersonal – macht selbe Tätigkeiten wie firmeneigene Mitarbeiter
2. Fremdpersonal am Standort arbeitet im Auftrag der Firma an Firmeneigenen Installationen (auch mit Einsatz eigener Werkzeuge) – alle Regeln gelten auch für diese Personen.
3. Komplette Anlageneinheit (z.B. Luftzerlegungsanlage, Tanklager,…) wird Kontraktor überlassen, aber Asset gehört noch der Firma, z.B. Tanklager wird von Kontraktor betrieben
4. Sowohl Arbeit als auch Asset macht Kontraktor, z.B. Gefahrenguttransporte
5. Joint Venture Konstellationen, wo nur Anteile an einer Firma gehalten werden

- Tiefe der Risikoanalyse adäquat zur Signifikanz einer Änderung

6.8 Betriebsbereitschaft (Operational Readiness)

Ziel:

Sicherstellen, dass eine Anlage sicher angefahren und abgefahren werden kann; dies ist durchzuführen nach: Neuerrichtung, Umbauten, geplanten Abstellung für Service oder Inspektion und nach ungeplanten Abstellungen.

Kriterien:

- Anlage ist sicher betriebsbereit für den Neustart (auch nach dem Abfahren)
- Vorbereitungen je nach Art des Anfahrens (z.B. Funktionstests, Dichtheitstest, Loop-Checks, Steckscheiben-/Armaturenliste, Inertisierungen)
- Verfügbarkeit von Betriebsmitteln (Utilities)
- Verfügbarkeit von ausreichend geschultem Personal,
- Übergabeprozedur bzw. Festlegung Verantwortlichkeiten (Projektteam - Anlagenbetreiber)

Indikatoren:

- Anzahl der Vorfälle während Start-Up
- Anzahl ungeplanter Shut-Downs nach Wiederanfahren (Eingrenzung auf sicherheitsrelevante Vorfälle je nach betrieblicher Festlegung),
- Anzahl der ausgebildeten Person für Start-Up (z.B. Simulator Training),
- Anzahl der Mängel die im Zuge der Start-Up - Checks gefunden werden,
- Zeitdauer zum Erreichen der Produktspezifikation nach Anfahren (anlagen - bzw. verfahrensspezifisch im Vergleich zum Zustand vor dem vorherigen Abfahren oder früheren Chargen)[29]

6.9 Sicherer Betriebsbereich (Safe Operating Window)

Ziel:

Stabiler Betrieb innerhalb der (vorgegebenen) Grenzen des sicheren Betriebs, rechtzeitige und richtige Reaktion auf sicherheitsrelevante Abweichungen

Kriterien:

- Die sicheren Grenzen müssen definiert sein (z.B. optimaler Produktionsbereich, Normalbereich, sicherer Bereich, unzulässiger Bereich)
- Zulässigkeit des Brückens/Umgehens von Verriegelungen (bypassing of Interlocks) abhängig von……
- Größe des Anlagenbereich im Verantwortungsbereich eines Operators
- Alarmmanagement (Abgrenzung zum Emergency Management, point of no return)

Indikatoren:

- Sind die sicheren Grenzen des Betriebs fixiert?
- Gibt es ein System zur Alarm Priorisierung?
- Wer (welche Berechtigung) darf die Grenzen des sicheren Betriebs verstellen?
- Werden die Grenzen des sicheren Betriebs „nur“ alarmiert oder gibt es eine Abschaltung?
- Anzahl und Dauer eingelegter Brücken;
- Wie viele Alarme kommen pro Operator pro Schicht?
- Wie viele Alarme stehen ständig an?

[29] Je nach Einzelfall kann es eine Korrelation zwischen der Produktqualität und der Anlagensicherheit geben, die zumindest als Trendaussage von Relevanz sein kann.

- Zu wie vielen Alarmen gibt es Anweisungen im Betriebshandbuch?
- Regelmäßige/protokollierte Schichtübergabe – mit standardisierten Protokollen
- Mindestschichtstärke/Vertreterregelung – Vorgangsweise bei Unterschreitung
- %-Satz Prozess Control Loops im „Hand“ Modus

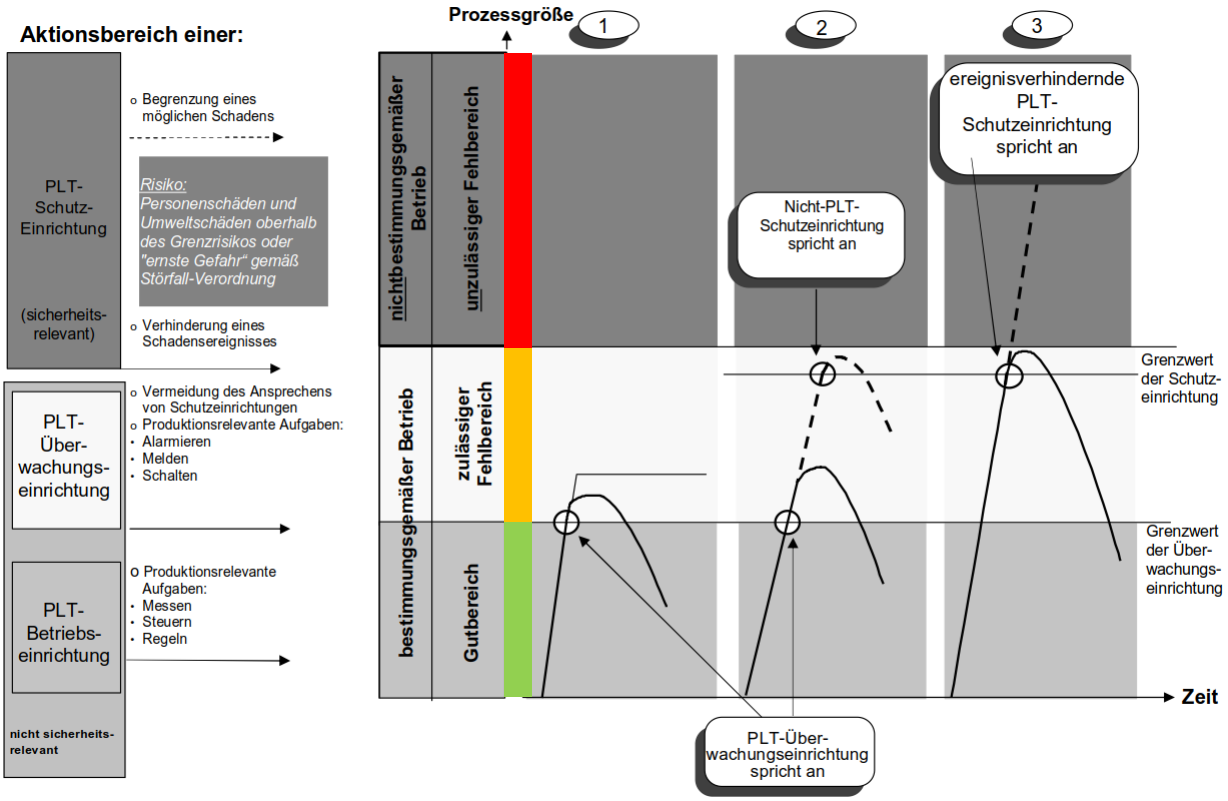

Abbildung 10: Schematische Darstellung der Wirkungsweise von PLT-Einrichtungen (VDI/VDE 2180-1, 2007, S.10)

6.10 Untersuchung von Vorfällen (Incident Investigation) [30]

Ziel:

Sensibilisierung des Betriebes gegenüber Anlagensicherheit, Anhäufungen zu erkennen und Gegenmaßnahmen einleiten, Reduzierung der Anzahl von Incidents und der Auswirkungen, Priorisierung von zukünftigen Schwerpunkten, Untersuchung der Ursachen und Einzelheiten, Lernen aus Vorfällen und Verhindern von Wiederauftreten in der gleichen Anlage und in ähnlichen Anlagen

Kriterien:

- Datensammlung von Vorfällen (Incidents, Near Misses, Process Safety Incidents)
- Auswertbarkeit der gesammelten Vorfälle
- Vorhandensein einer risikobasierenden Priorisierung vor der weiteren Ursachenermittlung und aufbauenden Festlegung von Gegenmaßnahmen
- Ausgeschiedene Incidents (keine Priorität) werden für Trendanalysen verwendet
- Standardisierte Form der Berichterstattung und Auswertung
- Analyse der prioritären Incidents
- System der Umsetzung von Empfehlungen, die aus dem Incident Reporting gewonnen wurden

[30] siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**

Indikatoren:

- Anzahl der gemeldeten und gewichteten Vorfälle (nach aktuellem Schweregrad bzw. potentiellem Schweregrad)
- Ist ein System für Incident Investigation etabliert?
- Anzahl der ausgebildeten Investigatoren.
- Angabe Zeitfenster/Zeitbedarf zur Aufarbeitung der Ergebnisse (unterteilt in die Zeit zur Investigation selbst und die Zeit zur Umsetzung der abgeleiteten Maßnahmen).
- Anzahl der Empfehlungen, die aus Incidents umgesetzt wurden (auch von anderen Standorten/Firmen)
- Anzahl oder Prozentsatz von Untersuchungen/Ereignissen/Empfehlungen, die ein unabhängiges Qualitätssichungsreview durchlaufen haben.
- Verhältnis Near Misses/ Process Safety Incidents

6.11 Effektivitätsnachweis[31]

Ziel:

Überprüfung, ob die Managementsysteme und die Sicherheitskultur auch so umgesetzt/gelebt werden, wie dies vorgesehen ist.

Kriterien:

- Vergleich des Zustandes der Umsetzung der Managementsysteme und der Sicherheitskultur mit vorgegebenen Standards in Bezug auf Qualität, Umsetzungsgrad und Effektivität
- Verfahren, Prozesse, Abläufe,… sollen nicht nur auf vorhanden sein überprüft werden, sondern an Hand eines Beispiels, z.B. ein konkreter MoC, tatsächlich durchlaufen werden, d.h. eine reine Formalüberprüfung ist zu wenig.
- Folgende Audits zählen nicht im Sinne von Process Safety: ISO 9001, ISO 18001, ISO 14001,…

Indikatoren:

- Anzahl der „Audits“ (eigentlich vor Ort – Kontrollen/in - depth checks) pro Jahr, wo die Wirksamkeit der Process Safety Barrier vor Ort überprüft wird[32]
- Anzahl der Audits durchgeführt von Führungskräften?
- Werden Audits auch von Personen anderer Standorte durchgeführt?
- Werden Audits von unabhängigen Dritten durchgeführt?
- Werden Empfehlungen der Audits zeitnahe umgesetzt? (Zeitraum, Anzahl…)
- Gibt es einen Audit-Plan, der sicherstellt, dass Audits flächendeckend und nicht immer nur auf denselben Fokus durchgeführt werden? (örtlich und inhaltlich)
- Priorisierung der Audits –sachlich/zeitlich (Häufigkeit)

[31] Das Element trägt eigentlich die Bezeichnung „Prüfung und Kontrolle (Auditing)“, hier liegt der Schwerpunkt aber nicht auf einer Gesamtaussage. Die Durchführung eines Audits selbst ist noch kein Indikator, aber ohne Audit ist keine Grundlage vorhanden.

[32] Ein reines System-Audit auf Grundlage von schriftlichen Dokumenten reicht nicht für eine Aussage, ob ein System gelebt wird.

7 QUELLENVERZEICHNIS

ACSNI (Advisory Committee on the Safety of Nuclear Installations) (1993) Study Group on Human Factors. (1993). Third report: Organising for safety. Advisory, Committee on the Safety of Nuclear Installations reprinted 1998, ISBN 071760865

API RP 754 (2010). Process Safety Performance Indicators for the Refining and Petrochemical Industries

Ashgate, Aldershot & Reason, J. (1998). Achieving a safe culture: theory and practice. Work and Stress 12 (3) (S. 293–306).

Bird, F.E. jr. & Germain, G.L. (1996). Practical Loss Control Leadership, 3. Auflage, DNV

CCPS (Center for Chemical Process Safety) (2007), Guidelines for Risk Based Process Safety

CCPS (Center for Chemical Process Safety) (2011). Process Safety Leading and Lagging Metrics

Cefic (European Chemical Industry Council) (2011). Guidance on Process Safety Performance Indicators, 2nd Edition

Daniel, K. (2008). Managementprozesse und Performance, Ed. Gabler Wissenschaft

Dyllich, Th., Probst, G. & Ulrich, H. (1984). Management, Haupt-Verlag

Heinrich, H. W. (1931). Accident Prevention: A Scientific Approach, McGraw-Hill

Herczeg, M. (2014). Prozessführungssysteme-sicherheitskritische Mensch/Maschinen-Systeme, De Gruyter/Oldenbourg-V.

Hinze, Thurman, Wehle (2013). Leading indicators on construction safety performance, Safety Science 2013, S. 27

IAEA (International Atomic Energy Agency) (1992). Safety Series Nr. 75-INSAG-7

Käfer, M. (1999). Das Arbeitsschutzsystem bei DuPont de Nemours, Hans-Böckler-Stiftung;
WWW: http://www.boeckler.de/pdf/p_arbp_010.pdf (27.2.2017)

Künzler C. (2002). Kompetenzförderliche Sicherheitskultur - Ganzheitliche Gestaltung risikoreicher Arbeitssysteme, ETH-Hochschulverlag Zürich

OHS (Occupational Health and Safety – Australia) (2012). Models of Causation: Safety,
WWW: http://www.ohsbok.org.au/wp-content/uploads/2013/12/32-Models-of-causation-Safety.pdf (27.2.2017)

Reason, J. (1990). The Contribution of Latent Human Failures to the Breakdown of Complex Systems, Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences. 327, Nr. 1241

Reason, J. (1993). Managing the Management Risk: New approaches to organisational safety in Reliability and Safety Hazardous Work Systems - Approaches to Analysis and Design, Lawrence Erlbaum, S. 8

Reason, J. (1997). Managing the Risks of Organisational Accidents

UBA (Umweltbundesamt Deutschland) (2008). Der Einfluss menschlicher Faktoren auf Unfälle in der verfahrenstechnischen Industrie, UBA - Forschungsbericht Nr. 206 48 300

VDI/VDE 2180-1 (2007), Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT) - Einführung, Begriffe, Konzeption, Beuth Verlag

Weinert, F.E. (2001). Leistungsmessungen in Schulen, Weinheim und Basel: Beltz
WWW: https://de.wikipedia.org/wiki/Kompetenz_(Psychologie) (18.04.2017)