Texte

Texte
22
08
ISSN
1862-4804

Einfluss menschlicher Faktoren auf Unfälle in der verfahrenstechnischen Industrie

Umwelt Bundes Amt
Für Mensch und Umwelt

UMWELTFORSCHUNGSPLAN DES
BUNDESMINISTERIUMS FÜR UMWELT,
NATURSCHUTZ UND REAKTORSICHERHEIT

Forschungsbericht 206 48 300
UBA-FB 001128

Texte
22
08
ISSN
1862-4804

Einfluss menschlicher Faktoren auf Unfälle in der verfahrenstechnischen Industrie

von

Dr. Babette Fahlbuch

Dr. Inga Meyer

Jörk Dubiel

TÜV NORD SysTec GmbH & Co. KG

Im Auftrag des Umweltbundesamtes

Diese Publikation ist auch als Download unter
http://www.umweltbundesamt.de
verfügbar.

Herausgeber: Umweltbundesamt
Postfach 1406
06844 Dessau-Roßlau
Tel.: +49-340-2103-0
Telefax: +49-340-2103 2285
Internet: http://www.umweltbundesamt.de

Redaktion: Fachgebiet III 1.2
Roland Fendler

Dessau-Roßlau, Juni 2008

Berichts-Kennblatt

1. Berichtsnummer 001128	2.	3.
4. Titel des Berichts Einfluss menschlicher Faktoren auf Unfälle in der verfahrenstechnischen Industrie		
5. Autor(en), Name(n), Vorname(n) Fahlbruch, Dr. Babette; Meyer, Dr. Inga; Dubiel, Jörk		8. Abschlussdatum Dezember 2007
6. Durchführende Institution (Name, Anschrift) TÜV NORD SysTec GmbH & Co. KG Große Bahnstraße 31 D-22525 Hamburg		9. Veröffentlichungsdatum 10. UFOPLAN-Nr. 206 48 300 11. Seitenzahl 196
7. Fördernde Institution (Name, Anschrift) Umweltbundesamt Wörlitzer Platz 1 D-06844 Dessau		12. Literaturangaben 104 13. Tabellen und Diagramme 11
		14. Abbildungen 9
15. Zusätzliche Angaben		

16. Kurzfassung

Die Aufdeckung von Zusammenhängen zwischen individuellen, organisatorischen und technischen Faktoren gewinnt aufgrund immer komplexer werdende Systeme für die Sicherheit von verfahrenstechnischen Anlagen an Bedeutung. Im Rahmen dieses Vorhabens und des OECD/CCA-Workshops „Einfluss menschlicher Faktoren auf Chemieunfälle“ am 08. & 09.Mai 2007 in Potsdam wurden folgende, in diesem Kontext relevante Einzelthemen betrachtet:

1. Arten menschlicher Fehler, Definition der relevanten Begriffe
2. Bewertung von Sicherheitskulturen
3. Kompetenzen im Thema menschliche und organisationale Faktoren
4. Zusammenwirken von Bedienern und Schutzsystemen
5. Menschliche und organisationale Faktoren im Alarmmanagement

Der Bericht enthält Definitionen, die bei der Analyse und Erfassung von Unfällen zur Deskribierung von menschlichen und organisatorischen Ursachen verwandt werden können. Vorgehensweisen zur Bewertung von Sicherheitskulturen werden diskutiert und deren Bedeutung aufgezeigt. Empfehlungen zur erforderlichen Kompetenz der Mitarbeiter von Behörden, Betreibern und Sachverständigen hinsichtlich menschlicher Faktoren werden gegeben. Die Bediener-Schutzsystem-Schnittstelle stellt einen für die Anlagensicherheit relevanten Spezialfall der Mensch-Maschine-Schnittstelle dar. Vier Konstellationen dieses Spezialfalles werden beschrieben und Empfehlungen zur Gestaltung der Schnittstelle gegeben. Bedeutung und empfehlenswerte Inhalte eines gezielten Managements der Gestaltung und des Betriebs von Alarmsystemen werden aufgezeigt.

Der Bericht enthält auch eine Zusammenfassung der Präsentationen und Ergebnisse des OECD/CCA-Workshops.

17. Schlagwörter

Menschliche Faktoren; organisationale Faktoren; Sicherheitskultur; Human-Factor-Kompetenz; Bediener-Schutzsystem-Schnittstelle; Alarmmanagement

18. Preis 94.498,75 €	19.	20.

Report Cover Sheet

1. Report No. 001128	2.	3.
4. Report Title Impact of Human Factors on Accidents and Incidents in the Process Industry		
5. Author(s), Family Name(s), First Name(s) Fahlbruch, Dr. Babette; Meyer, Dr. Inga; Dubiel, Jörk		8. Report Date December 2007
6. Performing Organisation (Name, Address) TÜV NORD SysTec GmbH & Co. KG Große Bahnstraße 31 D-22525 Hamburg		9. Publication Date 10. UFOPLAN-Ref.No. 206 48 300
		11. No. of Pages 196
7. Funding Agency (Name, Address) Umweltbundesamt Wörlitzer Platz 1 D-06844 Dessau		12. No. of References 104 13. No. of Tables, Diagrams 11 14. No. of Figures 8
15. Supplementary Notes		
16. Abstract Due to accelerating complexity of technical systems the identification of the relation between individual, organizational and technical factors gains in importance for the process industry. In this project as well as in the OECD/CCA-Workshop “Human Factors in Chemical Accidents and Incidents”, which took place on May 8-9, 2007 at Potsdam, the following special subjects with relevance in this context were evaluated: 1. Types of human factors, definition of relevant terms 2. Assessment of safety culture 3. Human-factors-competence 4. Interaction of operators and safety systems 5. Human factors in alarm management This report includes definitions, which can be used in analysis and documentation of incidents and accidents for a taxonomy of individual and organisational causes. Approaches for the assessment of safety culture are discussed and their relevance is highlighted. Recommendations are given on the required human-factors competence of staff of authorities, industry and of safety experts. For process safety the operator-safety-system-interface is a relevant special case of the man-machine-interface. Four configurations of this special case are described and recommendations on their design are given. The relevance and the recommended content of a special management for the design and operation of alarm systems are pointed out. Additionally this report encompasses a summary of the presentations and results of the OECD/CCA-Workshop.		
17. Keywords Human factors; organisational factors; safety culture; human-factors-competence; man-safety system-interface; alarm management		
18. Price 94,498.75 €	19.	20.

Inhaltsverzeichnis:

Einführung in das Thema „menschliche und organisationale Faktoren in der verfahrenstechnischen Industrie“ ..9

1 Arten menschlicher Fehler, Definition der relevanten Begriffe 12

1.1 Arten menschlicher Fehler in der Ereignisuntersuchung und Datenbanken 12

1.1.1.1 Major Accident Hazards Bureau (MARS) 12

1.1.1.2 Zentrale Melde- und Auswertestelle für Störfälle und Störungen in verfahrenstechnischen Anlagen (ZEMA) 13

1.1.1.3 Chemical Safety and Hazard Investigation Board (CSB) 16

1.1.1.4 U.S. Nuclear Regulatory Commission (NRC) 16

1.2 Stand der Wissenschaft 16

1.2.1 Arten menschlicher Fehler 17

1.2.1.1 Ereignisursachen nach Health & Safety Laboratory (HSL) 17

1.2.1.2 Klassifikation der Health & Safety Executive (HSE) 19

1.2.1.3 Modell nach Reason 20

1.2.2 Taxonomie in Verfahren zur Ereignisanalyse 22

1.2.3 Menschliche Faktoren, Relevante Definitionen 27

1.2.3.1 Allgemeine Begriffsdefinitionen zum Thema „Menschliche Faktoren“ 27

1.2.3.2 Relevante Definitionen zum Fehlerbegriff 28

1.2.4 Für ein Taxonomiemodell relevante Definitionen 35

1.3 Relevante Begriffe für die weiteren Themen des OECD/CCA-Workshops 37

1.4 Diskussion auf dem Workshop 40

1.5 Zusammenfassung und Fazit 42

2 Bewertung von Sicherheitskulturen 43

2.1 Stand der Wissenschaft 43

2.1.1 Was ist Sicherheitskultur? 44

2.1.1.1 Leitprinzipien der OECD 45

2.1.1.2 Definitionen und Schlüsselelemente der IAEA 49

2.1.1.3 Prinzipien der Initiative Responsible Care 50

2.1.1.4 Elemente der Sicherheitskultur der internationale Länderkommission Kerntechnik 51

2.1.2 Wie entwickelt sich Sicherheitskultur? 53
2.1.2.1 Entwicklungsmodell der Sicherheitskultur der IAEA 53
2.1.2.2 Reifegradmodell der Sicherheitskultur des Keil Zentrums 57
2.1.3 Wie kann man Sicherheitskultur messen? 60
2.2 Diskussion auf dem Workshop 69
2.3 Zusammenfassung und Fazit 70

3 Kompetenzen im Thema menschliche und organisationale Faktoren 75
3.1 Stand der Wissenschaft 75
3.1.1 Welche Gruppen sollten beim Thema Sicherheit beteiligt werden? 75
3.1.2 Für die Sicherheit relevante Kompetenzen bezüglich menschlicher und organisationaler Faktoren 76
3.2 Diskussion auf dem Workshop 79
3.3 Zusammenfassung und Fazit 81

4 Zusammenwirken von Bedienern und Schutzsystemen 83
4.1 Stand der Wissenschaft 83
4.1.1 Ergonomische Gestaltung der Mensch-Maschine-Interaktion 84
4.1.2 Der Mensch als Element von Sicherheitssystemen 88
4.1.2.1 Prozessleittechnik-Schutzeinrichtungen (VDI/VDE 2180 Blatt 1 /77/, S.10f) 96
4.2 Diskussion auf den Workshop 98
4.3 Zusammenfassung und Fazit 100

5 Menschliche Faktoren im Alarmmanagement 104
5.1 Stand der Wissenschaft 104
5.1.1 Gestaltung von Alarmsystemen 106
5.1.2 Bewertung von Alarmsystemen 112
5.2 Diskussion auf dem Workshop 116
5.3 Zusammenfassung und Fazit 117

6 Zusammenfassung der Workshoppräsentationen 120
6.1 Thematische Sitzung 1: Arten menschlicher Fehler, Definition der relevanten Begriffe 120
6.2 Thematische Sitzung 2: Bewertung von Sicherheitskulturen .. 123
6.3 Thematische Sitzung 3: Kompetenzen im Thema „Human Factors“ 129
6.4 Thematische Sitzung 4: Zusammenwirken von Bedienern und Schutzsystemen 132
6.5 Thematische Sitzung 5: Menschliche Faktoren im Alarmmanagement 137
6.6 Programm des OECD/CCA-Workshops 144

7 Gesamtzusammenfassung des Endberichtes 146

8 Literatur 152

9 Anhang I Menschliche Faktoren in Ereignisdatenbanken . 161
9.1 Major Accident Reporting System (MARS) 161
9.2 Nuclear Regulatory Commission (NRC) 163
9.3 Berichte des Chemical Safety Board (CSB) 166

10 Anhang II Types of Human Error, Definition of Related Terms 168
10.1 Human Factors, Definitions of General Terms 168
10.2 Types of Human Error, Definitions of Related Terms 168
10.3 Terms Relevant for Incident Investigation and Documentation . 174
10.4 Terms Relevant for Other Sessions of the Workshop 176

11 Anhang III Schlüsselelemente der Sicherheitskultur nach INSAG (/60/, S.5ff): 179

12 Anhang IV Screening-Verfahren zur Selbstbewertung der Sicherheitskultur/66/: 185

13 Anhang V Namur Empfehlung 31 / DIN EN 61511 189
13.1 Namur Empfehlung (Namur Recommendation) 31: Empfehlungen für Schutzeinrichtungen (5.2, /88/) 189
13.2 Aussagen und Anforderungen in der DIN EN 61511 /18/ bis 3 /84, 85/ bzgl. Operatorhandlungen, Berücksichtigung menschlicher und organisationaler Faktoren und deren SIS-Schnittstellen.....191
13.2.1 DIN EN 61511-1..... 192
13.2.1.1 Kap. 1 Anwendungsbereich.....192
13.2.1.2 Kap. 3.2.72 sicherheitstechnisches System (SIS) 192
13.2.1.3 Kap. 5.2.2.2 Kompetenz der Mitarbeiter.....192
13.2.1.4 Kap. 11.3 Anforderungen an das Systemverhalten bei Entdeckung eines Fehlers.....193
13.2.1.5 Kap. 11.7.1 Anforderungen an die Bediener-Schnittstelle.....193
13.2.2 DIN EN 61511-2..... 194
13.2.2.1 Kap. 8.2.1 Anforderungen an die Gefährdungs- und Risikoanalyse 194
13.2.2.2 Kap. 11.2.6 Rolle und Einfluss des Bedienpersonals 195
13.2.2.3 Kap. 11.7.1 Anforderungen an die Bediener-Schnittstelle.....196

Einführung in das Thema „menschliche und organisationale Faktoren in der verfahrenstechnischen Industrie“

Die Identifikation des menschlichen Beitrags und dessen Einflussgrößen ist bei der Analyse von Ereignissen, die zu Störfällen führten oder hätten führen können, von zunehmender Bedeutung. Je komplexer technische Systeme werden, umso mehr wird die komplexe Interaktion von Mensch-Technik-Organisation zum zentralen Thema von Sicherheitsfragen.

Analysen von Unfalldaten zeigen, dass menschliche Faktoren eine kausale oder beitragende Rolle in 50-80% der untersuchten Ereignisse spielen /1/. Der 600K Bericht des “US Chemical Safety and Hazard Investigation Board” konnte belegen, dass bei Ereignissen mit bekannter Ursache 49% durch technische Faktoren und 39% durch menschliche Faktoren verursacht wurden. Unter den Ereignissen mit technischen Ursachen, konnten 97% auf allgemeine Gerätefehler zurückgeführt werden und unter Ereignissen mit verursachenden menschlichen Faktoren, kristallisierten sich 63% als menschliche Fehler heraus. Eine Analyse der Ursachen von Unfällen, die an die deutsche ZEMA-Datenbank gemeldet wurden, ergab dagegen, dass nur 25% der Unfälle menschliche Fehler als angegebene Ursache hatten /103/.

Der Zusammenhang zwischen menschlichem Verhalten und Unfällen oder Beinahe-Unfällen ist für den typischen Fall einer Fehlbedienung eindeutig und erfassbar. Schwieriger nachweisbar ist ein derartiger Zusammenhang jedoch bei organisationalen Faktoren wie fehlenden oder fehlerhaften Managemententscheidungen. Das könnte ein Grund dafür sein, dass der Anteil menschlichen Verhaltens (menschliche und organisationale Faktoren) an der Unfallentstehung unterschiedlich hoch beziffert wird. Trotz unterschiedlicher Erfassung sind daher menschliche und organisationale Faktoren als Hauptrisikoquellen in Industrien anzusehen.

Das Anliegen dieses Berichtes ist es, den Faktor Mensch in Bezug auf Management und Tätigkeiten in gefährlichen Anlagen zu untersuchen. Menschliche und organisationale Faktoren beziehen sich generell auf alle Ebenen, die den Menschen beim Umgang mit der technischen Anlage beeinflussen. Die übergreifende Zielsetzung ist daher das Aufzeigen der Bedeutung von menschlichen Faktoren für die Leitung und den Betrieb von Anlagen, die der Störfall-Verordnung /72/, bzw. Seveso-II-Richtlinie[1] unterliegen.

Da das Vorhaben in Verbindung mit dem OECD/CCA-Workshop „Human-Factors in Chemical Accidents and Incidents“[2], der am 8. und 9. Mai 2007 vom

[1] Richtlinie 96/82/EG des Rates vom 9. Dezember 1996 zur Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen (Seveso-II-Richtlinie /73/)

[2] Vgl. http://www.umweltbundesamt.de/anlagen/oecd-cca-workshop.html

BMU in Potsdam ausgerichtet wurde, durchgeführt wurde, konzentriert es sich auf die Themen der fünf Sektionen dieses Workshops. Speziell sollen daher Fragen zur Berücksichtigung menschlicher und organisationaler Faktoren bei der Analyse von Ereignissen, zur Sicherheitskultur, der Kompetenz im Thema menschliche und organisationale Faktoren, der Bediener-Schutzsystem-Interaktion und zum Alarmmanagement diskutiert und Empfehlungen hinsichtlich einer jeweiligen „besten Praxis“ ausgearbeitet werden.

Der vorliegende Bericht ist daher nach folgenden fünf Themen der Sektionen des OECD/CCA-Workshops strukturiert:

1. Arten von menschlichem Fehlverhalten, Definition von relevanten Begriffen (Kapitel 1)
2. Beurteilung von Sicherheitskulturen (Kapitel 2)
3. Kompetenz im Thema menschliche und organisationale Faktoren (Kapitel 3)
4. Zusammenwirken von Bedienern und Schutzsystemen (Kapitel 4)
5. An menschliche Fähigkeiten angepasste Alarmsysteme (Kapitel 5)

Die Ziele der wissenschaftlichen Ausarbeitung sind im Einzelnen:

- Identifikation von verschiedenen Arten menschlicher Fehler, Definitionen von relevanten Begriffen sowie Taxonomiemodellen zur Ereignisanalyse und Dokumentation.
- Entwurf einer Liste relevanter Definitionen für die Thematik menschliche Faktoren für die Anlage I (Erläuterung der verwendeten Begriffe) der OECD-Leitprinzipien für die Verhinderung, Bereitschaft für den Fall und Bekämpfung von Chemieunfällen /2/. Diese Definitionen, sollen zukünftig von Industrien bei der Analyse, Dokumentation von Ereignissen und „Lessons Learnt“-Kommunikation verwendet werden /3/.
- Ableitung von Empfehlungen für eine Bewertung der Sicherheitskultur von Organisationen: Identifikation von Konzepten und Methoden zur Bewertung von Sicherheitskultur und deren Übertragbarkeit auf die verfahrenstechnische Industrie, Identifikation von Elementen einer guten Sicherheitskultur.
- Identifikation des aufgabenbezogenen Kompetenzbedarfs auf verschiedenen Management- und Personalebenen in Organisationen (Betreiber, Behörden, Sachverständigenorganisationen, Human-Factors-Beauftragte).
- Identifikation von geeigneten Funktionsallokationen an der Schnittstelle zwischen Sicherheitssystemen und den Bedienern einer Anlage.

- Identifikation eines geeigneten Alarmmanagements, die Integration von Alarmen und Reaktionen des Bedieners, z.B. Unterstützung des Bedieners beim Umgang mit Alarmsystemen, effiziente Meldesysteme, Alarmunterdrückung oder Priorisierung von Alarmen.

Dabei wurden folgende Quellen ausgewertet:

- Meldepflichtige Ereignisse in den OECD-Mitgliedstaaten, bei denen die genannten Themen eine verursachende Rolle gespielt haben
- Politische Konzepte, rechtliche Anforderungen, technische Regeln, Leitfäden und sonstige Empfehlungen
- Einschlägige wissenschaftliche Literatur zu den genannten Themen
- Erkenntnisse aus dem OECD/CCA Workshop „Einfluss menschlicher Faktoren auf Chemieunfälle“ 2007 in Potsdam /4/

Dieser Bericht beruht auf der wissenschaftlichen Ausarbeitung des Zwischenberichts /5/. Dabei wurde sowohl der derzeitige wissenschaftliche Stand zu den erwähnten Themen berücksichtigt als auch die im Rahmen des OECD/CCA Workshops /4/ erhaltenen Informationen. Die Ergebnisse des Workshops sind in Kapitel 6 komprimiert dargestellt. Darüber hinaus werden weitere Forschungs- und Kooperationsmöglichkeiten auf dem Gebiet der menschlichen Faktoren in Verbindung mit Unfällen und Ereignissen in der verfahrenstechnischen Industrie aufgezeigt.

1 Arten menschlicher Fehler, Definition der relevanten Begriffe

Auf der Grundlage des aktuellen wissenschaftlichen Standes sollen in diesem Kapitel verschiedene Arten menschlicher Fehler und relevante Definitionen identifiziert werden. Diese Zusammenstellung und Strukturierung soll zur Harmonisierung der Begriffe und Definitionen bei der Analyse und Dokumentation von (Beinahe-) Ereignissen in der verfahrenstechnischen Industrie beitragen.

1.1 Arten menschlicher Fehler in der Ereignisuntersuchung und Datenbanken

Um den Anteil der menschlichen und organisationalen Faktoren an den Ursachen von Ereignissen bestimmen zu können, ist es notwendig, mit der vergleichbaren Perspektive an die Untersuchung von Unfällen und Beinahe-Unfällen zu gehen und ein System mit abgestimmten Definitionen zu entwickeln.

Zur Klärung des derzeitigen Standes wurde eine Meta-Analyse in verschiedenen Datenbanken über Unfälle in der verfahrenstechnischen Industrie hinsichtlich der dort verwendeten Erfassung und Kategorisierung von als Unfallursache durchgeführt. Es sollte insbesondere aufgezeigt werden, wie und mit welchen Definitionen bzw. Deskriptoren menschliche und organisationale Faktoren (beispielsweise Fehlbedienung oder unzureichender Erfahrungsrückfluss) derzeit in den verschiedenen Datenbanken berücksichtigt und erfasst werden.

Es zeigte sich, dass in den untersuchten Datenbanken derzeit keine Definitionen von menschlichen Fehlern aufgeführt sind. Es konnten jedoch folgende Kategorisierungen in den verschiedenen Datenbanken (MARS, ZEMA, CSB) identifiziert werden:

1.1.1.1 Major Accident Hazards Bureau (MARS)

Die MARS Datenbank /7/ ist das zentrale Informationsnetzwerk der EU und der OECD Mitgliedsstaaten zur standardisierten Dokumentation von Ereignissen und Störungen. Die zentrale Datenbank wird vom Major Accident Hazards Bureau (MAHB) beim Joint Research Centre (JRC) in Ispra betreut und verfügt über 15 lokale Datenbanken auf einer MS-Windows Plattform in jedem Mitgliedsstaat der Europäischen Union. Die Datenbank verfügt über eine komplexe Suchfunktion und Musteranalysen. Insgesamt sind mehr als 600 Ereignisse erfasst, davon sind etwa 50% mit „Cause Human“ klassifiziert. Eine Beschreibung der „Ursache Mensch“ befindet sich in Tabelle 10 des Anhanges I.

1.1.1.2 Zentrale Melde- und Auswertestelle für Störfälle und Störungen in verfahrenstechnischen Anlagen (ZEMA)

In der Zentralen Melde- und Auswertestelle für Störfälle und Störungen in verfahrenstechnischen Anlagen (ZEMA) /8/ werden alle nach der Störfall-Verordnung (12. BImSchV) meldepflichtigen Ereignisse erfasst, ausgewertet und in Jahresberichten veröffentlicht. Die meldepflichtigen Ereignisse werden entsprechend ihrem Gefahrenpotential in Störfälle und in Störungen des bestimmungsgemäßen Betriebs unterteilt. Insgesamt werden 502 Ereignisse erfasst, davon sind 124 Ereignisse mit „Ursache ist menschlicher Fehler“ eingestuft. Die Ursachenklassifizierung erfolgt in den Kategorien:

- Ursache ist betriebsbedingt,
- Ursache ist menschlicher Fehler,
- Ursache ist umgebungsbedingt.

Die weiteren Subkategorien sind nicht vorgegeben, sondern ergeben sich aus der Beschreibung.

In den 124 Berichten mit der Ursache menschlicher Fehler sind die folgenden Formulierungen zur Ursachenbeschreibung enthalten (Umfang der Auswertung: alle Berichte seit 1995 bis 2004):

Tabelle 1: Klassifikationsschema der ZEMA Datenbank /8/

Nr.		
Ursache (Kategorie)	**Beschreibung**	
	Ursache ist menschlicher Fehler	
1	Organisatorische Fehler	
		Falsche Einweisung
		Keine Einweisung erhalten
		Eigenmächtige Fehlhandlung und unterlassene Alarmierung aufgrund unzureichender Anweisungen
		Fehlschaltung von Leitungen
		Anweisung nicht befolgt und Informationsmangel (Fremdfirma)

Nr.		
Ursache (Kategorie)	**Beschreibung**	
1	Organisatorische Fehler	
		Falsche Auswahl (der Heizkammer) durch unpräzise Betriebsanweisung
		Falsche Angabe (einer Rohrleitung)
		Arbeitsschritt (Spülen) vergessen
		Falsche Verfahrensauslegung
		Kein Atemschutzgerät getragen
2	Bedienfehler	
		Nicht erfolgte Abschottung
		Übermäßiges Anschrauben (Ventilabriss)
		Kurzschluss durch nicht entfernte Erdung nach Revision
		Verwechslung von Rohrleitungen
		Armatur fehlerhaft offen
		Alarm nicht wahrgenommen
		Unachtsamkeit bei Wartungsarbeiten (Absperrarmatur teilweise offen)
		Fehlerhaftes Öffnen einer Armatur
		Nicht erfolgte Umstellung der Betriebsart (manuelle Umst.)
		Falsche Maßnahme (Fehlchargierung) PLS war ungeeignet
		Fehlbedienung einer Armatur nach Verstopfung
		(unterlassene) Maßnahme entgegen der Anweisung
		Versehentliche Schieberöffnung
		Unterlassene Kontrolle (Zustand des Reaktors vor Befüllung)
		Verwechselung von Anschlüssen
		Überfüllung eines Behälters
		Ablesefehler an Messinstrument
		Fehlerhaftes Öffnen eines Ventils
		Vernachlässigung Erlaubnisscheinverfahren
		Irrtümlich geöffnetes Ventil
		Abdichtung Behälter entgegen Betriebsanweisung
		Ventil offen gelassen
		Falsche Dosierung
		Informationsdefizit (Ausführung der Stutzen am Kesselwagen anders als angenommen)

Nr.		
Ursache (Kategorie)	**Beschreibung**	
2	Bedienfehler	
		Zu schnelle Produktzugabe
		Ventil abgebrochen (mit Gabelstapler)
		Fass umgefahren (mit Gabelstapler)
		Produktvorlage unbekannt
		Unterdosierung (infolge Pumpenausfall) erkannt, aber nur protokolliert
		Falsche Produktlieferung nicht erkannt
		Falscher Werkstoff / falsche Produktzugabe
		Abdichtung vergessen
		Funkenbildung / Feuer durch Unachtsamkeit
		Falscher Anlagenumbau (Änderung ungeeignet)
		Fehlbedienung einer Armatur (wegen zu kurzer Leiter nicht einsehbar)
		Falsch gemessen (Produktzusammensetzung)
		Falsche Dosierung (Erfahrungswert aus Routinearbeit hier falsch)
		Fehlende Instruktionen / kein Gefahrenabwehrplan
		Irrtum (Ventilstellung falsch interpretiert)
		Unsachgemäßer Umgang mit Gefahrstoff (Erfahrungsmangel)
		Falsche Einschätzung der Produktkonzentration
3	während Reparaturarbeiten	
		Versehentliches Aufschrauben einer Armatur
		Anbohren eines Druckrohrs (NH3)
		Arbeiten an Behälter und Produktaustritt
		Verwendung eines nicht Ex-geschützten Gerätes im Ex-Bereich
		Verwechslung (Rohrleitung)
		Unsachgemäße Wartung (Leckage an Flansch)
		Unterlassene Kontrolle (des Rohrleitungsverlauf)
		Verwechslung (Rohrleitung)
		Montagefehler (Dichtung)
		Feuer / Explosion durch Schweißarbeiten nahe brennbaren Stoffen
		Rohrleitung angesägt (Fremdfirma)
		Unvollständige Entleerung

Die Einstufung der Ursachen in die bisherigen Subkategorien organisatorischer Fehler, Bedienfehler und Fehler während Reparaturarbeiten, erscheint in vielen Berichten fragwürdig.

1.1.1.3 Chemical Safety and Hazard Investigation Board (CSB)

Das Chemical Safety and Hazard Investigation Board (CSB) /9/ ist ein unabhängiges Gremium und befasst sich mit der Ermittlung von Ereignisursachen aus dem Bereich der verfahrenstechnischen Industrie in den USA. Eine Sammlung von aktuellen Unfallberichten ist im Internet verfügbar, jedoch ohne Selektierungsfunktionen entsprechend den Ursachen. Im Anhang I werden daher exemplarisch nur 3 Ereignisberichte, in denen menschliche Faktoren als eine Ursache erkannt wurden, aufgeführt und nach Untersuchungsergebnissen zusammengefasst.

1.1.1.4 U.S. Nuclear Regulatory Commission (NRC)

Die Nuclear Regulatory Commission (NRC) /10/ sammelt Daten aus eigenen Inspektionsberichten sowie lizenzierten Prüfungs- und Ereignisberichten (LERs).

Die NRC verwendet diese Information zur Bewertung von Trainings, organisationalen Prozessen, Mensch-System-Schnittstellen, Kommunikation und Inspektionen. Mit Hilfe von definierten Kriterien sortiert die NRC menschliche und organisationale Faktoren in die folgenden acht Kategorien ein und verschlüsselt sie:

1. Training
2. Vorgehensweisen und Referenzdokumente (procedures and reference documents)
3. Aufgabentauglichkeit (fitness for duty)
4. Flüchtigkeitsfehler (oversight)
5. Problemerkennung und Problemlösung (problem identification & resolution)
6. Kommunikation (communication)
7. Mensch-System-Schnittstelle und Umgebung (human-system interface and environment)
8. Arbeitsplanung und Arbeitsmethoden (work planning and practices)

Jede Kategorie wird weiter in Bereiche eingeteilt. Diese enthalten eine detaillierte Beschreibung (im Januar 2006 aktualisiert) leistungsbezogener Faktoren. In Tabelle 11 des Anhanges I ist eine Auflistung der möglichen Codes dargestellt.

1.2 Stand der Wissenschaft

In den folgenden Abschnitten soll ein Überblick über die Ergebnisse der wissenschaftlichen Arbeiten zu Arten von menschlichen Fehlern und Möglichkeiten

zur Klassifikation von menschlichen Faktoren gegeben werden, bevor in nachfolgenden Kapiteln für Letzteres nutzbare Definitionen aufgezeigt werden.

1.2.1 Arten menschlicher Fehler

Zur Darstellung des derzeitigen wissenschaftlichen Standes zum Thema „Arten menschlicher Fehler, Definitionen der relevanten Begriffe“ wurden die folgenden Quellen analysiert:

- Nationale und internationale technische Standards in verschiedenen Dokumenten der HSE (Health and Safety Executive), OECD (Organisation for Economic Cooperation and Development), VDI (Verein Deutscher Ingenieure), DIN (Deutsches Institut für Normung), ISO (Internationale Organisation für Normung) und Namur (Interessengemeinschaft Automatisierungstechnik der Prozessindustrie),
- Ausgewählte Analyse von Berichten über Ereignisse und Beinahe-Ereignisse,
- Forschungsliteratur aus den Bereichen Psychologie, Human Factors und Organisationswissenschaften.

1.2.1.1 Ereignisursachen nach Health & Safety Laboratory (HSL)

Das Health & Safety Laboratory (HSL) veröffentlichte 2006 einen Bericht über Ereignisursachen /50/. Einer der Hauptbefunde betont die Relevanz von organisatorischen Faktoren: „Die Literatur zur Steuerung von menschlichem Verhalten in Hochrisiko behafteten Industrien weist eher auf organisationale Faktoren (mittels der Sicherheitskultur) als auf individuelles Verhalten hin” /50/, S. iv.

Darüber hinaus zeigen viele der Fallstudien /50/ und der Ereignisberichte, dass Fehler, die durch menschliche und organisationale Faktoren beeinflusst wurden, implizite Ursachen für Ereignisse in Hochrisiko behafteten Industrien darstellen. Es ist bekannt, dass die Kontrolle von menschlichen und organisationalen Faktoren viel wichtiger ist als die Kontrolle der Technik, weil dort bedeutsame Verbesserungen zur Sicherstellung der inhärenten Sicherheit von Maschinen, Technik und Ausstattung bereits stattgefunden haben.

Die HSL hebt hervor, dass die Mehrheit der untersuchten Ereignisse durch ein komplexes Zusammenspiel aus organisatorischen, individuellen und technischen Faktoren verursacht wurde. Schlüsselfaktoren, die zu den Ereignissen geführt haben, waren /50/, S.8f.:

- Ungeeignetes Verhalten des Managements, z. B. unangemessene Supervision,
- Druck, um die Produktionsziele zu erreichen,

- unangemessenes Sicherheitsmanagementsystem,
- aus vorangegangenen Ereignissen wurde nichts gelernt,
- Kommunikation, z. B. zwischen Schichten oder Mitarbeiter und Vorgesetzten etc.,
- ungeeignetes Berichtswesen,
- Gleichgültigkeit
- Verstöße bzw. nicht-regelgerechtes Verhalten,
- ungeeignete Schulungen, z. B. in Bezug auf Notfälle, Feuer oder Sicherheit,
- Mangel von Fähigkeiten,
- viele Überstunden, die zu mentaler Ermüdung führen,
- unangemessene Vorgehensweisen,
- Veränderungen/Erneuerungen von Arbeitsmitteln, ohne dass der Operator davon erfährt oder die Risikobeurteilung geändert wird,
- unangemessene oder ungenügende Instandhaltung,
- Fehler bei der Instandhaltung.

Ähnliche Faktoren wurden zehn Jahre zuvor in einem Bericht der HSE über den Beitrag von Einstellungs- und Managementfaktoren in verfahrenstechnischen Industrien gefunden /51/. Obwohl in den Ereignisberichten wenig detaillierte Informationen über zugrunde liegende Ursachen gegeben wurden, konnten einige wesentliche menschliche Faktoren als beitragend identifiziert werden:

- Instandhaltungsfehler,
- unangemessene Vorgehensweisen,
- unangemessene Arbeitsplanung,
- unangemessene Risikobeurteilung,
- unangemessene Schulung des Personals,
- sicherheitswidriges Arbeiten wird von Vorgesetzten und Management stillschweigend geduldet.
- unangemessene Steuerung und Überwachung des Personals durch die Manager,
- unangemessene Überwachung von Mitarbeitern von Fremdfirmen.

Bei einer systematischen Analyse mit einem geeigneten Verfahren sollten auch organisationale Fehler identifiziert werden.

1.2.1.2 Klassifikation der Health & Safety Executive (HSE)

Die HSE /11/ schlägt ein Klassifikationsschema für menschliche Fehler (human failure) vor, welches zwischen Handlungsfehler (action errors), Prüffehler (checking errors), Informationsabfragefehler (information retrieval errors), Informationsübermittlungsfehler (information communication errors), Auswahlfehler (selection errors), Planungsfehler (planning errors) und Verstöße (violations) unterscheidet (siehe Tabelle 2):

Tabelle 2: Klassifikationsschema für menschliche Fehler nach HSE /11/, S. 5f.

	Handlungsfehler (action error)
A1	Arbeitsschritt zu lang oder zu kurz ausgeführt (operation too long/short)
A2	Arbeitsschritt war unpassend (operation mistimed)
A3	Arbeitsschritt wurde in die falsche Richtung ausgeführt (operation in wrong direction)
A4	Arbeitsschritt zu gering oder zu stark ausgeführt (operation too little / too much)
A5	Arbeitsschritt zu schnell oder zu langsam ausgeführt (operation too fast / too slow)
A6	Verschiebung (misalign)
A7	Richtiger Arbeitsschritt am falschen Objekt ausgeführt (right operation on wrong object)
A8	Falscher Arbeitsschritt am richtigen Objekt ausgeführt (wrong operation on right object)
A9	Arbeitsschritt wurde ausgelassen (operation omitted)
A10	Arbeitsschritt unvollständig ausgeführt (operation incomplete)
A11	Arbeitsschritt zu früh oder zu spät ausgeführt (operation too early/late)
	Prüffehler (checking errors)
C1	Prüfung wurde ausgelassen (check omitted)
C2	Prüfung war unvollständig (check incomplete)
C3	Richtige Prüfung am falschen Objekt (right check on wrong object)
C4	Falsche Prüfung am richtigen Objekt (wrong check on right object)
C5	Prüfung zu früh oder zu spät ausgeführt (check too early/late)
	Informationsabfragefehler (information retrieval errors)
R1	Information nicht erhalten (information not obtained)
R2	Falsche Information erhalten (wrong information obtained)
R3	Informationsabfrage unvollständig (information retrieval incomplete)
R4	Information falsch interpretiert (information incorrectly interpreted)
	Informationsübermittlungsfehler (information communication errors)
I1	Information nicht übermittelt (information not communicated)
I2	Falsche Information übermittelt (wrong information communicated)
I3	Informationsübermittlung unvollständig (information communication incomplete)
I4	Informationsübermittlung unklar (information communication unclear)

	Auswahlfehler (selection error)
S1	Auswahl ausgelassen (Selection omitted)
S2	Falsche Auswahl getroffen (wrong selection made)
	Planungsfehler (planning errors)
P1	Planung ausgelassen (plan omitted)
P2	Planung nicht korrekt (plan incorrect)
	Verstöße (violations)
V1	V1 vorsätzliche Handlungen (deliberate actions)

1.2.1.3 Modell nach Reason

Reason /6/ unterscheidet drei verschiedene Ansätze, mit unterschiedlichem Schwerpunkt bei der Analyse von Stör- und Unfällen, bei der Ursachenzuschreibung und sicherheitsgerichteten Interventionen:

Das **Personenmodell** wird am besten durch den traditionellen Arbeitssicherheitsansatz charakterisiert. Es werden vor allem Fehler, nicht sicherheitsgerichtete Handlungen und Regelverletzungen fokussiert. Die Ursachen von Stör- und Unfällen werden in der Regel in psychologischen Faktoren wie mangelnde Aufmerksamkeit, unzureichende Motivation oder fehlenden Fähigkeiten gesehen. Begründet ist dies in der impliziten Annahme, dass alle Mitarbeiter sich bewusst und frei zwischen sicherem und nicht sicherheitsgerichtetem Verhalten entscheiden können.

Das **Ingenieurmodell** steht in der Tradition von Ingenieurwissenschaft, Arbeitswissenschaft und Risikomanagement (risk control, loss control). Ursachenanalysen zielen vor allem auf Fehler an der Mensch-Maschine-Schnittstelle.

Das **Organisationsmodell** kann als eine Erweiterung des Ingenieurmodells angesehen werden. Grundlage ist die Annahme, dass neben technischem Versagen und Operateursfehlern auch weitere latente Faktoren in der Organisation zu der Entstehung von Unfällen beitragen. So kann die Instandhaltung beispielsweise zu lange Prüfintervalle haben, so dass Verschleiß oder Alterung nicht rechtzeitig bemerkt wird, was zum Ausfall einer technischen Komponente führen könnte. Als ein weiteres Beispiel sei hier eine ungünstige Arbeitsplanung genannt, durch welche die Wahrscheinlichkeit für das Auftreten von Operateurfehlern erhöht werden könnte. Dementsprechend werden Ursachenanalysen durchgeführt und menschliche und organisationale Faktoren identifiziert, die bei Analysen unter einer anderen Perspektive nicht in Betracht gezogen worden wären.

Reason /6, 12, 13/ schlägt ein weit akzeptiertes Modell für menschliche Fehler vor. Er definiert menschlicher Fehler als „die Störung von geplanten Tätigkeiten zur Zielerreichung, ohne das Eintreten von unvorhersehbaren Ereignissen“ /6/, S.71.

Diese Definition enthält drei Elemente:

1. einen Plan oder eine Absicht, mit einem Ziel und Wegen zur Zielerreichung;
2. eine Handlungssequenz, die durch den Plan initiiert wird und
3. das Ausmaß, inwieweit diese Handlungen zum Erreichen des Ziels beitragen.

Er unterscheidet eine Reihe von Fehlertypen, die in Tabelle 3 dargestellt sind.

Tabelle 3: Zusammenfassung der prinzipiellen Fehlertypen nach Reason /12, 13/

Menschliche Fehler (human failure)					
Fehler (errors)				Verstöße (violations)	
Schnitzer (slips)		Irrtümer (mistakes)		(misvention)	Fehlanwendung (mispliance)
Aufmerksamkeitsfehler (attentional slips of action)	Gedächtnisfehler (lapses of memory)	Regelbasierte Fehler (rule-based mistakes)	Wissensbasierte Fehler (knowledge-based mistakes)		

Die folgenden Erklärungen/Definitionen der verschiedenen Typen menschlicher Fehlhandlungen können im Sinne von Reason /13/ zusammengefasst werden (siehe Tabelle 3):

- **Schnitzer (slips)**

Der Plan ist angemessen, aber die Handlung verläuft nicht so wie geplant.

- **Aufmerksamkeitsfehler (attentional slips of action)**

beziehen sich auf beobachtbare Handlungen und sind assoziiert mit Aufmerksamkeits- oder Wahrnehmungsfehler

- **Gedächtnisfehler (lapses of memory)**

sind eher internal (schwer beobachtbar) und beinhalten generelle Gedächtnisfehler

- **Irrtümer (mistakes)**

Die Handlung verläuft nach Plan, aber der Plan ist nicht angemessen, um das intendierte Ziel zu erreichen. Der Fehler tritt auf einer höheren Ebene auf, d.h. der mentale Prozess verläuft falsch.

- **Regelbasierte Fehler (rule-based mistake)**

Die falsche Anwendung einer guten mentalen Regel oder die Anwendung einer schlechten mentalen Regel.

- **Wissensbasierte Fehler (knowledge-based mistake)**

treten auf, wenn keine vorgefertigte Lösung existiert und die Problemlösung somit erst noch generiert werden muss

- **Verstöße (violations)**

eine gute Regel wird nicht angewendet

- **Misvention**

das Verhalten beinhaltet sowohl eine Abweichung einer angemessenen sicherheitsrelevanten Prozedur als auch Fehler, die zu einem unsicheren Ergebnis führen

- **Fehlanwendung (mispliance)**

das Verhalten beinhaltet die irrtümliche Einhaltung einer nicht angemessenen oder nicht akkuraten Prozedur und führt zu einem unsicheren Ergebnis

1.2.2 Taxonomie in Verfahren zur Ereignisanalyse

Fahlbruch /54/ stellt eine Auswahl der veröffentlichten Ereignisanalyseverfahren vor: Die Mehrzahl der evaluierten Methoden (Change Analysis, ASSET – Assessment of Safety Significant Events Teams, CREAM – Cognitive Reliability and Error Analysis Method, HPES – Human Performance Enhancement System, MORT – Management Oversight and Risk Tree , SOL – Safety through Organizational Learning, STEP – Sequentially Timed Event Plotting, TOR – Technique of Operations and Review) bilden unmittelbare Ursachen als auch zu Grunde liegende Faktoren ab. Obwohl es einige Unterschiede hinsichtlich der vorgeschlagenen kausalen Kategorien gibt, werden menschliche und organisationale Faktoren in den Analysemethoden berücksichtigt außer bei der Change Analysis und bei STEP, die keine vorgegebenen Kategorien enthalten.

Es existieren zwei neuere Taxonomiemodelle, die vor allem auf latente Fehler näher eingehen: Das HFIT (Human Factors Investigation Tool) /55/ zur Untersuchung von Ereignisursachen in der Prozessindustrie und das DoD HFACS (Department of Defense Human Factors Analysis and Classification System) /56/ des Verteidigungsministeriums zur Identifikation von Gefährdungen und Risiken. Beide Modelle basieren auf einem Sequenzmodell des Ereignisablaufs, bei dem Ereignisse oder Beinahe-Ereignisse als Produkt von verschiedenen Ursachen angesehen werden. Die verwendeten Klassifikationsschemata werden im Folgenden näher beschrieben.

Das HFIT /55/ berücksichtigt vier verschiedene Informationen bezüglich menschlicher und organisationaler Faktoren: (1) Handlungsfehler unmittelbar vor dem Ereignis, (2) Mechanismen zur Fehlerbehebung im Falle von Beinahe-Ereignissen (3) der Gedankenprozess, der zum Handlungsfehler führt, und (4) die zugrundeliegenden Ursachen.

Die erste Kategorie beinhaltet **Handlungsfehler** („active error“). Sie beziehen sich auf beobachtbare Fehler, welche unmittelbar vor dem Ereignis passieren und meistens durch Mitarbeiter an vorderster Front verursacht werden. Handlungsfehler liefern keine Kausalinformationen, das heißt, sie erklären nicht, warum oder wie es zu dem Ereignis gekommen ist. Die Kategorie „Handlungsfehler“ enthält sechs weitere Elemente:

- Unterlassungen („omission“): Aufgaben oder Teile der Aufgabe werden nicht durchgeführt;
- Fehler in der zeitlichen Koordination der Aufgabe („timing error“): Handlung zu kurz, zu lang, zu früh oder zu spät;
- Fehler im Handlungsablauf („sequence error“): Handlungswiederholung, Handlung an falscher Stelle;
- Fehler in der Qualität der Handlung („quality error“): Handlung zu viel, zu wenig, in der falschen Reihenfolge, falsche Handlung richtige Arbeitsmaterialien;
- Fehler in der Handlungsauswahl („selection error“): richtige Handlung falsche Arbeitsmaterialien;
- Kommunikationsfehler („communication error“): Informationen werden nicht weitergegeben, unklare Informationen, unvollständige Informationen, falsche Informationen;
- Verstöße („violations“): unbeabsichtigt, ungewöhnlich, routinemäßig, generell.

Diese Handlungsfehler werden teilweise von einem verringerten Situationsbewusstsein verursacht. Daher wird die zweite Kategorie als **Situationsbewusstsein** („situation awareness“) bezeichnet. Situationsbewusstsein bezeichnet die Wahrnehmung der Objekte in der Umgebung, das Verstehen ihrer Bedeutung, die Veränderungen in der Umgebung und dass der zukünftige Zustand der Objekte zutreffend für eine ausreichende Zeitspanne vorhergesagt wird. Innerhalb von HFIT wird „Situationsbewusstsein“ in sieben Elemente unterteilt:

- Aufmerksamkeit („attention“): Ablenkung, Konzentrationsmangel, geteilte Aufmerksamkeit, fokussierte Aufmerksamkeit;
- Erkennung und Wahrnehmung („detection/perception“): ein Signal wird nicht erkannt; visuelle, verbale, taktile Fehlwahrnehmung;

- Gedächtnis („memory“): Schritt auslassen oder vergessen, nicht berücksichtigen von Faktoren;
- Interpretation („interpretation“): Missverstehen;
- Entscheiden („decision making“): falsche/unpassende/einseitige Entscheidung treffen;
- Annahme („assumption“): bezieht sich auf die Aufgabe, das Zubehör, Systeme, Prozeduren;
- Reaktion („response execution“): stereotypisch, motorisch variabel.

Die dritte Kategorie **Fehlerbehebung** („error recovery“) kann sowohl nach einem Handlungsfehler (erste Kategorie: „action error“) als auch während dem Prozess des Situationsbewusstseins (zweite Kategorie: „situation awareness“) auftreten. Es wird zwischen zwei Elementen der Fehlerbehebung unterschieden. Das erste ist die Verhaltensreaktion („behavioural response“), die sich auf den möglichen Prozess der Fehlerbehebung bezieht (Fehlerentdeckung, Fehlermeldung, Fehlerkorrektur). Das zweite Element, Merkmale der Fehlerentdeckung („detection cues“), bezieht sich darauf, wie der Fehler als solcher erkannt wird (internale Rückmeldung, Systemrückmeldung, externale Kommunikation und Planungsverhalten).

Situationen, die das Auftreten von Fehlern fördern könnten, werden als **Gefährdungen** („threats“) bezeichnet und stellen die vierte HFIT-Kategorie dar. Im Rahmen von HFIT werden 12 Gefährdungen genannt. Dazu zählen:

- Prozeduren („procedures“)
- Arbeitsvorbereitung („work preparation“)
- Arbeitsfaktoren („job factors“)
- personelle Faktoren („person factors“)
- Kompetenz und Training („competence and training“)
- Kommunikation („communication“)
- Teamarbeit („team work“)
- Supervision („supervision“)
- Organisations- und Sicherheitskultur („organisational and safety culture“)
- Arbeitsumwelt („work environment“)
- Systemschnittstelle („system-equipment interface“)
- Tools und Arbeitsgeräte („tools and equipment“).

Das DOD-HFACS beschreibt ebenfalls vier Ebenen von Fehlern oder Bedingungen: (1) Handlungen („acts“), (2) Voraussetzungen/Vorbedingungen („preconditions“), (3) Supervision („supervision“) und (4) organisationale Einflüsse („organizational influences“). Die Ebenen mit den dazugehörigen Kategorien

und Unterkategorien werden im Folgenden beschrieben, beginnend mit der Ebene, die dem Ereignis zeitlich am nächstens ist:

1. **Handlungen** sind die Faktoren, die eng mit dem Ereignis verbunden sind. Sie werden auch als aktive Fehler oder als unsichere oder fehlerhafte Handlungen des Operateurs bezeichnet. Bei aktiven Fehlern kann es sich entweder um Fehler („errors“) oder Verstöße („violations“) handeln. Fehler sind Handlungen des Operateurs, die das intendierte Ziel nicht erreichen. Sie werden nicht mit Absicht begangen. Es werden drei Fehlertypen unterschieden:

- Fertigkeitsbasierte Fehler („skill-based errors“) sind nicht beabsichtigte Verhaltensweisen und treten vor allem bei Routinehandlungen auf. Dazu zählen zum Beispiel: unachtsames Arbeiten („inadvertant operation“), Fehler der Checkliste („checklist error“), Über-/Untersteuerung („over-control/undercontrol“).
- Entscheidungs- und Beurteilungsfehler („judgement and decision making errors“) sind beabsichtigte Verhaltensweisen, wo der ausgewählte Handlungsplan nicht angemessen ist, um das angestrebte Ziel zu erreichen. Hier werden unter anderem eine falsche Priorisierung der Aufgabe („task misprioritization“), notwendige Handlungen werden zu schnell oder verspätet ausgeführt („necessary action – rushed/ delayed“), Warnung wird ignoriert („caution/warning-ignored“) genannt.
- Fehler aufgrund einer Sinnestäuschung („misperception errors“) von Objekten, Gefahren oder Situationen (visuell, auditiv, Illusion, Aufmerksamkeitsfehler etc.)

2. **Voraussetzungen/Vorbedingungen** für unsichere Handlungen oder menschliche Fehler sind gegeben, wenn bestimmte aktive oder latente Bedingungen der Umgebung, des Operateurs oder personelle Faktoren individuelle Handlungen beeinflussen. Als Voraussetzungen für unsichere Handlungen oder menschliche Fehler werden Umgebungsfaktoren („environmental factors“), individuelle Bedingungen („conditions of the individuals“) und personelle Faktoren („personnel factors“) genannt. Umgebungsfaktoren können in technische („technical environment“) und physikalische Faktoren („physical environment“) unterteilt werden.

   Unter individuellen Bedingungen werden kognitive Faktoren („cognitive factors“), psychische Verhaltensfaktoren („psycho-behavioral factors“), ungünstige physische Zustände („adverse physiological states“), mentale Begrenzungen („physical mental limitations“) oder Faktoren der Wahrnehmung („perceptual factors“) verstanden, die die individuelle Handlung negativ beeinflussen können.

Personelle Faktoren beziehen sich hauptsächlich auf die Koordination, Kommunikation und Planung („coordination, communication, planning“) zwischen Individuen, Crews und Teams sowie auf selbst auferlegte Stressoren („self-imposed stress“).

3. **Supervision** beinhaltet vier Kategorien im Hinblick auf eine unsichere Aufsicht/Überwachung:

- Unzureichende Aufsicht/Überwachung („inadequate supervision“) beinhaltet Faktoren wie unangemessene Führung/Überwachung/Aufsicht, keine Trainingsprogramme, mangelnde Rückmeldung, Aufsichtspolitik.
- Geplantes unangemessenes Arbeiten („planned inappropriate operations“) durch begrenzte Erfahrung, rein formale Risikobewertung, befugte unnötige Gefährdungen etc.
- Bekannte Probleme werden („failed to correct a known problem“) durch das Personalmanagement oder das operative Management nicht gelöst
- Verstöße seitens der Aufsicht („supervisory violations“) durch Allgemeingültigkeit, Zwangsdurchführung, allgemeine Politik, gezielter Verstoß (gegen Regeln, Instruktionen)

4. **Organisationale Einflüsse** sind latente Bedingungen, die sowohl die Supervision als auch die Handlungen des Operateurs direkt oder indirekt beeinflussen. Sie beinhalten:

- Ressourcen- oder Erfassungsmanagement („resource/acquisition management“) wie zum Beispiel Ressourcen der Flugsicherung, des Landeplatzes und des Personals, finanzielle Ressourcen, Hilfsmittel für den Operateur.
- Organisationsklima („organizational climate“) beinhaltet organisationale Werte/Kultur, organisationale Struktur, Wahrnehmung der Arbeitsmittel/ -unterlagen etc.
- Organisationsprozess („organizational process“) bezieht sich zum Beispiel auf das Arbeitstempo und die Arbeitsbelastung, Programme und politische Risikobewertung, verfahrensorientierte Publikationen/Leitlinien, Trainingsprogramme etc.

Insgesamt wurden sehr unterschiedliche Formulierungen und Kategorisierungen zur Ursachenbeschreibung von Störfällen gefunden, so dass es zum besseren Verständnis und zur klaren Abgrenzung zwischen den verschiedenen Begriffen sinnvoll erscheint, ein allgemein akzeptiertes Taxonomiemodell zu entwickeln. Dieses spiegelte sich auch in der Diskussion im Workshop wieder.

1.2.3 Menschliche Faktoren, Relevante Definitionen

Aufgrund der durchgeführten Analysen erscheint es sinnvoll, nachfolgend zwischen Definitionen für unterschiedliche Handlungszwecke wie die Beschreibung menschlicher Faktoren oder Fehler zu differenzieren.

1.2.3.1 Allgemeine Begriffsdefinitionen zum Thema „Menschliche Faktoren“

Menschliche Faktoren

“Menschliche Faktoren beziehen sich die Umgebungs-, organisatorische und Jobfaktoren und auf menschlichen und individuelle Eigenschaften, welche das Arbeitsverhalten so beeinflussen, dass es Gesundheit und Sicherheit herbeiführen kann“ /14/, S. 10 nach /15/.

„Der Begriff menschliches Verhalten wird oft in einem negativen Kontext verwendet (indem er mit menschlichem Fehlverhalten gleichgesetzt wird). Menschen sind jedoch oft das einzige Mittel, um wirksam auf außergewöhnliche Betriebszustände reagieren zu können, da die Menschen in der Lage sind logisch zu denken und sich über die automatischen Reaktionen von Maschinen hinwegzusetzen. Menschen sind auch in der Lage, Handlungen zu prognostizieren, komplexe und unscharfe Informationen zu integrieren und aufgrund von Erfahrung und Schulung zu wissen, wie mit ungewöhnlichen Zuständen umzugehen ist.“ /2/, S.55.

„Das menschliche Verhalten ist von Bedeutung für die Gestaltung von Maschinen, betrieblichen Prozessen und Arbeitsumgebungen in einer an die menschlichen Fähigkeiten, Grenzen und Bedürfnisse angepassten Weise (und geht daher über die Belange der Mensch-Maschine-Schnittstelle hinaus). Als Ausgangsbasis dienen die Beobachtungen der Menschen in ihrer Arbeitsumgebung (Bediener, Leitungskräfte, Wartungspersonal und andere) und die Untersuchung der Faktoren, die Menschen normalerweise in ihrem Verhältnis zu den technischen Einrichtungen beeinflussen (unter Einbeziehung des Individuums, der Organisation und der Technologie)“ /2/, S.180.

Menschliches Leistungsvermögen

„Alle Aspekte menschlichen Handelns, die für den sicheren Betrieb einer gefährlichen Anlage in allen anlagentechnischen Phasen von der Konzeption und Auslegung über den Betrieb, die Wartung/Instandhaltung, die Stilllegung und Schließung/Abfahren von Belang sind“ /2/, S.180.

1.2.3.2 Relevante Definitionen zum Fehlerbegriff

In den im Folgenden aufgeführten Dokumenten /2, 6, 13, 14, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 42, 43, 44, 45/ wurden verschiedene Definitionen zum Fehlerbegriff identifiziert. Die Definitionen sind sowohl relevant für Ereignisanalysen und Dokumentation als auch für die Themen des Workshops.

Fehler (error)

„Nicht-Übereinstimmung zwischen dem Ziel des Benutzers und der Reaktion des Systems. Fehler können unter anderem Navigationsfehler, Syntaxfehler, Interpretationsfehler usw. sein“ /16/, S.35.

Menschlicher Fehler (human error)

„Hierbei sollte anerkannt werden, dass Menschen gelegentlich versagen und dass die meisten Unfälle zu einem gewissen Teil menschlichem Fehlverhalten zuzuschreiben sind, das heißt menschlichen Handlungen oder Unterlassungen, die sich unabsichtlich Schwachpunkte in den Einrichtungen, Vorschriften und Systemen und/oder Organisationen zunutze machen” /2/, S. 55.

„Menschliches Fehlverhalten beschränkt sich nicht auf Bedienfehler, sondern kann an den verschiedenen Punkten in der Unternehmenshierarchie vorkommen, beispielsweise auch auf der Ebene der Verantwortlichen für die Wartung/ Instandhaltung, die sichere Durchführung von Änderungen oder Arbeitsgenehmigungen oder auf der Ebene der Ausführenden und der Leitung. Als Beispiele für menschliche Fehlhaltungen sind neben Bedienerfehlern folgende zu nennen: Probleme mit der Weitergabe von Wissen, insbesondere wenn erfahrene Fachleute in den Ruhestand gehen, die Komplexität des Systems einschließlich Verfahrensauslegung und Verfahrenstechnik, die Alterung von Anlagen und damit verbundene Reparaturen ohne ausreichende Wartung und Inspektion sowie der Notwendigkeit, mit organisatorischen und technischen Änderungen einschließlich Automation zurechtzukommen.“ /2/, S.134

„Menschliche Fehlhandlung = Arbeitsfehler = Fehlhandlung = Fehler. Jede menschliche Handlung, die die gesetzten Akzeptanzgrenzen überschreitet“ /17/, S.3.

„Handlung oder Unterlassung eines Menschen, die zu einem unerwünschten Ergebnis führt“ /18/, S.18.

Menschliches Versagen und menschlicher Fehler (human failure and human error)

„Ein menschlicher Fehler ist eine unbeabsichtigte Handlung oder eine Entscheidung, die eine Abweichung von einem geltenden Standard enthält und zu einem nicht erwünschten Ergebnis führt. Menschlicher Ausfall bezieht sich auf

Fehler und auf Verstöße (d.h. Zuwiderhandlung gegen Richtlinien oder Verfahren)“ /14/, S. 83.

Menschliches Versagen (human failure)

„[…] bezieht sich auf Fehler von denjenigen am Ende der Unfallverursachung, die direkt den Unfall ausgelöst haben“, /19/, S. 9. Laut der Definition der HSE /14/ ist es „wichtig zu bedenken, dass menschliche Fehler kein Zufallsprodukt sind, sondern dass es Muster gibt“, S.10.

Es gibt drei unterschiedliche Arten unsicherer Handlungen die zu großen Störfällen führen können /14/, S.11:

1. **Unbeabsichtigte Fehler (unintentional errors):** Fehler (Schnitzer / Versehen) sind „Handlungen, die nicht geplant abliefen (nicht intendierte Handlungen). Diese können bei bekannten Aufgaben geschehen, z.B. Auslassungen, vergessen, etwas zu tun, besonders relevant sind diese für Reparatur, Wartung, Kalibrierung oder Prüfung. Es ist unwahrscheinlich, dass sie durch Training eliminiert werden können und sie müssen daher durch Designlösungen verhindert werden.
2. **Irrtümer (mistakes)** sind auch Fehler, aber Fehler in der Beurteilung oder bei der Entscheidung (absichtliche Handlungen sind falsch) –wir machen etwas falsches, aber denken, dass es richtig. Das kann in Situationen der Fall sein, wo das Verhalten auf erinnerten Regeln oder vertrauten Prozeduren beruht oder in unbekannten Situationen, in denen Entscheidungen nach dem erstbesten Prinzip getroffen werden und zu Fehldiagnosen und Fehlkalkulationen führen. Training ist der Schlüssel zum Vermeiden von Irrtümern.“
3. **Absichtliche Fehler (intentional errors): Verstöße (violations)** unterscheiden sich von den oben genannten Fehlern, da sie mit Absicht begangen werden (aber oft wohlmeinend) wie beispielsweise eine Abkürzung nehmen oder das Nichtbefolgen von Prozeduren wie eine absichtliche Abweichung von einer Regel oder Prozedur. Verstöße sind selten vorsätzlich (z. B. Sabotage) und entspringen meistens der Absicht, die Arbeitsaufgabe zu erfüllen, trotz der Konsequenzen. Verstöße können situationsabhängig, regelmäßig, ungewöhnlich oder böswillig sein.

Weitere Fehlerdefinitionen sind:

„… ein absichtlicher Bruch von Richtlinien und von Verfahren“ /20/, S. 3.

„… ein Fehler, der auftritt, wenn Handlungen ergriffen werden, die bekannten funktionsfähigen Richtlinien, Beschränkungen und/oder Verfahren zuwiderlaufen. Die Definition von Verstößen schließt die Handlungen aus, die ergriffen werden, um das System absichtlich zu schädigen, d.h. Sabotage“ /14/, S. 83.

In der Literatur existieren verschiedene Definitionen von menschlichen Fehlern, wie die folgenden Beispiele zeigen:

Nach Hollnagel (2005) besteht das grundlegende semantische Problem darin, „dass die Bezeichnung menschlicher Fehler mindestens drei unterschiedliche Bedeutungen hat, so kann sie entweder die *Ursache* von etwas, das *Ereignis* selbst (die Handlung) oder das Resultat der Handlung bedeuten“ /21/, S.1:

„Menschlicher Fehler als Ursache“: „Das Überlaufen des Öls wurde durch einen menschlichen Fehler verursacht“. Hier ist der Fokus auf der Handlung (der „menschliche Fehler“) als angebliche Ursache des beobachteten Resultates (das Überlaufen des Öls).

„Menschlicher Fehler als Ereignis oder Handlung“: „Ich vergaß, das Wasserniveau zu überprüfen“. Hier ist der Fokus auf der Handlung oder dem Prozess selbst, während das Resultat oder die Konsequenz nicht betrachtet wird.

„Menschlicher Fehler als Folge“: „Ich machte den Fehler, Salz in den Kaffee zu tun“. Hier ist der Fokus auf dem Resultat, obgleich es eine linguistische Beschreibung der Handlung ist. [...] Ein korrekteres Beispiel ist der Gebrauch der Bezeichnung „latenter menschlicher Fehler“. Dieses beinhaltet fälschlicherweise, dass ein oder mehrere „menschliche Fehler“ irgendwo im System versteckt sind und sich noch zeigen müssen. Die beabsichtigte Bedeutung geht eher dahin, dass das System eine oder mehrere latente Konsequenzen eines „menschlichen Fehlers“ versteckt, die bereits aufgetreten sind.“ /21/, S.1. „In der Industrie werden normalerweise nur die Fehler als Fehler bezeichnet, die nicht akzeptable Konsequenzen haben (d.h. außerhalb des Feldes der Sicherheitsoperationen, wie durch Verfahren, Anweisungen und Sicherheitsanalysen definiert). Andererseits definieren Psychologen Fehler als eine fehlerhafte Handlung, was auch immer ihre Konsequenzen oder ihr Niveau, auf dem es ermittelt und wiederhergestellt wird, ist.“ /22/, S.112.

„Rasmussen, Duncan und Leplat (1987) definierten menschliche Fehler als Handlung, die in Bezug auf die (privaten oder subjektiven) Absichten oder Ziele der Person unproduktiv ist. Eine Expertengruppe der OECD definierte dagegen menschliche Fehler als Verhalten oder seine Auswirkungen, die ein System dazu führen, vorgegebene Begrenzungen (Nicolet, 1987) zu übersteigen. Für Mashour (1974) ist ein Fehler die Abweichung der aktuellen Ist-Leistung von der gewünschten Leistung des Kriteriums. Kruglanski und Ajzen (1983) beschreiben Fehler als Art der Erfahrung einer Person, die aufgrund einer erlebten Inkonsistenz zwischen einer vorhandenen Hypothese, Zusammenfassung oder Schlussfolgerung und einem festen Glauben.” /23/, S.420f.

Nach Leplat sind menschliche Fehler „ein Muster menschlicher *Aktivität:* sie beschreiben die Art der Aktivität, die das kontrollierte System verursachen, von seinem Toleranzspielraum abzuweichen. […]. Menschlicher Fehler ist ein ambi-

ger Ausdruck, der nicht zwangsläufig zu einer unikausalen Konzeption des Fehlers führen muss, sondern die Suche nach multiplen Bestimmungsfaktoren für seine Entstehung anregen sollte. Das Ziel einer Analyse menschlicher Fehler sollte die Identifikation dieser Bestimmungsfaktoren sein." /24/, S.126.

Rasmussen fragt sich, wie Störungen und Fehler definiert sind. „Im Allgemeinen werden sie als Ursachen eines nicht erreichten Zwecks angesehen. [...] Menschliche Fehler können mit zeitweiligen Störungen in einem elektronischen System verglichen werden. Nach solchen Störungen hält man häufig an der deterministischen Erklärung fest und sucht nach externen Ursachen wie eine Impulsstörung" /25/, S.98f. Rauterberg geht davon aus, wenn „ein System weniger leistet als normalerweise – weil ein Mensch handelt – wird als *Ursache* sehr wahrscheinlich ein menschlicher Fehler ermittelt" /26/, S.827.

Duffey und Saull „definieren einen Fehler als die integrierte unbeabsichtigte Ursache eines Unfalles, einer Verletzung oder eines Todes, ob es vielfältige Mitwirkungen, Systeme, Fehlerarten oder betroffene Personen gibt oder nicht" /27/, S.279.

Nach Zapf et al. gibt es „drei Elemente einer handlungstheoretisch basierten Definition eines Fehlers: (a) Fehler treten nur bei zielor*ientierten Handlungen* auf; (b) ein Fehler bedeutet die *Nichterreichung* eines Ziels; (c) ein Fehler sollte möglichst vermeidbar gewesen sein" /28/, S. 313f. Ähnlich definieren Shaban, Smith und Cumming einen Fehler als „Störung geplanter Handlungen, die ausgeführt werden, um ein gewünschtes Ziel zu erreichen [...]"/29/, S.4 nach /13/ definiert. Für Shappell und Wiegmann dagegen stellen Fehler „geistige oder körperliche *Handlungen* von Personen, die ihr beabsichtigtes Ergebnis nicht erzielen können, dar" /30/, S.1.

Helmreich weitet das Fehlerverständnis aus: [...] „Fehler kann als *Handeln* oder *Nichthandeln* definiert werden, der zur Abweichung von gruppenspezifischen oder organisatorischen Interventionen führt" /31/, S 781.

Aus dem Kontext von Flugmanagement in der Flugsicherung definiert Bove wie folgt: „Jede mögliche Handlung (oder Unterlassen einer Handlung), die möglicherweise oder tatsächlich zu negativen Systemeffekten führt, obwohl in der Situation andere Möglichkeiten vorhanden waren. Dieses schließt jede mögliche Abweichung von Betriebsverfahren, von guten Arbeitsweisen oder Absichten ein. Diese Definition hat einigen Nutzen. Zuerst ist die Definition des menschlichen Fehlers hinsichtlich jeder möglichen Frage der Schuld neutral. Zweitens braucht ein Fehler keine Systemkonsequenzen mit einzubeziehen. Dieses steht in Übereinstimmung mit der Grundregel, dass ein Fehler auf der Grundlage der zugrundeliegenden Prozesse und nicht auf das Produkt hin beurteilt werden sollte. Drittens kann eine Handlung oder ein Unterlassen einer Handlung nur als Fehler bezeichnet werden, wenn keine andere Alternative

vorhanden war. Schließlich erkennt die Definition unterschiedliche Kriterien oder Standards, mit denen die Leistung verglichen werden kann an, nämlich die Betriebsverfahren, gute Arbeitsweisen oder einfach die Absichten des Handelnden“ /32/, S.22. Yemelyanov definiert hinsichtlich der Schuldfrage ähnlich: „Der menschliche Fehler wird hier als jede mögliche Handlung oder Störung der Handlung des Menschen bei seiner Tätigkeit, die selbstverständliche Normen oder annehmbare Grenzen des Verhaltens verletzt (Kotik und Yemelyanov, 1985; Miller und Swain, 1986), betrachtet. Der Begriff des Fehlers ist nicht notwendigerweise mit Schuld, den Konsequenzen des Fehlers oder dem Vorhandensein oder dem Fehlen einer Absicht verbunden“/33/, S.2437.

Nach Klumb werden Fehler „als Phänomene betrachtet, die eng mit der korrekten *Durchführung* der jeweiligen *Tätigkeit* zusammenhängen, d. h. die zwei sind wie zwei Seiten einer Münze verbunden (z. B., Reason, 1979; Fromkin, 1980; Wehner u. Stadler, im Druck). Als Folge, und im Gegensatz zu anderen Disziplinen wie der Technik, geht die psychologische Fehlerforschung mit beidem um, der Beschreibung und der Ursachenanalyse von Fehlern, mit deren Phänotypen und Genotypen (cf. Becker et al., 1994)“ /34/, S. 3.

Das U.S. Department of Labor fokussiert dagegen die *Konsequenzen* und definiert „[...] jede menschliche Handlung, die irgendeine Grenze der Annehmbarkeit übersteigt (d.h. eine Handlung außerhalb der Toleranzen), die durch das System als menschliche Leistungsgrenze definiert werden“ /35/.

Im Gegensatz zur vorherigen Definition sieht Singleton den Fehler als *Regelverstoß* an: „[...] Fehler sind mit Zielen und Zwecken verbunden. Ein Individuum zielt immer in Richtung auf ein Ziel, hat es aber noch nicht erreicht. Sobald es ein Ziel erreicht hat, richtet es seine Aufmerksamkeit auf ein anderes, wodurch es den Fehlerzustand willentlich fortführt oder ihn neu herstellt. [...] ein Fehler kann als *Übertretung einer Regel* definiert werden“ /36/, S.727.

An anderer Stelle geht Rasmussen auf die Fehleridentifikation ein. „Fehler werden im Allgemeinen als menschliche *Handlungen* definiert, die von jemand beurteilt werden, ob sie von einer Referenzhandlung abweichen. Diese Referenz ist jedoch nicht beständig, sondern hängt von den Umständen der Beurteilung ab [...]. Infolgedessen hängt die Wahrnehmung einer Handlung als Fehler von der Identität des Beurteilers und des Zeitpunktes der Beurteilung ab. Somit ist das Konzept des ’menschlichen Fehlers’ eines, das annimmt, er sei subjektiv und schwanke mit der Zeit. Zusätzlich scheint sich die Definition des Fehlers mit der Art der Arbeitsumgebung bewusst zu ändern.“ /37/, S.1

Moore und Abu-Khader definieren auch eher hinsichtlich der *Konsequenz*: „Das Abweichen von annehmbarer oder wünschenswerter Praxis von Seiten einer Person, dass zu nicht annehmbaren oder nicht wünschenswerten Resultaten führt“ /38/, S. 538; /39/, S. 432.

Leplat und Rasmussen gehen in einer gemeinsamen Veröffentlichung davon aus, dass „[...] menschliche Fehler Umstände einer Mensch-Maschine-*Fehlanpassung* sind, d.h. Umstände, bei denen die menschliche Veränderlichkeit nicht innerhalb der akzeptablen Spannweite für eine erfolgreiche Aufgabenerfüllung ist. Schwankungen der Leistung werden nur zu menschlichen Fehlern in einer ‚unfreundlichen' Umgebung, die keine augenblickliche Korrektur zulässt. Dies heißt, dass zur Kennzeichnung menschlicher Fehler, die Veränderlichkeit des menschlichen Verhaltens berücksichtigt und die dabei akzeptierten Grenzen für Veränderungen in der Arbeitssituation festgestellt werden müssen. Im Allgemeinen werden menschliche Fehler im Sinne von fehlerhaften, externen Aufgabenelementen definiert und entsprechende Daten werden gesammelt" /40/, S. 82.

Viel weiter gehend wird auf einer Konferenz festgestellt, dass „[...] jede mögliche Störung in einem System als menschlicher Fehler gesehen werden" /45 /, S.10.

Zum besseren Verständnis und zur klareren Abgrenzung der mehrdeutigen Begriffsvielfalt von Human Error und menschlichen oder organisationalen Faktoren erscheint es sinnvoll, die entsprechenden Definitionen folgenden Aspekten zuzuordnen: Aufgabe, Handlung, Konsequenzen, Organisation.

1. Aufgabenbezogene Definitionen

Auslassung (omission): „Fehler überhaupt zu handeln", „was nicht getan wurde", „Fehler das Richtige zu tun" /23/, S. 419; /42/, S. 126; /43/ zitiert nach /13/.

Handlungsfehler: „korrekte Funktion zur falschen Zeit", „was getan wurde", „etwas falsches tun" /23/, S. 419; /42/, S. 126; /43/ zitiert nach /13/.

2. Handlungsbezogene Definitionen

verwendete Begriffe: Schnitzer (slips),Versehen (lapses), Irrtum (mistakes)

„Fehler als Verfehlung des gewünschten Ziels bei geplanten Handlungen" /6/, S.71

„Der Plan ist adäquat, aber die Handlung läuft nicht wie geplant" /6/, S. 71.

„Die Handlungen können exakt mit dem Plan übereinstimmen, aber der Plan ist ungeeignet, um das gewünschte Ziel zu erreichen" /6/, S. 71.

3. Auf Konsequenzen bezogene Definitionen

Regelabweichung (violation): „Abweichung von sicherer Handlungspraxis" /29/, S.6 nach /13/.

„Der Fehler eine gute Regel anzuwenden" /29/, S.6 zitiert nach /13/.

„Fehlanpassung (mistake): Fehler, die als Eintritt von Mensch-Aufgaben-Fehlanpassung gesehen werden" /44/, S.11.

4. Auf organisationale Aspekte bezogene Definitionen

verwendete Begriffe: latente Fehler (latent failures), verhaltensbeeinflussende Faktoren (performance shaping factors; PSFs), generelle Fehlertypen (general failure types)

Reason unterscheidet Fehler hinsichtlich ihres Ursprungs: aktiv oder latent. „Aktive Fehler entstehen an der Stelle, an der es einen Kontaktpunkt zwischen dem Menschen und Aspekten des Systems (Mensch-Maschine-Schnittstelle) gibt. Normalerweise sind sie offensichtlich (Drücken eines falschen Knopfes, Ignorieren eines Warnlichts) und irgendjemand an vorderster Stelle ist involviert. Latente Fehler oder Bedingungen, im Gegensatz dazu, beziehen sich auf weniger offensichtliche Fehler in der Organisation oder im Design, die die Fehlerentstehung fördern“ /43/ zitiert nach /13/.

„Unsichere Handlungen und Situation treten nicht einfach ein. Sie werden von Mechanismen generiert, die in der Organisation vorhanden sind…. Manchmal resultieren diese Mechanismen aus Entscheidungen, die an der Organisationsspitze getroffen wurden und so viele unsichere Handlungen verursachen. … Diese Mechanismen werden generelle Fehlertypen (GFTs) genannt“ /45/, S. 151.

Bei der Identifikation des unterschiedlichen menschlichen Beitrags auf verschiedenen Ebenen in Bereichen mit hohem Gefährdungspotential (z. B. Design, Konstruktion, Anfahren, Prozess, Umgang, Aufbewahrung, Herunterfahren, etc.) erscheint es sinnvoll, eine empirisch belegte Klassifikation zu verwenden, z. B. das bereits erwähnte GFT-Modell /45/:

- Hardwareschwächen
- ungeeignetes Design
- schlechtes Wartungsmanagement
- schlechte Betriebsprozeduren
- fehlerfördernde Bedingungen
- schlechte Haushaltung
- unvereinbare Ziele
- Kommunikationsfehler organisationale Fehler
- inadäquates Training
- inadäquate Sicherheitseinrichtungen

Diese Zusammenstellung und Strukturierung soll zur weiteren Harmonisierung der Terminologien und Definitionen bei der Analyse und Dokumentation von Beinahe- bzw. Ereignissen in der verfahrenstechnischen Industrie beitragen sowie zur Verbesserung der Kommunikation zwischen allen Beteiligten verwendet werden.

1.2.4 Für ein Taxonomiemodell relevante Definitionen

Die nachfolgend, in der Literatur /2, 13, 14, 16, 17, 19, 23, 42, 43, 49, 50, 51/aufgeführten Definitionen sind relevant für Ereignisanalysen und Dokumentation sowie für Taxonomiemodelle.

1. **Handlungsfehler (error of commission)**

Handlungsfehler sind Fehler überhaupt zu handeln („failure to act at all“) oder etwas nicht zu tun („what is not done”), oder das Richtige zu tun („failing to do the right thing”) /23/, p. 421; /42/, p. 126; /43/ zitiert nach /13/.

2. **Gedächtnisfehler (error of omission)**

Gedächtnisfehler sind eine richtige Handlung zur falschen Zeit auszuführen („the correct function at the wrong time“) oder Fehler etwas zu tun („what is done”), oder etwas falsch zu machen („doing something wrong”) /23/, S. 421; /42/, S. 126; /43/ zitiert nach /13/.

3. **Menschliche Fehler (human error)**

„Hierbei sollte anerkannt werden, dass Menschen gelegentlich versagen und dass die meisten Unfälle zu einem gewissen Teil menschlichem Fehlverhalten zuzuschreiben sind, das heißt menschlichen Handlungen oder Unterlassungen, die sich unabsichtlich Schwachpunkte in den Einrichtungen, Vorschriften und Systemen und/oder Organisationen zunutze machen“ /2/, S. 55.

4. **Unbeabsichtigte Fehler (unintentional errors):**

Fehler (**Schnitzer / Versehen**) sind „Handlungen, die nicht geplant abliefen (nicht intendierte Handlungen). Diese können bei bekannten Aufgaben geschehen, z. B. Auslassungen, vergessen, etwas zu tun, besonders relevant sind diese für Reparatur, Wartung, Kalibrierung oder Prüfung. Es ist unwahrscheinlich, dass sie durch Training eliminiert werden können und müssen daher durch Designlösungen verhindert werden.“ /14/, S. 11

„**Irrtümer** sind auch Fehler, aber Fehler in der Beurteilung oder bei der Entscheidung (absichtliche Handlungen sind falsch) – wir machen etwas Falsches, aber denken es ist richtig. Das kann in Situationen der Fall sein, wo das Verhalten auf erinnerten Regeln oder vertrauten Prozeduren beruht oder in unbekannten Situationen, in denen Entscheidungen nach dem erstbesten Prinzip getroffen werden und zu Fehldiagnosen und Fehlkalkulationen führen. Training ist der Schlüssel zum Vermeiden von Irrtümern.“ /14/, S. 11

5. **Beabsichtigte Fehler (intentional errors):**

„**Verstöße** unterscheiden sich von den oben genannten Fehlern, da sie mit Absicht begangen werden (aber oft wohlmeinend) wie beispielsweise eine Abkürzung nehmen oder das Nichtbefolgen von Prozeduren wie eine absichtliche

Abweichung von einer Regel oder Prozedur. Verstöße sind selten vorsätzlich (z. B. Sabotage) und entspringen meistens der Absicht, die Arbeitsaufgabe zu erfüllen, trotz der Konsequenzen. Verstöße können situationsabhängig, regelmäßig, ungewöhnlich oder böswillig sein.“ /14/, S. 11

6. Aktiver Fehler (active failures)

bezieht sich auf menschliche Fehler oder menschliches Versagen:

menschlicher Fehler/Ausfall: „[...] aktive Ausfälle entstehen an vorderster Stelle der Ereignisverursachung, z. B. bei den Operateuren, dem Instandhaltungspersonal, dem Piloten […]. Die Ausfälle, die an vorderster Stelle verursacht werden, führen im Allgemeinen zu direkten Konsequenzen und derjenige, der der den Ausfall verursacht hat, spürt folglich auch die Konsequenzen“ /19/, S.11, zitiert nach /13/.

7. Latente Fehler (latent failure)

bezieht sich hauptsächlich auf organisationale Fehler: „latente Ausfälle werden an anderer Stelle von denen verursacht, deren Tätigkeiten von Zeit und Raum und von der vordersten Stelle der Ereignisverursachung abgetrennt sind (z. B. Entscheider auf hohen Entscheidungsebenen, Designern, …). Diese latenten Fehler verursachen die Bedingungen, damit aktive Fehler gemacht können.“ /19/, S.11 zitiert nach /13/

8. Organisationskultur

„Kultur ist ein Muster gemeinsamer Grundannahmen, das die Gruppe bei der Bewältigung ihrer Probleme externer Anpassung und interner Integration erlernt hat, das sich bewährt hat und somit als bindend gilt, und das daher an Mitglieder als rational und emotional korrekter Ansatz für den Umgang mit diesen Problemen weitergegeben wird.“ /49/, S. 9

9. Qualifikation/ Eignung

„Das Vorhandensein körperlicher, geistiger und charakterlicher Befähigung für Arbeiten mit bestimmten Anforderungen. Wesentlich ist dazu der Besitz von Fähigkeiten (physisch und psychisch) und Fertigkeiten (erlernte und eingeübte Verhaltensweisen), um sich anforderungsgerecht verhalten zu können“ /17/, S. 4.

10. Sicherheitskultur

Sicherheitskultur ist auch eine Mischung von Werten, Einstellungen, von moralischen Prinzipien und Normen zu akzeptablem Verhalten. Diese zielen darauf ab, eine selbstdisziplinierte Vorgehensweise aufrecht zu erhalten, um Sicherheit über rechtliche und regulatorische Anforderungen hinaus zu erhöhen. Sicherheitskultur muss daher im Denken und Handeln aller Individuen auf allen Ebenen einer Organisation inhärent sein. Die Führung durch das Topmanagement

ist entscheidend. Sicherheitskultur gilt für konventionelle und Personen- sowie für kerntechnische Sicherheit. Alle Sicherheitsüberlegungen werden durch gemeinsame Annahmen, Einstellungen, Verhalten beeinflusst und kulturelle Unterschiede sind eng verknüpft mit einem geteilten Werte- und Standardsystem. /50/ S. 3

11. Sicherheitsklima

„Die Einstellungen und Wahrnehmungen der Mitarbeiter zu einem definierten Zeitpunkt. Es ist ein Schnappschuss des Sicherheitsstatus und kann als Indikator für die zu Grunde liegende Sicherheitskultur einer Organisation gesehen werden“ /51/, S.1.

12. Training

„Organisierte Ausbildung, die zielgerichtet auf Steigerung und Aufrechterhaltung der physischen und psychischen Leistungsfähigkeit des Menschen ausgerichtet ist“ /17/, S.4.

13. Belastung/ Arbeitsbelastung

„Die Gesamtheit der äußeren Bedingungen und Anforderungen im Arbeitssystem, die den physischen und/oder psychischen Zustand einer Person ändern kann“ /17/, S. 2f.

14. Arbeitsbelastung/ äußere Einwirkung

„Gesamtheit der äußeren Bedingungen und Anforderungen im Arbeitssystem, die auf den physiologischen und/oder psychologischen Zustand einer Person einwirken“ /16/, S.116.

1.3 Relevante Begriffe für die weiteren Themen des OECD/CCA-Workshops

Zur Förderung der internationalen und interdisziplinären Diskussionen der weiteren Themen des Workshops war ebenfalls zu prüfen, welche bereits vorhandenen Definitionen in Regelwerken und Literatur für die Kommunikation und Formulierung von Ergebnissen genutzt werden könnten.

Folgende Definitionen konnten als relevant für die weiteren Themen des Workshops identifiziert werden:

15. Alarm

„Meldung, die eine unverzügliche Reaktion des Operators erfordert. Reaktion kann dabei z.B. ein Bedieneingriff, erhöhte Aufmerksamkeit oder das Veranlassen weiterer Untersuchungen bedeuten. *Hinweis: Dies ist ein gegenüber der VDI/VDE 3699 erweiterter Alarmbegriff, der dem gängigen Sprachgebrauch im*

Bereich der Prozessleitsysteme und der Begriffsverwendung in der englischen Sprache folgt.“ /46/, S. 6.

16. Alarmschauer/Alarmflut

„Situation, in der Alarme schneller eintreffen, als sie vom Operator wahrgenommen und bearbeitet werden können“ /46/, S.6.

17. Alarmmanagement

„Ein Alarmmanagement unterstützt den Operator bei der Vermeidung und Beherrschung abnormaler Zustände“ /46/, S.6.

18. Alarmpriorität

„Einteilung von Alarmen nach Wichtigkeit (z.B. Schwere der Auswirkung) und Dringlichkeit“ /46/, S.6.

19. Alarmrate

„Anzahl der auftretenden Alarme pro Zeiteinheit“ /46/, S.6.

20. Verhalten

„**fertigkeitsbasiertes Verhalten:** Verhalten bei oft ausgeübten Aufgaben. Ein geringer Grad von bewusster Denktätigkeit ist erforderlich.

regelbasiertes Verhalten: Verhalten bei meist weniger vertrauten Aufgaben, die auf der normalen Erfahrung und Fähigkeit des Betreffenden basieren. Das Verhalten resultiert aus dem Vergleich der Informationen mit vertrauten Mustern oder Regeln auf einer wenn-dann-Basis.

wissensbasiertes Verhalten: Verhalten bei meist neuen Aufgaben, bei denen vertraute Muster und Regeln nicht direkt angewendet werden können. Ein hoher Grad von bewusster Denktätigkeit ist erforderlich.“ /17/, S. 4f

21. Kritischer Alarm

„Sicherheitskritische Alarme unterscheiden sich von Betriebsalarmen. Für kritische Alarme wird die erwartete Operateurreaktion dokumentiert. Der Status aller kritischen Alarme ist immer sichtbar. Kritische Alarme werden mit anlagendefinierten Häufigkeiten überprüft“ /47/, S. 217.

22. Menschliche Zuverlässigkeit

bezieht sich auf die Abwesenheit von menschlichen Fehlern: „Die Fähigkeit des Menschen, eine Aufgabe unter vorgegebenen Bedingungen für ein gegebenes Zeitintervall im Akzeptanzbereich durchzuführen“ /17/, S. 4.

23. Ergonomie

„Das Teilgebiet der Arbeitswissenschaft zur menschengerechten Gestaltung der Arbeitsbedingungen. Die Disziplin, die sich mit dem Entwurf von Maschinen, Bedienungen und Arbeitsumgebungen befasst, so dass sie menschlichen Fähigkeiten und Grenzen entsprechen“ /17/, S. 3.

24. Mensch-Maschine-Systeme (MMS)

„Das Zusammenwirken und die Gesamtheit der Wechselbeziehungen zwischen Mensch und Betriebsmitteln bei der Arbeit“ /17/, S. 3.

25. Meldung

„Anzeige oder Bericht vom Eintreten eines Ereignisses, d.h. vom Übergang aus einem diskreten Zustand in einen anderen (nach VDI/VDE 3699). Hinweis: Der Begriff Meldungen wird in der Literatur sowohl als Oberbegriff als auch als Unterbegriff verwendet. Im vorliegenden Arbeitsblatt wird der Begriff genau für die Meldungen verwendet, die keine unverzügliche Reaktion des Operators erfordern.“ /46/, S. 7

26. Leistungsbeeinflussende Faktoren

„Bei der Modellierung des menschlichen Verhaltens für die probabilistische Risikoanalyse ist es notwendig, diejenigen Faktoren zu bedenken, die den höchsten Effekt auf die Leistung haben. Einige dieser verhaltensbeeinflussenden Faktoren (PSF) sind außerhalb der Person, andere innerhalb angesiedelt. Die externalen PSF beinhalten die gesamte Arbeitsumgebung, besonders die Gestaltung der technischen Ausstattung sowie die schriftlichen Prozeduren und mündlichen Anweisungen. Die internalen PSF repräsentieren die individuellen Charakteristika der Person - ihre Fähigkeiten und Fertigkeiten, ihre Motivation und ihre Erwartungen – die ihr Verhalten beeinflussen.“ /48/, S. 2-5.

27. Sicherheitsfunktion

„Funktion, die von einem SIS (safety instrumented system/ sicherheitstechnisches System), einem sicherheitsbezogenen System anderer Technologie oder von externen Einrichtungen zur Risikominderung ausgeführt wird, mit dem Ziel, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für den Prozess zu erreichen oder aufrecht zu erhalten. Anmerkung: Diese Definition weicht wegen in der Prozessindustrie vorhandener Unterschiede in der Terminologie von der Definition in DIN EN 61508-4 ab.“ /18/, S. 24

28. Sicherheitstechnisches System (SIS)

„Sicherheitstechnisches System zur Ausführung einer oder mehrerer sicherheitstechnischer Funktionen. Ein SIS besteht aus Sensor(en), Logiksystem und Aktoren(n).“ /18/, S. 25

29. Sicherheitslebenszyklus

„Notwendige Tätigkeiten im Rahmen der Realisierung von sicherheitstechnischen Funktionen während eines Zeitraumes, der mit der Konzeptphase eines Projektes beginnt und endet, wenn alle sicherheitstechnischen Funktionen nicht mehr für die Verwendung verfügbar sind“ /18/, S.26.

30. Aufgabenanalyse

„Analytischer Prozess, angewendet zur Bestimmung der Anforderungen an das spezifische Verhalten von Personen bei der Benutzung von Arbeitsmitteln oder bei der Verrichtung der Arbeit (ISO 9241-5:1998)“ /16/, S. 102.

1.4 Diskussion auf dem Workshop

Insgesamt wurden sehr unterschiedliche Formulierungen und Kategorisierungen zur Beschreibung von Ereignisursachen gefunden, so dass es zum besseren Verständnis und zur klaren Abgrenzung zwischen den verschiedenen Begriffen sinnvoll erscheint, ein allgemein akzeptiertes Taxonomiemodell zu entwickeln. Dieses spiegelte sich auch in der Diskussion und der daran anschließenden Abstimmung zwischen den Beteiligten des Workshops wider, so dass der Schwerpunkt der Schlussfolgerungen ebenfalls auf der Entwicklung einer Taxonomie zur Klassifikation von menschlichen und organisationalen Faktoren liegt:

- Relevante Begriffe in Bezug auf menschliche und organisationale Faktoren müssen für die Ereignisuntersuchung und –dokumentation innerhalb eines Taxonomiemodells definiert werden. Das Ziel sollte es sein, von den Ereignissen etwas über relevante menschliche Fehlerarten zu erlernen und die Implementierung adäquater Präventionsmaßnahmen zu unterstützen.
- Die Analyse von Daten bezüglich des Beitrags von menschlichen und organisationalen Faktoren zu Unfallszenarien ist für Experten interessant, wird aber ebenfalls von der Führungsebene von Unternehmen und Behörden, die Entscheidungen zur Sicherheitspolitik und zu verfügbaren Ressourcen trifft, verlangt. Folglich sollte die Taxonomie für den Endbenutzer verständlich sein. Jedoch muss eine zu starke Vereinfachung vermieden werden. Es ist notwendig, eine wohlüberlegte Wahl zwischen den folgenden Eigenschaften zu treffen: allgemein, einfach oder genau. Dabei sollte berücksichtigt werden, dass nur zwei aus drei dieser Eigenschaften gleichzeitig erreicht werden können.
- Die MARS-Datenbasis /7/ muss bezüglich menschlicher und organisationaler Faktoren weiterentwickelt werden. Dazu ist weitere Arbeit empfehlenswert.

Darüber hinaus wurden folgende Empfehlungen im Rahmen der Diskussion formuliert:

- Ein zweistufiger Ansatz wird empfohlen: Zunächst sollte eine Analyse vor Ort durchgeführt werden. Des Weiteren sollte es Experten geben, die den Austausch der „gelernten Lektionen“ und der Ereignisgeschichte sicherstellen. Es wird empfohlen, mit einem einfachen Taxonomiemodell zu beginnen, welches später präzisiert und im Detail weiter entwickelt werden könnte.
- Modelle zur Klassifikation von „Human Factors“ sollten zwischen individuellen und organisationalen Faktoren unterscheiden. Korrektive Maßnahmen sollten diese Begriffe separat ansprechen und die Wirksamkeit unterschiedlich, auch unter der Lebensdauerperspektive (Design, Errichtung, Betrieb, Wartung), sicherstellen.
- Ein spezielles Training wird für die, die Ereignisse analysieren und die Taxonomie anwenden, empfohlen. Zur Anwendung der Taxonomie sollten die Vorgehensweisen bei der Ereignisanalyse exakt beschrieben werden, um eine Angemessenheit sicherzustellen. Um diese zu erzielen, müssen die Vorgehensweisen genau, vollständig und im Ansatz sowie der Form konsistent sein.

1.5 Zusammenfassung und Fazit

Insgesamt kann festgehalten werden, dass es eine Vielzahl von Definitionen der Begriffe menschlicher Fehler sowie menschlicher und organisationaler Faktoren gibt. Diese unterscheiden sich in Bezug auf ihren Umfang, ihren Detailliertheitsgrad und ihr zugrunde liegendes Verständnis. Ein weiterer Unterschied besteht im Inhalt der Definitionen, einige beziehen sich auf Handlungsfehler des ausführenden Personals, andere beziehen Entscheidungsfehler beispielsweise des Managements mit ein. Eine Auswahl erscheint sehr schwierig und könnte nur mit Hilfe eines allgemein akzeptierten Taxonomiemodells hinreichend begründet werden. Es bestehen erste Ansätze für solche Taxonomien wie beispielsweise von Groeneweg /45/ oder Gordon, Flin und Mearns /55/. Die Verfasser dieses Berichts gehen in Übereinstimmung mit dem HSL /52/ und dem HSE /53/ davon aus, dass für eine zufriedenstellende Analyse von Ereignissen und deren Dokumentation ein Modell notwendig ist, das eine Klassifikation von aktiven Fehlern, also Fehlern des Bedienpersonals, und ebenfalls eine Klassifikation von latenten Fehlern, also Fehlern, die auf Organisationsebene entstehen, zulässt.

Ein solches Modell sollte jedoch von den Institutionen entwickelt werden, die für die jeweiligen Ereignisdatenbanken zuständig sind. Wünschenswert wäre, wenn die verschiedenen Institutionen sich auf ein gemeinsames Taxonomiemodell verständigen könnten, so dass die Ergebnisse der verschiedenen Datenbanken vergleichbar wären und verlässliche Zahlen über den menschlichen Beitrag zu Ereignissen abgeleitet werden könnten. Offensichtlich sind die unterschiedlichen Angaben über Ursachen im menschlichen Bereich vor allem aufgrund verschiedener Taxonomien und nicht vergleichbarer Untersuchungstiefe entstanden.

Diese Forderungen stimmen auch mit Schlussfolgerungen des OECD/CCA Workshops 2007 in Potsdam überein, in denen festgehalten wurde,

- dass die MARS-Datenbasis /7/ bezüglich menschlicher und organisationaler Faktoren weiter entwickelt werden sollte,
- dass ein zweistufiger Ansatz durch eine Analyse vor Ort und eine Expertenanalyse empfohlen wird,
- dass Modelle einer Taxonomie menschlicher und organisationaler Faktoren zwischen individuellen und organisationalen Faktoren unterscheiden sollten und
- dass für die Analysierenden ein spezielles Training in Hinblick auf menschliche und organisationale Faktoren empfohlen wird.

2 Bewertung von Sicherheitskulturen

In dem Kapitel „Bewertung von Sicherheitskulturen“ wird den Fragen nachgegangen, was Sicherheitskultur ist (Kap. 2.1.1), wie sich Sicherheitskultur weiterentwickeln kann (Kap. 2.1.2) und wie man Sicherheitskultur messen kann (Kap. 2.1.3). Im Anschluss daran, wird die Diskussion auf dem Workshop skizziert (Kap. 2.2) und eine abschließende Zusammenfassung mit Fazit gezogen (Kap. 2.3).

2.1 Stand der Wissenschaft

Trotz der großen Verbreitung und Gebrauch des Begriffes Sicherheitskultur ist das Verständnis und die theoretische Modellbildung noch sehr vage: Die Begriffsdefinitionen erstrecken sich von kognitiven Kriterien der Organisationsmitglieder über weiter reichende Begriffe, die die Organisation als Ganzes betrachten (einzelne Organisationsmitglieder, Arbeitsteams, organisationale Merkmale und Einheiten, organisationale Umwelt, Technologien).

Insgesamt gibt es jedoch einen Konsens darüber, dass **Sicherheitskultur** als holistisches und integratives Konzept verstanden werden sollte /57/. Sicherheitskultur sollte als ein Aspekt der Organisationskultur angesehen werden, in welcher Sicherheit als kritischer Faktor in den Normen, Werten, Einstellungen und Verhalten der Mitglieder einer Organisation widergespiegelt wird. Das in diesem Zusammenhang am meisten referierte Modell ist das von Schein /49/. Er definiert Kultur als „ein Muster gemeinsamer Grundannahmen, das die Gruppe bei der Bewältigung ihrer Probleme externer Anpassung und interner Integration erlernt hat, das sich bewährt hat und somit als bindend gilt, und das daher an Mitglieder als rational und emotional korrekter Ansatz für den Umgang mit diesen Problemen weitergegeben wird“ /49/, S.9. Im Gegensatz zur Sicherheitskultur stellt das **Sicherheitsklima** die Wahrnehmung der Mitarbeiter zum Thema Sicherheit dar. Das Sicherheitsklima wird in der Regel mit Hilfe von Befragungen ermittelt und spiegelt die wahrgenommenen Sicherheitsaspekte wider. Es kann mit einer Momentaufnahme verglichen werden und unterliegt stärkeren Schwankungen. Vergleicht man die Themen Sicherheitskultur und Sicherheitsklima so ist die Kultur das umfassendere und tiefer gehende Konzept, das Sicherheitsklima stellt lediglich eine Teilmenge auf einer Ebene der Kultur dar.

In Übereinstimmung mit Olive, O’Connor und Mannan /58/ können die Konzepte Sicherheitskultur und Sicherheitsklima verwendet werden, um die zugrunde liegenden Sicherheitseinstellungen einer Organisation zu beschreiben. Die Autoren argumentieren, dass „sich Sicherheitsklima gewöhnlich auf die Haltung, die Mitarbeiter einer Organisation gegenüber Sicherheit haben, bezieht. […] Kultur

kann als hintergründiger Einfluss auf die Organisation gesehen werden, während Klima vordergründig beeinflusst. Infolgedessen führt das Sicherheitsklima schneller und leichter als die Sicherheitskultur zu Veränderungen. Als Nachwirkung eines bedeutsamen Unfalles macht also eher das Klima als die Kultur einer Organisation eine unmittelbare Veränderung durch“ /58/, S. 133. Vor dem Hintergrund der empirischen Forschung und der Frage nach der praktischen Relevanz, sind beide Konzepte denkbar. Da es viele Probleme hinsichtlich der Beurteilung von Sicherheitskultur gibt, aber ausreichend Referenzen über Sicherheitsklima-Tools existieren, werden häufig Verbindungen zum Sicherheitsklima gezogen.

Insgesamt erscheint es deshalb notwendig, das Konzept der Sicherheitskultur inhaltlich genauer zu differenzieren, um den verschiedenen Aspekten des Konzeptes angemessen Rechnung zu tragen:

- Was ist Sicherheitskultur?
- Wie entwickelt sich Sicherheitskultur?
- Wie kann man Sicherheitskultur messen?

2.1.1 Was ist Sicherheitskultur?

Beschleunigte technologische Entwicklungen und eine weiter zunehmende Komplexität der Systeme erfordern eine Zunahme der sicherheitsorientierten Bemühungen auf der Seite der Technologie sowie auf der Seite der Organisation. Insbesondere in Industrien mit hohem Gefahrdungspotenzial wurde Sicherheitskultur ein sich immer weiter ausbreitendes Thema. Trotz seiner weiten Verbreitung und seines häufigen Gebrauches ist der Begriff Sicherheitskultur in seinem Verständnis und in seiner theoretischen Fundierung vage. Seine Bedeutung variiert von den kognitiven Eigenschaften der Mitglieder einer Organisation bis zu einem umfangreicheren Verständnis des Begriffes einschließlich des Verhaltens nicht nur der Mitglieder einer Organisation sondern aller Beteiligter eines Systems im weiteren Sinn: Organisationsmitglieder, Arbeitsgruppen, organisationale Eigenschaften und Einheiten, organisationale Umgebung sowie die Technologie.

Demzufolge existiert eine Vielzahl von Dokumenten über Sicherheitskultur, hauptsächlich aus der Kerntechnik. In diesen Quellen konnte in einigen Punkten ein gemeinsames Verständnis festgestellt werden, wie z. B. „Was ist Sicherheitskultur?“, aber auch offene Fragen und verdeckte Punkte konnten ermittelt werden. Obwohl es einige Unterschiede in den verschiedenen Ansätzen gibt, sind sich die Schlüsselelemente der Sicherheitskultur sehr ähnlich (Selbstverpflichtung, organisationales Lernen, Kommunikation). Es fehlen jedoch übereinstimmende Schlüsselelemente für die verfahrenstechnische Industrie.

Folgende Dokumente wurden im Einzelnen betrachtet: OECD-Leitprinzipien für die Verhinderung, Bereitschaft für den Fall und Bekämpfung von Chemieunfällen /2/, OECD-Leitfaden für sicherheitsbezogene Leistungsindikatoren (Guidance on Safety Performance- bislang nur auf Englisch /59/) verschiedene Publikationen der IAEA /50, 60, 61/, Grundelemente von Responsible Care /62/, eine Stellungnahme der internationalen Länderkommission Kerntechnik (ILK) /63/ und Berichte der Health and Safety Laboratory/Executive /64, 65/.

2.1.1.1 Leitprinzipien der OECD

Die OECD formuliert in ihren „Leitprinzipien für die Verhinderung, Bereitschaft für den Fall und Bekämpfung von Chemieunfällen“ sechs generelle Prinzipien zur Schaffung und Förderung einer betrieblichen Sicherheitskultur /2/, S. 33f:

1. Jedes Unternehmen sollte eine betriebliche Sicherheitskultur schaffen und fördern, die sich in einer betrieblichen Sicherheitspolitik widerspiegelt.

- Eine wirksame Sicherheitskultur ist wesentlicher Bestandteil des Sicherheitsmanagements.
- Die Sicherheitskultur sollte sich aus den Werten, Einstellungen und Verhaltensweisen der obersten Leitung ableiten und innerhalb der gesamten Organisation kommuniziert werden. Sie beginnt mit dem sichtbaren Engagement der Vorstandsmitglieder und der leitenden Führungskräfte des Unternehmens, die durch ihre aktive Mitwirkung an Sicherheitsfragen ein Beispiel geben und eine Leitfunktion übernehmen sollten.
- Neben diesem vorrangig hierarchischen („Top-Down“) Sicherheitsengagement sollte auch ein partizipatorisches („Bottom-Up“) Engagement in Form einer aktiven Anwendung der Sicherheitspolitik durch alle Beschäftigten stattfinden. Im Rahmen dieser Sicherheitskultur sollten alle Beschäftigten bemüht sein, ihre Arbeit auf sichere Art und Weise und unter Befolgung festgelegter Betriebsvorschriften zu verrichten und ihre Kollegen bei der Erfüllung dieser Aufgabe zu unterstützen.

- Ein weiterer wesentlicher Bestandteil der Sicherheitskultur sollte die Überzeugung sein, dass alle Unfälle vermeidbar sind.
- Ein Unternehmen sollte als Teil seiner Sicherheitskultur umfassende Regeln für die Aufgaben, Rechte und Pflichten aller mit der Gewährleistung und Aufrechterhaltung der Sicherheit befassten Personen aufstellen.
- Im Sinne einer wirksamen Verhinderung von Unfällen sollten Sicherheitserwägungen unter anderem in folgende Bereiche einbezogen werden: Planung, Auslegung, Errichtung und Inbetriebnahme von Anlagen, Betriebskonzepte und -vorschriften, einschließlich organisatorischer und personeller Regelungen, Wartung/Instandhaltung, vorübergehende Außerbe-

triebnahme, Sicherheitsüberwachung und -bewertung sowie Stilllegung, Schließung und Abbruch gefährlicher Anlagen.

2. In einem Unternehmen sollte als Teil der Sicherheitskultur ein klar formuliertes und sichtbares Sicherheitsengagement vorhanden sein, das darauf ausgerichtet ist, dass alle Beschäftigten in einer im Hinblick auf die Sicherheit angemessenen Weise handeln. Dieses Engagement wird belegt durch Handlungsweisen wie etwa:

- ein klares und sichtbares Interesse der Leitung an der Sicherheitsleistung, das sie durch persönliche Beteiligung an Sicherheitsangelegenheiten bekundet;
- eine rege Kommunikation über Sicherheitsfragen zwischen der Leitung und den übrigen Beschäftigten;
- positive Rückmeldung zu Maßnahmen, die zur Erhöhung der Sicherheit ergriffen worden sind;
- eine rasche Reaktion, um identifizierte Mängel zu beseitigen;
- finanzielle und laufbahnbezogene Anreize für die Erzielung einer guten Sicherheitsleistung;
- die Beteiligung der Beschäftigten auf allen Ebenen an der Entwicklung und Überprüfung von Vorschriften, die das Sicherheitsmanagement betreffen;
- zeitnahe Untersuchungen aller Unfälle und relevanten Beinaheunfälle und rasche Weiterleitung der Untersuchungsergebnisse.

3. Die Sicherheitskultur sollte zu Initiative und Wachsamkeit im Interesse der Sicherheit anhalten.

- Die Sicherheitskultur sollte Schutz vor Selbstzufriedenheit oder vor strukturellen/ verfahrenstechnischen Mängeln bieten, die allesamt zu unsicheren Handlungen oder Verfahrensweisen führen.
- Ein wichtiges Merkmal einer funktionierenden Sicherheitskultur ist die „Fehlertoleranz“: eine solche Sicherheitskultur sollte die Fähigkeit der Beschäftigten fördern, ihre Pflichten effizient zu erfüllen, und nicht allein auf die Ermittlung des Schuldigen oder die Ahndung von Fehlern abgestellt sein. Die Sicherheitskultur sollte eine Atmosphäre der Kooperation und der Offenheit begünstigen, in der die Beschäftigten spannungsfrei über Fehler und Beinaheunfälle diskutieren können, um daraus zu lernen. Nichtsdestoweniger setzt eine fehlertolerante Kultur eine angemessene Verantwortlichkeit und Rechenschaftspflicht voraus.
- Zur Förderung einer solchen Sicherheitskultur sollten die Beschäftigten und ihre Vertreter Gelegenheit zur Beteiligung an der Entwicklung und Überprüfung von Vorschriften bekommen und in die Lage versetzt werden, mit einem sicheren Betrieb und/oder mit dem Schutz von Leben im Ein-

klang stehende Maßnahmen zu ergreifen, ohne Angst vor Repressalien haben zu müssen.

4. Die Leitung sollte alle angemessenen Schritte unternehmen, um sicherzustellen, dass sich alle Beschäftigten ihrer Aufgaben und Verantwortlichkeiten in Bezug auf die Sicherheit bewusst sind und dass sie über die Fähigkeiten, Schulung, Ausbildung, Unterstützung und Mittel verfügen, die zur Wahrnehmung dieser Aufgaben und Verantwortlichkeiten notwendig sind. Die Leitung sollte sich vergewissern, dass alle Sicherheitsvorschriften weitergegeben worden sind und sie allen Beschäftigten (und gegebenenfalls auch anderen) bekannt und von ihnen verstanden worden sind.
5. Die Leitung und die übrigen Beschäftigten sollten nicht selbstzufrieden werden, wenn in einer Anlage längere Zeit keinerlei Unfälle aufgetreten sind. Zur Aufrechterhaltung der Sicherheit bedarf es ständiger Bemühungen.
6. Die Sicherheitskultur eines Unternehmens kann durch eine offene Haltung der Leitung gegenüber der Öffentlichkeit an Sicherheitsfragen verbessert werden.

Bezogen auf die Sicherheitspolitik, stellt die OECD folgende sieben Leitsätze auf /2/, S. 34f:

1. Jedes Unternehmen sollte über eine klare und aussagefähige schriftliche Darlegung seiner im gesamten Unternehmen verbreiteten, akzeptierten und angewendeten Sicherheitspolitik verfügen, die die betriebliche Sicherheitskultur widerspiegelt und die sowohl die übergeordneten Ziele und Prinzipien im Hinblick auf die Sicherheit von Chemikalien als auch das „Null-Ereignisse“-Ziel und die von den Behörden festgelegten Sicherheitsziele beinhaltet.

- Die Sicherheitspolitik sollte in der Dokumentationshierarchie zur Sicherheit von Chemikalien im Unternehmen an oberster Stelle stehen, während jede nachfolgende Stufe die genaueren Einzelheiten der Anwendung der Politik erläutern und auch Arbeitsvorschriften und Betriebsanweisungen einschließen sollte.
- Die Politik sollte auf die Verhinderung, Bereitschaft für den Fall und Bekämpfung von Unfällen und die einzelnen Elementen des Sicherheitsmanagementsystems gerichtet sein.
- Ziel der Sicherheitspolitik sollte der Schutz und die Gesundheit aller an der Herstellung, Verarbeitung, Handhabung, Verwendung, Lagerung, Entsorgung oder Beseitigung gefährlicher Stoffe beteiligten oder möglicherweise davon betroffenen Personen sowie der Schutz der Umwelt und von Eigentum sein.

- Die Sicherheitspolitik sollte in regelmäßigen Abständen überprüft und gegebenenfalls unter Berücksichtigung der gewonnenen Erfahrung und einschlägiger Änderungen auf technischem oder rechtlichem Gebiet fortgeschritten werden.

2. Die Leitung sollte bei der Entwicklung, Überprüfung und Ergänzung der Sicherheitspolitik die Beschäftigten auf allen Ebenen konsultieren und einbeziehen. Die für die Entwicklung der betrieblichen Sicherheitspolitik verantwortlichen Beschäftigten sollten von den für das Management der Produktion verantwortlichen Beschäftigten unabhängig sein und direkten Zugang zur obersten Leitungsebene haben.
3. Die Sicherheitspolitik sollte im gesamten Unternehmen in großem Umfang kommuniziert werden. Die Leitung sollte darauf hinwirken, dass der Zweck der Sicherheitspolitik von allen Beschäftigten im gesamten Unternehmen begriffen und gewürdigt wird.
4. Die Leitung und die übrigen Beschäftigten sollten bei der Einhaltung der betrieblichen Sicherheitspolitik und der Erfüllung seiner Sicherheitsziele zusammenarbeiten.

- Der Leitung und der Belegschaft fallen bei der Verhinderung von Unfällen unterschiedliche, aber einander ergänzende Aufgaben und Verantwortlichkeiten zu, die darin bestehen, dass sie ihre Arbeit in sicherer Art und Weise verrichten, aktiv zur Entwicklung und Anwendung von Sicherheitspolitik und Betriebsweisen beitragen und untereinander und mit anderen Beteiligten zusammenarbeiten.
- Die Beschäftigten auf allen Ebenen sollten dahingehend motiviert und ausgebildet/geschult werden, dass sie Sicherheit als oberste Priorität und ihre ständige Verbesserung als zentrales Unternehmensziel anerkennen.
- Die Belegschaft und ihre Vertreter sollten mit der Leitung bei der Förderung der Sicherheit von Chemikalien zusammenarbeiten und mit wirksamen Mitteln (Strukturen und Prozessen) zur Erreichung dieses Ziels ausgestattet werden.

5. Die Sicherheitspolitik sollte der Öffentlichkeit zugänglich gemacht werden.
6. Jeder Standort innerhalb eines Unternehmens sollte ein eigenes Sicherheitsprogramm entwickeln und fortschreiben, das der Sicherheitspolitik des Unternehmens entspricht und sich eingehender mit den standortspezifischen Sicherheitsbelangen und Anforderungen befasst. Dieses Programm sollte unter aktiver Beteiligung der Beschäftigten auf allen Ebenen erarbeitet werden und Gegenstand einer regelmäßigen Überprüfung sein.

- Die Verantwortung für das laufende Sicherheitsmanagement sollte in den Händen des Linienmanagements der einzelnen Anlagen liegen.

- Das Linienmanagement sollte auf die Vorschläge und Anregungen der Belegschaft und des Betriebsrats zu Sicherheitsaspekten eingehen oder sie an Vorgesetzte weiterleiten.
- Die Leitungsspitze sollte dem Linienmanagement bei sicherheitsbezogenen Entscheidungen und Maßnahmen die gebotene Unterstützung gewähren.

7. Die Entwicklung und Anwendung einer betrieblichen Sicherheitspolitik sowie die Maßnahmen zur Verhinderung von Unfällen und zur Begrenzung von Unfallauswirkungen sollten mit den anderen Aktivitäten des Unternehmens im Bereich des Arbeitsschutzes und des Gesundheits- und Umweltschutzes im Rahmen eines umfassenden Risikomanagementprogramms koordiniert und abgestimmt werden.

2.1.1.2 Definitionen und Schlüsselelemente der IAEA

Der Begriff Sicherheitskultur wurde erstmals im Zusammenhang mit der Tschernobyl-Katastrophe als erklärendes Konzept von der IAEA verwendet und fand schnell Eingang in die Literatur und in Industrien mit komplexen Systemen wie beispielsweise verfahrenstechnische Industrien, zivile und militärische Luftfahrt oder Weltraumforschung und der Bahn. Die Mehrheit der Definitionen stammt allerdings aus dem Bereich der Kerntechnik.

Die **INSAG** /60/ definiert Sicherheitskultur wie folgt: „Sicherheitskultur ist die Gesamtheit von Merkmalen und Einstellungen bei Organisationen und Individuen, die als oberste Priorität durchsetzt, dass Sicherheitsfragen von Kernkraftwerken die ihre Bedeutung entsprechende Aufmerksamkeit erhalten“ /60/, S.1.

Die **IAEA** /50/ definiert weiterhin: „Sicherheitskultur ist auch eine Mischung von Werten, Einstellungen, von moralischen Prinzipien und Normen akzeptablen Verhaltens. Diese zielen darauf ab, eine selbstdisziplinierte Vorgehensweise aufrecht zu erhalten, um Sicherheit über rechtliche und regulatorische Anforderungen hinaus zu erhöhen. Sicherheitskultur muss daher im Denken und Handeln aller Individuen auf allen Ebenen einer Organisation inhärent sein.“ /50/, S.3.

Die Hauptkomponenten von Sicherheit im Verständnis der IAEA /50/ sind Verantwortlichkeiten auf folgenden Ebenen:

1. Verantwortlichkeiten der Politik

- Statement zur Sicherheitspolitik
- Managementstrukturen
- Ressourcen
- Selbstregulation

2. Verantwortlichkeiten der Führungskräfte
- Formulierung und Verbreitung von Sicherheitspraktiken
- Gewährleistung von sicherheitsbezogener Qualifikation und sicherheitsbezogenen Training
- sicherheitsbezogene Gestaltung von Sanktionen und Belohnungen
- Durchführung von Auditierungsverfahren

3. Verantwortlichkeiten der Mitarbeiter
- Vorhandensein einer hinterfragenden Grundhaltung
- Sorgfältiges und vorsichtiges Handeln
- Offene Kommunikation

Um praktische und pragmatische Leitlinien zur Entwicklung von Sicherheitskultur bereitzustellen, definiert die INSAG /61/, S. 5 f. folgende Elemente einer "guten Sicherheitskultur": Selbstverpflichtung, sich für die Sicherheit und die Verbesserung der Sicherheitskultur einzusetzen; das Vorhandensein und die Einhaltung von Vorschriften und Verfahrensanweisungen (Gebrauch von Prozeduren); die in Bezug auf Sicherheit konservative Entscheidungsfindung, die Offenheit, auch scheinbar unbedeutende Vorkommnisse und Beinaheereignisse zu melden (Berichtskultur); Ablehnung von unsicheren Handlungen und Bedingungen; der Wille sich weiter zu verbessern und zu lernen (Lernende Organisation); Zugrundeliegende Fragen: Kommunikation, klare Prioritäten und Organisation. Eine detaillierte Beschreibung der genannten Elemente befindet sich im Anhang III.

2.1.1.3 Prinzipien der Initiative Responsible Care

Die weltweite Initiative Responsible Care /62/ wird durch folgende acht grundlegende Merkmale gekennzeichnet, die vom internationalen Chemieverband ICCA (International Council of Chemical Associations) abgestimmt wurden. Die acht grundlegenden Merkmale von Responsible Care sind:

- Leitsätze (guiding principles): die formelle Verpflichtung eines Unternehmens zur Einhaltung von Leitsätzen, die auf internationaler Ebene von der verfahrenstechnischen Industrie vereinbart wurden.
- Statuten, Anleitungen, Prüflisten (codes, guidance notes, checklists): sollen den Unternehmen bei der Erfüllung ihrer Verpflichtung helfen.
- Kennzahlen (performance indicators): wachsende Anzahl der Vorgaben von Kennzahlen zur Messung der tatsächlichen Leistung.
- Meinungsaustausch (communication): Meinungsaustausch mit interessierten Kreisen zu Themen aus den Bereichen Gesundheit, Sicherheit und Umwelt.

- Ausschüsse für den Erfahrungsaustausch (information sharing fora): geben den Unternehmen die Möglichkeit zum Austausch von Meinungen und Erfahrungen in der Umsetzung der Verpflichtung zu Responsible Care.
- Bezeichnung und Logo (title and logo): verdeutlichen bei internationalen Programmen den Einklang mit Responsible Care.
- Ermutigung aller Chemieunternehmen (encouragement of all chemical companies): Überlegungen, wie alle Unternehmen der verfahrenstechnischen Industrie in am besten geeigneter Form einzubeziehen und zu motivieren sind.
- Überprüfung (verification): Verfahren zur Überprüfung der Umsetzung von Responsible Care durch die Mitgliedsunternehmen.

2.1.1.4 Elemente der Sicherheitskultur der internationale Länderkommission Kerntechnik

Die **ILK (internationale Länderkommission Kerntechnik)** definiert generelle Elemente der Sicherheitskultur im Rahmen ihrer „Stellungnahme zum Umgang der Aufsichtsbehörde mit den von Betreibern durchgeführten Selbstbeurteilungen der Sicherheitskultur“ /63/. Die Auflistung der ILK (S.21) übersteigt die Anzahl der Elemente aus zuvor genannten Quellen:

- Verpflichtung der Unternehmensspitze zur Sicherheit,
- erkennbares Führungsverhalten,
- hoher Stellenwert der Sicherheit,
- systematische Betrachtungsweise der Sicherheit,
- strategisch-wirtschaftliche Bedeutung der Sicherheit,
- keine Konflikte zwischen Sicherheit und Betrieb,
- Verhältnis zu Behörden und anderen externen Organisationen,
- Initiative und langfristige Perspektive,
- dynamisches Management,
- Qualität der Dokumentation und der Abläufe,
- Einhaltung von Vorschriften und Regelungen,
- ausreichendes und kompetentes Personal,
- geeignete Mittelzuteilung,
- arbeitswissenschaftliche Kenntnisse, einschließlich Gesundheitsschutz und Mensch-Technik-Organisation (MTO),
- eindeutige Rollen und Verantwortlichkeiten,

- klar organisierte Teamarbeit,
- Offenheit und Kommunikation,
- Motivation und Arbeitszufriedenheit,
- Einbindung aller Mitarbeiter,
- gute Arbeitsbedingungen (Zeit, Arbeitsbelastung, Stress),
- Ordnung und Sauberkeit,
- Ermittlung der realisierten Sicherheit,
- organisatorisches Lernen.

Diese Elemente können den beiden Hauptkomponenten „organisatorische Rahmenbedingungen“ und „Einstellungen des Personals“ zugeordnet werden.

Wilpert et al. /66/ führen die nachfolgenden Schlüsselelemente für Sicherheitskultur ein, die eindeutig eine organisationspsychologische Perspektive betonen:

- Selbstverpflichtung aller Ebenen und Mitarbeiter (commitment)
- hinterfragende Grundhaltung
- systematisches Denken
- Vorbildfunktion von Führungskräften
- Professionalität
- Umgang mit Fehlern
- implizite Normen

Viele Merkmale einer guten Sicherheitskultur gehören in Industrien mit hohem Gefährdungspotential schon seit langem zur guten Praxis. Neuerdings wird die systematische Verbesserung der Sicherheitskultur betont und der Beitrag, den die Verhaltenswissenschaften dazu liefern können. Konzepte zur Veränderung der Kultur sind sowohl Bottom-Up- als auch Top-Down-Ansätze. Ein entscheidender Faktor dabei ist eine konsistente und transparente Führung auf der Seite des Managements. Die IAEA /50/ betont: „Technische Fachleute, Human-Factors-Experten, Betriebspersonal und Management müssen zusammen arbeiten, um ein gemeinsames Verständnis über ihre verschiedenen Funktionen zu entwickeln. Dieses ist in sich ein Lernprozess und als solcher eine Eigenschaft einer guten Sicherheitskultur. Kontinuierliche Lern- und Verbesserungsprozesse spielen eine zentrale Rolle in der Entwicklung und Aufrechterhaltung einer guten Sicherheitskultur“ (S. 4f.).

2.1.2 Wie entwickelt sich Sicherheitskultur?

Sicherheitskultur wird als ein Prozess mit verschiedenen Niveaus oder Stufen betrachtet. Es werden auch in diesem Zusammenhang verschiedene Modelle zur Verbesserung der Sicherheitskultur verwendet. Einerseits werden Modelle verwendet, die Verhaltensaspekte betonen, andererseits existieren auch Qualitätsmanagement-Ansätze zur Verbesserung sicherheitsgerichteter Leistung. In diesem Kapitel werden zwei Prozessmodelle zur Entwicklung der Sicherheitskultur ausführlich beschrienen. Dabei handelt es sich um das Entwicklungsmodell der Sicherheitskultur der IAEA /50/ und um das Reifegradmodell der Sicherheitskultur vom Keil Centre /64/.

Die Bemühungen, die gemacht werden, um Sicherheitskultur zu verbessern, können zu einer besseren Organisation, Analysen, Vorhersagen und Arbeitsprozessen führen. Eine starke Sicherheitskultur kann somit zu einer effektiveren Arbeit und zu mehr Verantwortlichkeit unter Managern und Angestellten beitragen.

2.1.2.1 Entwicklungsmodell der Sicherheitskultur der IAEA

Nach der IAEA /50/, scheinen sich drei verschiedenen Stufen der Entwicklung einer Sicherheitskultur herauszubilden. Die Merkmale jeder Stufe liefern Organisationen eine Basis zur Selbstdiagnose:

Erstes Entwicklungsstadium: Sicherheit basiert vornehmlich auf der Befolgung von Vorschriften und Anweisungen

Sicherheit wird als ein externes Erfordernis und nicht als ein Aspekt des Verhaltens betrachtet, der der Organisation hilft, erfolgreich zu sein. Externe Erfordernisse sind Vorschriften bzw. Anweisungen der Regierung, regionalen Verwaltungen oder ausführenden Behörden. Sicherheit wird als technisches Konzept gesehen, wobei die Befolgung von extern auferlegten Vorschriften und Regeln als ausreichend zur Gewährleistung von Sicherheit betrachtet wird. Für eine Organisation, die überwiegend von Regeln abhängt, können folgende Merkmale beobachtet werden /50/, S. 5f.

- Probleme werden nicht antizipiert; die Organisation reagiert jeweils auf ihr Aufkommen.
- Wenig Kommunikation zwischen Abteilungen und Funktionen.
- Abteilungen und Funktionen verhalten sich als semi-autonome Einheiten, es gibt wenig Kooperation zwischen ihnen sowie kaum gemeinsame Entscheidungen.
- Entscheidungen von Abteilungen und Funktionen betreffen wenig mehr als zur Regelbefolgung notwendig ist.

- Mitarbeiter, die Fehler machen, werden beschuldigt, dass sie sich nicht an die Regeln gehalten haben.
- Konflikte werden nicht gelöst; Abteilungen und Funktionen konkurrieren miteinander.
- Die Rolle des Managements wird darin gesehen, dass Regeln verstärkt, Mitarbeiter gedrängt und Resultate erwartet werden.
- Zuhören oder Lernen findet innerhalb und außerhalb der Organisation kaum statt, bei Kritik wird eine defensive Haltung eingenommen.
- Sicherheit wird als eine notwendige Beeinträchtigung angesehen.
- Behörden, Kunden, Zulieferer und Auftragnehmer werden vorsichtig oder feindlich behandelt.
- Kurzzeitige Profite werden als Allerwichtigstes gesehen.
- Mitarbeiter werden als „Systemkomponenten“ betrachtet – sie werden nur über ihre Arbeit definiert und bewertet.
- Es gibt eine feindliche Beziehung zwischen Management und Mitarbeitern.
- Es gibt kein oder wenig Bewusstsein für Arbeit- oder Geschäftsprozesse.
- Mitarbeiter werden für Gehorsam und Ergebnisse belohnt, unabhängig von Langzeitkonsequenzen.

Zweites Entwicklungsstadium: Sicherheitsgerichtetes Verhalten wird als organisationales Ziel wahrgenommen

Die Unternehmensführung nimmt sicherheitsbezogenes Verhalten wahr. Obwohl Verhaltensaspekte bewusster berücksichtigt werden, fehlen sie in den wesentlichen Sicherheitsmanagementmethoden, die verfahrenstechnische Lösungen fokussieren. Sicherheitsgerichtetes Verhalten wird als Organisationsziel von jedem einzelnen Mitarbeiter wahrgenommen. Es werden sicherheitsbezogene Ziele vermittelt. Die Organisation fragt sich, warum sicherheitsgerichtetes Verhalten ein „Plateau“ erreicht und ist bereit, von anderen Organisationen zu lernen. Die folgenden Merkmale charakterisieren die zweite Entwicklungsstufe /50/, S. 6f:

- Die Organisation konzentriert sich vor allem auf das Tagesgeschäft. Es gibt kaum strategisches Denken.
- Das Management bestärkt Teams und Kommunikation über Abteilungen und Funktionen hinweg.
- Das Management funktioniert als Team und beginnt, Abteilungs- und funktionale Entscheidungen zu koordinieren.

- Entscheidungen sind häufig kosten- oder funktionszentriert.
- Die Reaktion des Managements auf Fehler besteht aus mehr Kontrolle durch Regeln und Schulung. Es gibt etwas weniger Schuldzuweisungen.
- Konflikte werden als störend und abschreckend für Teamarbeit angesehen.
- Die Rolle des Managements wird darin gesehen, Managementtechniken anzuwenden, wie Führung durch Zielvereinbarung.
- Die Organisation ist zum Teil bereit von anderen Unternehmen zu lernen, besonders im Hinblick auf Techniken und best practices.
- Sicherheit, Kosten und Produktivität werden als sich gegenseitig beeinträchtigend angesehen. Sicherheit wird als Kosten erhöhend und produktivitätssenkend angesehen.
- Die Beziehung der Organisation mit Behörden, Kunden, Zulieferern und Auftragnehmern ist eher locker als fest; es gibt eine behutsame Annäherung, bei der Vertrauen gewonnen werden muss.
- Es ist wichtig, die kurzfristigen Gewinnziele zu erreichen oder zu übertreffen. Mitarbeiter werden für Zielübertreffung belohnt unabhängig von Langzeitergebnissen oder –konsequenzen.
- Die Beziehung zwischen Mitarbeitern und Management ist schlecht mit wenig Vertrauen oder Respekt.
- Es gibt ein wachsendes Bewusstsein für den Einfluss kultureller Aspekte am Arbeitsplatz. Es wird nicht verstanden, warum zusätzliche Kontrolle nicht zu den erwarteten Ergebnissen hinsichtlich Sicherheit führt.

Drittes Entwicklungsstadium: Sicherheit als kontinuierlicher Verbesserungsprozess

Sicherheit wird als kontinuierlicher Verbesserungsprozess betrachtet, wozu jeder in der Organisation beitragen kann. ‚Weiche' Faktoren wie Kommunikation, Training und Führungsstile werden betont. Die Mitglieder der Organisation verstehen, dass ihr Verhalten einen Einfluss auf die Sicherheit hat. Der Bewusstseinsgrad von sicherheitsgerichteten Verhalten und Einstellungen ist hoch. Es werden Maßnahmen ergriffen, um das Verhalten zu verbessern. Folgende Merkmale sind charakteristisch für die dritte Entwicklungsstufe /50/, S. 7f.:

- Die Organisation beginnt, strategisch zu handeln mit einem weiter reichenden Fokus aber auch einem Bewusstsein für die Gegenwart. Sie antizipiert Probleme und kümmert sich um deren Ursachen, bevor sie aufkommen.

- Mitarbeiter begreifen und erklären die Notwendigkeit abteilungs- und funktionsübergreifender Zusammenarbeit. Sie erhalten vom Management Unterstützung und Ressourcen für die Zusammenarbeit.
- Mitarbeiter kennen die Arbeits- und Geschäftsprozesse und helfen den Vorgesetzten bei deren Bewältigung.
- Entscheidungen werden mit vollem Wissen über deren Sicherheitseinfluss auf die Arbeits- oder Geschäftsprozesse sowie auf Abteilungen und Funktionen getroffen.
- Es gibt keinen Zielkonflikt zwischen Sicherheit und Produktion, so dass die Sicherheit nicht durch das Streben nach Produktionszielen gefährdet wird.
- Fast alle Fehler werden im Sinn von Variabilität der Arbeitsprozesse gesehen. Es ist wichtiger zu verstehen, was passiert ist, als einen Schuldigen zu finden. Das gewonnene Verständnis wird zur Modifizierung der Arbeitsprozesse genutzt.
- Konflikte werden wahrgenommen und so behandelt, dass nach positiven Lösungen für die Beteiligten gesucht wird.
- Die Rolle des Managements wird darin gesehen, dass Mitarbeiter gefördert werden, um die Geschäftsleistung zu erhöhen.
- Lernen von anderen sowohl innerhalb als auch außerhalb der Organisation wird geschätzt. Zeit zur Wissensaneignung hinsichtlich Leistungsverbesserung wird zur Verfügung gestellt.
- Sicherheit und Produktion werden als voneinander abhängig gesehen.
- Kooperationsbeziehungen werden zwischen der Organisation und Behörden, Kunden, Zulieferern und Auftragnehmern entwickelt.
- Kurzzeitleistung wird gemessen und analysiert, so dass Veränderungen für die Langzeitverbesserung eingeleitet werden können.
- Mitarbeiter werden respektiert und für ihren Beitrag geschätzt.
- Die Beziehung zwischen Management und Mitarbeitern ist respektvoll und unterstützend.
- Mitarbeiter sind sich über den Einfluss kultureller Aspekte bewusst und diese werden bei Entscheidungen in Betracht gezogen.
- Die Organisation belohnt nicht nur diejenigen, die produzieren, sondern auch die, die die Arbeit der anderen unterstützen. Mitarbeiter werden auch für die Verbesserung von Prozessen und Ergebnissen belohnt.

2.1.2.2 Reifegradmodell der Sicherheitskultur des Keil Zentrums

Für den U.K. HSE Offshore Technology Report 2000/049 entwickelte das Keil Zentrum /64/ ein Reifegradmodell der Sicherheitskultur, das auf einem Ansatz von Hudson /67/ basiert. Das Modell umfasst fünf Entwicklungsstufen, d. h. zwei Stufen mehr als das Modell der IAEA /50/. Die in den Modellen beschriebenen Elemente unterscheiden sich hauptsächlich darin, dass die Elemente des Reifegradmodells besonders die Mitarbeiterperspektive berücksichtigen:

- Selbstverpflichtung und Transparenz auf Seiten des Managements,
- Kommunikation,
- Produktivität vs. Sicherheit,
- organisationales Lernen,
- Sicherheitsressourcen,
- Partizipation,
- gemeinsame Wahrnehmung über Sicherheit,
- Vertrauen,
- industrielle Verbindungen und Arbeitszufriedenheit,
- Training.

Folgende Annahmen stellen die Basis dieses Modells dar: Kulturelle oder verhaltensbezogene Ansätze zur Verbesserung der Sicherheit sind am effektivsten, wenn die technischen und systembezogenen Sicherheitsaspekte adäquat funktionieren und die Mehrheit der Ereignisse aufgrund von verhaltensbezogenen oder kulturellen Faktoren zustande kommen. Das Reifegradmodell ist deshalb nur für Organisationen relevant, die bestimmte Kriterien erfüllen.

Diese beinhalten:

- ein adäquates Sicherheitsmanagementsystem,
- technisches Versagen ist nicht die Hauptursache von Ereignissen,
- die Organisation hält sich an Gesetze zu Gesundheit und Sicherheit,
- Sicherheit wird nicht durch den Gedanken geleitet, eine Strafe zu umgehen, sondern von dem Wunsch, Ereignisse zu verhindern.

Die fünf Stufen des Modells sind in Anlehnung an die Stufen von Hudson /67/ gebildet:

Stufe 1: ..... pathologisch

Stufe 2: ..... reaktiv

Stufe 3: ..... kalkulativ

Stufe 4: ..... proaktiv

Stufe 5: ..... generativ

Aufbauend auf den Stufen von Hudson /67/ benennt das Keil Zentrum /64/ die Stufen um, ohne ihre Bedeutung im Wesentlichen zu verändern. Die Benennung der Stufen und ihre Bedeutung ist im Folgenden beschrieben und wird in Abbildung 1 dargestellt /64/:

Stufe 1: Aufkeimend (emerging)

Sicherheit ist in Bezug auf technische und prozessbezogene Lösungen sowie auf das Einhalten von Bestimmungen definiert. Es wird angenommen, dass die Hauptverantwortung für Sicherheit die Sicherheitsabteilung trägt. Ereignisse werden als unvermeidlich und Teil der Arbeit angesehen. Die meisten Beschäftigten zeigen ein Desinteresse an Sicherheit. In dieser Stufe sind Aussagen wie beispielsweise: „Wen kümmert es, solange wir nicht erwischt werden“ üblich.

Stufe 2: Organisiert (managing)

Die Ereignisrate der Organisation ist durchschnittlich für den industriellen Sektor, aber die Organisation weist tendenziell überdurchschnittlich viele schwere Ereignisse auf. Zeit und Bemühungen seitens des Managements, werden in die Ereignisprävention investiert. Sicherheit wird in Bezug auf die Einhaltung von Regeln und Prozeduren sowie Technikkontrollen definiert. Ereignisse werden generell als vermeidbar angesehen. Manager führen die Ereignisentstehung auf unsicheres Verhalten des Bedienpersonals zurück. Sicherheitsbezogene Leistungen werden mit Hilfe von reduzierten Indikatoren wie beispielsweise den Ausfalltagen („lost time injury“ (LTI)) gemessen. Sicherheitsanreize basieren auf reduzierten LTI-Raten. Argumente wie: „Sicherheit ist wichtig: Wenn Unfälle passieren, tun wir eine Menge“, lassen sich dieser Entwicklungsstufe zuordnen.

Stufe 3: Einbeziehend (involving)

Ereignisraten sind relativ gering, haben aber einen bestimmten Level erreicht. Die Organisation ist überzeugt davon, dass die Beteiligung des Bedienpersonals an Fragen zu Gesundheit und Sicherheit kritisch für zukünftige Verbesserungen ist. Manager erkennen, dass viele zu den Ereignissen beitragende Faktoren sowie sogenannte Grundursachen („root cause“) aus dem Bereich Managemententscheidungen stammen. Ein bedeutender Anteil der Angestellten ist bereit, mit der Unternehmensleitung zusammenzuarbeiten, um Sicherheit

und Gesundheit zu verbessern. Die Mehrheit des Personals akzeptiert die persönliche Verantwortung für ihre eigene Gesundheit und Sicherheit. Sicherheitsbezogene Leistungen werden überwacht und die jeweiligen Daten werden effektiv genutzt. Die Äußerung: „Wir haben Systeme, um Gefährdungen zu kontrollieren“ kann als Beispiel für diese Entwicklungsstufe genannt werden.

Stufe 4: Kooperativ (cooperating)

Die Mehrheit der Organisationsmitglieder ist überzeugt, dass Gesundheit und Sicherheit sowohl von einem moralischen als auch von einem ökonomischen Standpunkt her wichtig ist. Manager und Angestellte erkennen, dass Ereignisursachen auf Managemententscheidungen zurückzuführen sind. Die Mehrheit des Personals akzeptiert die persönliche Verantwortung für ihre eigene Gesundheit und Sicherheit sowie für die ihrer Arbeitskollegen. Die Organisation initiiert proaktive Maßnahmen zur Verhinderung von Ereignissen. Sicherheitsbezogene Leistungen werden aktiv mit Hilfe aller verfügbaren Daten überwacht. Ereignisse, die nicht während der Arbeit auftreten, werden auch überwacht. Ein gesunder Lebensstil wird gefördert. Ein Beispiel der proaktiven Sicht auf Sicherheitskultur sind Aussagen wie: „Wir arbeiten an den Problemen, die wir finden“.

Stufe 5: Kontinuierliche Verbesserung (continuous improvement)

Die Verhütung aller Verletzungen oder Schäden an Angestellten (sowohl bei der Arbeit als auch zu Hause) ist ein zentraler Unternehmenswert. Die Organisation weist eine längere Periode (Jahre) ohne meldepflichtige Ereignisse oder schwere Vorfälle auf. Ein Gefühl der Selbstzufriedenheit stellt sich dadurch nicht ein. Mögliche Ereignisquellen werden vorausschauend identifiziert. Das Unternehmen verwendet eine Vielzahl von Indikatoren zur Leistungsbeurteilung. Die Beurteilungen sind nicht leistungsgesteuert, sondern die Organisation hat Vertrauen zu ihren Sicherheitsprozessen. Man ist konstant bestrebt, die Mechanismen zur Gefahrenkontrolle zu verbessern. Der Gedanke, dass Gesundheit und Sicherheit kritische Aspekte der Arbeit darstellen, wird von allen Angestellten geteilt. Die Bedeutung der Prävention von Verletzungen oder Schäden außerhalb der Arbeit wird von allen Mitgliedern akzeptiert. Die Organisation investiert beträchtliche Bemühungen darin, Gesundheit und Sicherheit zu Hause zu fördern. Typisch für diese Stufe sind Angaben der Angestellten wie etwa: „Sicherheit gehört zu unserem täglichen Geschäft“.

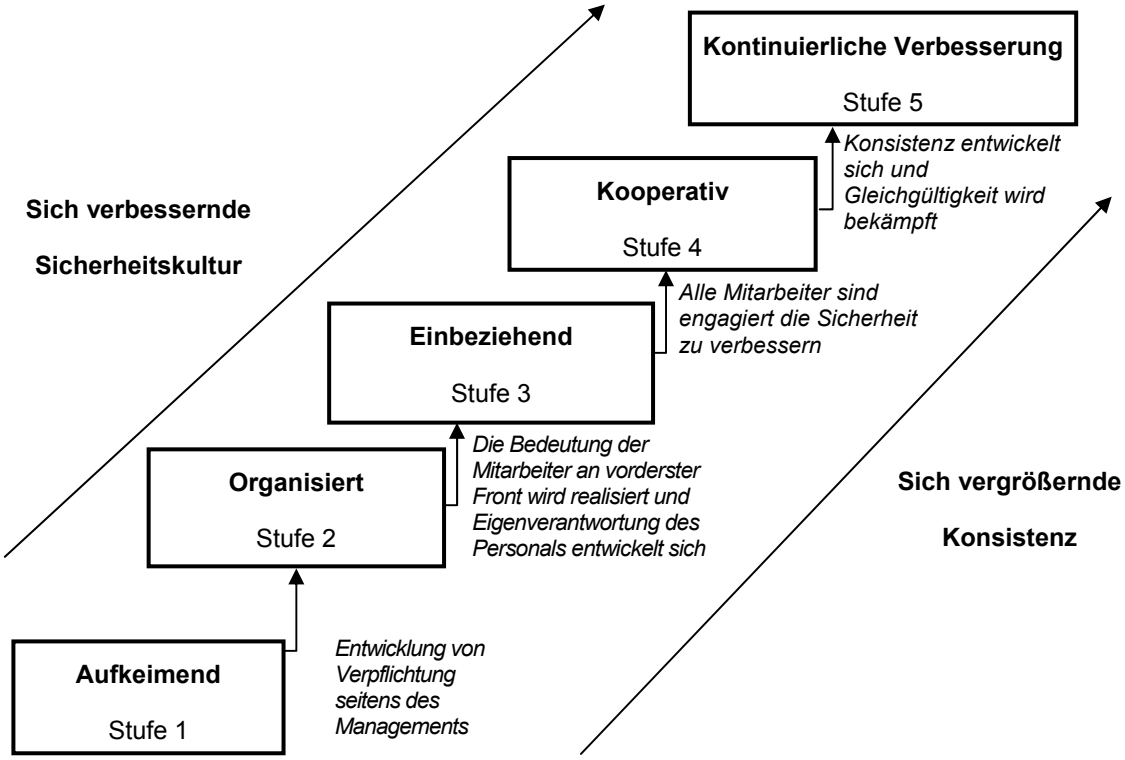


Abbildung 1: Reifegradmodell der Sicherheitskultur /64/

Insgesamt zeigt sich aufgrund der Analysen, dass Organisationen sich in ihrem Verständnis von Sicherheitskultur und in ihren Handlungen, um diese positiv zu beeinflussen, unterscheiden. Diese Unterschiedlichkeit spiegelt den Bewusstseingrad hinsichtlich der Bedeutung menschlichen Verhaltens und Einstellungen für die Sicherheit selbst in hoch technologischen Organisationen wider.

2.1.3 Wie kann man Sicherheitskultur messen?

Es existiert eine Vielzahl an Literatur über Sicherheitskultur und Sicherheitsklima sowie deren Beurteilungen. Die folgende Auswahl basiert auf spezifischen Referenzen der Prozessindustrie oder auf Literatur, die über den vorherigen Abschnitt „Offizielle Dokumente“ hinausgeht.

Die bisher umfangreichste Beschreibung und Diskussion verschiedener Modelle und analytischer Instrumente in Bezug auf Sicherheitskultur lieferten Wilpert et al. /66/ mit einem Review von über 20 verschiedenen Ansätzen. Die beschriebenen Ansätze unterscheiden sich sowohl in Bezug auf die Tiefe der Analyse, den psychometrischen Qualitätskriterien: Zuverlässigkeit, Objektivität und Gültigkeit als auch in Bezug auf ökonomischen Nutzen und Handhabung. Ein grundlegender und wichtiger Unterschied besteht jedoch in der Konzeption der Durchführung der Analyse: durch entweder externe Experten (Fremdbeurtei-

lung) oder anhand von Selbstbeurteilungen durch Mitglieder der Organisation selbst.

Die Analysen durch **externe Experten** basieren gewöhnlich auf Sicherheitsaudits, Fragebögen, Interviewleitfäden, Beobachtung und Dokumentenanalysen. Der Vorteil bei Untersuchungen durch Externe liegt hauptsachlich darin, dass die Analyse durch eine andere Perspektive geleitet wird und dadurch Erfahrungen aus verschiedenen Kontexten mit einfließen. Der Nachteil solcher Analysen besteht daran, dass sie meistens nur direkt beobachtbare Phänomene, Einstellungen und Werte erfassen. Tiefere Ebenen der Organisationskultur sind hingegen externen Analytikern kaum zugänglich.

Selbstbeurteilungen hingegen werden meistens durch interne Spezialisten durchgeführt, die mit ihrer eigenen Organisation vertraut sind. Selbstbeurteilungen können leicht und ökonomisch ausgeführt werden. Sie haben häufig eine unmittelbare pädagogische Wirkung, da Probleme sofort identifiziert und entsprechende Maßnahmen zeitnah abgeleitet und umgesetzt werden können. Andererseits besteht bei Selbstbeurteilungen die Gefahr, dass die Analyse nur auf Aspekte der Organisation abzielt, die nicht tabuisiert und somit von der Unternehmensführung schnell akzeptiert werden und damit leichter optimiert werden können. Externe Beurteilungstechniken und Selbstbeurteilungen schließen sich gegenseitig nicht aus, sondern sollten komplementär eingesetzt werden. Die Forschungsstelle Systemsicherheit der TU-Berlin hat sich bei der Entwicklung eines Screening-Verfahrens zur Bewertung von Sicherheitskultur hauptsächlich auf Selbstbeurteilungsmethoden fokussiert /66/.

Unter den funktionalen Aspekten von Industrien mit hohem Gefährdungspotential, werden alle Merkmale zusammengefasst, die eine Organisation lebensfähig machen: Führung, Gruppennormen, Kontrolle, Regeln und Prozeduren. Strukturelle Elemente dagegen sind Merkmale die eine Organisation zum Aufbau benötigt wie beispielsweise organisatorische Ebenen einschließlich der wichtigsten Verbindungen zu externen Institutionen zum Beispiel zu Aufsichtsbehörden oder zu anderen Referenzorganisationen.

Die Autoren /66/ unterscheiden dabei fünf relevante funktionelle Systeme:

- Technik, z. B. Hardware,
- Individuum, z. B. Verhalten, kognitive Fähigkeiten,
- Gruppenebene, z. B. Gruppendynamik,
- Organisation, z. B. Führung, Kontrolle und
- Umwelt, z. B. Medien, Öffentlichkeit.

Auf der Basis von prototypischen organisationalen Eigenschaften von kerntechnischen Anlagen wurden die folgenden strukturellen Elemente identifiziert /66/:

- Regulation,
- Nutzen,
- Anlagenmanagement,
- interne Mitarbeiter, z. B. Betriebsstab, Instandhaltung, Systemtechnik, Überwachung, Buchführung, Logistik, Generalstab,
- externe Mitarbeiter.

Die Zuweisung der funktionalen Faktoren führte zur folgenden Gruppierung:

- **individuelle Ebene:** kognitive Fähigkeiten, Regelbefolgung, Qualifikation, Risikowahrnehmung, Einstellung/Motivation, physiologische Einflüsse, Engagement für Sicherheit, Verhalten,
- **Gruppenebene:** Kommunikation, Gruppendynamik, Führung/ Kontrolle, soziale Normen, Vorbild,
- **organisationale Ebene:** Grundannahmen der Organisation, Ziele und Visionen, Ressourcen, Prozessmanagement und Prozessevaluation, organisationales Lernen, Training, Information und Dokumentation, Anreizsysteme, Technik (Hardware, Software, Ergonomie).

Diese strukturellen und funktionellen Dimensionen lieferten die Basis für die Entwicklung eines Screening-Verfahrens zur Selbstbeurteilung der Sicherheitskultur und der vorgeschlagenen Begriffsbildung für die Einführung und Erhaltung einer nachhaltigen Sicherheitskultur in Kernkraftwerken /66/.

Eine neue Dimension und ein neues Element wurde von Olive et al. /58/ eingeführt: Elastizität und Flexibilität: „Eine starke Sicherheitskultur ist durch verschiedene Merkmale gekennzeichnet: eine klare Selbstverpflichtung zur Verbesserung von sicherem Verhalten und Sicherheitseinstellungen auf allen Organisationsstufen; eine organisationale Struktur und Atmosphäre, die offene und klare Kommunikation fördert, in der sich die Menschen nicht eingeschüchtert fühlen und vor Strafe fürchten; eine Neigung zur Elastizität und Flexibilität, sich neuen Situationen effektiv und sicher anzupassen; eine vorherrschende Haltung zur ständigen Wachsamkeit” /58/, S. 139.

Lardner /51/ weist dazu auf folgenden Zusammenhang hin: „Seitdem Sicherheitskultur mit Arbeitsunfällen in Verbindung gebracht wird, haben Organisationen mit einer im Vergleich geringen Unfallrate wahrscheinlich auch eine positive Sicherheitskultur“ (S. 13).

Die folgenden Eigenschaften charakterisieren Organisationen mit niedrigen Unfallraten:

- häufige, aber wenig formalisierte Kommunikation zu Sicherheit auf allen Organisationsebenen,
- gutes organisationales Lernen,
- starke Fokussierung auf Sicherheit bei allen Mitarbeitern,
- starke Selbstverpflichtung des gehobenen Managements,
- demokratischer und kooperativer Führungsstil,
- qualitativ hochwertiges Training inklusive Sicherheitstraining,
- gute Arbeitsbedingungen und gute Hausservice,
- hohe Arbeitszufriedenheit,
- gute Arbeitsgeber-Arbeitnehmer-Beziehungen,
- Auswahl und Bevorzugung von Mitarbeitern, die zuverlässig und sicher arbeiten.

Nach Lardner /51/ werden folgende Eigenschaften aus verschiedenen Fragebogenstudien mit einer positiven Sicherheitskultur assoziiert (S.14):

1. Hardware: gute Anlagengestaltung, Arbeitsbedingungen und Housekeeping (Ordnung und Zustand der Anlage); geringes wahrgenommenes Risiko aufgrund des Vertrauens in das technische System.
2. Managementsysteme: Vertrauen in die Sicherheitsregeln, -prozeduren und -vorkehrungen; Zufriedenheit mit Trainings, Sicherheit steht über Profiten und Produktion, gutes organisationales Lernen, Gute Kommunikation am Arbeitsplatz.
3. Mitarbeiter: Hohe Mitarbeiterbeteiligung beim Thema Sicherheit, Vertrauen in die Belegschaft, Risiken zu bewältigen, für das Management haben Sicherheitsbelange eine hohe Bedeutung, hoher Grad an Sicherheitsbeteiligung und Selbstverpflichtung gegenüber Sicherheitsfragen.
4. Verhalten: Akzeptanz der persönlichen Verantwortung für Sicherheit; häufige informale Sicherheitskommunikation; Bereitschaft über Sicherheit zu sprechen; eine umsichtige Einstellung zum Risiko.
5. Organisationale Faktoren zum Sicherheitsklima: Geringe Arbeitsbelastung; hohe Arbeitszufriedenheit

Aufgrund der Tatsache, dass Sicherheitsmanagement allein zu kurz greift, schlagen Kadri und Jones /68/ einen Ansatz vor, der Organisationen hilft, den Zustand ihrer Sicherheitskultur selbst zu beurteilen. Die Verbesserung der Sicherheitskultur kann durch eine Sensibilisierung für Sicherheitskulturthemen und deren Anwendung auf das eigene Unternehmen geschehen, sowie durch

die Verwendung spezifischer Indikatoren, durch die Verbesserungspotenziale identifiziert werden können. Die vorgeschlagenen Indikatoren decken mögliche Mängel auf, d. h. es sind Indikatoren für eine eher schlechte Sicherheitskultur:

Als Indikatoren, die auf die fehlende Aufrechterhaltung eines Gefährdungsbewusstseins hinweisen werden folgende genannt /68/:

- Es wird angenommen, dass die Sicherheitssysteme ausreichend sind.
- Kritische Alarme werden als Handlungsindikatoren verwendet.
- Es werden Verzögerungen in der vorbeugenden Instandhaltung von kritischen Arbeitsmitteln gestattet.
- Es findet keine Auseinandersetzung mit Störfällen aus verwandten Industrien auf den verschiedenen Organisationsebenen statt und es wird nicht aus ihnen gelernt.
- Es wird nicht gehandelt, wenn vergleichbare Mängel festgestellt wurden.

Als Indikatoren, die auf eine Duldung von Abweichungen hinweisen, werden folgende genannt:

- Es wird gestattet, dass das System außerhalb von festgelegten Sicherheitsgrenzen arbeitet ohne eine detaillierte Risikobewertung.
- Es werden Abweichungen von festgelegten Vorgehensweisen ohne die Überprüfung und Zustimmung des Veränderungsmanagements gestattet.
- Absichtliche bewusste Verletzung von festgelegten Vorgehensweisen wird ohne eine Abschätzung der Konsequenzen für die beteiligten Personen toleriert.
- Das Personal kann nicht dazu gebracht werden, den Vorgehensweisen streng zu folgen, wenn die Einhaltung nicht überwacht wird.

Indikatoren, die zeigen, dass geeignete Gefährdungsanalysen und Risikoabschätzungen fehlen, sind folgende:

- Die Verfügbarkeit von bewährten Hilfsmitteln zur Risikobewertung ist begrenzt.
- Die Empfehlungen aus der Risikobeurteilung sind nicht aussagekräftig.
- Die Empfehlungen aus der Risikobeurteilung werden nicht rechtzeitig umgesetzt.
- Die Umsetzung der Maßnahmen weicht von der Zielsetzung der ursprünglichen Empfehlungen ab.

- Die Zurückweisung von Empfehlungen der Risikobewertung basiert hauptsächlich auf subjektiven Bewertungen oder vorhergehender Erfahrung und Beobachtung.

Als Indikatoren für fehlende Unabhängigkeit der Sicherheitsbelange werden die Folgenden identifiziert:

- Personen, die sicherheitsrelevante Entscheidungen begleiten, sind nicht ausreichend technisch qualifiziert und nicht unabhängig.
- Schlüsselpositionen im Prozesssicherheitsmanagement wurden im Laufe der Zeit herabgestuft.
- Empfehlungen zur Verbesserung der Sicherheit wurden aus Kostengründen oder aus Gründen der Arbeitsplanung zurückgestellt.
- Es existiert kein System vor Ort, das die hauptsächlichen Sicherheitsprobleme unabhängig überprüft.
- Prüfungen werden als negativ oder bestrafend angesehen und von Personen durchgeführt, die technisch nicht kompetent sind.

Indikatoren, die auf fehlende offene und freie Kommunikation auf allen Ebenen hindeuten, sind die Folgenden:

- Der Überbringer von “schlechten Nachrichten” wird als “nicht teamfähig“ angesehen.
- Das Stellen sicherheitsbezogener Fragen wird dadurch „belohnt“, dass überprüft wird, ob der/ die Fragende im Recht ist.
- Kritische sicherheitsrelevante Nachrichten, die offizielle Kanäle umgehen, sind nicht gerne gesehen.
- Die Kommunikation wird abgeändert, die Nachrichten abgemildert, je höher sie die Managementebenen heraufsteigt.
- Angestellte können mit niemandem frei und ohne Furcht vor Karrierere-pressalien über ihre persönlichen Sicherheitsbelange sprechen. (S. 19).

Die HSE veröffentlichte in ihrem Offshore Technology Report 1999 /65/ einen zusammenfassenden Leitfaden über Sicherheitsklima-Tools. Der Leitfaden soll dabei helfen, einen Überblick über fragebogenbasierte Werkzeuge zur Messung des Sicherheitsklimas einer Organisation zu geben. Dafür werden nützliche und notwendige Skalen beziehungsweise Items vorgestellt. In dem Bericht werden die folgenden Empfehlungen zur Methodik der Durchführung des Sicherheitsklimas gegeben:

- Die Vorbereitung des Einsatzes eines Befragungsinstrumentes zum Sicherheitsklima ist wesentlich. Es ist unwahrscheinlich, dass ein Instrument gut funktioniert, es kann sogar negative Effekte erzeugen, wenn

das Management zu wenige Bemühungen in die Vorbereitung investiert. Wenn es sich nicht verpflichtet fühlt aufgrund der Ergebnisse, welche es auch immer sein mögen, zu handeln und wenn es nicht gelingt, die gesamte Belegschaft über den gesamten Prozess zu beteiligen.

- Die Teilnehmer der Befragung müssen wissen, warum die Befragung durchgeführt wird und wie die Ergebnisse verwendet werden.
- Es ist wichtig, dass es einen schnellen, aber realistischen Umsetzungsplan nach der Befragung gibt. Es müssen nach Abschluss der Befragung so schnell wie möglich sichtbare Ergebnisse erreicht werden.
- Die Ergebnisse der Befragung müssen so schnell wie möglich an die Befragtengruppe zurückgemeldet werden.
- Themen und Bereiche, in denen Schwächen durch die Befragung identifiziert wurden, müssen mit den Verantwortlichen diskutiert werden, um Details ihrer Belange zu klären.
- Nach der Klärung der Details sollte ein Handlungsplan erstellt werden, der die größten Schwächen benennt. Der Plan kann auch Schulungen zur Verhaltensmodifikation enthalten.
- Während der Umsetzung des Handlungsplans sollte eine Überprüfung durchgeführt werden, um den Fortschritt festzustellen. Die Ergebnisse der Überprüfung sollten den Mitarbeitern zurückgemeldet werden.
- Eine Wiederholungsmessung sollte nicht eher durchgeführt werden, bis der Handlungsplan für die in der ersten Betragung festgestellten Mängel umgesetzt wurde. /65/, S. 11.

In Bezug auf Items und Skalen, werden die folgenden Kernitems identifiziert:

- Training und Kompetenzen
- Arbeitsplatzsicherheit und Arbeitszufriedenheit
- Produktionsdruck
- Kommunikation
- Wahrnehmung der persönlichen Beteiligung an Gesundheit und Sicherheit
- Unfälle, Störfälle und Beinahe-Ereignisse
- Wahrnehmung der organisationalen und führungsbezogenen Verpflichtung für Gesundheit und Sicherheit im Allgemeinen und Speziellen.
- Verdienste der gesunden und sicheren Vorgehensweisen, Anweisungen und Regeln.
- Regelverstöße

- Standpunkt der Belegschaft zum Zustand der Sicherheitskultur.
- Beurteilung der Sicherheitsstufen.

Des Weiteren werden zusätzliche Items genannt, die Bestandteil einer Bewertung sein können:

- Notfallplanung
- Instandhaltung
- Aufgabenverteilung und Arbeitsgestaltung
- Arbeitsdruck
- Arbeitsumgebung
- Individuelle Fähigkeiten, Eigenschaften, Fertigkeiten und die Gesundheit
- Handlungsweisen
- Sicherheitsprioritäten
- Führung und Führungsstrukturen einschließlich Entscheidungen und Gruppenarbeit

Die ILK /63/ nennt Beispiele von Indikatoren, die bei einer Selbstbewertung berücksichtigt werden sollen (S.22). Die ILK schlägt weiterhin vor, alle 2-3 Jahre und nach bedeutsamen organisationalen Veränderungen eine Selbstbeurteilung bezüglich der folgenden Elemente mit den dazugehörigen Indikatoren durchzuführen.

1. Verantwortlichkeit für Sicherheit ist eindeutig festgelegt:

- Führungskräfte müssen definierte Sicherheitsziele erreichen
- Anerkennungen für erreichte Leistungen
- Mitarbeiter werden bei der Verbesserung der Sicherheit eingebunden
- Teambewertungen berücksichtigen die realisierte Sicherheit

2. Sicherheit ist lerngesteuert:

- Programme zur Umsetzung von Erkenntnissen aus Betriebserfahrungen
- Vertrautheit mit Lernprozessen
- Programme zur Behandlung wiederkehrender Ereignisse
- Prozesse zur Fehlervermeidung durch Stärkung des Barrierenprinzips
- Fehler stellen eine Möglichkeit zum Lernen dar

3. Hoher Stellenwert der Sicherheit:

- Sicherheitsressourcen sind der Arbeitsbelastung angemessen
- Sicherheitsbedenken können offen angesprochen werden und sicherheitsgerichtetes Verhalten wird aktiv unterstützt
- Teamarbeit zwischen Abteilungen wird gefördert

4. Sicherheit ist eine eindeutige Führungsaufgabe:

- Die oberste Führungsebene wendet Zeit und Einsatz zur Verbesserung der Sicherheit auf
- Sicherheitskulturtraining ist verfügbar und wird von Führungskräften genutzt
- Häufige Kommunikation zwischen Führungskräften und Mitarbeitern
- Niveau der persönlichen Verantwortlichkeit für Sicherheit

5. Führungsverhalten:

- Eindeutige Vorgaben und Erwartungen
- Führungskräfte bestärken das erwartete Verhalten

Zum Zusammenhang von Sicherheitsmanagement und Sicherheitskultur stellt das U.S. Chemical Safety and Hazard Investigation Board zusammenfassend in seinem Bericht /69/ über die Explosion der Raffinerie in Texas City fest, dass „Sicherheitsmanagementsysteme zum Schutz notwendig sind, aber das es viel mehr erforderlich ist, schwere Unfälle zu verhindern. Wirkungsvolle organisatorische Beispiele, wie die Analyse und Dokumentation von Ereignissen und dass angemessene Möglichkeiten für sicheres Handeln ermittelt werden, sind erforderlich, damit Sicherheitssysteme erfolgreich arbeiten" /69/, S. 139.

Eine der identifizierten kulturellen Ursachen war, dass die BP Gruppe und die Manager von Texas City vor dem Unfall Sicherheitsveränderungen vornehmen wollten, „aber der Fokus war weitgehend auf die persönliche Sicherheit anstatt auf die Prozesssicherheit gelegt worden. Weil sich die Statistik der Personenschäden verbesserte, dachten die Verantwortlichen der BP Gruppe, dass sich die Sicherheit in die richtige Richtung entwickelte" /69/, S. 139f.

Aus dem Bericht geht hervor, dass die Anzahl von Personenschäden kein geeigneter Indikator zur Messung von Prozesssicherheit ist.

2.2 Diskussion auf dem Workshop

In der thematischen Sitzung „Bewertung von Sicherheitskulturen“ wurden verschiedene existierende Ansätze, Methoden und Instrumente zur Bewertung von Sicherheitskulturen vorgestellt.

Von besonderer Bedeutung war in dieser thematischen Sitzung die Identifizierung von Schlüsselelementen für die Beschreibung und Bewertung von Sicherheitskulturen, um auf dieser Grundlage Empfehlungen zu Bewertungskriterien für Sicherheitskulturen in der verfahrenstechnischen Industrie abzuleiten. Ein weiterer Fokus der Betrachtungen lag auf der Identifikation von relevanten Elementen, Dimensionen, Strukturen, Gruppen und verschiedenen Entwicklungsstufen der Sicherheitskultur in Unternehmen. Darüber hinaus sollte der Nutzen der Bewertungen von Sicherheitskulturen diskutiert werden.

In diesem Zusammenhang bleibt festzuhalten, dass es bis zum heutigen Zeitpunkt keine allgemein verbindlichen Empfehlungen über Methoden zur Bewertung und Sicherstellung von Sicherheitskultur gibt. Trotz der weiten Verbreitung und der Verwendung des Begriffes Sicherheitskultur sowie der Betonung der Wichtigkeit dieser in Organisationen bleiben das theoretische Verständnis und die praktische Umsetzung des Konzeptes weiterhin vage.

Ein ungeklärtes Problem stellt nach wie vor die Beurteilung der Sicherheitskultur insbesondere in Abgrenzung zum Konzept des Sicherheitsklimas dar. Es werden zwar viele Schlüsselelemente der Sicherheitskultur und ebenso viele verschiedene Instrumente zur Bewertung dieser vorgeschlagen, doch erweist sich die Messung/Beurteilung der Indikatoren als äußerst schwierig, da eine Validierung von Verfahren für die verfahrenstechnische Industrie bisher noch aussteht. Spezifische Probleme ergeben sich insbesondere bei der Wahl der Bewertungsebene (individuelle, organisationale oder Gruppenebene), der Bewertungstiefe (Screening oder differenzierte Analyse) oder Bewertungsart (Selbst- oder Fremdbeurteilung).

Weitgehende Übereinstimmung besteht hingegen darin, dass Bewertungen der Sicherheitskultur regelmäßig und nach bedeutsamen Veränderungen in der Organisation durchgeführt werden sollten; dass Selbstbeurteilungen lernende Organisationen unterstützen können; dass sich das fünfstufige Reifegradmodell /67/ gut bewährt hat und als Grundlage für die Bewertung und Entwicklung von Sicherheitskulturen verwendet werden könnte und dass die Bewertung der Sicherheitskultur über die Analyse von Artefakten und ausgesprochenen Werten (espoused values) hinausgehen muss.

2.3 Zusammenfassung und Fazit

Aus Sicht der Autoren ist Sicherheitskultur ein holistisches und ganzheitliches Konzept, das nicht nur das Verhalten der Mitglieder einer Organisation selbst, sondern aller Mitglieder eines System im weiteren Sinne einschließt: einzelne Organisationsmitglieder, Arbeitsgruppen, organisatorische Eigenschaften und Einheiten, besondere organisatorische Umgebungen, z.B. Aufsichtbehörden, Technologie.

Zur Identifizierung von relevanten Schlüsselelementen der Sicherheitskultur wurden in diesem Kapitel verschiedene Quellen hinsichtlich der Gemeinsamkeiten und Unterschiede in den Elementen bzw. Komponenten analysiert:

- Offizielle Dokumente der OECD /2, 59/, IAEA /50, 60, 61/, Responsible Care /62/, ILK /63/ und HSE /64, 65/
- Wissenschaftliche Literatur aus den Bereichen Psychologie, Human Factors, Organisationswissenschaften

Die daraus resultierenden Schlüsselelemente der Sicherheitskultur sind:

- Förderung einer betrieblichen Sicherheitskultur und Spiegelung in der betrieblichen Sicherheitspolitik,
- ein klares und sichtbares Interesse an Sicherheit,
- Förderung von Initiativen und Aufmerksamkeit im Sinne der Sicherheit,
- Sicherheit als Führungsaufgabe: Sicherstellen durch das Management, dass sich alle Beschäftigten ihrer Aufgaben und Verantwortlichkeiten in Bezug auf Sicherheit bewusst sind und dass sie über die Fähigkeiten, Schulung, Ausbildung, Unterstützung und Mittel verfügen, die dazu notwendig sind. Die Leitung sollte sich vergewissern, dass alle Sicherheitsvorschriften weitergegeben worden sind und sie allen Beschäftigten bekannt und von ihnen verstanden worden sind.
- Vermeidung von Selbstzufriedenheit, ständige Bemühungen, um die Sicherheit aufrechtzuerhalten,
- Verbesserung der Sicherheitskultur durch eine offene Haltung des Managements gegenüber der Öffentlichkeit in Bezug auf Sicherheitsfragen,
- eine klare und schriftliche Darlegung der im gesamten Unternehmen verbreiteten Sicherheitspolitik, die die betriebliche Sicherheitskultur widerspiegelt und die übergeordneten Ziele und Prinzipien im Hinblick auf Sicherheit in der verfahrenstechnischen Industrie enthält,
- Partizipation der Beschäftigten auf allen Ebenen im Hinblick auf die Sicherheitspolitik,

- Unabhängigkeit der für die Entwicklung der betrieblichen Sicherheitspolitik verantwortlichen Beschäftigten vom Produktionsmanagement mit einem direkten Zugang zur obersten Leitungsebene,
- Kommunikation der Sicherheitspolitik, Verstehen und Würdigung der Inhalte durch allen Beschäftigten,
- Zusammenarbeit von Management und Beschäftigten bei der Einhaltung der betrieblichen Sicherheitspolitik und der Erfüllung der Sicherheitsziele
- Zugänglichkeit der Sicherheitspolitik für die Öffentlichkeit,
- Entwicklung von Sicherheitsprogrammen für jeden Standort, die sich eingehend mit standortspezifischen Sicherheitsbelangen und Anforderungen befassen,
- Koordination und Abstimmung der betrieblichen Sicherheitspolitik mit den Bereichen Arbeits-, Gesundheits- und Umweltschutz,
- organisationales Lernen und Fehlerbehandlung (Fehlerkultur),
- hinterfragende Einstellung,
- systemisches Denken,
- Rollenbild von Managern und Vorgesetzten, der Führung,
- Professionalität,
- Übereinstimmung von impliziten und expliziten Normen,
- Motivation und Arbeitszufriedenheit.

Die Bewertung der Sicherheitskultur ist in verschiedenen Industriebereichen eingeführt und hat als wichtiges Werkzeug die Verbesserung der Sicherheit in der Prozessindustrie gefördert. Erforderlich ist die Entwicklung und Verbreitung von geeigneter Information und die Anleitung von Unternehmen, so dass sie ihre Sicherheitskultur selbst beurteilen und deren Qualität weiterentwickeln und verbessern können. Obwohl es unterschiedliche Instrumente zur Bewertung von Sicherheitskultur gibt, bleibt es nach wie vor unklar, welche Ebenen zu beurteilen sind und wie sie zu messen sind: Normen, Werte oder Grundannahmen und wie beobachtbares Verhalten und Artefakte gemessen werden sollen. Die in der Literatur genannten Indikatoren erheben nur Einstellungen und Verhalten und ausgesprochene Werte (espoused values) und sind schwierig zu messen und zu beurteilen. Indikatoren für zugrundeliegende Normen, Werte und Grundannahmen existieren bislang nicht. Außerdem gibt es für die verfahrentechnische Industrie bislang kein validiertes Instrument zur Bewertung der Sicherheitskultur.

Des Weiteren gibt es keinen Konsens darüber, welche Gruppen bzw. Strukturen die Bewertung umfassen soll, nur den Operateur, Manager, Top-Management oder auch Gruppen außerhalb der Organisation, wie Aufsichtsbehörden und Gesetzgeber.

Wilpert et al. /66/ benennen nicht nur relevante Schlüsselelemente der Sicherheitskultur, sondern auch welche Gruppen in die Analyse einzubeziehen sind. Externe und interne Gruppen, die in die Bewertung der Sicherheitskultur eingebunden sind, sollten aus folgenden Bereichen stammen /66/, die aus Sicht der Autoren dieses Berichts hier für die verfahrenstechnische Industrie leicht angepasst wurden:

1. interne und externe Aufsicht (wie Aufsichtsbehörden, Störfallbeauftragte)
2. leitendes Management
3. Betriebsleitung
4. Vorgesetzte (wie Schichtführer)
5. Mitarbeiter
   - Betrieb
   - Instandhaltung
   - Überwachung (wie Werksschutz, Werksfeuerwehr, Objektschutz)
   - Rechnungswesen
   - Logistik
   - Einkauf
   - Personalabteilung
6. Fremdpersonal

Bei einer ersten Bewertung der Sicherheitskultur müssten dann die folgenden Faktoren auf den unterschiedlichen Beurteilungsebenen verwendet werden:

1. individuelle Ebene
   - kognitive Fähigkeiten
   - Regelbefolgung
   - Qualifikation
   - Risikowahrnehmung
   - Einstellungen /Motivation
   - physiologische Einflüsse
   - Engagement für Sicherheit
   - Verhalten
2. Gruppenebene
   - Kommunikation
   - Gruppendynamik
   - Führung/Kontrolle
   - soziale Normen, Vorbild

3. organisationale Ebene:
   - Grundannahmen der Organisation
   - Ziele und Visionen
   - Planung
   - Ressourcen
   - Prozessmanagement und Prozessbewertung
   - Erfahrungslernen (organisationales Lernen)
   - Schulung, Training
   - Information und Dokumentation
   - Anreizsysteme
4. Technik

Übereinstimmung hingegen herrscht in der Fachliteratur dahingehend, dass Sicherheitskulturbewertungen regelmäßig wiederholt und zusätzlich nach bedeutsamen Änderungen der Organisation durchgeführt werden sollten. Unterschiedliche Vorschläge werden nur hinsichtlich der Form der Durchführung der Bewertungen gemacht. Es kommen hierfür einerseits Selbstbewertungen der Organisation in Frage anderseits sind auch Fremdbewertungen durch Dritte denkbar.

Weiterhin wird darauf hingewiesen, dass das Sicherheitsklima als ein erster Zugang zur Sicherheitskultur mit Hilfe eines Fragebogens mit den oben genannten Inhalten beurteilt werden kann. Ebenfalls geeignet erscheint ein Screening-Verfahren als eine erste Annäherung an die Bewertung der Sicherheitskultur. Ein Beispiel für ein solches Verfahren, das die oben genannten Faktoren und Ebenen beinhaltet, ist in Anhang IV dargestellt. Die bereits aufgeführten Mitarbeitergruppen sollten bei einer Selbstbewertung befragt werden.

Für die Beurteilung der Sicherheitskultur ist jedoch insgesamt ein eher holistischer Ansatz erforderlich, das heißt, Fragebögen sollten zusätzlich durch Beobachtungen, Dokumentanalysen, Interviews oder Gruppenfeedback-Analysen ergänzt werden /66/.

Es herrscht Konsens darüber, dass Sicherheitskultur verschieden weit entwickelt sein kann, wie das Stufenmodell zeigt. Zu klären bleibt allerdings, wie geeignete Interventionen aussehen sollen, die zu einer Verbesserung oder Förderung der Sicherheitskultur führen.

Zur Umsetzung und Vertiefung der Ergebnisse des OECD/CCA-Workshops und dieses Vorhabens wird daher ein weiteres Vorgehen in zwei Schritten vorgeschlagen.

Im ersten Schritt sollte auf der Basis des Screening-Verfahrens (Anhang IV) ein Leitfaden zur Selbstbewertung der Sicherheitskultur für die verfahrenstechni-

sche Industrie in Deutschland entwickelt werden. Dieser Leitfaden sollte sowohl Hinweise für die einzubeziehenden Gruppen, Ebenen und Inhalte als auch über die Erhebung (wie Wiederholungshäufigkeit) und Analyse (wie quantitativ vs. qualitativ oder Geltungsbereich) enthalten.

In einem zweiten Schritt sollten die Anwendung und die Umsetzung des Leitfadens in der Praxis anhand von ausgewählten Betrieben überprüft und gegebenenfalls Anpassungen vorgenommen werden.

Im Rahmen der Überprüfung des vorgeschlagenen Leitfadens in ausgewählten Betrieben sollten auch Ansätze zur Ergänzung einer Befragung entwickelt sowie geklärt werden, wie die unterschiedlichen Mitarbeitergruppen am besten in den Veränderungsprozess eingebunden werden sollten und wie eine nachhaltige Verbesserung zu erreichen ist.

In der Literatur bleiben jedoch einige Fragen offen, die auch trotz intensiver Diskussion auf dem Workshop nicht umfassend beantwortet werden, so dass hier weiterhin Forschungsbedarf besteht:

1. Welche Alternativen bestehen hinsichtlich Indikatoren zur Bewertung der Sicherheitskultur?
2. Sollten die Ergebnisse der Bewertung der Sicherheitskultur in Geschäftsberichten der Unternehmen veröffentlicht werden?

3 Kompetenzen im Thema menschliche und organisationale Faktoren

Im Folgenden werden für verschiedene Management- und Mitarbeiterebenen unterschiedlicher Organisationen die erforderlichen Kompetenzen im Thema menschliche und organisationale Faktoren anhand einer Literaturanalyse ermittelt. Dabei wird den Fragen nachgegangen, welche Gruppen für die Sicherheit relevant sind und beteiligt werden sollten (Kap. 3.1.1) und welche Kompetenzen hinsichtlich Sicherheit relevant sind (Kap. 3.1.2). Im Anschluss daran erfolgt eine Darstellung des Workshops (Kap. 3.2) und eine abschließende Zusammenfassung mit Fazit (Kap. 3.3).

3.1 Stand der Wissenschaft

Die unterschiedlichen Management- und Mitarbeiterebenen in Organisationen (Industrie, Aufsichtsbehörden, Sachverständigenorganisationen) haben verschiedene Verantwortlichkeiten, die spezifische Kenntnisse und Kompetenzen im Thema menschliche und organisationale Faktoren erfordern. Das Personal im Sicherheitsbereich ist in Sicherheitsfragen technisch kompetent und gut ausgebildet, hat aber normalerweise keine spezifischen Kenntnisse über soziale Sicherheitsaspekte. Auch die Kompetenzen im Thema menschliche und organisationale Faktoren sind häufig wenig entwickelt.

Weil dieses Thema relativ neu ist, gibt es nur einige wenige Quellen aus den Bereichen Kerntechnik und Luftfahrt, die die Grundlage für dieses Kapitel bilden.

3.1.1 Welche Gruppen sollten beim Thema Sicherheit beteiligt werden?

Die IAEA /70/ identifiziert die folgenden relevanten vier Akteure mit den dazugehörigen Kompetenzfeldern, die in Tabelle 4 dargestellt werden.

Tabelle 4: Relevante Akteure und Kompetenzfelder für ein Rahmenprogramm für Training und Ausbildung in nuklearer Sicherheit /70/

Relevante Akteure	**Kompetenzfelder**
Aufsichtsbehörden	Aufsicht und Kontrolle
Hersteller- und Zulieferorganisationen	Planung & Design von Kernkraftwerken
Anlagen- und Betreibermitarbeiter	Kraftwerksbetrieb
Forschungs- und Trainingsorganisationen	Forschungsreaktordesign, Betrieb & Nutzung

Die EU reguliert in ihrer Verordnung (EG) Nr. 2042/2003 der Kommission vom 20. November 2003 /71/ über „die Aufrechterhaltung der Lufttüchtigkeit von Luftfahrzeugen und luftfahrttechnischen Erzeugnissen, Teilen und Ausrüstungen und die Erteilung von Genehmigungen für Organisationen und Personen“, unter anderem Qualifikationsanforderungen für Personen, die diese Tätigkeiten ausführen. Für folgende Personengruppen werden Qualifikationsanforderungen definiert:

- Kategorie A: **Wartungsmechaniker** (“line maintenance certifying mechanic”)
- Kategorie B1: **Wartungstechniker/-mechaniker** (“maintenance certifying technician/mechanical”)
- Kategorie B2: **Wartungstechniker/Avionik** (“maintenance certifying technician/avionic”)
- Kategorie C: **Wartungsingenieur** (“base maintenance certifying engineer”)

Die Klassifikationen aus beiden Industriebereichen haben einige Relevanz für die verfahrentechnische Industrie, sind aber nicht einfach übertragbar. Für die verfahrenstechnische Industrie erscheint in Bezug auf Kompetenz im Thema menschliche und organisationale Faktoren die folgende erste Gruppenbildung relevant:

- Mitarbeiter von Aufsichtsbehörden
- Management
- Sicherheitspersonal (Sicherheitsingenieure, -fachkräfte) und Sachverständige
- Operateure

3.1.2 Für die Sicherheit relevante Kompetenzen bezüglich menschlicher und organisationaler Faktoren

In ihrem Rahmenprogramm für Training und Ausbildung in der nuklearen Sicherheit identifiziert die IAEA vier Kompetenzkategorien und entsprechende Trainingsinhalte /70/:

1. **Behördliche Kontrolle**
   - Arbeitsgenehmigung (authorization process)
   - Überprüfung und Bewertung (review and assessment)
   - Begehung und Durchführung (inspection and enforcement)
   - Entwicklung von Vorschriften und Leitfäden (development of regulation and guides)
   - Behördliche Effektivität (regulatory effectiveness)

2. **Sicherheitsbewertung von Kernkraftwerken**
   - Methoden zur Unfallanalyse (accident analysis methods)
   - Probabilistische Sicherheitsanalyse (probabilistic safety assessment)
   - Störfallmanagement (accident management)
   - Alterungsmanagement (ageing management)
   - Sicherheitsbewertung von Änderungen (safety assessment of modifications)
3. **Betriebliche Sicherheit von Kernkraftwerken**
   - Sicherheitskultur und Sicherheitsmanagement (safety culture and management of safety)
   - Bediener-Regler-Schnittstelle (NPP operator regulator interface)
   - Handlungserfahrung und Rückmeldung (operational experience and feedback)
   - Betriebliche Praktiken (operational practices)
4. **Sicherheit von Forschungsreaktoren**
   - Behördliche Vorgaben und Sicherheitsdokumentation (regulatory aspects and safety documentation)
   - Sicherheitsanalysen (safety analysis)
   - Handlungssicherheit und Sicherheit bei Auslastung (safety in operation and utilization)
   - Alterungsmanagement (management of ageing)
   - Sicheres Abfahren und Stilllegung (safe shutdown and decommissioning)

In Bezug auf die Kompetenz der Mitarbeiter in der Luftfahrt stellt die EU fest /71/: “Der Betrieb muss die Befähigung des mit Instandhaltungsarbeiten, Verwaltungsaufgaben und/oder Qualitätskontrollen befassten Personals in Übereinstimmung mit Verfahren und Bestimmungen festlegen und überwachen, die von der zuständigen Behörde genehmigt sind. Zusätzlich zu der für die Arbeitsaufgabe erforderlichen Sachkenntnis muss die Befähigung das Wissen um die Bedeutung menschlicher Faktoren und des menschlichen Leistungsvermögens einschließen entsprechend der Funktion der Person in dem Betrieb. „Menschliche Faktoren” stehen für Prinzipien, die für den Flugzeugbau, die Zulassung, die Schulung, den Betrieb und die Instandhaltung in der Luftfahrt gelten und die auf eine sichere Wechselbeziehung zwischen menschlichen und anderen Systembestandteilen bei angemessener Berücksichtigung der menschlichen Leistung abzielen. „Menschliches Leistungsvermögen” sind menschliche Fähigkeiten und Grenzen, die sich auf Sicherheit und Leistung von Vorgängen in der Luftfahrt auswirken.“/71/, S.50

In der Verordnung werden Vorgaben für den Wissenstand beschrieben. Die Wissensstandindikatoren sind wie folgt definiert:

Wissensstand 1

Kenntnis der Hauptelemente des Themas. Ziele: Der Antragsteller sollte die Grundelemente des Themas kennen. Der Antragsteller sollte eine einfache Beschreibung des gesamten Themas in gängigen Worten und Beispielen geben können. Der Antragsteller sollte typische Begriffe verwenden können.

Wissensstand 2

Allgemeine Kenntnis der theoretischen und praktischen Aspekte des Themas. Fähigkeit zur Anwendung dieser Kenntnisse. Ziele: Der Antragsteller sollte die theoretischen Grundlagen des Themas verstehen können. Der Antragsteller sollte eine allgemeine Beschreibung des gesamten Themas unter Verwendung von jeweils typischen Beispielen geben können. Der Antragsteller sollte mathematische Formeln in Verbindung mit physikalischen Gesetzen, die das Thema beschreiben, verwenden können. Der Antragsteller sollte Skizzen, Zeichnungen und schematische Darstellungen, mit denen das Thema beschrieben wird, lesen und verstehen können. Der Antragsteller sollte sein Wissen unter Verwendung von detaillierten Verfahren praktisch anwenden können.

Wissensstand 3

Detaillierte Kenntnis der theoretischen und praktischen Aspekte des Themas. Fähigkeit zur Kombination und Anwendung der einzelnen Elemente seiner Kenntnisse auf logische und umfassende Weise. Ziele: Der Antragsteller sollte die Theorie des Themas und die Verknüpfungen mit anderen Themen kennen. Der Antragsteller sollte eine detaillierte Beschreibung des gesamten Themas unter Verwendung der theoretischen Grundlagen und spezifischer Beispiele geben können. Der Antragsteller sollte mathematische Formeln in Bezug auf das Thema verstehen und anwenden können. Der Antragsteller sollte Skizzen, einfache Zeichnungen und schematische Darstellungen, mit denen das Thema beschrieben wird, lesen, verstehen und erstellen können. Der Antragsteller sollte seine Kenntnisse unter Verwendung der Herstelleranweisungen praktisch anwenden können. Der Antragsteller sollte die Resultate aus verschiedenen Quellen und Messungen interpretieren und ggf. Korrekturmaßnahmen anwenden können.

Das Training von Mitarbeiterkompetenzen soll in Modulen durchgeführt werden, Modul 9 betrifft menschliche und organisationale Faktoren und hat die folgenden Inhalte:

1. **Generelle Aspekte:** Notwendigkeit der Berücksichtigung menschlicher Faktoren, auf menschliche Faktoren / menschliche Fehler zurückzuführende Zwischenfälle, Murphys Gesetz

2. **Menschliche Leistung und Einschränkung:** Sehen, hören, Informationsverarbeitung, Aufmerksamkeit und Wahrnehmung, Gedächtnis, Klaustrophobie und Zugänglichkeit
3. **Sozialpsychologie:** Verantwortung Einzelner und Gruppe, Motivation und Demotivation, Gruppendruck, “kulturelle” Belange, Teamarbeit, Management, Überwachung und Führung
4. **Leistungsbeeinflussende Faktoren:** Fitness / Gesundheit, Stress: häuslich und arbeitsbezogen, Zeitdruck und Termine, Arbeitsbelastung: Überforderung und Unterforderung, Schlaf und Müdigkeit, Schichtarbeit, Alkohol, Medikamente, Drogenmissbrauch
5. **Physikalische Umgebung:** Lärm und Abgase, Beleuchtung, Klima und Temperatur, Bewegung und Vibration, Arbeitsumgebung
6. **Aufgaben:** körperliche Arbeit, Routineaufgaben, Sichtprüfung, komplexe Systeme
7. **Kommunikation:** innerhalb des Teams und zwischen Teams, Arbeitsprotokollierung und -aufzeichnung, „auf dem Laufenden bleiben“, Aktualität, Informationsverbreitung
8. **Menschliche Fehler:** Fehlermodelle und -theorien, Fehlerarten bei Instandhaltungsarbeiten, Fehlerauswirkungen (d. h. Unfälle), Vermeiden und Bewältigen von Fehlern
9. **Gefahren am Arbeitsplatz:** Erkennen und Vermeiden von Gefahren, Umgang mit Notfällen

3.2 Diskussion auf dem Workshop

In der thematischen Sitzung „Kompetenz im Thema menschliche und organisationale Faktoren“ wurden für verschiedene Management- und Mitarbeiterebenen unterschiedlicher Organisationen - unter Berücksichtigung der jeweiligen Verantwortungsbereiche - die erforderlichen Kompetenzen im Thema menschliche und organisationale Faktoren ermittelt. Auf der Grundlage dieser systematischen Analyse wurden Empfehlungen für Trainings- und Ausbildungsprogramme zum Thema menschliche und organisationale Faktoren für die einzelnen Gruppen in der verfahrenstechnischen Industrie abgeleitet.

Aufgrund der Diskussion im Workshop wurde deutlich, dass für die verschiedenen beteiligten Gruppen in Abhängigkeit von den jeweiligen Verantwortlichkeiten unterschiedliche sicherheitsrelevante Kompetenzen im Thema menschliche und organisationale Faktoren in der verfahrenstechnischen Industrie wichtig sind. Darüber hinaus wurden der mögliche Trainingsbedarf und Trainingsprogramme besprochen.

Zu „Kompetenz im Thema menschliche und organisationale Faktoren“ konnten aufgrund der thematischen Sitzung folgende Schlussfolgerungen zusammengefasst formuliert werden:

- Insgesamt konnten 12 relevante Trainingsinhalte aus dem Bereich menschliche und organisationale Faktoren (generelle Aspekte, menschliche Leistung und Einschränkung, Human Resource Management, Ergonomie, Sozialpsychologie, leistungsbeeinflussende Faktoren, physikalische Umgebung, Aufgaben, Kommunikation, menschliche Fehler, Gefahren am Arbeitsplatz und Risikoanalysen, Krisenmanagement) und sechs relevante Gruppen (Gesetzgeber, Aufsichtsbehörden, strategisches und operative Management, Sicherheitspersonal und Operateure) identifiziert werden. Weiterhin werden drei verschiedene Wissensniveaus für die relevanten Gruppen empfohlen.
- Es ist erforderlich, dass eine “Toolbox“ für Methoden, Checklisten, wenn geeignet, und unterstützende Anleitungen für Inspektoren zur Identifikation sicherheitskritische menschliche Faktoren in der Anlage entwickelt werden. Vorhandene Anleitungen für Inspektionen sollten um das Element “menschliche und organisationale Faktoren” erweitert werden.

Weiterhin wurden als erforderlich angesehen:

- eine spezifischere Definition der Organisationsstufen, z. B. Mitarbeitergruppen, die ähnliche Kompetenzen im Thema menschliche und organisationale Faktoren benötigen.
- eine handlungszentrierte Definition von notwendigen Kompetenzen
- Ausbilder für Belange menschlicher und organisationaler Faktoren
- Evaluationskriterien für Trainingsprogramme

Aus der Diskussion dieses Themas in der Sitzung „Kompetenzen im Thema menschliche und organisationale Faktoren“ gingen abschließend folgende Empfehlungen hervor:

- Industrie und Behörden sollen Anforderungen an die „Kompetenzen im Thema menschliche und organisationale Faktoren“ ihres Personals definieren. Eine einfache Matrix mit vorgegebenen Kompetenzstufen kann als Basis dienen.
- Einbeziehung des Lebenszyklus einer Anlage führt ggf. der Mitarbeiter-Kompetenz-Gruppen: z. B. Planung, Entwicklung, Konstruktion, Instandhaltung, Lieferanten.
- Es sollte Inspektoren geben, die arbeits- und organisationspsychologische Kompetenzen besitzen, um relevante menschliche Faktoren in der Inspektion zu berücksichtigen.

Konkreter Forschungsbedarf besteht jedoch weiterhin zur Beantwortung der folgenden Fragen:

- Sind die genannten Gruppen mit den zugehörigen Verantwortlichkeiten relevant und vollständig?
- Sind die genannten Kompetenzfelder relevant und vollständig?
- Sind die genannten Wissensniveaus für die genannten Gruppen sinnvoll?

3.3 Zusammenfassung und Fazit

Für die verfahrenstechnische Industrie wurden in Bezug auf Kompetenzen im Thema menschliche und organisationale Faktoren folgende sechs Gruppen als relevant herausgearbeitet:

- Mitarbeiter regelsetzender Stellen
- Mitarbeiter von Aufsichtsbehörden,
- das strategische Management,
- das operative Management,
- das Sicherheitspersonal und Sachverständige,
- die Operateure.

Aus der Betrachtung von relevanten Kompetenzfeldern für die Luftfahrt und für die Kerntechnik /70, 71/ ist erkennbar, dass bereits umfangreiche Inhalte zum Thema „menschliche und organisationale Faktoren“, in Trainingsmodulen vermittelt werden. Insgesamt konnten zwölf Themenfelder identifiziert werden. Für die verfahrenstechnische Industrie sind die dort behandelten Themenfelder ebenfalls zu vermitteln, sollten jedoch um die Themen “Ergonomie“, „Krisen- und Human Ressource Management“ ergänzt werden:

- Ergonomie: Wissen über Mensch-Maschinen Interaktionen und Design
- Human Ressource Management: Rekrutierung und Training, Umgang mit leistungsbezogenen Belangen und Motivation
- Krisenmanagement: Prognose über potentielle Krisen and Planung darüber, wie damit umgegangen wird, Ursachenidentifikation von gegenwärtigen Krisen, Intervention, um Schäden zu minimieren und Risikokommunikation.

Zusammenfassend ergeben sich aus Sicht der Autoren für die verfahrenstechnische Industrie folgende Kompetenzfelder und entsprechende Trainingsinhalte, die in Tabelle 5 dargestellt werden.

Tabelle 5: Gruppenspezifische Kompetenzfelder

Kompetenzfelder	Wissenstand					
	Mitarbeiter von Aufsichtsbehörden		Management			
	Regel-setzer	Auf-sicht	Opera-tionales Mana-gement	Strate-gisches Mana-gement	Sicher-heits-perso-nal/ Sach-verstän-dige	Opera-teure
Generelle Aspekte	2	2	2	2	3	2
Menschliche Leistung und Einschränkung	1	2	2	1	3	2
Human Ressource Management	1	2	2	1	3	1
Ergonomie	1	2	2	1	3	1
Sozialpsychologie	2	2	2	2	3	2
Leistungsbeeinflus-sende Faktoren	1	2	2	1	3	2
Physikalische Umge-bung	1	2	2	1	3	2
Aufgaben	1	2	2	1	3	2
Kommunikation	1	2	2	2	3	2
Menschlicher Fehler	1	2	2	1	3	2
Gefahren am Arbeits-platz	1	2	2	1	3	3
Krisenmanagement	2	3	3	1	3	2

Entsprechend der Empfehlungen des OECD/CCA-Workshops wird vorgeschlagen, die obenstehenden Ergebnisse mittels eines Leitfadens zu präzisieren und zu implementieren.

Im ersten Schritt sollten in diesem Leitfaden die Kompetenzfelder, relevanten Gruppen und jeweils geforderten Kompetenzanforderungen genauer definiert werden.

Da es jedoch nicht nur um die Frage geht, wer welche Kompetenzen benötigt, sondern auch, wie diese erworben werden können, sollte in einem zweiten Schritt im Leitfaden die gruppenspezifischen Kompetenzfelder mit Lernzielen, Ausbildungsinhalten und adäquaten didaktischen Methoden beschrieben werden.

In der Luftfahrt ist der Nachweis der Vermittlung von Kompetenzen im Thema menschliche und organisationale Faktoren eine Anforderung des Regelwerkes. Für die verfahrenstechnische Industrie sollte daher diskutiert werden, inwieweit eine entsprechende Kompetenzvermittlung als ein Teil der Ausbildung einzuführen bzw. ein entsprechender Kompetenznachweis zu fordern ist.

4 Zusammenwirken von Bedienern und Schutzsystemen

In den folgenden Kapiteln werden zunächst die Grundlagen für eine anforderungsgerechte Gestaltung von Mensch-Maschine-Interaktionen dargestellt (Kap. 4.1.1) und dann spezifische Aspekte der Interaktion von Mensch und Schutzsystem insbesondere in nicht bestimmungsgemäßen Systemzuständen (Kap. 4.1.2) erläutert. Abschließend folgt die Diskussion auf den Workshop (Kap. 4.2) und eine Zusammenfassung mit Fazit (Kap. 4.3) im Hinblick auf dieses Kapitel.

4.1 Stand der Wissenschaft

Das Design und die Zuverlässigkeit von Schutzsystemen („interlock-systems“, „shut-off-systems“, „cut-off-systems“, „safety instrumented systems“ und nicht „control systems“) und ihre Interaktion mit dem Bediener haben eine Schlüsselrolle bei der Entwicklung von Beinahe-Ereignissen zu größeren Unfällen. Weniger Bedeutung wurde bisher der Tatsache beigemessen, dass die Schnittstelle zwischen Bediener und der Anlage im Störungsbetrieb anders als im Vergleich zum Normalbetrieb ist. Im Störungsfall hat der erfolgreiche Betrieb von Schutzsystemen eine übergeordnete Priorität und die Verhütung von größeren Unfällen hängt auch von der Qualität der Schnittstellen zwischen Schutzsystem und Bedienern ab und stellt damit ein spezielles Feld der Mensch-Maschine Funktionsteilung dar.

Für die Erarbeitung dieses Themas wurden die folgenden Quellen genauer analysiert:

1. Störfall-Verordnung (12.BImSchV) /72/, Seveso-II-Richtlinie /73/ und technische Normen (DIN EN 61511 /18, 74, 75/; DIN EN 61508 /76/; ISO/TC 159 /16/, VDI/VDE 2180-1 /77/; NE 031 /78/), EEMUA 191 /93/
2. Wissenschaftliche Quellen aus den Bereichen Psychologie und Human Factors

Im Fokus der Analysen stand die Klärung der Frage nach angemessenen Strategien basierend auf der Kenntnis menschlicher und organisationaler Faktoren für die Entwicklung effizienter Schnittstellen zwischen Bedienern und Schutzsystem.

4.1.1 Ergonomische Gestaltung der Mensch-Maschine-Interaktion

In komplexen Arbeitssystemen wie beispielsweise an Prozessleitsystemen in der verfahrenstechnischen Industrie bestehen die Aufgaben der Operateure heutzutage hauptsächlich in der Überwachung, Regelung und Steuerung von technischen Subsystemen. Mit zunehmender Automatisierung verändern sich die Aufgaben der Operateure, so dass sie mehr Überwachungsaufgaben höherer Ordnung auszuführen haben, weil sie die die Leistung der technischen Komponenten überwachen. Die Funktionsteilung zwischen Mensch und Maschine ist in komplexen Systemen also stark vom Automatisierungsgrad des Systems abhängig. Die aus der Aufgabenverteilung zwischen Mensch und Maschine resultierenden Anforderungen bezüglich der Prognose zukünftigen Systemverhaltens oder Systemzuständen auf der Grundlage von aktuell verfügbaren Systemparametern nehmen mit steigendem Automatisierungsgrad stetig zu und bestimmen damit maßgeblich die Interaktion zwischen Mensch und Maschine im Normalbetrieb, aber insbesondere auch im nichtbestimmungsgemäßen Betrieb. Generell lassen sich mit Hilfe der MABA-MABA (men are better at-machines are better at)-Prinzipien Hinweise zur Zuordnung von Funktionen an den Menschen oder die Maschine ableiten. In Tabelle 6 wird eine solche Liste dargestellt.

Tabelle 6: Funktionsverteilung zwischen Mensch und Maschine: MABA-MABA (men-are-better-at-machines-are-better-at) - Liste nach /83/ (nach Fitts, 1951)

Der Mensch ist besser im Bereich	Maschinen sind besser im Bereich
Signalentdeckung bei geringer Signalanzahl	Rasche Antwort auf Signale
Mustererkennung	Aufbringen großer Kräfte
Improvisation und Flexibilität	Kurzzeitige Informationsspeicherung
Langzeitige Informationsspeicherung und Zugriff	Deduktives Schließen
Induktives Schließen	Exaktes Ausführen von Operationen
Beurteilung	

Die Problematik, die mit einer Zunahme der Automatisierung verbunden ist, wird in der wissenschaftlichen Literatur seit langem diskutiert. So definieren beispielsweise Parasuraman und Riley /79/ „Automatisierung als Ausführung einer Funktion, die vorher von einem Menschen erledigt wurde und die nun von einem Maschinenagenten (normalerweise einen Computer) ausgeführt wird“ (S. 231).

In ihrem Rahmenmodell zur Automatisierung diskutieren Parasuraman et al. /80/ ebenfalls die Frage, an welchem Punkt des Informationsverarbeitungsprozesses automatisiert werden soll: Informationsaufnahme, Informationsverar-

beitung, Entscheidungsprozesse und Ausführungsprozesse, und an welchem dieser Punkte welcher Automatisierungsgrad realisiert wird (hoch vs. niedrig). Für die Stufe Entscheidung scheint nur ein niedriger Automatisierungsgrad angemessen.

Nach Endsley and Kiris /81/ gibt es fünf Automatisierungsstufen mit den zugeordneten Rollen (vgl. Abbildung 2).

Automatisierungsgrad		**Rollen**	
		Mensch	**System**
Keiner	1	entscheidet, handelt	-
Entscheidungsunterstützung	2	entscheidet, handelt	schlägt vor
Konsensueller Automatisierungsgrad	3	wirkt mit	entscheidet, handelt
Überwachter Automatisierungsgrad	4	Einspruch	entscheidet, handelt
Vollautomatisierung	5	-	entscheidet, handelt

Abbildung 2: Automatisierungsstufen (Endsley & Kiris /81/)

Sheridan /82/ diskutiert im Gegensatz dazu die folgenden acht Automatisierungsgrade:

1. Der Computer liefert keine Hilfe, der Mensch macht alles alleine
2. Der Computer schlägt alternative Wege zur Aufgabenausführung vor.
3. Der Computer schlägt eine Entscheidungsalternative vor und
4. …führt diese aus, wenn der Mensch sie bejaht.
5. …erlaubt dem Menschen für eine beschränkte Zeit zu widersprechen, bevor er sie automatisch ausführt.
6. …führt automatisch aus, informiert den Menschen darüber.
7. …führt automatisch aus, informiert den Menschen nur auf Anfrage.
8. Der Computer wählt aus, handelt und ignoriert den Menschen.

In der Fachliteratur sind verschiedene Forschungsergebnisse zu unterschiedlichen Problemen im Zusammenhang mit der Automatisierung dargestellt worden. Nachfolgend wird eine Auswahl von relevanten Erkenntnissen für die verfahrenstechnische Industrie aufgeführt.

Eines der bekanntesten Probleme ist das sogenannte „out-of-the-loop-unfamiliarity (OOTLUF)"-Phänomen, das die Effektivität der Beobachtungsvigilanz und –kontrolle einschränkt und so zu einem Verlust des Situationsbewusstseins führen kann /80, 83, 84/. Dabei zeigte sich, dass der Fähigkeitsverlust für kognitive Fähigkeiten größer ist als für routinierte psychomotorische Fähigkeiten. Um dem Fähigkeitsverlust entgegen zu wirken, ist es notwendig mit den Operateu-

ren ein regelmäßiges Training ohne Automatisierungsbedingungen durchzuführen /80/. Weiterhin konnte beobachtet werden, dass häufig ein Verlust des Situationsbewusstseins auftritt, der auf fehlendes Feedback, Übervertrauen in die Automatisierung und fehlendem Systemwissen zurückgeführt werden kann. In diesem Zusammenhang definiert Endsley das Situationsbewusstsein „als Wahrnehmung von Elementen aus der Umgebung innerhalb einer bestimmten räumlichen und zeitlichen Spanne, das Begreifen ihrer Bedeutung und die Übertragung auf deren zukünftigen Zustand“ /85/.

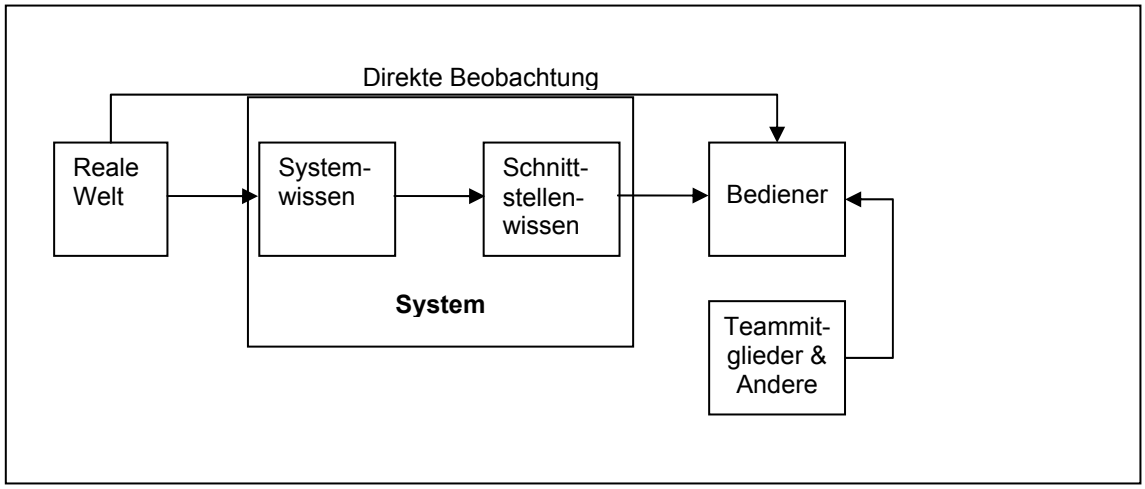


Abbildung 3: Informationsquellen für Situationsbewusstsein /85/

Ein hoher Automatisierungsgrad führt jedoch nicht zwangsläufig zu OOTLUF-Problemen, sondern die Art der Implementierung ist wichtig /86/: d. h. die Systemtransparenz (Information und Feedback für Wahrnehmung, Verstehen und Vorhersage des Systemstatus). Die vorgeschlagene Lösung ist die flexible Automatisierung, die von definierten Kriterien abhängen sollte und in Abbildung 4 dargestellt wird.

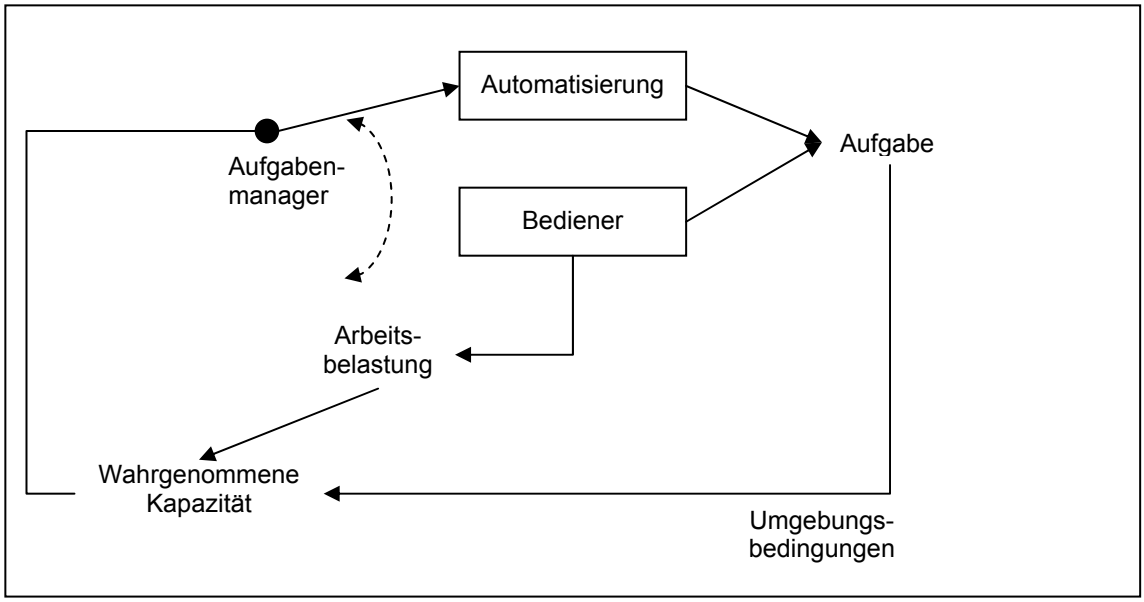


Abbildung 4: Modell der flexiblen Automatisierung /84/

Neben dem Grad der Automatisierung bereitet auch die Funktionsverteilung zwischen Mensch und Maschine bei der Gestaltung von Mensch-Maschine-Systemen immer wieder Probleme. Die ISO/TC 159/SC 1/WG 1 N 88 (2006) /16/ definiert Funktionszuordnung als „die Festlegung, durch wen Systemfunktionen zu erfüllen sind - durch Menschen, durch Arbeitsmittel und/oder Hardware und/oder Software“ (S.3) und Aufgabenzuordnung als „Aufteilung von Arbeitsaufgaben oder Arbeitsaufgabenelementen zwischen Operatoren und Systemen“ /16/, S.102.

In Abhängigkeit vom gewählten Automatisierungskonzept lassen sich unterschiedliche Kriterien zur Gestaltung konkreter Mensch-Maschine-Funktionsteilungen formulieren:

1. Kostenzentrierte Ansätze
   - Aufgaben werden dann automatisiert bzw. beim Menschen belassen, wenn die gewählte Lösung kostengünstiger ist.
   - Kostenfaktor „Mensch“ bzw. Technik soll minimiert werden,
   - Rein betriebswirtschaftliche Perspektive, psychologische Erkenntnisse und Aspekte bleiben unberücksichtigt.
2. Technikzentrierte Ansätze
   - Alle Aufgaben, die sich prinzipiell automatisieren lassen, werden automatisiert.
   - Risikofaktor „Mensch“ soll weitgehend ausgeschaltet werden.
   - Reduktion auf nicht-automatisierbare Resttätigkeiten (left-over principle) /87/.

- Primär ingenieurwissenschaftliche Perspektive.

3. Fähigkeitszentrierte Ansätze
   - Funktionsallokation nach Leistungsvorteilen.
   - Leitungsoptimierung (Geschwindigkeit, Genauigkeit).
   - MABA-MABA-Listen (men-are-better-at-machines-are-better-at).
   - Kompensationsgedanke (compensatory principle) /87/.
4. Menschenzentrierte Automatisierungskonzepte
   - Mensch und Maschine bilden ein kooperatives System, dessen Gesamtleistung optimiert werden muss
   - Aus dem menschenzentrierten Automatisierungskonzept lassen sich folgende übergeordnete Kriterien zur Funktionsallokation ableiten, die einer arbeitspsychologischen Perspektive zugeordnet werden können:
   - Erhalt vollständiger Arbeitstätigkeiten auf Seiten der Operateure - Arbeits- vs. technikorientierte Gestaltung /80/,
   - Erhalt von Gestaltungs- und Handlungsspielräumen - möglichst geringe zeitliche und inhaltliche Kopplung an die Technik /81/,
   - Nutzung vorhandener Qualifikationen, Erhalt von Prozessnähe durch Prozesstransparenz,
   - Aufbau und Erhalt von Erfahrungswissen.

Diese Ansätze fokussieren hauptsächlich auf direkte Schnittstellen. Wichtige Schnittstellen zu anderen Operatoren, zur Organisation oder der Umgebung werden jedoch nicht berücksichtigt.

4.1.2 Der Mensch als Element von Sicherheitssystemen

Die Richtlinie 96/82/EG des Rates vom 9. Dezember 1996 zur Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen (Seveso-II-Richtlinie /73/) dient der Verhütung schwerer Unfälle und der Begrenzung der Unfallfolgen für Mensch und Umwelt und soll in der gesamten Gemeinschaft konsequent und wirksam ein hohes Maß an Schutz gewährleisten.

Insbesondere ist nach Artikel 9 /73/ unter c) in einem Sicherheitsbericht nachzuweisen, dass "…die Auslegung, die Errichtung sowie der Betrieb und die Wartung sämtlicher Anlagen, Lager, Einrichtungen und die für ihr Funktionieren erforderlichen Infrastrukturen, die im Zusammenhang mit der Gefahr schwerer Unfälle im Betrieb stehen, ausreichend sicher und zuverlässig sind."

Weitere Konkretisierungen finden sich in der Störfall-Verordnung /72/. Zur Verhinderung von Störfällen sind Betriebsbereiche mit ausreichenden Warn-, Alarm- und Sicherheitseinrichtungen auszurüsten (§ 4, Nr. 2, StörfallV) und die Anlagen des Betriebsbereichs mit zuverlässigen Messeinrichtungen und

Steuer- oder Regeleinrichtungen auszustatten, die, soweit dies sicherheitstechnisch geboten ist, jeweils mehrfach vorhanden, verschiedenartig und voneinander unabhängig sind (§ 4 Nr. 3 StörfallV). Zur Begrenzung von Störfallauswirkungen sind die Anlagen des Betriebsbereichs mit den erforderlichen sicherheitstechnischen Einrichtungen auszurüsten sowie die erforderlichen technischen und organisatorischen Schutzvorkehrungen zu treffen (§ 5 Abs. 1 Nr. 2 StörfallV). Darüber hinaus wird von Betreibern gefordert, die Errichtung und den Betrieb der sicherheitsrelevanten Anlagenteile zu prüfen sowie die Anlagen des Betriebsbereichs in sicherheitstechnischer Hinsicht ständig zu überwachen und regelmäßig zu warten, die Wartungs- und Reparaturarbeiten nach dem Stand der Technik durchzuführen, und die erforderlichen sicherheitstechnischen Vorkehrungen zur Vermeidung von Fehlbedienungen zu treffen (§ 6, Abs. 1 StörfallV).

Zum Erhalt nutzbarer Empfehlungen zur Umsetzung dieser Anforderungen unter Beachtung menschlicher Faktoren müssen vier verschiedene, in Normen und Empfehlungen genannte /18, 74, 75, 78, 93/ Konstellationen der Interaktion von Bediener und Sicherheitssystem differenziert werden.

Erstens kann die Schnittstelle Bediener-Schutzsystem sich entweder zentral oder dezentral darstellen. Zentral ist die Schnittstelle in Leitwarten. Dezentral ist die Schnittstelle, wenn die Leitwarte nicht ständig besetzt ist oder keine Leitwarte vorhanden ist, z.B. weil die Anlagenteile dezentral von Steuerständen bedient werden.

Zweitens können die Schutzsysteme entweder vollautomatisch oder nur teilautomatisch sein. Bei Letzterem wird dadurch der Bediener Teil des Schutzsystems (der Sicherheitsfunktion).

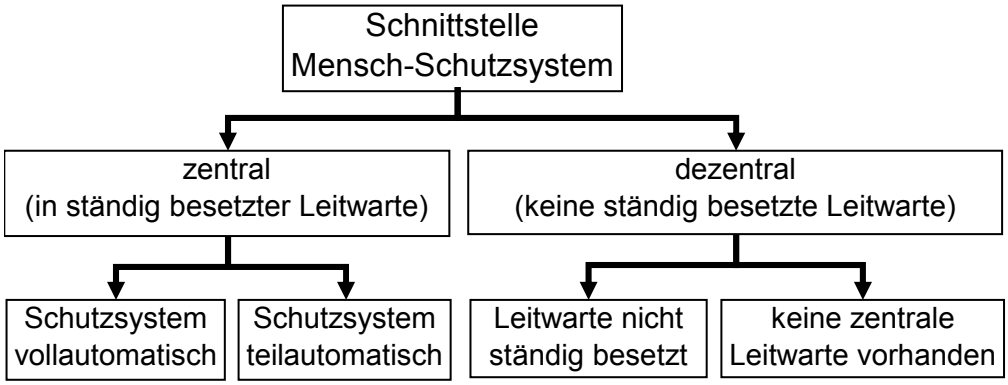


Abbildung 5: Mögliche Konstellationen der Schnittstelle Bediener-Schutzsystem

Die vier Systemvarianten von Sicherheitssystemen unterscheiden sich grundlegend in den Aufgaben, die die Bediener im Zusammenspiel mit dem Sicherheitssystem zu erfüllen haben. Während der Bediener in vollständig automa-

tisierten Systemen reine Überwachungsaufgaben ausführt, muss er in teilautomatisierten Systemen neben der Überwachung zusätzlich Steuerungs- und Regelungsaufgaben als Teil des Sicherheitssystems ausführen, um Störfälle durch sein Eingreifen zu verhindern. Bei Anlagen mit Batchprozessen befindet sich der Bediener u. U. nicht ständig in der Leitwarte, weil der Prozess häufig Tätigkeiten vor Ort erfordert, was ebenfalls bei der Gestaltung der Schnittstelle berücksichtigt werden muss. Schließlich ist auch der Fall denkbar, dass keine zentrale Leitwarte existiert, womit die Schnittstelle Schutzsystem-Bediener dezentral wird. Bei der Gestaltung der Bediener-Sicherheitssystem-Schnittstelle sollten deshalb die verschiedenen Aufgabenanforderungen, die durch den Automatisierungsgrad, die technische Auslegung des Systems und des Prozesses bedingt sind, stärker berücksichtigt werden.

Für die Gestaltung der Schnittstelle Schutzsystem-Bediener in zentralen Leitwarten ist die DIN EN 61511 /18, 74, 75/ von hoher Bedeutung. Diese DIN EN setzt das Konzept der „Funktionalen Sicherheit“, wie es in der Grundnorm DIN EN 61508 /76/ für die Gestaltung sicherheitstechnischer Systeme beschrieben ist, branchenspezifisch für die Prozessindustrie um. Ein sicherheitstechnisches System umfasst dabei alle zur Ausführung der sicherheitstechnischen Funktion erforderlichen Komponenten und Subsysteme vom Sensor bis zum Aktor und schließt ausdrücklich das Bedienungspersonal mit ein.

Nach DIN EN 61511-1 /18/ können drei Ebenen mit verschiedenen sicherheitsrelevanten Funktionen des Bedieners unterschieden werden, wie in Abbildung 6 dargestellt.

Abbildung 6: Anforderungen an Betriebseinrichtungen, die als Schutzsysteme eingesetzt werden /18/.

Die erste (innere) Ebene ist das Regelungs- und Überwachungssystem.

Das Regelungs- und Überwachungssystem soll die optimalen Bedingungen für den Prozess sicherstellen. Ein Versagen auf dieser Ebene führt nicht zu einem größeren Unfall. Wie die Abbildung 6 zeigt, hat der Operator auf dieser Ebene zwei Funktionen:

1. Prozesskontrolle

Der Operator soll zur Optimierung der Prozessbedingungen fertigkeits- oder regelbasiert auf die Alarme des Regelungs- und Überwachungssystems reagieren. Ein Versagen sollte nicht zu einem größeren Unfall führen. Auf das Alarmmanagement wird ausführlich in Kapitel 5 eingegangen.

2. Überwachung

Der Operator soll auf der fertigkeits- oder regelbasierten Verhaltensebene den Prozess überwachen, zum Beispiel soll er auch in abnormalen Situationen in der Lage sein, mit wenig oder keinem passenden Instrumentarium die Prozessbedingungen zu korrigieren.

Die zweite (mittlere) Ebene ist das Schutzsystem.

Die Abbildung 6 zeigt nur eine Operatorfunktion, aber in Realität gibt es zwei Funktionen, da die DIN EN 61511-1 /18/ Sicherheitssysteme mit niedrigen und hohen Automatisierungsgrad berücksichtigt.

a) Der Bediener ist Teil der Sicherheitsfunktion

Dieser Aspekt ist relevant, wenn das Sicherheitssystem der Anlage weniger automatisiert ist, das heißt, wenn es beispielsweise nur ein Sensor-Sender Alarmsystem gibt und es die Aufgabe des Bedieners ist, entweder der Sender oder der Akteur zu sein.

Das ist relevant, wenn die Sicherheitssysteme der Anlage weniger automatisiert sind.

b) Das Sicherheitssystem ist komplett automatisiert

Das bedeutet, dass alle möglichen größeren Unfälle durch komplett automatisierte Systeme verhindert werden. Diese beinhalten eine komplette Sensor-Transmitter-Aktor Kette. Damit hat der Operateur ausschließlich eine Überwachungsfunktion.

Im Rahmen eines definierten Sicherheitslebenszyklus (SIL)-Prozesses fordert die Norm /18/ die Durchführung einer Gefährdungs- und Risikoanalyse (Phase 1), um daraus die Spezifikation und Planung sicherheitstechnischer Systeme (Phasen 2…4) ableiten zu können. Die weiteren Lebenszyklus-Phasen definieren die Montage, Validierung, Inbetriebnahme, Betrieb, Instandhaltung und Änderung (Phasen 5…7) und die Außerbetriebnahme (Phase 8). Die DIN EN 61511-1 /18/ betont hinsichtlich der Anforderungen an den Sicherheitslebenszyklus: „Jede Phase des Sicherheitslebenszyklus muss unter Angabe der notwendigen Eingaben, der erwarteten Ergebnisse und der durchzuführenden Verifikationstätigkeiten beschrieben werden” (S.36). In jeder Phase des Sicherheitslebenszyklus „muss eine Sicherheitsplanung stattfinden, in der die Kriterien, Arbeitstechniken, Maßnahmen und Vorgehensweisen für folgende Punkte festgelegt werden: Sicherstellen, dass die Sicherheitsanforderungen an das SIS in jeder relevanten Betriebsart des Prozesses erreicht werden […]; Sicherstellen einer einwandfreien Montage und Inbetriebnahme des sicherheitstechnischen Systems; Sicherstellen der Sicherheitsintegrität der sicherheitstechnischen Funktionen nach der Montage; Aufrechterhalten der Sicherheitsintegrität während des Betriebes (z.B. Wiederholungsprüfungen, Analyse von Ausfällen); Beherrschen möglicher Gefährdungen durch den Prozess während der Durchführung von Instandhaltungsarbeiten am sicherheitstechnischem System“ (S. 37f). Das in der DIN EN 61511-1 /18/ verwendete Modell für den Sicherheitslebenszyklus ist in Abbildung 7 dargestellt (S.34).

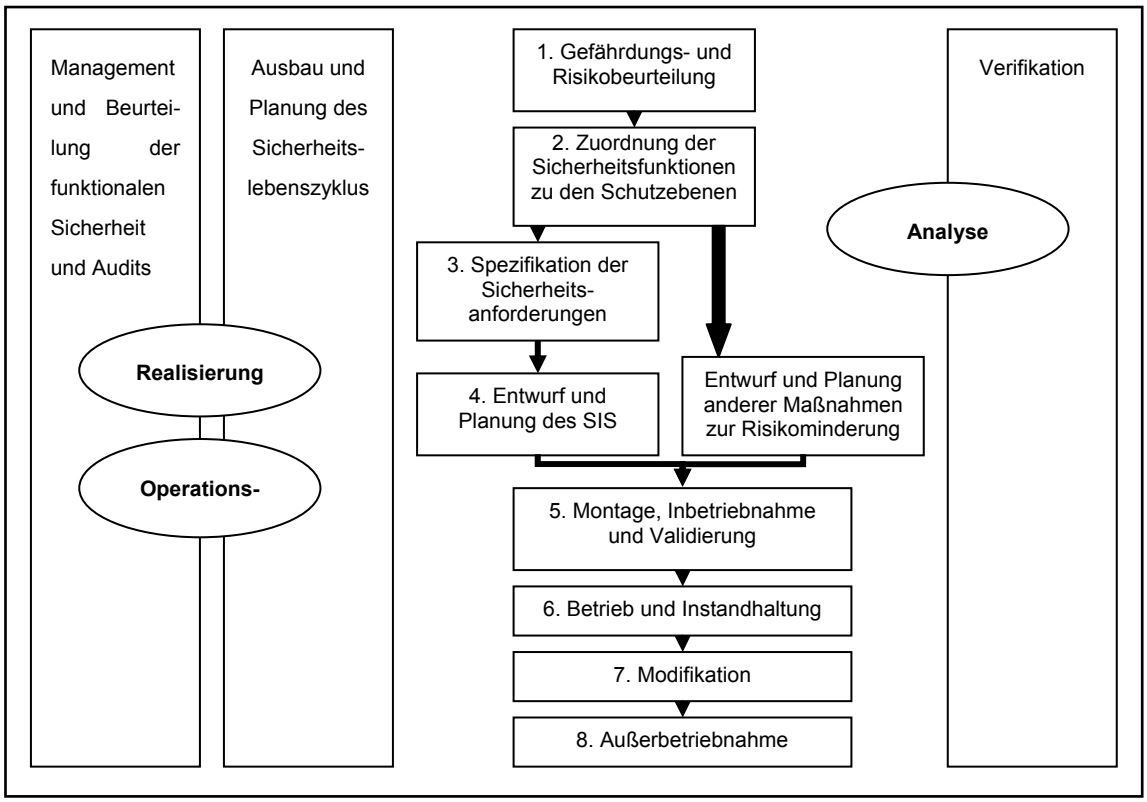


Abbildung 7: Modell des Sicherheitslebenszyklus nach /18/

Dieses Dokument deckt auch die Analyse, die Realisierung und die Operationsphasen ab. Es hebt die kontinuierlichen Funktionen der Planung, Leitung, Beurteilung und Verifikation hervor, die die sequentiellen Bestandteile der Lebenszyklusstruktur unterstützen.

Die wesentlichen Details der Analyse, der Gestaltung, der Verifikation und der Dokumentation werden in allen Sicherheitsstandards erörtert und definiert. Es ist wichtig, dass eine Organisation die wesentlichen Aspekten des SIL besonders wichtig nimmt, um sicherzustellen, dass die gewünschte Sicherheitsebene erreicht ist.

Dabei ist der gesamte Prozess der Planung, Realisierung und Aufrechterhaltung der funktionalen Sicherheit in einem Sicherheitsmanagementsystem zu organisieren.

In allen diesen Lebenszyklusphasen sind jeweils spezifische Anforderungen an die sicherheitsbezogene Einbeziehung von menschlichen und organisationalen Faktoren zu stellen:

Tabelle 7: Anforderungen bezüglich menschlicher und organisationaler Faktoren /74, 75/

Kap. in DIN EN 61511-2	Kurzinhalt zu Anforderungen
11 Entwurf und Planung des SIS (Safety Instrumented System, sicherheitstechnisches System)	• Die „menschliche Leistung“ von Bedienungspersonal, Instandhaltungspersonal, Betriebsleitung hinsichtlich eines sicheren Anlagenbetriebes ist beim System-Entwurf (Mensch-Maschine-Schnittstelle) zu berücksichtigen. • Die „menschliche Zuverlässigkeit“ ist hinsichtlich der Bedingungen, die Menschen zu Fehlern veranlassen, qualitativ und quantitativ zu analysieren. • Als Beispiele für „menschliche Fehler“, die zu einem Sicherheitsrisiko in Chemieanlagen beitragen können, werden genannt: • versteckte Planungsfehler • Fehler im Betrieb (beispielsweise falscher Sollwert) • fehlerhafte Instandhaltung (beispielsweise Ersatz eines Ventils durch ein anderes mit einem falschen Ausfallverhalten) • Fehler bei der Kalibrierung, beim Prüfen oder bei der Interpretation von Ausgabewerten leittechnischer Systeme • fehlerhafte Reaktion im Notfall
11.7 Schnittstellen	• Wenn eine Handlung des Bedienungspersonals Teil der sicherheitstechnischen Funktion ist, dann sollte alles, was für die Durchführung dieser Handlung erforderlich ist, als Teil der sicherheitstechnischen Funktion angesehen werden. • Für Bedienerschnittstellen (Videobildschirme, Tafeln mit Lampen, Drucktastern und Schaltern, Melder, Drucker) sind ergonomische Anforderungen aufgeführt worden. Beispiele: • Hervorhebung der sicherheitstechnischen Bestandteile des MMI gegenüber betrieblichen • Während Notfallsituationen sollten die Update- und Bildwiederholraten der Anzeige für das Bedienungspersonal ausreichend hoch sein

Kap. in DIN EN 61511-2	Kurzinhalt zu Anforderungen
	• Informationsausgabe über vorgenommene Überbrückungen des SIS (Überbrückungsalarm, außerhalb des betrieblichen Prozessleitsystems aufbauen!) • Farben, blinkende Anzeigen und ein klarer Aufbau der Daten sollten den Bediener zu wichtigen Informationen hinführen und so Verwechslungen vorbeugen • Meldungen sollten klar, prägnant und unzweideutig sein
12.1 Anforderungen an den Sicherheitslebenszyklus der Anwendungssoftware	• Beschreibung von Anforderungen an die Software-Ergonomie
13 Werksendprüfungen	• Empfehlung zur Einbeziehung des Betriebspersonals in die Werksendprüfung

Diese, im Wesentlichen ergonomischen Anforderungen stellen jedoch nur einen, wenn auch wichtigen, Teil der Merkmale dar, die ein optimales Mensch-Technik-Organisations-System (MTO-System) kennzeichnen. So werden z.B. die komplexe Bedienkonzeption, Erwerb und Aufrechterhaltung wissens- und fähigkeitsbasierte Eigenschaften des Bedienpersonals, die Einbindung von Fremdpersonal, der Einfluss von Management, Organisation, Unternehmenspolitik, Motivation (wesentliche Elemente einer „Sicherheitskultur“) auf die Bediensicherheit nicht erfasst.

Für den Systementwickler, den Betreiber und für das Genehmigungs- und Aufsichtsverfahren müssen deshalb weitere Referenzen herangezogen werden, um den Stand der Sicherheitstechnik, der wesentlich auch von anerkannten Verfahren zur Gewährleistung der Bediensicherheit bestimmt wird, zu bestimmen und anforderungsgemäß zu berücksichtigen.

4.1.2.1 Prozessleittechnik-Schutzeinrichtungen (VDI/VDE 2180 Blatt 1 /77/, S.10f)

Die PLT-Schutzeinrichtungen haben die Aufgabe eine oder mehrere Prozesssicherungsgrößen auf Übereinstimmung mit zulässigen Werten zu prüfen. Besteht keine Übereinstimmung wird das ständig anwesende Bedienungspersonal durch eine Meldung zur Durchführung notwendiger, vorher festgelegter Maßnahmen veranlasst. Die Funktionen der PLT-Schutzeinrichtungen haben in jedem Fall Vorrang gegenüber Funktionen von PLT-Betriebseinrichtungen und PLT-Überwachungseinrichtungen und sollen prozessnah, das heißt mit möglichst geringer Verarbeitungstiefe ausgeführt werden. Es werden zwei Arten von Aufgaben von PLT-Schutzeinrichtungen unterschieden:

- Ereignisverhindernde Aufgaben: es ist ein unzulässiger Zustand der prozesstechnischen Anlage zu verhindern. Bei Nichtvorhandensein der (aufgrund der Sicherheitsbetrachtung als notwendig befundenen) PLT-Schutzeinrichtung muss mit solchen Zuständen der prozesstechnischen Anlage gerechnet werden, die unmittelbar zu Personenschäden oder Umweltschäden oberhalb des vertretbaren Risikos führen können oder bei denen eine „ernste Gefahr“ im Sinne der Störfall-Verordnung /72/ entstehen kann (vgl. § 4 StörfallV).
- Schadenbegrenzende Aufgaben: sie wirken im nicht bestimmungsgemäßen Betrieb und verhindern bei Eintritt eines unerwünschten Ereignisses die Auswirkungen auf Personen oder Umwelt (vgl. § 5 StörfallV, /72/). In diesem äußerst seltenen Fall halten sie dadurch das Ausmaß des Schaden in Grenzen (in DIN EN 61511-1: „schadensbegrenzende Maßnahmen“, /18/).

Im Rahmen der Planung und Gestaltung von PLT-Schutzeinrichtungen sind folgende Anforderungen festzulegen:

1. Prüfen, ob andere unmittelbar wirkende Einrichtungen zweckmäßiger und wirtschaftlicher sind, wie inhärent sichere Auslegung oder Verwendung von mechanischen oder baulichen Schutzmaßnahmen,
2. notwendige Risiko-Reduzierung: Risiko ist durch Nicht-PLT- und PLT-Schutzmaßnahmen mindestens auf das vertretbare Risiko (= Grenzrisiko) zu reduzieren; Methoden zur Bestimmung der Sicherheitsintegritätslevel: Risikograph, ALARP-Methode, Verwendung Risikomatrix, LOPA-Methode, HAZOP-Analyse.

Weitere Empfehlungen zur Auslegung von Sicherheitssystemen finden sich beispielsweise in den Namur-Empfehlungen 31 /78/. Im Gegensatz zu den Betriebsystemen ist die Aufgabe des Schutzsystems ausdrücklich darauf beschränkt, zu verhindern, dass Prozessparameter in einen nicht zulässigen Bereich gelangen.

Die Funktionen der Schutzsysteme müssen immer denen der Betriebssysteme übergeordnet sein. Das Anfordern der Funktionen der PLT-Schutzeinrichtungen ist äußerst selten, zum einen wegen der geringen Eintrittswahrscheinlichkeit des unerwünschten Ereignisses und zum anderen wegen der häufig vorhandenen gestaffelten Anordnung von PLT-Betriebs-, PLT-Überwachungs- und PLT-Schutzeinrichtungen.

Werden Komponenten der PLT-Schutzeinrichtung, wie z. B. Stellgeräte, durch die PLT-Betriebseinrichtung mitbenutzt, sind die gemeinsamen Komponenten entsprechend den Anforderungen für PLT-Schutzeinrichtungen auszulegen.

PLT-Schutzeinrichtungen der Klasse A sind vor Ort und in der Dokumentation besonders zu kennzeichnen. Die Anforderungen an PLT-Schutzeinrichtungen sind im Anhang IV zusammengefasst.

Zum Betreiben der PLT-Schutzeinrichtungen sind organisatorische Maßnahmen erforderlich. Dabei sind zu unterscheiden:

- Ständige Überwachung durch Betrieb und PLT-Fachpersonal,
- Inspektion (Funktionsprüfung),
- Wartung,
- Instandhaltung.

Darüber hinaus hat der Arbeitskreis „Menschliche Faktoren“ in seinem Statusbericht (2005) folgende Thesen formuliert /88/:

1. „Die Entwicklung und das Design des Mensch-Technik-Systems der verfahrenstechnischen Anlage sind auf menschliche Fähigkeiten und Bedürfnisse auszurichten, damit der Mensch die ihm zugedachte Leistung erbringen kann. Der technisch-ökonomische Ansatz ist zu überwinden und der Mensch als Systembestandteil zu integrieren. Bei Gestaltung der Bedieneigenschaften von Anlagen ist das Erfahrungswissen der Mitarbeiter produktiv einzubringen (S. 27).“
2. „Durch eine entsprechende, an die menschlichen Eigenschaften ausgerichtete Gestaltung der Aufgabenschnittstellen zwischen Mensch und Technik ist sicherzustellen, dass bei den Mitarbeitern jederzeit eine sicherheitsgerichtete Handlungskompetenz (Handeln können) und Handlungsautonomie (Handeln dürfen) besteht (S 27f.).“

In Anlehnung an die Standards /18, 74, 75, 76, 77, 78/ für Schutzsysteme, können vier verschiedene Typen von Mensch-Maschine-Interaktionen unterschieden werden:

1. Der menschliche Einfluss auf Schutzsysteme während des gesamten Kreislaufes von Design, Wartung, Operation, Qualitätsmanagement und Supervision sowie das 4-Augen-Prinzip (unabhängige Prüfungen).

2. Mensch-Maschine-Interaktion durch Überwachung des Schutzsystems und durch Fehlerrückmeldung.
3. Menschlicher Einfluss via humane Gestaltung als Teil des Schutzsystems, als Teil der Sicherheitsfunktion – entweder als Signaldetektor/Teil des Informationsprozesses oder als aktiver Teil.
4. Einfluss des Menschen beim Durchlaufen des Schutzsystems, geplant oder erlaubt, als manuelle Eingriffsmöglichkeiten.

Wenn der Operateur ein Teil der Sicherheitsfunktion darstellt,

1. sollte eine vollständige Aufgabenanalyse erfolgen und es sollten Regeln für Notfälle aufgestellt werden,
2. sollte der maximale Beitrag für die Risikominderung durch den Bediener der Sicherheitsfunktion mit der DIN EN 61511-1 /18/ abgestimmt werden.

Es scheint offensichtlich, dass in den Standards der Bediener als Teil des Schutzsystems angesehen wird, aber es existieren nur sehr wenig Empfehlungen und Anforderungen, die diesem Potenzial gerecht werden, z.B. entsprechende Schulungen/ Weiterbildungen, Aufgaben und Aufgabendesign, Training und notwendige Kompetenzen etc. Es scheint daher notwendig, entsprechende Anforderungen zu formulieren und die Schutzfunktion der Mensch-Maschine-Schnittstelle diesbezüglich zu prüfen.

Des Weiteren sollten die vier verschiedenen Typen des menschlichen Einflusses auf die Sicherheit technischer Systeme in den Standards und Verordnungen stärker betont werden. Es besteht weiterhin die Notwendigkeit, Forschungsergebnisse in die bestehende Regulierung zu integrieren, besonders die Notwendigkeit von Bedieneranalysen beispielsweise durch eine REFA-Untersuchung /104/ für ergonomische Anforderungen, für Ausbildung und Training sowie für Verbesserungen hinsichtlich Sicherheitskultur sollte formuliert und zukünftig beachtet werden.

4.2 Diskussion auf den Workshop

In der thematischen Sitzung „Zusammenwirken von Bedienern und Schutzsystemen“ wurden Strategien basierend auf der Kenntnis menschlicher und organisationaler Faktoren für die Entwicklung effizienter Schnittstellen zwischen Bediener und Schutzsystem diskutiert.

Inhaltliche Schwerpunkte lagen auf der Funktionsallokation und den Automatisierungsstrategien im Mensch-Maschine-System, insbesondere in nichtbestimmungsgemäßen Systemzuständen. Als Grundlage dienten verschiedene Verordnungen, technische Normen und Empfehlungen wie die DIN EN 61511 /18, 74, 75/, VDI/VDE 2180 /77/, die Namur-Empfehlung 31 /78/ oder die EEMUA 191 /93/ sowie eine wissenschaftliche Literaturrecherche zu den Themen Funktionsallokation und Automatisierung.

In Rahmen der Diskussion zeigte sich deutlich, dass angemessene Modelle und Konzepte zur Gestaltung der Mensch-Schutzsystem-Schnittstellen fehlen und damit ein dringender Entwicklungsbedarf identifiziert werden konnte. Ein Modell des Mensch-Maschine-Systems sollte die für die verfahrenstechnische Industrie relevanten Kerndimensionen, wie z. B. zeitabhängige Leistungen, dynamische Umgebungen und soziotechnische Faktoren berücksichtigen und für verschiedene Anwendungsbereiche wie die Gestaltung, die Schulung, die Sicherheitseinschätzung sowie die Ereignisuntersuchung einsetzbar sein. Zur Verbesserung der Mensch-Maschine-Schnittstellen sollte ebenfalls ein umfassendes Prozessmodell Anwendung finden.

Weitgehende Übereinstimmung besteht hinsichtlich der Bedeutung der Risikobeurteilung des Prozesses und der Anlage. In diesem Zusammenhang wurde jedoch noch einmal ausdrücklich darauf hingewiesen, dass sichergestellt werden muss, dass alle relevanten Risiken analysiert und die Sicherheitsfunktionen definiert wurden, so dass die Zuverlässigkeit aller Sicherheitssysteme und -funktionen zu einem akzeptablen Gesamtrisiko des Prozesses oder der Anlage führt. Dazu ist jedoch eine Ausweitung der Analysen und der Sicherheitsanforderungen auf die komplette Sicherheitsanlage, d. h. vom Sensor über den Prozessor bis zum Akteur, unerlässlich.

Als Ergebnis kann festgehalten werden, dass die untersuchten Ansätze zur Mensch-Maschine-Schnittstelle für die Gestaltung von direkten Schnittstellen zwischen Mensch und Maschine konzipiert sind, jedoch Schnittstellen zwischen anderen Operateuren, zur Organisation oder zur Umgebung nicht explizit berücksichtigen. Damit kann festgestellt werden, dass bestimmte Formen der Mensch-Maschine-Interaktion bisher nicht ausreichend berücksichtigt werden. Weiterhin wird deutlich, dass der Bediener, wenn er als Teil der Sicherheitsfunktion angesehen wird, auch in den entsprechenden Normen und Verordnungen berücksichtigt werden sollte. Weiterhin besteht sowohl Forschungs- als auch Regulierungsbedarf bezüglich der Festlegung detaillierter Aufgabenanforderungen, Trainingsinhalte sowie Ausbildungskonzepte für die Operateure, die auch den nichtbestimmungsgemäßen Betrieb mit einschließen sollten, um eine Verbesserung der Sicherheitskultur insgesamt zu erreichen.

4.3 Zusammenfassung und Fazit

Auf der Basis der durchgeführten Literaturanalysen zum Forschungsstand der Schnittstellengestaltung zwischen Bedienern und Schutzsystemen wird deutlich, dass es nach wie vor viele ungeklärte Fragen gibt, die einer weitergehenden Beschäftigung bedürfen. Inhaltliche Schwerpunkte lagen auf der Funktionsallokation und den Automatisierungsstrategien im Mensch-Maschine-System, insbesondere in nichtbestimmungsgemäßen Systemzuständen. Als Grundlage dienten verschiedene Verordnungen, technische Normen und Empfehlungen wie die DIN EN 61511 /18, 74, 75/, VDI/VDE 2180 /77/, die Namur-Empfehlung 31 /78/ oder EEMUA 191 /93/ sowie eine wissenschaftliche Literaturrecherche zu den Themen Funktionsallokation und Automatisierung.

So kann als richtungweisendes Ergebnis für die Zukunft festgehalten werden, dass die Ansätze zur Gestaltung der Mensch-Schutzsystem-Schnittstelle bisher nur die direkten Schnittstellen berücksichtigen und unzureichend auf die Schnittstellen zu anderen Operateuren, zur Organisation oder zur Umgebung eingehen, was besonders in Hinsicht auf nichtbestimmungsgemäße Systemzustände verheerende Konsequenzen haben kann. Hier besteht sowohl Forschungs- als auch Regulierungsbedarf bezüglich der Festlegung detaillierter Anforderungen an Aufgaben, Training sowie Ausbildung der Operateure im bestimmungsgemäßen aber insbesondere auch für den nicht bestimmungsgemäßen Betrieb, um eine Verbesserung der Sicherheitskultur insgesamt zu erreichen.

Aber selbst bei der Betrachtung der Schnittstelle zwischen Mensch und Schutzsystem stellt sich aus Sicht der Autoren heraus, dass die Systemgestaltung dort nach wie vor Mängel aufweist, die als sicherheitsrelevant einzuschätzen sind.

So werden die unterschiedlichen Konstellationen der Bediener-Schutzsystem-Interaktion aufgrund unterschiedlicher Automatisierungsgrade, z. B. Vollautomatisierung oder Teilautomatisierung, oder spezifischer System- und Prozessauslegungen, beispielsweise zentrale oder dezentrale Schnittstellen nicht ausreichend in der Gestaltung der Mensch-Bediener Schnittstelle berücksichtigt. Obwohl es aufgrund der verschiedenen Aufgaben, die der Bediener in Abhängigkeit dieser System- und Prozessbedingungen zu erfüllen hat, deutliche Unterschiede in den Anforderungen an das Schutzsystem insgesamt und den Bediener als Teil des Gesamtsystems gibt, werden bisher kaum spezifische Gestaltungsstrategien entwickelt und in die Praxis umgesetzt. Hier besteht dringender Bedarf nach differenzierten Gestaltungsstrategien, die alle relevanten Systemaspekte auch im Hinblick auf die Schnittstellengestaltung zwischen Bediener und Schutzsystem berücksichtigen.

Folglich sollte die Schnittstellengestaltung konsequent auf die grundsätzlich anwendbaren MABA-MABA-(man-are-better-at-machines-are-better-at)-Prinzipien ausgerichtet sein, um sowohl die Stärken des Menschen angemessen einzusetzen, als auch seine Schwächen, wenn notwendig, kompensieren zu können. Hierzu ist es jedoch erforderlich, systematische Aufgabenanalysen durchzuführen, die möglichst viele verschiedene Bedingungen und Situationen berücksichtigen, um eine im Sinne der Systemsicherheit optimierte Aufgabenverteilung zwischen Mensch und Technik vorzunehmen. Dazu muss „die Systemgestaltung an der Schnittstelle Mensch-Technik so erfolgen, dass der Operator in die Lage versetzt wird, bei Vorfällen aktiv Sicherheit herzustellen“ /90/ S.70. Das erfordert die Integration von Systemplanung, Systemgestaltung und Operator-Training in Abstimmung mit verschiedenen Betriebszuständen und Lebenszyklen der Anlage.

Weiterhin offen bleibt jedoch die Frage, welche Aufgabenarten generell dem Bediener oder dem Schutzsystem zugeordnet werden sollen. In diesem Zusammenhang erscheint es ebenfalls sinnvoll zu prüfen, ob Aufgaben in Abhängigkeit vom Betriebszustand (bestimmungsgemäßer und nicht-bestimmungsgemäßer Betrieb) dem Bediener oder dem Schutzsystem fest oder im Sinne einer flexiblen Aufgaben- und Funktionsallokation zu geordnet werden sollten. Diese Fragestellungen würden ebenfalls neue Ansätze an die Gestaltung der Mensch-Maschine-Schnittstelle im Allgemeinen und die Bediener-Schutzsystem-Schnittstelle im Speziellen erforderlich machen.

Einen denkbaren Zugang zur Klärung der genannten offenen Fragestellungen könnten Ereignisanalysen liefern, die Ereignisse während verschiedener Betriebszustände und verschiedene Formen der Aufgabenallokation zwischen Bediener, Maschine, insbesondere Schutzsystemen, und Organisation in der Realität betrachten. Dabei könnte der Schwerpunkt der Analysen auf der Identifizierung von Aufgaben bei Ereigniseintritt, die tatsächlich beim Bediener verblieben sind, liegen. Es könnte sich jedoch als schwierig erweisen, ausreichend viele, hinsichtlich dieser Fragestellung ausreichend dokumentierte Ereignisse zu finden, um die verschiedenen Betriebszustände und die verschiedenen Aufgabenarten und deren Verteilung repräsentativ abzubilden.

Für diese Analysen ist es notwendig, ein umfassendes Prozessmodell zu verwenden, das alle relevanten Aspekte wie beispielsweise Zeitabhängigkeit, unterschiedliche Systemzustände oder dynamische Veränderungen des Systemverhaltens berücksichtigt und beschreibt, so dass dieses Modell die gemeinsame Grundlage für verschiedene Fragestellungen in den Bereichen Gestaltung, Schulung, Sicherheitsbewertung und Unfalluntersuchung bilden kann. Unerlässlich ist in diesem Rahmen die konsistente und stimmige Einbeziehung praktischer Erfahrungen, organisatorischer Faktoren sowie kognitiver Aspekte des menschlichen Verhaltens. Bei der Betrachtung von Mensch-Maschine-

Schnittstellen sollten aber ebenfalls die internationalen und nationalen Normenreihen berücksichtigt werden, insbesondere DIN EN 61511-1 /18/, ISA S84 /89/ und VDI 2180 /77/.

Ein weiteres Problem bzgl. der Mensch-Maschine-Schnittstelle besteht in der Auswahl und Festlegung geeigneter Modelle, Taxonomien und Analysemethoden. Deshalb erscheint es auch hier sinnvoll, verschiedene Methoden und Instrumente wie beispielsweise prospektive und retrospektive Analysen, miteinander zu kombinieren, wenn sichergestellt werden kann, dass ihnen eine gemeinsame Modellvorstellung und Datenbasis der Mensch-Maschine-Interaktion zugrunde liegt, um ein umfassendes System- und Schnittstellenverständnis zu erreichen. Diese Methoden und Techniken sollten in einer integrierten Methodologie für spezifische Probleme wie die Gestaltung, Schulung, Sicherheitsbewertung, Unfalluntersuchung etc. anwendbar sein.

Die DIN EN 61511-1 /18/ fordert eine Risikobeurteilung des Prozesses und der Anlage, bevor ein Sicherheitssystem benutzt wird. Dabei muss sichergestellt werden, dass alle relevanten Risiken analysiert, die Sicherheitsfunktionen definiert wurden und die Zuverlässigkeit aller Sicherheitssysteme und Sicherheitsfunktionen zu einem akzeptablen Gesamtrisiko des Prozesses oder der Anlage führt. Kriterien in Rechtsvorschriften müssen in diesem Zusammenhang beachtet werden.

Für die Entscheidung, ob automatische Sicherheitssysteme verwendet werden oder der Operateur Teil der Sicherheitsfunktion sein soll, könnte eine Analyse auf der Grundlage der MABA-MABA (men-are-better-at-machines-are-better-at)-Prinzipien helfen, angemessene Entscheidungen zu treffen. Wenn der Operateur ein Teil der Sicherheitsfunktion ist, sollte sichergestellt sein, dass alle diese Systeme zu den menschlichen Fähigkeiten passen.

Wird der Operateur als Teil der Sicherheitsfunktion betrachtet, sollen menschliche Faktoren angemessen in der Risikoanalyse berücksichtigt werden, d.h. eine Ausweitung der Analysen und der Sicherheitsanforderungen auf die komplette Sicherheitsfunktion (Schutzsystem und Bediener) und deren diesbezügliche Überprüfung (DIN EN 61511-1 /18/). Dabei sollen beispielsweise Handlungen oder Störungen, die Sicherheitsfunktionen auslösen, Fehler, die bei der Reaktion auf Alarme auftreten, und Fehler, die bei der Testung und der Instandhaltung des Systems auftreten und die Effizienz des Schutzes reduzieren, betrachtet werden. Es sollte besonders beachtet werden, wie die Zuverlässigkeit des Operateurs in der damit in Verbindung stehenden Berechnung der Zuverlässigkeit der Sicherheitsfunktion enthalten ist und welches die max. benötigte Zuverlässigkeit für menschliche Handlungen bei dieser Sicherheitsfunktion ist.

Außerdem erscheint es notwendig, Regeln für Notfälle aufzustellen und die Operateure für Notfälle zu schulen.

Zusätzlich zu den eher inhaltlichen Problemen der Gestaltung der Bediener-Schutzsystem-Schnittstelle wurde ein weiteres eher generelles Problem identifiziert, das jedoch ebenfalls in Zukunft verstärkt gelöst werden muss. Der Bekanntheitsgrad und damit die Verbreitung der Inhalte der relevanten Normen, wie die IEC/DIN 61508 /76/, DIN EN 61 511 /18, 74, 75/, und Empfehlungen, wie EEMUA 191 /93/ und die NAMUR 31 /46/, in der verfahrenstechnischen Industrie ist unzureichend. Die Verbreitung der spezifischen Inhalte sollte deshalb zukünftig mit größerem Nachdruck betrieben werden. Es bietet sich an, in diesen Kontext die Klärung des Forschungs- und Entwicklungsbedarfs für die belastbare Berücksichtigung des Bedienerverhaltens im Rahmen der o.g. speziellen Risikoanalysen für den Einsatz vollautomatischer und teilautomatischer Schutzsysteme einzubetten.

5 Menschliche Faktoren im Alarmmanagement

In diesem Kapitel werden verschiedene Quellen im Hinblick auf die Gestaltung (Kap. 5.1.1) und Bewertung von Alarmsystemen (Kap. 5.1.2) analysiert und auf deren Anwendbarkeit in der verfahrenstechnischen Industrie diskutiert. Abschließend werden die gewonnenen Erkenntnisse aus der Literaturanalyse und der Diskussion auf dem Workshop (Kap. 5.2) zusammenfassend diskutiert (Kap. 5.3).

Zur Aufbereitung des Themas menschliche und organisationale Faktoren im Alarmmanagement wurden folgende Dokumente analysiert:

- HSE Informationsblatt Nr. 6: Besserer Umgang mit Alarmen /91/
- HSE Human Factor Briefing Note No 9: Alarm Handling /92/
- Namur-Empfehlung 102: Alarmmanagement /46/
- EEMUA Publication No 191: Alarm systems – a guide to design, management and procurement /93/
- Wissenschaftliche Literatur

Das nachfolgende Kapitel betrachtet die Fälle,

a) dass ein vollständig automatisiertes Schutzsystem existiert oder
b) dass der Bediener zumindest partiell ein Teil des Schutzsystems darstellt.

Als wichtigstes Ergebnis zeigt sich nämlich, dass Empfehlungen zum Alarmmanagement in der Regel für beide Fälle sinnvoll anwendbar sind. Allerdings muss der Anwender klären, mit welchem der beiden Fälle er sich auseinandersetzt und erforderlichen Einschränkungs- oder Ergänzungsbedarf identifizieren.

5.1 Stand der Wissenschaft

Die technische Entwicklung der Prozessleittechnik verleitete dazu, alles, was zu messen möglich war auch tatsächlich zu messen und mit Alarmen auszustatten. In Extremfällen führte dies dazu, dass in einem Prozessleitsystem einer verfahrenstechnischen Anlagen 5000 bis 10.000 Alarme vorgesehen sein konnten. Dieses hatte zur Folge, dass die Operateure aufgrund der bei Störungen auftretenden Alarmraten kaum noch handlungsfähig waren.

Für ein Alarmmanagement ist deshalb primär erforderlich, die verschiedenen Arten von Informationen über Prozess- und Anlagenzustände nach Handlungserfordernissen und Relevanz für die Sicherheit zu verschiedenen Kategorien zusammenzufassen.

Generell gibt es Meldungen und verschiedene Alarmarten mit unterschiedlicher Relevanz in Hinblick auf Wichtigkeit und Dringlichkeit für die Verhinderung von Unfällen:

1. Meldungen, die das Eintreten eines Ereignisses anzeigen im Sinne von NAMUR 102 /46/, aber keine unverzügliche Reaktion des Operateurs erfordern.
2. Alarme, die Abweichungen des Prozesses oder der Anlage vom Sollzustand anzeigen und eine unverzügliche Reaktion des Operateurs erfordern.
3. Alarme, die über das Auslösen von PLT-Schutzeinrichtungen informieren.

Eine ähnliche Unterscheidung zwischen Meldungen und verschiedenen Alarmarten findet sich in der DIN EN 61511-1 /18/:

- Überwachungssystem: Meldungen
- Regelungssystem: **Alarme**
- Schutzsystem: **kritische Alarme**, das sind Prozessalarme mit Erfordernis des Bedienereingriffs zur Verhinderung von größeren Unfällen,
  SIS–Alarme zur betrieblichen Überwachung des Schutzsystems durch den Bediener

Weiter sollten bei der Gestaltung, der Veränderung und Wartung von Alarmsystemen und der Bewertung des Alarmmanagements menschliche Leistungsfaktoren bestmöglich berücksichtigt werden, um sicherzustellen, dass der Bediener bei einer Störung erfolgreich unterstützt wird und dadurch schwerwiegendere Unfälle verhindert werden.

In dem Leitfaden der EEMUA /93/, S.8 werden generellere Empfehlungen für das Design von Alarmsystemen und dessen Evaluation gegeben. Relevante Mittel sind:

- Risikoabschätzung (Entwicklung eines „safety case", Identifikation der Sicherheitsbedeutung des Bedienpersonals, Risikoabschätzung, um Alarme zu identifizieren, die Schutz gegen Sicherheits-, Umwelt- und ökonomische Risiken bieten, Bewertung zur Identifizierung von Alarmen, die zur signifikanten Risikoreduktion führen),
- Ergonomische Gestaltung (Identifikation der Operateursanzahl und ihrer Aufgaben, Schnittstellengestaltung, Alarmschnittstellengestaltung),
- Design von Einzelalarmen (Bewertung vorgeschlagener Alarme, die nicht aus der Risikoabschätzung gewonnen wurden, Identifikation von Alarmen mit speziellen Integritäts- oder Bildschirmanforderungen, Vervollständigung der Daten für jeden Einzelalarm, Erstellen von Unterlagen zur Alarmreaktion, Planung von Alarmsensoren, Hardwaredesign zur Realisierung der individuellen Alarmsignale, Installation der Alarmsensoren und Signale),

- Designintegration (Rationalisierung von Alarmlisten, Bewertung hinsichtlich von Gestaltungsprinzipien, Identifikation von Anforderungen für die Alarmverarbeitungsfunktion),
- Alarmsystem-Konfiguration (Installation der Hardware, Konfiguration von Hardware/Software für das Alarmsystem, Erstellen einer Informationsdatenbank für Alarme, Konfiguration von Hardware/Software für Einzelalarme, Konfiguration der Alarmkombinationslogik),
- Tests und Prüfungen (Test der Alarmsystemeinrichtungen, Test der Alarmsensoren und Signale, Test der Konfiguration von Einzelalarmhardware/-software, Evaluation der ergonomischen Gestaltung, Messung der Leistung des Alarmsystem, Bestimmung von wiederkehrenden Prüfungen, Optimierung des Betriebsverhaltens).

Weiterhin werden einzelne Elemente einer nutzerorientierten Gestaltung beschrieben, die für die Gestaltung und Bewertung von Alarmsystemen als notwendig erachtet werden: Aufgabenanalysen, Bedienerbeteiligung, Gestaltungsbewertung, frühe ergonomische Evaluation und Monitoring.

5.1.1 Gestaltung von Alarmsystemen

Zur angemessenen Gestaltung von Alarmsystemen lassen sich in Hinblick auf Interaktionen zwischen dem Operateur und dem Melde- und Alarmsystem verschiedene Gestaltungsprinzipien identifizieren, die in einer zeitlichen Abfolge zueinander stehen.

Die unterschiedlichen Phasen des Alarmierungsprozess, die sich in weitere Gestaltungsprinzipien aufgliedern lassen, sind folgende:

1. Alarmgenerierung: Welche Alarmarten werden generiert? Welche Methoden der Alarmverarbeitung (Alarmgruppierung, Alarmfilterung, Alarmunterdrückung, Alarmpriorisierung) werden verwendet?
2. Alarmdarstellung: Welche Darstellungsarten werden eingesetzt? Wie werden Alarme kodiert (optisch, akustisch), Welche Alarmkategorisierung wird verwendet? Welches Quittierungssystem wird verwendet?
3. Alarmbewertung: Wird der Operateur durch das Melde- und Alarmsystem unterstützt? Wird der Operateur unnötig belastet?

Der Sinn eines Alarmsystems besteht darin, die Aufmerksamkeit des Bedieners auf die Gegebenheit der Anlage zu lenken, um diese zu beurteilen und im Notfall rechtzeitig zu Handeln. Deshalb sollte jeder Alarm warnen, informieren und leiten. Bezogen auf den Operateur sollte jeder ausgelöste Alarm relevant und nützlich sein und zu einer definierten Benutzerreaktion führen. Jeder Alarm sollte berechtigt, genau geplant und konsistent mit der Alarmphilosophie und der Risikobeurteilung der Anlage sein. Voraussetzung zur Alarmgestaltung ist deshalb eine systematische Herangehensweise, in der wichtige Designent-

scheidungen dokumentiert werden. Bei der Gestaltung von Alarmsystemen sollte sichergestellt sein, dass Ausfälle für den Bediener offensichtlich sind. Dabei sollten die betrieblichen Auswirkungen von potenziellen Ausfällen des Alarmsystems sorgfältig beurteilt werden.

Ein grundlegender Punkt bei der Gestaltung von Alarmen ist die Überlegung, wie wichtig und zuverlässig diese sein sollten. Dazu ist es notwendig, qualitative und quantitative Risikobeurteilungen durchzuführen. Die Prinzipien der Risikobeurteilung, die bei der Alarmgestaltung berücksichtigt werden sollten, sind:

- Risikominderung sollte bereits während der Anlagengestaltung beginnen, durch die Auswahl von geeigneten Prozessen und Anlagenkonfigurationen die eine inhärente Sicherheit aufweisen.
- Die Gestaltung des Alarmsystems sollte einerseits die Schadensrisiken für Menschen und die Umwelt berücksichtigen und andererseits Aussagen darüber treffen, welche Risiken das Alarmsystem reduzieren soll.
- Sogar in hoch automatisierten Anlagen mit aufwendigen Schutzsystemen lassen sich potenzielle Fehlerszenarien identifizieren, die eine Bedienerreaktion erfordern. Diese Szenarien sollten identifiziert werden und es sollte bestimmt werden ob und wie das Alarmsystem den Bediener dabei unterstützen kann.
- Es gibt eine Grenze der Risikoreduktion, welche bei der Verwendung von (kritischen) Alarmen, selbst wenn das System einwandfrei funktioniert, erreicht wird.
- Wenn ein Alarmsystem nicht für eine Implementierung und für eine signifikante Risikoreduktion geeignet ist, dann sollten alternative Mittel dafür eingesetzt werden (Einsatz zusätzlicher Technologien oder Prozessmodifikation).

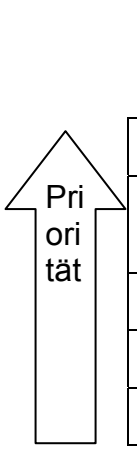
Von der EEMUA /93/ werden für die Gestaltung von Alarmsystemen Empfehlungen vorgeschlagen, die Orientierungswerte für die Anzahl von Alarmmeldungen in verschiedenen Betriebszuständen liefern.

Als Methoden der Alarmverarbeitung werden die Alarmgruppierung, Filterung bei der Alarmgenerierung, Erstwertmeldung und Alarmunterdrückung genannt /46/. Es wird geraten, dass die Alarmpriorisierung nach den Kriterien a) potenzielle Auswirkungen und b) zur Verfügung stehende Zeitspanne, um eingreifen zu können, vorgenommen wird.

Die Langzeitquote für Alarme während Normalbetrieb sollte nicht mehr als ein Alarm alle zehn Minuten betragen und nicht mehr als zehn Alarme sollten in den ersten zehn Minuten nach einer Störung dargestellt werden. Dazu bedarf es einer effektiven Alarmpriorisierung, d.h. es müssen Regeln definiert werden und diese dann konsequent auf jeden Alarm angewendet werden.

Drei Priorisierungsgrade erscheinen geeignet, die auf den möglichen Konsequenzen basieren sollten, die eintreten, falls der Operator nicht richtig reagiert. Die Verteilung der Prioritäten sollte wie folgt aussehen: 5% hohe Priorität, 15% mittlere und 80% niedrige /93/, S.65. Prioritäten der Alarme sollten farblich gekennzeichnet werden.

Die folgende Priorisierungsmatrix wird beispielhaft vorgeschlagen:



Potenzielle Auswirkungen			
Reaktionszeit	Anlagenstill-stand	Produktqualitätsverlust	Produktionsverzögerung
< 5 min	Hoch	Mittel	Niedrig
5-20 min	Mittel	Niedrig	Niedrig
> 20 min	Niedrig	Niedrig	Niedrig

Abbildung 8: Priorisierungsmatrix /46/, S. 12

Ist der Bediener Teil des Schutzsystems (der Sicherheitsfunktion) oder soll das Schutzsystem überwacht werden so wäre diese Matrix um jeweils eine Spalte zu ergänzen sowie die Prioritätensetzung entsprechend anzupassen.

Alarmpriorisierung kann durch Lautstärke bei akustischen Signalen sowie durch Pulsfrequenz und durch Farbe sowie Blinkfrequenz bei optischen Signalen realisiert werden.

Ein Alarmdarstellung sollte nach Namur /46/ und EEMUA /93/ die folgenden Merkmale aufweisen: relevant, eindeutig, zeitgerecht, priorisiert, verständlich, diagnostisch, hinweisend und fokussierend. Wegen ihrer physiologischen Eigenschaften und Leistungsgrenzen sind Menschen zwar in der Lage, relative Signale (Farben, Töne) im Verhältnis zueinander sehr differenziert zu unterscheiden, zeigen diese Fähigkeit allerdings nicht im Hinblick auf absolute Signale (bestimmte Farben, bestimmte Tonhöhen, Blinkfrequenzen), was zu einer Einschränkung ihres möglichen Einsatzes führt (z. B. max. 5-9 verschiedene Farben, 2 verschiedene Blinkraten, siehe auch VDI 3699 /94, 95/, IEC 73 /96/, DIN 2403 /97/). Die Bereitstellung von vorverarbeiteten Informationen (Metazeichen) wirkt sich positiv auf das schnelle Erkennen und Zuordnen aus.

Bezüglich der Zuverlässigkeit der Bediener wird gefordert, dass die Darstellung jedes einzelnen Alarms eindeutig ist, es wenig Fehlalarme gibt sowie eine niedrige Bedienerbelastung, einfache und vorgeschriebene Bedienerreaktionen, gut ausgebildetes Bedienpersonal und eine Überprüfung der Effektivität der Bedie-

nerreaktionen. Ein effektives Alarmsystem sollte warnen, informieren und die Bediener so leiten, dass sie Probleme diagnostizieren können und unnötige Ausfälle vermeiden. Nur nützliche und relevante Alarme sollten dargestellt werden, sie sollten ergonomisch gestaltet sein und dem Bediener genügend Zeit zur Reaktion lassen sowie vorher festgelegte spezifische Reaktionshandlungen haben. In der HSE Human Factor Briefing Note No 9 /92/ werden in Abhängigkeit von verschiedenen Problemen folgende Lösungsmöglichkeiten (vgl. Tabelle 8) beschrieben:

Tabelle 8: Umgang mit Alarmen (/92/, S.3)

Problem	Lösungsmöglichkeit
Gestaltung	
Alarmmaskierung: Die akustische Alarmierung übertönt nicht den normalen Geräuschlevel. Die Alarme übertönen die Kommunikation. Beleuchtete Alarme können bei normalen Beleuchtungsgraden nicht erkannt werden.	Erhöhung Lautstärke von Alarmen um 10 dB (A) über der normalen Umgebungslautstärke; Erlaubnis für die Operateure die Lautstärke der Alarme zu reduzieren, nach der ersten Alarmierung. Alarme müssen hell genug sein bei verschiedenen Beleuchtungsbedingungen. Verwendung von Farben zum Hervorheben von Alarmen und Kombination von optischen und akustischen Alarmen.
Alarmflut: Es werden mehr Alarme ausgegeben als der Operator gleichzeitig bearbeiten kann.	Das System sollte unnötige Alarme unterdrücken oder herausfiltern und die Alarme nach Prioritäten ordnen, die Operateure benötigen klare Vorgehensweisen und Schulungen, in denen sie lernen, ihre Handlungen zu priorisieren.
Alarme sind schwierig zu unterscheiden, weil sie sich sehr ähnlich anhören bzw. aussehen.	Es sollten Kodierungen, z. B. verschiedene Farben und Klänge Ansteigen der Lautstärke, Aufleuchten, verwendet werden, um die Wichtigkeit der Alarme und deren Zugehörigkeit zur Sicherheitsfunktion anzuzeigen.
Ungerechtfertigte Alarme: falsche Alarme, “flutende” oder stehende Alarme	Veränderung von Sollwerten, Hysterese oder Totzonen, um das System für kurzzeitige unbedeutende Schwankungen weniger empfindlich zu machen. Wenn Alarme erwartet, aber nicht ausgeschaltet werden können, z. B. im Testbetrieb oder Instandhaltung, kennzeichne sie, um anzuzeigen, dass sie getestet werden.

Problem	Lösungsmöglichkeit
Organisation/Vorgehen	
Nachdem der Alarm eingegangen ist, hat der Operateur zu wenig Zeit, um die richtige Handlung auszuführen.	Einführung von Alarmstufen, um Veränderungen in der Alarmsituation anzuzeigen, z.B. bei der drohenden Überfüllung eines Tanks ertönt ein Alarm bei den Stufen „Hoch“ und Hoch-Hoch“.
Nachdem der Alarm eingegangen ist, hat der Operateur zu wenig Zeit, um die richtige Handlung auszuführen.	Einführung von Alarmstufen, um Veränderungen in der Alarmsituation anzuzeigen, z.B. bei der drohenden Überfüllung eines Tanks ertönt ein Alarm bei den Stufen „Hoch“ und Hoch-Hoch“.
Operateure verbinden mit Alarmen irrelevante oder unwichtige Informationen oder es werden nicht aussagekräftige Bezeichnungen benutzt.	Beteiligung der Operateure bei Problemen mit Alarmen, Beteiligung an Lösungsvorschlägen. Überprüfung von Vorschlägen auf Übereinstimmung mit empfohlenen Leitlinien (vgl. Literatur).
Alarme werden generiert, wenn eine Meldung ausreichte (Alarme sind sicherheitskritischen Ereignissen vorbehalten).	Alarme wurden ohne die Risikobeurteilung, die zeigt, welche Anlagenbedingungen Alarme auslösen sollen, einzubeziehen, gestaltet.
Alarme haben sich etabliert, weil es zu schwierig ist den Prozess zu automatisieren, dadurch liegt die Verantwortung zum Handeln beim Operateur.	Alarmgestaltung anhand von guten Praxisbeispielen schützt nicht davor den Operateur zu überlasten.

Folgende Darstellungsarten für Alarme können eingesetzt werden /46/, S. 13ff.:

- Bereichsübersicht von Alarmen
- Alarmdarstellung über Alarmliste
- Alarmdarstellung im schematischen Fließbild
- Erstwertmeldesystem
- Folgende Prinzipien der Alarmstrukturierung sollten ebenfalls berücksichtigt werden:
- Verfügbarkeit von schriftlichen Regeln, wie die Prioritäten gesetzt werden sollen. Diese sollten konsistent auf alle Alarmsysteme angewendet werden.
- Der Bediener sollte nicht durch die Darstellungsart der Alarme überlastet werden, weder während des Normalbetriebes, beim Anfahren und bei wechselnden Prozessbedingungen noch beim Abfahren.
- Die Alarmpriorisierung erfolgt gewöhnlich nach zwei Kriterien: den potenziellen Auswirkungen (die der Bediener durch eine entsprechende Handlung verhindern könnte) und die zur Verfügung stehende Zeitspanne, um eingreifen zu können.

- Erfahrungsgemäß sind Prioritätenbänder ergonomisch effektiv für die normale Alarmdarstellung. Die Definitionen der Alarmpriorisierung sollten über das gesamte System hinweg konsistent sein.
- Alarmanzeigen sollten so gestaltet werden, dass der Bediener einen schnellen Zugriff auf alle wichtigen Informationen hat, auch wenn das System überlastet ist.
- Der Bediener sollte im Falle einer Alarmüberladung in der Lage sein, aus der Alarmliste nur die hoch priorisierten Alarme auszuwählen und alle mittleren und niedrig eingestuften Alarme zu ignorieren oder alle Alarme der Überwachungseinrichtungen zu ignorieren und nur die Alarme zu berücksichtigen, die unabhängig vom System gegeben werden.
- Es gibt zwei parallele Ansätze, die Designer verwenden sollten um die mit einer Alarmüberladung verbundenen Probleme zu reduzieren: Eliminierung der Alarmflut oder die Verbesserung des Alarmmanagements. Maßnahmen sollten ergriffen werden, um sicherzustellen, dass der Bediener auch während eines Überlastungsvorfalles so gut wie möglich arbeiten kann.

Zusammengefasst zeichnet sich ein „guter“ Alarm nach den Leitlinien der EEMUA /93/ durch folgende Eigenschaften aus:

- Der Alarm identifiziert eindeutig die aufgetretene Situation,
- verwendet Begriffe, die den Bedienern bekannt sind,
- verwendet konsistente Abkürzungen aus Betriebsunterlagen,
- hat eine konsistente Nachrichtenstruktur,
- baut nicht auf Auswendiglernen von Zeichen und Zahlen auf,
- wurde auf Nutzerfreundlichkeit bei normalem Anlagenbetrieb getestet.

Die zusätzliche Auswertung wissenschaftlicher Literatur ergab nur wenig Zusätzliches oder Neues. Smith et al. /98/ beschreiben eine Lücke in Sicherheitsmanagementsystemen in Bezug auf Alarmbehandlung: keine klare Identifikation von Sicherheitsalarmen, zu viele Alarme mit Topppriorität, keine Anlagenleitlinie oder -philosophie für Alarme, keine Kompetenzbewertung des Bedienpersonals, keine Spezifikation für die Alarmbeschaffung.

Dunn und Sands /99/ identifizieren beeinträchtigende Alarme, stehende Alarme, Alarmflut und fehlende Klarheit als Probleme bezüglich Alarmsysteme. Sie stellen einen Lebenszyklus des Alarmmanagements dar: Philosophie, Identifikation, Rationalisierung, Design, Implementierung und Training, Betrieb, Monitoring, Wartung, Bewertung, Veränderungsmanagement mit drei Schleifen für Wartungs- und Verbesserungskreis, Monitoring- und Veränderungsmanagementkreis, Bewertungskreis.

Honeywell /100/ identifiziert als weiteres Problem, die Tatsache, dass Alarme eindimensionale Darstellungen von in der Regel multidimensionalen Problemen sind.

5.1.2 Bewertung von Alarmsystemen

Die HSE stellt in ihrem Informationsblatt No 6 /91/ fest, dass ein verbesserter Umgang mit Alarmen signifikante Effekte auf die Sicherheit haben kann, weil er zu einer strengeren Qualitätskontrolle, verbesserter Fehlerdiagnose und effektiveren Anlagenbedienung durch die Operatore führen kann. Um festzustellen, ob ein vorhandenes Alarmsystem verbessert werden sollte, werden die folgenden Fragen vorgeschlagen (S.1f.):

- Wie viele Alarme gibt es?
- Sind alle Alarme notwendig, erfordern sie alle das Eingreifen eines Bedieners? (Hinweis: Prozessstatusanzeigen sollten nicht als Alarme aufgeführt werden)
- Wie viele Alarme treten bei normalem Betrieb auf?
- Wie viele Alarme treten bei einer Störung der Anlage auf?
- Wie viele ständig auftretende Alarme gibt es?
- Werden die Bediener manchmal von Alarmfluten überwältigt?
- Gibt es Fehlalarme, werden z.B. viele Alarme in schneller Abfolge bestätigt, oder werden regelmäßig auftretende akustische Alarme zunehmend ignoriert?
- Ist die Alarmpriorisierung hilfreich für den Bediener?
- Wissen die Verantwortlichen, was sie bei jedem Alarm zu tun haben?
- Sind die Anzeigen im Kontrollraum gut gestaltet und einfach zu verstehen?
- Ist leicht verständliche Hilfe verfügbar, in schriftlicher Form oder auf dem Bildschirm?
- Wie einfach ist das „Navigieren” auf den Alarmseiten?
- Sind die auf dem Bildschirm benutzten Begriffe dieselben Begriffe, die auch von den Bedienern benutzt werden?
- Gab es schon einmal kritische Vorfälle oder Beinahe-Unfälle, bei denen die Bediener Alarme nicht wahrgenommen oder falsch auf Alarme reagiert haben?
- Gibt es eine schriftlich festgelegte Betriebsstrategie zu Alarmen?
- Gibt es einen Unternehmensstandard für Alarme?
- Gibt es für die Erweiterung bzw. Veränderung des Alarmsystems einen strukturierten Ablauf? Gefahrenanalysen (HAZOP-Studien) führen z.B. oft dazu, dass viele Alarme als „Schnelllösung“ installiert werden.

- Wie viele neue Alarme hat ihre letzte HAZOP-Untersuchung generiert und wie wurden diese gerechtfertigt?
- Können die Bediener diese Alarme richtig erkennen und korrekt auf sie reagieren?
- Wurden die Auswirkungen auf die Gesamtalarmbelastung der Bediener berücksichtigt?

Die Namur-Empfehlung 102 /46/ zielt darauf ab, eine Richtlinie für das Design von Alarmmanagement mit den folgenden Charakteristika zu geben:

- “Handlungsaufforderungen je nach Prozesszustand,
- Unterstützung bei situationsgerechter Bewertung und Bedieneingriffen,
- Übersichtlichkeit, Transparenz und Konsistenz von Meldungen und Alarmen,
- Anzahl und Auftrittshäufigkeit von Meldungen und Alarmen sind minimiert,
- geringe Bedienerlast beim Auftreten von Meldungen und Alarmen,
- Tools zur Dokumentation und Auswertung” /46/, S. 5.

Für einen kontinuierlichen Verbesserungsprozess, d.h. ständige Verbesserung, Optimierung, Pflege und Verwaltung des Alarmsystems werden die folgenden Funktionen gefordert /46/, S.19:

- Folgende Informationen können für eine Analyse im Sinne der Verbesserung eines Alarmsystems (“Performanzmonitor“) herangezogen werden:
- Alarmzahl pro Alarmtyp, Alarmsignal, Alarmquelle und Blocktyp;
- Anzahl der Prozessalarme einer Alarmquelle pro Zeiteinheit, Anzahl eines bestimmten Alarmsignal pro Zeiteinheit, Anzahl der “flackernde” Alarme, Anzahl der Daueralarme;
- Zeitdauer im Alarmzustand;
- Zeitverlauf aktivierter Alarmsignale einer Alarmquelle (Alarmketten), die Zeitdauern anstehender bzw. unquittierter Signale separiert in Zeiteinheiten;
- Häufigkeitsverteilung der Zeiten anstehender bzw. unquittierter Alarme;
- Zeitdauer der Quittierung von Alarmen;
- Anzahl der nicht quittierten Alarme;
- Folgealarme auf Bedieneingriffe;
- Folgebedieneingriffe auf Prozessalarm und auf Quittierung;
- Alarmprotokolle, Grenzwerte und unterdrückte Alarme;
- Zugriff und Berechtigungen”

Wichtige Merkmale wie Priorisierung, Gruppenbildung und situationsbedingte Alarmunterdrückung sollen sorgfältig dokumentiert werden.

Die zusätzliche Auswertung wissenschaftlicher Literatur ergab ebenfalls wenig neue Erkenntnisse.

Nimmo /101/ schlägt zwei Bewertungsmethoden für das Alarmmanagement vor: eine physische Verhaltensbewertung mit Szenarien und eine Leiterbewertung von Management und kulturellen Eigenschaften, die der Steuerung des Betriebes zugrunde liegen. Dazu gehören individuelle Faktoren (Situationsbewusstsein, Teamarbeit, Aufmerksamkeit und Erschöpfung, Training and Entwicklung, Rollen und Verantwortlichkeiten, Bereitschaft zum Handeln) und organisationale Faktoren (Management der Betriebsunterlagen, Veränderungsmanagement, kontinuierlicher Verbesserungsprozess der Sicherheit und des Kontrollraums)

Entsprechend der EEMUA /93/ sollten vier Kernprinzipien für die Gestaltung und Bewertung von Alarmsystemen berücksichtigt werden:

- Benutzungsfreundlichkeit: Alarmsysteme sollten so gestaltet werden, dass sie den Bedarf des Bedieners abdecken und innerhalb seiner Fähigkeiten funktionieren.
- Sicherheit: Der Beitrag des Alarmsystems zum Schutz der Menschen, der Umwelt und der Anlage sollte eindeutig identifiziert werden.
- Leistungsüberwachung: Die Leistung des Alarmsystems sollte bei der Gestaltung und Inbetriebnahme festgelegt werden, um die Betriebsfähigkeit und die Effektivität unter allen Bedienerbedingungen sicherzustellen. Regelmäßige Prüfungen sollten während des Anlagenlebens fortgesetzt werden, um zu bestätigen, dass das Alarmsystem gut funktioniert.
- Investition in Engineering: Alarmsysteme sollten unter angemessen hohen Standards konstruiert werden. Die Entwicklung neuer Alarmsysteme sollte einer strukturierten Methodologie folgen, das heißt insbesondere, dass jeder Alarm berechtigt und ausgereift sein sollte.

Des Weiteren sollen Alarmsysteme den Bediener unterstützen:

- potentiell gefährliche Situationen zu korrigieren bevor die Schutzsysteme eingreifen,
- zu erkennen und entsprechend zu Handeln, um gefährliche Situationen zu vermeiden,
- größere Unfälle zu verhindern oder seine Folgen einzugrenzen.

Da das Alarmmanagement ein kontinuierlicher Verbesserungsprozess ist, sollte die Alarmsituation ständig oder in sinnvollen Zeiträumen ausgewertet werden. Die Leistung des Alarmsystems sollte regelmäßig überprüft werden, vor allem um eine mögliche Alarmflut zu vermeiden.

Deshalb sollte der Designer für mögliche Unfallszenarien sicherstellen, dass die Alarmanzahl und die maximale Alarmrate den Bediener nicht überlasten.

Daher sollte ein Alarmmanagement folgendes beinhalten:

- Design von Alarmsystemen einschließlich Risikobeurteilung, Alarmpriorisierung, Zuverlässigkeitsbewertungen und die Bewertung von ergonomischen Erfordernissen
- Dokumentation, Validierung, Testen von Alarmsystemen
- Veränderungsmanagement (Change Management) und Außerbetriebnahme
- Darüber hinaus sollte es definierte Verfahren geben, die Veränderungen des Alarmsystems kontrollieren, einschließlich der Außerbetriebnahme einzelner Teile. Auf diese Art sollten alle vorgeschlagenen Änderungen vollständig analysiert, ihre Folgen bestimmt und zugestimmte Änderungen sollten mit Begründungen dokumentiert werden.
- Die folgenden Punkte sollten berücksichtigt werden:
- Jeder Alarm sollte schriftlich mit der entsprechenden Antwortprozedur dokumentiert werden, damit der Bediener die richtige Entscheidung über eine Reaktion auf einen Alarm treffen kann. Viele Alarme erfordern eine einfache Antwort und können durch generelle Verfahren abgedeckt werden. Auf kritische Alarme sollte jedoch einzeln, durch jeweils ein separates Verfahren, reagiert werden.
- Alle Alarmeinstellungen (während des Designs, der Inbetriebnahme und des Normalbetriebes) sollten systematisch festgestellt und dokumentiert werden. Alle Änderungen sollten gut begründet dokumentiert werden.
- Es sollte eine Strategie für die Validierung und das Testen von Alarmsystemen entwickelt werden. Dafür sollte es eine dokumentierte Prozedur/Verfahren geben. Das Verfahren sollte realistische Toleranzen angeben, ab wann ein Alarm aktiv wird.
- Leistungsmessungen des Alarmsystems können verwendet werden: als Zielgröße für die Akzeptanz von neueren Systemen, um die Angemessenheit von bereits existierenden Systemen zu beurteilen, als Management Tools zur Bewertung der Effektivität von laufenden Verbesserungsprogrammen, zur Identifizierung von unnötigen Alarmen.
- Leistungsvergleiche hinsichtlich der Bedienerfreundlichkeit können bei der Beurteilung helfen, ob der Bediener gut mit dem Alarmsystem arbeiten kann.
- Ein Programm zur Überprüfung sollte initiiert werden, um unnötige und schlecht gestaltete Alarme zu identifizieren und umzugestalten. Die Überprüfung sollte letztlich jeden Alarm im System abdecken.
- Ein leistungsstarkes Tool zur Optimierung des Alarmsystems ist die Übertragung dieser Aufgabe an spezielle Teams.

- Leistung sollte auditiert werden, Ausfälle durch Überlastungen sollten identifiziert werden und Maßnahmen sollten ergriffen werden, um ihre Häufigkeit zu reduzieren.

5.2 Diskussion auf dem Workshop

Die thematische Sitzung „An menschliche Fähigkeiten angepasste Alarmsysteme“ diente zur Vorbereitung von Vorschlägen für ein geeignetes Alarmmanagement.

Ein geeignetes Alarmmanagement muss als wichtiger Bestandteil eines kontinuierlichen Verbesserungsprozesses des Gesamtsystems angesehen werden. Über die Analyse der Alarme können nicht nur Schwächen im Alarmsystem selbst, sondern darüber hinaus auch Schwachstellen in der Anlage aufdeckt werden. In der Praxis hat sich häufig gezeigt, dass nur wenige Alarme für den Großteil der Alarmmeldungen verantwortlich sind. So kann mit der Beseitigung von Schwächen in der Anlage und im Alarmsystem eine deutliche Reduzierung der Alarmrate erzielt werden. Damit kann insgesamt die Beanspruchung der Benutzer aufgrund von Alarmmeldungen entscheidend optimiert und die Systemsicherheit so insgesamt verbessert werden.

Bei der Gestaltung, Änderung und Wartung eines Alarmsystems sollten sowohl menschliche Leistungsfaktoren als auch Leistungsgrenzen berücksichtigt werden, um ein Ereignis für den Operateur beherrschbar zu machen. In dieser Sitzung erschien es deshalb besonders relevant, Empfehlungen aus den Überlegungen der EEMUA /93/, der NAMUR /46/ und den OECD Leitlinien /2/ zu präsentieren und deren Anwendbarkeit in der verfahrenstechnischen Industrie zu diskutieren, vor allem im Hinblick auf ergonomische Anforderungen.

Weitere Möglichkeiten der Benutzerunterstützung wurden in den verschiedenen Vorträgen dieser Sitzung vorgestellt und bezogen sich erwartungsgemäß ebenfalls auf die Bereiche Alarmpriorisierung, Alarmdarstellung, Methoden der Alarmverarbeitung sowie situationsbedingte Alarmunterdrückung.

Insgesamt kristallisierten sich vier Kernprinzipien zur Gestaltung eines effizienten Alarmsystems heraus, die in verschiedene Schlussfolgerungen und Empfehlungen mündeten. Generell sollten die Alarme nach Wichtigkeit geordnet sein und eine hohe Zuverlässigkeit besitzen. Dazu ist eine qualitative und quantitative Risikobeurteilung notwendig. Ziel muss es sein, für mögliche Unfallszenarien die maximale Alarmrate zu ermitteln und die entsprechenden Antwortprozeduren schriftlich festzulegen. Zudem ist es erforderlich, dass eine Strategie für das Testen und die Validierung des Alarmsystems entwickelt wird und die Prozeduren entsprechend dokumentiert werden.

Da das Alarmmanagement aber keine einmalige Aufgabe ist, sollte das System regelmäßig überprüft und wenn möglich, optimiert werden, vor allem um eine

Alarmflut zu vermeiden. Bezüglich geplanter Veränderungen am Alarmsystem sollten ebenfalls definierte Verfahren existieren, mit denen die vorgeschlagenen Änderungen vollständig analysiert, ihre Folgen abgeschätzt und durchgeführte Änderungen dokumentiert werden.

5.3 Zusammenfassung und Fazit

Angesichts immer umfangreicher und komplexer werdender Industrieanlagen sind immer aufwendigere Alarmsysteme erforderlich, um die Operateure über mögliche Probleme zu informieren.

Die konsequente Anwendung eines gut durchdachten und gut geplanten Alarmmanagements ist deshalb unerlässlich, um die Anzahl und Häufigkeit von Alarmen und Meldungen zu reduzieren, ohne damit die Sicherheit der Anlage bzw. eine sichere Fahrweise zu gefährden. Es hat sich immer wieder gezeigt, dass ein intelligentes Alarmmanagement dazu führt, dass sich der Operateur besser auf seine wesentliche Aufgabe, nämlich die Prozessführung konzentrieren kann und nicht von „unnötigen Alarmen“ - eigentlich richtiger Meldungen - abgelenkt wird. Bei vielen parallel ablaufenden Vorgängen ist es selbst im Normalbetrieb schwierig, jeden Alarm bzw. Meldung zu berücksichtigen. Deshalb wird es ohne ein sorgfältiges Alarmmanagement nicht ausbleiben, dass selbst gewissenhafte Operateure die eine oder andere Information ignorieren. Weiterhin ist aus der Praxis bekannt, dass als störend empfundene Alarme von den Operateuren deaktiviert werden, was katastrophale Konsequenzen nach sich ziehen können.

Nach Meinung der Autoren dieses Berichtes ist die Frage, wie ein intelligentes Alarmmanagementsystem in der verfahrenstechnischen Industrie generell aussehen müsste, pauschal nicht zu beantworten und bei genauerer Betrachtung auch nicht sinnvoll.

Festzustehen scheint hingegen, dass es verschiedene Komponenten gibt, die in einem erfolgreichen Alarmmanagementsystem realisiert werden sollten.

Primär ist erforderlich, die verschiedenen Arten von Informationen über Prozess- und Anlagenzustände nach Handlungserfordernissen und Relevanz für die Sicherheit klar zu differenzieren. Weiter sollten generell bei der Gestaltung, Änderung und Wartung eines Alarmsystems sowohl menschliche Leistungsfaktoren als auch Leistungsgrenzen berücksichtigt werden, um ein Ereignis für den Operateur beherrschbar zu machen.

Insgesamt kristallisieren sich als Ergebnis der Literaturanalysen vier Kernbereiche zur Gestaltung eines effizienten Alarmmanagementsystems heraus. In Abhängigkeit vom Prozesszustand im Normalbetrieb und möglichen Notfallszenarien unter Beachtung der Situationsbedingungen sollten unterschiedliche Möglichkeiten der Benutzerunterstützung, die die Bereiche *Alarmpriorisierung*

(Alarmkategorisierung), Alarmverarbeitung (maximale Alarmrate, Festlegung einer Bearbeitungsreihenfolge der Alarme), *Alarmdarstellung* sowie *situationsbedingte Alarmunterdrückung* umfassen, umgesetzt werden.

In Bezug auf die Alarmpriorisierung, die Alarmverarbeitung und Alarmdarstellung sollte bei jedem auftretenden Alarm immer klar erkennbar sein, ob unverzüglich reagiert werden muss und wenn ja, wie dann reagiert werden sollte. Dazu ist es notwendig, eine Kategorisierung (Alarme oder Meldungen) nach Dringlichkeit der Reaktion des Operateurs vorzunehmen und diese dann auch konsequent zu verfolgen.

Eine solche Kategorisierung der Alarme sollte sich auch in der optischen und akustischen Alarmdarstellung wiederfinden lassen, beispielsweise sind Alarme immer rot und Meldungen immer gelb dargestellt. Darüber hinaus erscheint es innerhalb der Kategorien ebenfalls sinnvoll, in Abhängigkeit von den möglichen Folgen eines Ereignisses verschiedene Prioritätenstufen zu unterscheiden. Ein solches Kategorisierung-Priorisierungssystem unterstützt den Operateur dahingehend, welche Alarme in welcher zeitlichen Reihenfolge bearbeitet werden müssen und ermöglicht es in gewisser Weise die Bearbeitung von Alarmen zu standardisieren. Auf dieser Grundlage ist es dann ebenfalls möglich, in bestimmten Situationen „unnötige“ Meldungen/Alarme zu unterdrücken und die Belastung der Operateure zu reduzieren.

Da das Alarmmanagement jedoch keine einmalige Aufgabe, sondern ein kontinuierlicher Verbesserungsprozess ist, sollte das Alarmmanagementsystem regelmäßig überprüft und wenn möglich, optimiert werden, vor allem um negative Auswirkungen von Alarmen zu vermeiden. Bezüglich geplanter Veränderungen am Alarmsystem sollten ebenfalls definierte Verfahren existieren, mit denen die vorgeschlagenen Änderungen vollständig analysiert, ihre Folgen abgeschätzt und durchgeführte Änderungen dokumentiert werden.

Hierzu ist es aber dringend notwendig, validierte Evaluationsmethoden für Alarmmanagementsysteme zu entwickeln und die Ergebnisse aus den Evaluationen von Alarmmanagementsystemen entsprechend zu dokumentieren.

Neben diesem Forschungsbedarf, lässt sich umfangreicher Handlungsbedarf bei der konkreten Umsetzung und Anwendung bereits vorhandener Erkenntnisse bzgl. eines Alarmmanagements erkennen. Die Autoren schließen sich der Einschätzung des OECD-CCA-Workshops bezüglich des weiteren Handlungsbedarfs an und setzen die Prioritäten für die Umsetzung der OECD-Empfehlungen auf folgende Aspekte des Alarmmanagement:

- Ganzheitliches Alarmmanagement für alle verfahrenstechnischen Anlagen mit hohem Gefährdungspotential, d. h. die Festlegung einer Alarmmanagementstrategie, Entwicklung eines Leitfadens für das Alarmdesign auf dieser Grundlage, Festlegung von Schlüsselindikatoren zur

Leistungsbeurteilung, Benennung einer verantwortlichen Person und die Anwendung eines Auditprogramms.

- Berücksichtigung der Aufgaben und Bedürfnisse der Operateure bei der Planung und Implementierung neuer Alarmsysteme, d. h. Analyse der Aufgabenanforderungen an den Operateur in verschiedenen Betriebszuständen zur Sicherstellung ausreichender Informationsverarbeitungs- und Zeitressourcen bei der Aufgabenbewältigung.
- Kontinuierliche Verbesserung vorhandener Alarmmanagementsysteme, d. h. regelmäßige Überwachung, Analyse und Umsetzung der Ergebnisse zur Erhöhung der Qualität des Alarmmanagementsystems. Schlüsselelemente sind dabei die Verbindlichkeit seitens des Managements, ein passendes und adäquates Design, passende Alarmprioritäten und definierte Operateurhandlungen auf Alarme.

Aktuelle Beispiele guter Praxis für das Alarmmanagement sind in der EEMUA 191 /93/ und NAMUR 102 /46/ zusammengetragen. Ergänzend ist die DIN EN 61511-1 (2003) /18/ zu beachten.

6 Zusammenfassung der Workshoppräsentationen

Im Folgenden werden die wesentlichen Präsentationsinhalte der einzelnen Redner für jede thematische Sitzung zusammenfassend dargestellt. Die präsentierten Themen und Redner können dem Workshopprogramm (vgl. Kap. 6.6) entnommen werden.

6.1 Thematische Sitzung 1: Arten menschlicher Fehler, Definition der relevanten Begriffe

Die OECD führte im September 2004 einen Workshop zum Thema „Lernen aus Ereignissen“ durch /3/. Aus dem Workshop, resultierten Empfehlungen zur Harmonisierung der Fachsprache, um den Austausch von Informationen hinsichtlich organisationalen Lernens, Erkenntnissen aus Ereignissen, Ereignisstatistiken und Ereignisanalysen zu verbessern. Die Empfehlung bezieht sich auch auf die verwendeten Terminologien für menschliche Fehler. Eine Harmonisierung der Terminologien und Definitionen könnten in Zukunft für die Analyse und Dokumentation von (Beinahe-) Ereignissen in der der verfahrenstechnischen Industrie sowie zur Verbesserung von „Lessons Learnt“ verwendet werden.

Zur Vorbereitung der ersten Sitzung wurden technische Standards, ausgewählte Berichte über Ereignisse und Beinahe-Ereignisse sowie Forschungsliteratur aus verschiedenen Bereichen analysiert. Insgesamt wurden zu 28 Begriffen die verwendeten Definitionen zusammengetragen, wovon zwölf Begriffe spezifisch für den Bereich Ereignisanalyse und Dokumentation von Ereignissen relevant sind. Des Weiteren wurden Definitionen zu 16 Begriffen, die einen thematischen Bezug zu den Sitzungen des Workshops oder einen höheren Generalisierungsgrad aufwiesen, gesammelt. Dabei war es wichtig, dass die ausgewählten Begriffe sowohl individuelle als auch organisationale Faktoren abdecken. Darüber hinaus sollten die Begriffe und Definitionen nicht zu detailliert und in Bezug auf das individuelle Verhalten formuliert werden. Bei der Identifikation der verschiedenen menschlichen Fehlertypen erscheint es sinnvoll eine empirisch belegte Klassifikation zu verwenden, wie zum Beispiel die generellen Fehlertypen (GFT) von Groeneweg /45/. (Fahlbruch, B., Terms in the context of human factors /102/)

Der Begriff menschliche Faktoren kann für verschiedene Personen unterschiedliche Bedeutungen haben. Es bestehen Möglichkeiten die verschiedenen Terminologien zu klären und zu harmonisieren. Eine Analyse von zwei Ereignisdatenbanken der verfahrenstechnischen Industrie in Kanada zeigte, dass auf menschliche Faktoren bezogene Ereignisursachen feiner unterteilt werden sollten. Dabei ist es wichtig zwischen Management/Systemversagen und individuellen Versagen zu unterscheiden sowie deren relativen Beitrag zur Ereignis-

entstehung zu identifizieren. Letztere können als menschliche Faktoren im engeren Sinne bezeichnet werden. In diesem Zusammenhang werden zwei Typen von menschlichen Faktoren vorgeschlagen: (1) individuelles Verhalten und damit verbundene Interaktionen (Auslassungen, Unterlassungen) und (2) Management oder systembezogene Faktoren. Darüber hinaus sollten für jeden Typ korrigierende Maßnahmen unter Berücksichtigung der Lebenszyklusperspektive (Design, Betrieb, Wartung) definiert werden. Der erste Bereich menschlicher Faktoren, erfordert geeignete Maßnahmen, um speziell individuelle Handlungsfehler zu vermeiden. Für den zweiten Bereich wird die Einführung eines prozessbezogenen Sicherheitsmanagement als wichtig erachtet. (Marta, M., Review of two incident database from the Canadian chemical industry and discussion of human factors related terms/parameters, incident data and opportunities /102/)

Anfänglich dominierte in der Sicherheitsforschung eine individuumzentrierte Sichtweise. Diese Zentrierung des Sicherheitsdenkens hat sich jedoch in den letzten Jahren erweitert. Eine ganzheitliche Betrachtungsweise setzt sich zunehmend durch. Analysen von Ereignissen zeigten, dass für ein Verständnis der zugrundeliegenden Ursachen die organisationale Perspektive eine entscheidende Rolle spielt. Organisationale Faktoren beziehen sich auf die Beurteilung der Organisation als Ganzes innerhalb der Grenzen bestehender Sicherheitspraktiken. Einige wichtige Bereiche der organisationalen Sichtweise auf Ereignisse sind: die Verwendung und Auswirkung von Macht, kulturelle Einflüsse, Entscheidungsprozesse, Lernen durch Betriebserfahrung, Auseinandersetzung mit Sicherheitsbarrieren unter dem Druck der Produktion, soziale Einflüsse sowie Probleme mit Sicherheitsindikatoren. (Le Coze, J.C., Accidents: From human factors to organisational factors /102/)

Die MARS Datenbank (European Community´s Major Accident Reporting System) /7/ ist das zentrale Informationsnetz der EU und der OECD Mitgliedstaaten zur standardisierten Dokumentation, Analyse und Weitergabe von Ereignissen und Störungen entsprechen der Seveso und Seveso II Richtlinie. Insgesamt sind über 600 Ereignisse erfasst, davon sind etwa 50% mit Ursache „Mensch“ klassifiziert. Das übergeordnete Ziel ist, die Sensitivität und Exaktheit der Identifikation des menschlichen Beitrages an einem Ereignis zu erhöhen. In diesem Zusammenhang sind zwei Fragen besonders von Interesse: Was für Informationen über menschliche Faktoren werden in der MARS Datenbank erfasst und sind diese Informationen ausreichend und nachvollziehbar, um den Zweck von MARS zu erfüllen?

Auf menschliche Faktoren bezogene Daten sind in MARS nach ihren Ursachen klassifiziert und umfassen sowohl menschliche als auch organisationale Fehler. Ein wichtiger Punkt dabei ist die Nachvollziehbarkeit von menschlichen Faktoren in der MARS Datenbank. Baranzini definiert diese als „a system´s capability

for complete tracing of human factors events along a process“. Die Nachvollziehbarkeit in MARS ist generell konsistent, sollte aber im Hinblick auf Vollständigkeit, Nützlichkeit und Zuverlässigkeit der Daten weiterentwickelt werden. (Baranzini, D., Human factors data traceability analysis in MARS /102/)

Als Teil des Programms „Verbesserung der Berufssicherheit in den Niederlanden“ („Improving Occupational Safety In the Netherlands“) wurden 9000 Vorfälle in den Niederlanden zwischen 1998 und 2004 in Bezug auf die zugrunde liegenden Ursachen für diese Vorfälle analysiert. Dafür wurde die Methode des sogenannten „Storybuilder“ entwickelt. Er ermöglicht eine systematische Unfallanalyse durch die Darstellung der Unfälle als Ereignissequenzen. Die Vorfälle wurden nach ihrer Gefährdung klassifiziert, wie zum Beispiel Verlust an Sicherheit („loss of containment“), Explosion („explosion“), Schlag von sich bewegenden Objekten („hit by moving objects“), von einer bestimmten Höhe fallen („falling from hights“). Die Analyse basiert auf einem Ereignismodel, welches im Rahmen des IRSK-Projektes entwickelt wurde. Der Schwerpunkt des Projektes lag auf organisationalen und menschlichen Faktoren. Die Analyse der Vorfälle ergab im wesentlichen vier zugrundeliegende Faktoren in Bezug auf Human Factors: Bereitstellung („provide“), Gebrauch/Verwendung („use“), Wartung („maintain“) und Überwachung („monitor“). (Oh, J., The use of “storybuilder” as an accident analysis tool /102/)

In der Diskussion und daran anschließenden Abstimmung zwischen den Beteiligten spiegelte sich wider, dass es zum besseren Verständnis und zur klaren Abgrenzung zwischen den verschieden Begriffen sinnvoll erscheint, ein allgemein akzeptiertes Taxonomiemodell zu entwickeln.

- Der Begriff menschlicher Faktor kann für unterschiedliche Personen unterschiedliche Bedeutungen haben. Die OECD könnte ein geeignetes Forum sein, um die Entwicklung eines Modells zur Klassifikation von menschlichen Faktoren zu leiten.
- Begriffe in Bezug auf menschliche Faktoren, die relevant sind für die Ereignisuntersuchung und –dokumentation müssen innerhalb eines Taxonomiemodells definiert werden. Das Ziel sollte es sein, von Ereignissen etwas über relevante menschliche Fehlerarten zu lernen und Präventionsmaßnahmen ausreichend zu unterstützen.
- Aufgrund der Erfahrung in anderen Industrien sollte die Taxonomie nicht zu ausführlich sein. Es gibt bereits Taxonomien, die sich auf menschliche Faktoren beziehen in anderen Industrien: HFACS – Human Factors Analysis and Classification System (Luftfahrt) and HFIT – Human Factors Investigation Tool (Öl).
- Diese Modelle sollten betrachtet werden, wenn man ein Modell für die Prozessindustrie entwickelt. Prozessindustrien erfordern Systemmodelle und

Prozessperspektiven, um die Rückverfolgbarkeit von menschlichen Faktoren zu verstehen.

- Die Analyse von Daten bezüglich des Beitrags von menschlichen Faktoren zu Unfallszenarien ist für Experten interessant, wird aber ebenfalls von der Führungsebene, die Entscheidungen zur Sicherheitspolitik und zu verfügbaren Ressourcen trifft, verlangt. Folglich sollte die Taxonomie für den Endbenutzer verständlich sein. Jedoch muss eine Übervereinfachung vermieden werden. Es ist notwendig, eine wohlüberlegte Wahl zwischen den folgenden Eigenschaften zu treffen: allgemein, einfach oder genau. Es können aber nur zwei aus drei dieser Eigenschaften gleichzeitig erreicht werden.
- Die MARS-Datenbasis /7/ muss bezüglich menschlicher Faktoren weiter entwickelt werden. Dazu ist weitere Arbeit empfehlenswert.

Darüber hinaus wurden folgende Empfehlungen im Rahmen der Diskussion formuliert:

- Ein zweistufiger Ansatz wird empfohlen: Eine Stufe ist die Analyse vor Ort. Eine Stufe sind Experten, die den Austausch von „Lessons Learnt“ und der Ereignisgeschichte sicherstellen. Es sollte mit einfachen Modellen begonnen werden, die später präzisiert und im Detail entwickelt werden könnten.
- Modelle zur Klassifikation von menschlichen Faktoren sollten zwischen individuellen und organisationalen Faktoren unterscheiden. Korrektive Maßnahmen sollten diese Begriffe separat ansprechen und die Wirksamkeit unterschiedlich auch unter der Lebensdauerperspektive sicherstellen (Design, Betrieb, Wartung).
- Ein spezielles Training zum Thema menschliche Faktoren wird für die, die Ereignisse analysieren und die Taxonomie anwenden, empfohlen. Zur Anwendung der Taxonomie sollten die Vorgehensweisen exakt beschrieben werden, um eine Angemessenheit sicherzustellen. Um diese zu erzielen, müssen sie genau, vollständig und im Ansatz und der Form konsistent sein.

6.2 Thematische Sitzung 2: Bewertung von Sicherheitskulturen

Der Hauptfokus dieser Sitzung lag auf der Verhütung von Unfällen in der verfahrenstechnischen Industrie. Hierfür wurden Wege zur Charakterisierung und Differenzierung von Sicherheitskultur sowie Möglichkeiten zur Beurteilung oder Bewertung von Sicherheitskultur aufgezeigt. Die OECD Leitlinien /2, 59/ betonen die Wichtigkeit von Sicherheitskultur und geben verschiedene Vorschläge hinsichtlich der Elemente von Sicherheitskultur. Zurzeit existieren jedoch keine

allgemein akzeptierten Empfehlungen über Methoden zur Bewertung, Sicherstellung und Verbesserung der existierenden Sicherheitskulturen. Als Ergebnis dieser thematischen Sitzung sollten abgestimmte Empfehlungen zur Verbesserung und Erhebung von Sicherheitskultur sowie Referenzen für relevante Indikatoren von sicherheitsgerichteten Verhalten für die OECD-Leitlinien generiert werden.

Das Konzept Sicherheitskultur ist ein relativ neues Konzept und wurde erstmals im Zusammenhang mit der Tschernobyl-Katastrophe verwendet. Trotz der häufigen Verwendung und Popularität des Begriffes, existieren theoretische und methodische Mängel. Der Begriff der Sicherheitskultur ist dabei ein Omnibusbegriff zu werden, bei dem jeder sich etwas vorstellen kann, nur leider jeder etwas anderes. Angefangen von kognitiven Merkmalen der Organisationsmitglieder bis hin zu einer eher umfangreichen, systemischen Sichtweise, welche die Organisation als Ganzes betrachtet. Dazu zählen: einzelne Organisationsmitglieder, Arbeitsteams, organisationale Eigenschaften und Bereiche, Technik und die Organisationsumwelt. Es zeichnet sich jedoch ein wachsender Konsens ab, dass Sicherheitskultur als holistisches und integriertes Konzept verstanden wird.

Ein weiteres Problem bezieht sich auf die Beziehung von Sicherheitskultur und Sicherheitsklima. Dabei wird das Konzept Sicherheitsklima häufig als erster Ansatzpunkt zur Beurteilung von Sicherheitskultur verwendet und basiert hauptsächlich auf Fragebogenuntersuchungen. Diese sind jedoch nicht ausreichend, um die tieferen Ebenen von Kultur zu untersuchen.

Es bleibt festzuhalten dass, um den konzeptionellen Anspruch von Sicherheitskultur gerecht zu werden, man sich mit den grundlegenden Problemen eines heterogenen Begriffsverständnisses, unzureichender Theoriebildung und Schwierigkeiten bei der Operationalisierung kritisch auseinandersetzen sollte. In diesem Zusammenhang sind drei grundlegende methodische Herausforderungen bei der Beurteilung von Sicherheitskultur relevant. Erstens, die Beurteilung von Sicherheitskultur muss über die Analyse von Artefakten und Erwartungen hinausgehen. Kultur bezieht sich auf sozial geteilte Grundüberzeugungen, welche Einstellungen und Verhalten beeinflussen. Zweitens, sollte sich die Bewertung von Sicherheitskultur nicht nur auf individuelle Denkweisen beschränken, sondern unterschiedliche Dimensionen, Elemente und Gruppen mit einbeziehen. Es sollten qualitative, quantitative und kontextbezogene Instrumente eingesetzt werden, die sich gegenseitig ergänzen. Da Sicherheitskultur auf einen gemeinsamen Handlungsrahmen basiert, sollten die eingesetzten Bewertungstechniken auf die jeweilige Organisation und Gruppen zugeschnitten werden. Das bezieht auch alle Management- und Mitarbeiterebenen mit ein. (Wilpert, B. & Schöbel, M., Challenges and opportunities of assessing safety culture, /102/)

Das niederländische Ministerium für soziale Angelegenheiten begann 2003 mit einem Projekt über Sicherheitskultur und Ereignisanalysen, innerhalb des Programms „Verbesserung der Arbeitssicherheit in den Niederlanden“. Die Zielsetzung ist, die Anzahl von Arbeitsunfällen auf weniger als zehn Prozent zu verringern. Insgesamt fanden Untersuchungen in 22 Unternehmen aus verschiedenen Branchen statt. Das übergeordnete Ziel war es, die Sicherheitskultur der Unternehmen zu verbessern. Dazu sollten die beteiligten Unternehmen einen Plan erstellen, der den Prozentsatz zu reduzierender Unfälle, die dafür eingeplante Zeit und die dafür vorgesehenen Instrumente beschreibt. Auf der Basis der Untersuchungsergebnisse kann festgehalten werden, dass für die Beurteilung von Sicherheitskultur sowohl quantitative, qualitative und kontextbezogene Daten von allen Ebenen einer Organisation nötig sind. (Van Wissen, P., Improving occupational safety in the Netherlands /102/)

Sicherheitskultur ist ein umfassendes Konzept, das aus einzelnen Sicherheitsvorkehrungen auf der Strategie-, Management- und individuellen Ebene besteht. Im Sicherheitsmanagement sind diese einzelnen Sicherheitsvorkehrungen zu einem Managementsystem zusammengefügt. Eine Kritik am Konzept der Sicherheitskultur ist die mangelnde Einbindung in ein übergeordnetes Managementsystem. Veränderungsmanagement, als Bestandteil von Sicherheitsmanagementaktivitäten kann zu einem erweiterten Verständnis und Konzeptualisierung von Sicherheitskultur beitragen. Ein gutes Veränderungsmanagement sollte von den Mitarbeitern sowohl als kritisches Element als auch als geeignete Maßnahme für organisationale Veränderungen, Transparenz und Innovation akzeptiert werden. Das Verständnis von Sicherheitskultur im Sinne von einem „Managen von Unsicherheit“ hilft dabei sich von impliziten Annahmen und Normen zu lösen, um letztendlich sicheres Handeln zu fördern. (Grote, G., Diagnosis of safety culture: A replication and extension towards assessing “safe” organizational change processes, /102/)

Das Konzept Sicherheitskultur ist erwähnt schwer zu definieren und damit auch zu messen. Die meisten Definitionen konzentrieren sich auf die Identifikation von Charakteristiken die eher eine ideale und damit schwer zu erreichende Sicherheitskultur widerspiegeln. Dies macht es schwierig für Organisationen Verbesserungspläne zu strukturieren und zu implementieren. Ein alternativer Ansatz beinhaltet die Berücksichtigung von mehreren Kulturen oder verschiedenen Entwicklungsstufen von Sicherheitskultur. Angefangen von einer rein pathologischen bis hin zu einer weiterentwickelten generativen Sicherheitskultur. Letzteres wird auch als hoch zuverlässige Organisation („High Reliability Organisation“) bezeichnet. Der Vorteil von diesem Ansatz ist, dass er beides berücksichtigt: die Messung der aktuellen Sicherheitskultur auf der jeweiligen Entwicklungsstufe der Organisation und die Definition von dahinter liegendem Verhalten und Praktiken, die dabei helfen können die vorherrschende Sicherheitskultur weiterzuentwickeln und zu verbessern. In diesem Zusammenhang

hat sich das in Abbildung 9 dargestellte fünfstufige Reifegradmodell /67/ bewährt. Es unterstützt die Bemühungen zur Verbesserung der Sicherheitskultur in vielen Hochrisikoindustrien und könnte daher eine gute Grundlage für die Bewertung und Entwicklung von Sicherheitskulturen sein. Das Modell beinhaltet die Elemente des Sicherheitsmanagementsystems. Die grundlegende Idee ist, die lokale Sicherheitskultur (auf jeder Stufe) durch kleine zweckmäßige Schritte zu entwickeln. (Hudson, P., Safety culture models as a basis for improvement, /102/)

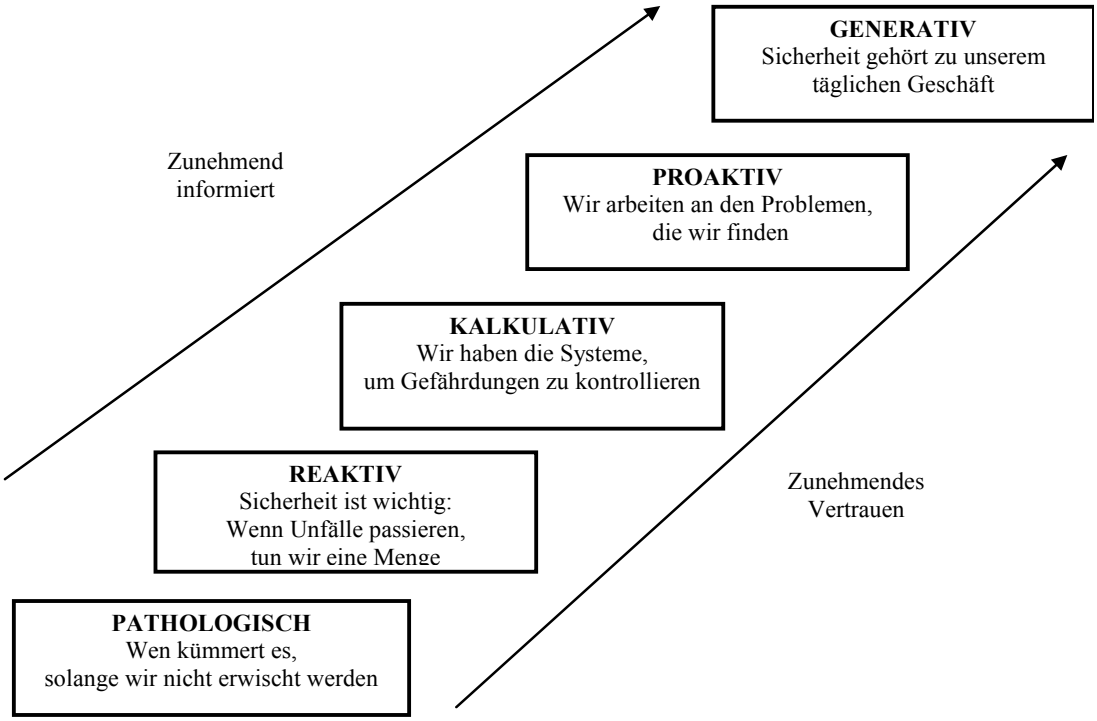


Abbildung 9 : Reifegradmodell der Sicherheitskultur /67/

Besonders die Unternehmen, die bereits eine gute Sicherheitskultur aufweisen, sollten versuchen, einen tiefer gehenden analytischen Einblick in ihre Sicherheitskultur zu erreichen. Dieser beinhaltet die Einstellungen und Motivationen der Mitarbeiter; die informellen, sozialen und gruppenspezifischen Normen; kognitive Aspekte wie Lernprozesse und die individuelle Risikoabschätzung. Die Diagnose tiefer gehender Aspekte von Sicherheitskultur erfordert einen flexiblen und analytischen Ansatz. Dieser sollte in der Lage sein, mehr Informationen zu liefern als ein Standard-Auditprogramm. Die gewonnenen Informationen sollten die Realität möglichst genau abbilden und es sollten kulturelle Muster der Organisation erkennbar werden. Darüber hinaus spielt das Management- und Führungsverhalten eine wichtige Rolle bei der Bewertung von Sicherheitskultur und sollte berücksichtigt werden. (Adolph, L., The International Safety Rating System “ISRS” and the “SAMOS” interview technique, /102/)

Aufgrund der Präsentation der verschiedenen Beiträge in der thematischen Sitzung und der daran anschließenden Diskussion, konnten folgende Schlussfolgerungen in Bezug auf Sicherheitskulturen und deren Beurteilung formuliert werden:

- Sicherheitskultur ist ein relativ neues Konzept. Dennoch wird es in vielen hochrisiko-behafteten Industrien angewendet. Sicherheitskultur bedeutet, zu verstehen, wie Gefahren entstehen, zu wissen, dass die Beherrschung von Gefahren möglich ist und Priorität hat, sich gemeinsam entsprechend dieser Annahmen zu verhalten und offen für Lernen und Verbesserung zu sein.
- Selbstbeurteilungen können lernende Organisationen unterstützen.
- Das fünfstufige Reifegradmodell /67/ hat sich gut bewährt und unterstützt die Bemühungen zur Verbesserung der Sicherheitskultur in vielen Hochrisiko behafteten Industrien. Es könnte eine Grundlage für Bewertung und Entwicklung von Sicherheitskulturen sein. Das Modell ist mit dem einfachen Sicherheitsmanagement durch die Elemente des Sicherheitsmanagementsystems verbunden. Die Idee dahinter ist, die lokale Kultur (auf jeder Stufe) durch kleine zweckmäßige Schritte zu entwickeln.
- Besonders die Unternehmen, die bereits ein gutes Sicherheitsniveau erreicht haben, müssen einen tiefgreifenderen analytischen Einblick in ihre Sicherheitskultur erreichen: Die Einstellungen und Motivationen der Mitarbeiter, die informalen Normen , die sozialen und gruppenspezifischen Normen, kognitive Aspekte wie etwa Lernprozesse und die individuelle Risikoabschätzung müssen betrachtet werden. Einige der organisationalen Kriterien können ebenso gemessen werden wie technische.
- Die Bewertung der Sicherheitskultur könnte für die Prioritätensetzung bei der Inspektion und der Auditierung nützlich sein. Dies könnte Anleitungen zur Bewertung der Sicherheitskultur für die Unternehmen, Auditoren und Inspektoren erforderlich machen.
- Unterschiedliche Dimensionen, Elemente und Gruppen müssen bei der Evaluation der Sicherheitskultur betrachtet werden.
- Die Bewertung der Sicherheitskultur muss über die Analyse von Artefakten und ausgesprochenen Werten hinausgehen. Die Kultur umfasst gemeinsame Grundüberzeugungen, die Einstellungen und Verhalten beeinflussen.
- Zur Diagnose dieser tieferen Stufen der Sicherheitskultur wird ein flexibler und analytischer Ansatz benötigt. Das Management- und Führungsverhalten sollte ein bedeutsames Kriterium bei der Bewertung der Sicherheitskultur sein.

Weiterhin konnten als Ergebnis dieser thematischen Sitzung die folgenden Empfehlungen bezüglich der Bewertung von Sicherheitskulturen formuliert werden:

- Die Bewertung der Sicherheitskultur ist in verschiedenen Industriebereichen gebräuchlich und hat als wichtiges Werkzeug die Verbesserung der Sicherheit in der Prozessindustrie gefördert. Erforderlich ist die Entwicklung und Verbreitung von geeigneter Information und die Anleitung von Unternehmen, so dass sie ihre Sicherheitskultur selbst beurteilen und deren Qualität weiterentwickeln und verbessern können.
- Sicherheitskultur ist ein gemeinsamer Handlungsrahmen. Die Bewertungstechniken müssen auf die Organisationen und Gruppen zugeschnitten werden. Sie sollten alle Managementebenen und Mitarbeiter erfassen und besonders das mittlere Management berücksichtigen.
- Unterschiedliche Dimensionen, Elemente und Gruppen müssen bei der Evaluation der Sicherheitskultur betrachtet werden.
- Die Bewertung der Sicherheitskultur muss über die Analyse von Artefakten und ausgesprochenen Werten hinausgehen. Die Kultur umfasst gemeinsame Grundüberzeugungen, die Einstellungen und Verhalten beeinflussen.
- Zur Diagnose dieser tieferen Stufen der Sicherheitskultur wird ein flexibler und analytischer Ansatz benötigt. Das Management- und Führungsverhalten sollte ein bedeutsames Kriterium bei der Bewertung der Sicherheitskultur sein.
- Die Betrachtung der Sicherheitskultur sollte ebenfalls den Umgang von Organisationen mit Unsicherheit enthalten.
- Die Veränderung von Organisationen muss im Sicherheitsmanagement eingeschlossen werden. Organisatorische Veränderungen sollten nicht schneller durchgeführt werden, als eine Entwicklung der Organisation möglich ist. Die Bewertung der Sicherheitskultur sollte während der Veränderung der Organisationen durchgeführt werden. Veränderungsmanagement sollte mehr im Hinblick auf seine Einbettung in und seine Effekte auf die Organisationskultur reflektiert werden, was außerdem zu einem vertieftem Verständnis und einer Konzeptualisierung der Sicherheitskultur führen könnte.
- Es sollten qualitative, quantitative und kontextbezogene Instrumente für alle Organisationsebenen entwickelt werden.
- Als erster Zugang kann ein kurzer Fragebogen benutzt werden.
- Das fünfstufige Reifegradmodell /67/ hat sich gut bewährt und unterstützt die Bemühungen zur Verbesserung der Sicherheitskultur in vielen Hochrisiko behafteten Industrien. Es könnte eine Grundlage für die Bewertung

und Entwicklung von Sicherheitskulturen sein. Das Modell ist mit dem einfachen Sicherheitsmanagement durch die Elemente des Sicherheitsmanagementsystems verbunden. Die Idee dahinter ist, die lokale Kultur (auf jeder Stufe) durch kleine zweckmäßige Schritte zu entwickeln.

- Besonders die Unternehmen, die bereits ein gutes Sicherheitsniveau erreicht haben, müssen einen tiefgreifenderen analytischen Einblick in ihre Sicherheitskultur erreichen: Die Einstellungen und Motivationen der Mitarbeiter, die informalen Normen , die sozialen und gruppenspezifischen Normen, kognitive Aspekte wie etwa Lernprozesse und die individuelle Risikoabschätzung müssen betrachtet werden. Einige der organisationalen Kriterien können ebenso gemessen werden wie technische.
- Sicherheitskultur schließt nicht nur das Verhalten der Mitglieder einer Organisation selbst, sondern aller Mitglieder eines System im weiteren Sinne ein: einzelne Organisationsmitglieder, Arbeitsgruppen, organisatorische Eigenschaften und Einheiten, besondere organisatorische Umgebungen, z. B. Aufsichtbehörden, Technologie. Sicherheitskultur sollte als holistisches und integratives Konzept begriffen werden.

6.3 Thematische Sitzung 3: Kompetenzen im Thema „Human Factors“

Die unterschiedlichen Management- und Mitarbeiterebenen in Organisationen (Industrie, Aufsichtsbehörden, Sachverständigenorganisationen) haben verschiedene Verantwortlichkeiten, die spezifische Kenntnisse und Kompetenzen im Bereich menschliche Faktoren erfordern. In dem Workshop sollten Empfehlungen über geeignete Kompetenzen in Bezug auf Human Factors hinsichtlich unterschiedlichen Verantwortlichkeiten auf Seiten des Managements und der Mitarbeiter formuliert werden. Daraus können dann adäquate Trainingsprogramme über menschliche Faktoren in der verfahrenstechnischen Industrie entwickelt werden, die auf die Reduzierung von Ereignissen und deren Folgen abzielen.

Die Notwendigkeit von Human Factors-Kompetenzen konnte anhand von Beispielen chemischer Unfälle in Korea gezeigt werden und lieferte zusätzliche Informationen, die zur Analyse solcher Unfälle genutzt werden können. Es konnte gezeigt werden, dass nicht vorhandene Human Factors-Kompetenzen zu unerwünschten Verhaltensweisen wie beispielsweise eine hohe Risikobereitschaft und starkes Konkurrenzdenken führen. (Pak, S., Human factors related chemical accidents occured in Korea /102/)

Kenntnisse im Hinblick auf menschliche Faktoren sind notwendig, um die menschliche Leistungsfähigkeit in komplexen Arbeitsumgebungen vor allem in Sicherheitssystemen sicherzustellen. Der Fokus auf spezielle Bereiche

menschlicher Faktoren für die verschiedenen Mitarbeiterebenen sollte in Abhängigkeit von deren Verantwortung formuliert werden. Das Management beispielsweise weist einen eher geringen aktiven Anteil an der Bedienung der Anlage auf. Daher ist hier Grundlagenwissen über aktive Fehler, Eskalationsmechanismen und Gruppendynamik ausreichend. Auf der anderen Seite sollten Themen wie strategisches Denken und Problemlösen in komplexen Situationen ausführlicher behandelt werden. Das Bedienpersonal sollte hingegen vor allem ein solides Wissen über aktive Fehler, menschliche Ressourcen und Grenzen im Umgang mit kritischen Situationen in einer komplexen Arbeitsumgebung aufbauen. Das Erlernen entsprechender Kompetenzen sollte möglichst nah an der realen Arbeitsumgebung stattfinden. Hierfür bieten sich beispielsweise Fallstudien in Workshops an. Beispiele aus der Prozessindustrie verdeutlichen, dass ein einseitiges Training menschlicher Faktoren nicht ausreicht. Vielmehr sollte die Bedeutung menschlicher Faktoren als wichtiger Sicherheitsfaktor auf allen organisationalen Ebenen etabliert werden. Dabei spielt die Unterstützung durch das obere Management eine entscheidende Rolle. Während des Trainings sollte eine Feedbackschleife verbunden mit einem kontinuierlichen Verbesserungsprozess auf allen Hierarchieebenen eingeführt werden. Insbesondere in der verfahrenstechnischen Industrie sollte dieser Lernprozess durch Regierungsvertreter begleitet werden. (Horn, G., What they should have known: Human factors competencies in plant environments /102/)

Bei der Ausbildung von entsprechenden Kompetenzen über menschliche Faktoren auf verschiedenen organisatorischen Ebenen ist es wichtig, Lerninhalte sowie Ausbildungsformen zu definieren. Je nachdem, wer was lernen soll, ist es notwendig zu diskutieren, wie gelernt werden sollte: Faktenwissen kann über traditionelle Methoden wie beispielsweise Frontalunterricht und Lesen vermittelt werden. Dagegen können spezielle Fähigkeiten nur durch praktische Übungen erlernt werden. Aus ökonomischen Gründen sollte nicht jeder Mitarbeiter gleich intensiv in Bezug auf menschliche Faktoren trainiert werden. Es sollte genau festgelegt werden, wer wie viel über menschliche Faktoren wissen sollte (faktisches oder deklaratives Wissen) und wer dieses Wissen auf verschiedene Art und Weise anwenden muss (prozedurales Wissen, Fähigkeiten). Für verschiedene organisationale Ebenen sollten verschiedene Trainingsschemata entwickelt werden. Mögliche Trainingsinhalte sind: Coaching, strategisches Denken, Problemlösen, Kommunikationskonzepte, Gruppendynamik, Fehlerentdeckung, Bewusstsein zur Beeinflussung von Deeskalationen, Pragmatiken und Fallstudien.

Weitere Bemühungen, bezogen auf das Training von menschlichen Faktoren, sollten spezifischere Inhalte der verschiedenen Ebenen einer Organisation (Mitarbeitergruppen), handlungsorientierte Definitionen von notwendigen Kompetenzen und Kriterien zur Evaluation von Trainingsprogrammen beinhalten.

(Hofinger, G., How to learn human factors competencies at different organisational levels /102/)

Menschliche Faktoren sind nicht zwangsläufig direkt messbare Quantitäten. Die Durchführung von Inspektionen erfordert die Bewertung einer realen Situation. Dafür benötigen Inspekteure Methoden, um die aktuelle Situation mit dem angestrebten Referenzstatus zu vergleichen. Daher wird die Entwicklung einer Toolbox aus Methoden, Checklisten und Beratung empfohlen, um Inspekteure bei der Identifikation von sicherheitskritischen Faktoren zu unterstützen. (Reddehase, B., Inspecting for human factors within the German major hazards ordinance: Examples, experience and future needs /102/)

Zum Thema Kompetenz in Bezug auf menschliche Faktoren konnten aufgrund der thematischen Sitzung folgende Schlussfolgerungen zusammengefasst formuliert werden:

- Insgesamt konnten 12 relevante Trainingsinhalte aus dem Bereich menschliche Faktoren (generelle Aspekte, menschliche Leistung und Einschränkung, Human Resource Management, Ergonomie, Sozialpsychologie, leistungsbeeinflussende Faktoren, physikalische Umgebung, Aufgaben, Kommunikation, menschliche Fehler, Gefahren am Arbeitsplatz und Risikoanalysen, Krisenmanagement) und sechs relevante Gruppen Regelsetzer, Aufsichtsbehörden, strategisches und operative Management, Sicherheitspersonal und Operateure) identifiziert werden. Weiterhin werden drei verschiedene Wissensniveaus für die relevanten Gruppen empfohlen. Die genannten Trainingsinhalte, Gruppen und Wissensniveaus werden in einer einfachen Matrix dargestellt. Die Matrix könnte die Grundlage für Industrie und Behörden sein, Anforderungen an die Kompetenzen in Bezug auf menschliche Faktoren der Belegschaft zu definieren.
- Es ist erforderlich, dass eine “Toolbox“ für Methoden, Checklisten (wenn geeignet) und unterstützende Anleitungen für Inspektoren zur Identifikation sicherheitskritischer menschlicher Faktoren in der Anlage entwickelt werden. Vorhandene Anleitungen für Inspektionen sollten um das Element „menschliche Faktoren“ erweitert werden.

Darüber hinaus sind erforderlich:

- eine spezifischere Definition der Organisationsstufen, z. B. Mitarbeitergruppen, die ähnliche Kompetenzen im Bereich menschliche Faktoren benötigen,
- eine handlungszentrierte Definition von notwendigen Kompetenzen,
- Ausbilder für Belange zum Thema menschliche Faktoren,
- Evaluationskriterien für Trainingsprogramme

- Aus der Diskussion dieses Themas in dieser thematischen Sitzung gingen abschließend folgende Empfehlungen hervor:
- Industrie und Behörden sollen Anforderungen an die Kompetenzen im Thema menschliche Faktoren ihres Personals definieren. Eine einfache Matrix und die darin postulierten Kompetenzstufen könnten die Basis sein.
- Berücksichtigt man den Lebenszyklus einer Anlage, könnten weitere Spalten erforderlich sein: z. B. Planung, Entwicklung, Konstruktion, Instandhaltung, Lieferanten.
- Der Bedarf, die Stufe und die Methode des Trainings sollte für jede Zelle definiert werden.
- Es sollte Inspektoren geben, die arbeits- und organisationspsychologische Kompetenzen besitzen, um relevante menschliche Faktoren in der Inspektion zu berücksichtigen.

6.4 Thematische Sitzung 4: Zusammenwirken von Bedienern und Schutzsystemen

Das Hauptziel dieser Sitzung war die Identifikation von Operateuraufgaben in Mensch-Maschine-Systemen, vor allem in anormalen Situationen und deren Bewertung für das Design von Schutzsystemen im Hinblick auf die DIN EN-Richtlinien /18, 74, 75, 76/.

Die Norm DIN EN 61511-1 vom Europäischen Komitee für Elektrotechnische Normung „Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie“/18/ ist von großer Bedeutung für verfahrenstechnische Anlagen und den damit in Beziehung stehenden menschlichen Faktoren. Sie wurde als Anwendung der internationalen Norm DIN EN 61508 „ Funktionale Sicherheit – Sicherheitssysteme“ /76/ für die Prozessindustrie entwickelt. Die Norm verfolgt im Wesentlichen zwei Ziele: (1) Schutz der Mitarbeiter und der Umwelt sowie (2) eine Risikobeurteilung und die Definition der Sicherheitsfunktionen. Es existieren zwei systematische Ansätze der Anlagensicherheit die für die Berücksichtigung von menschlichen Faktoren in der Prozessindustrie nützlich sein könnten:

1. Ansatz der Schutzebenen unter Berücksichtigung des Automatisierungsgrades der Sicherheitssysteme
2. Berücksichtigung des Sicherheitslebenszyklus für Sicherheitssysteme

Allgemein kann in Bezug auf Mensch-Maschine Systeme festgehalten werden, dass es nicht in erster Linie um voll automatisierte Systeme geht, aber um Systeme, in denen dem Operateur eine aktive Rolle im Kontroll-, Überwachungs- und Schutzsystem zukommt. Demzufolge ist es wichtig, ein an den Bedürfnissen des Operateurs orientiertes Designkonzept zu verwirklichen. Da-

bei sollte es nicht darum gehen den Menschen zu ersetzen, sondern ihn in seiner Aufgabenerfüllung zu unterstützen.

Bei der Gestaltung von Mensch-Maschine-Systemen wird daher folgende Vorgehensweise vorgeschlagen: (1) eine systematische Aufgabenanalyse, (2) Aufstellung von Listen mit Anforderungen, die von Maschinen beziehungsweise von Menschen besser erfüllt werden können (MABA-MABA-Analyse: men-are-better-at-machines-are-better-at) (3) die Festlegung der Funktionsteilung zwischen Mensch und Maschine, (4) die Beurteilung der Sicherheitsimplikationen (z.B. Festlegung des Sicherheitsintegritätslevels (SIL), die erlaubte Fehlerrate), (4) Festlegung von Bedingungen für eine zuverlässige Leistung der Subsysteme Mensch und Maschine. (Hermann, B & Drahten, H., Relevant characteristics of the human system as determining factors fort he man-machine-interface in process plant /102/)

Cacciabue betont in diesem Zusammenhang die Notwendigkeit von Methoden zur Bestimmung der menschlichen Zuverlässigkeit, als ein Beitrag zur Verbesserung der Mensch-Maschine-Interaktion. Die HERMES (Human error risk management for engineering systems)-Methode liefert eine Struktur für die Auswahl und konsistente Anwendung des Human Factors-Ansatzes in verschiedenen Bereichen. Im Rahmen von HERMES ist es möglich sowohl retrospektiv Unfallursachen zu untersuchen als auch proaktiv Gefahren und Risiken zu bewerten. (Cacciabue, P., Human risk management for engineering systems (Hermes): A methodology for design, safety assessment, accident investigation and training /102/)

In der an die thematische Sitzung anschließende Diskussion wurden folgende Schlussfolgerungen abgeleitet:

- Zur Verbesserung der Mensch-Maschine-Schnittstellen sollte ein umfassendes Prozessmodell angewendet werden. Ein solches Modell sollte die Operateur-Maschine-Interaktion für die Ereignisuntersuchung und für die Gestaltung, für die Schulung und die Sicherheitseinschätzung darstellen.
- Ein Konzept des Mensch-Maschine-Systems sollte entwickelt werden, welches relevante Kernpunkte, z.B. zeitabhängige Leistung, dynamische Umgebung, soziotechnische Umgebung berücksichtigt. Es sollte bedacht werden, dass jedes Modell Vereinfachung erfordert, aber keine relevanten Aspekte verloren gehen.
- Zur Betrachtung von Mensch-Maschine-Schnittstellen sollten die neuen internationalen und nationalen Normenreihen berücksichtigt werden, insbesondere DIN EN 61511-1 /18/, ISA S84 /89/ und VDI 2180-1 /77/.
- DIN EN 61511-1 /18/ fordert eine Risikobeurteilung des Prozesses und der Anlage, bevor ein Sicherheitssystem benutzt wird. Es muss sichergestellt werden, dass alle relevanten Risiken analysiert, die Sicherheitsfunktionen

definiert wurden und die Zuverlässigkeit aller Sicherheitssysteme und Sicherheitsfunktionen zu einem akzeptablen Gesamtrisiko des Prozesses oder der Anlage führt. Freigabekriterien in gesetzlichen Vorschriften müssen in diesem Zusammenhang beachtet werden.

Die Risikoanalyse und die Betrachtung des Operateurs als Teil der Sicherheitsfunktion sollte folgendes enthalten:

- Ausweitung der Analysen und der Sicherheitsanforderungen auf die komplette Sicherheitsanlage: vom Sensor über den Prozessor bis zum Akteur. Es sollen Informationsmodelle verwendet werden, um die Relevanz menschlicher Eigenschaften als Sensor, Prozessor und Akteur für die Mensch-Maschine-Schnittstelle zu erklären.
- Die Bestimmung von Gefahren und Gefahrensituationen in Risikoanalysen. Die DIN EN 61508 /76/ fordert die Berücksichtigung von menschlichen Faktoren in Risikoanalysen. Dabei sollten beispielsweise Handlungen oder Störungen, die Sicherheitsfunktionen auslösen, Fehler, die bei der Reaktion auf Alarme auftreten, und Fehler, die bei der Testung und der Instandhaltung des Systems auftreten und die Effizienz des Schutzes reduzieren, berücksichtigt werden.
- Anforderungen an den Nachweis des resultierenden Risikos auf der Grundlage der Berechnung der Ausfallwahrscheinlichkeit. Dieser Nachweis sollte auf der Grundlage des SIL (Sicherheitsintegritätslevel)-Klassifikationssystems durchgeführt werden. Es sollte besonders beachtet werden, wie die Zuverlässigkeit des Operateurs in der damit in Verbindung stehenden Berechnung der Zuverlässigkeit der Sicherheitsfunktion enthalten ist und welches die maximal benötigte Zuverlässigkeit für menschliche Handlungen bei dieser Sicherheitsfunktion ist.
- Für die Entscheidung, ob automatische Sicherheitssysteme verwendet werden oder der Operateur Teil der Sicherheitsfunktion sein soll, könnte eine Analyse auf der Grundlage der MABA-MABA-Prinzipien helfen, angemessene Entscheidungen zu treffen. Wenn der Operateur ein Teil der Sicherheitsfunktion ist, sollte sichergestellt sein, dass alle diese Systeme zu den menschlichen Fähigkeiten passen.
- Die DIN EN-Normen /18, 74, 75, 76/ fordern klar definierte Vorgehensweisen für die Handlungen des Operateurs und geeignete Schulungen, wenn er Teil der Sicherheitsfunktion ist.
- Es gibt verschiedene Stufen in Sicherheitssystemen, die zum Schutz oder zur Minderung vor Gefahren benutzt werden und der Operateur kann ein Teil der Sicherheitsfunktion sein oder nicht.
- Den Operateur in Verhaltensweisen für Notfallsituationen zu schulen, bedeutet, die Vermeidung von einer Verringerung der Selbstreflexion, eine Reduzierung von systematischen Vorgehensweisen, den Verlust der

Selbstkontrolle (bewusste Verstöße) sowie einem Anstieg von Regelverletzungen und riskanten Verhalten.

Weiterhin wurden folgende Empfehlungen erarbeitet, die für die Aufnahme in die OECD-Leitprinzipien für die Verhinderung, Bereitschaft für den Fall und Bekämpfung von Chemieunfällen vorgeschlagen werden /2/:

- Zuerst müssen Probleme und Ziele, die für den Prozess relevant sind, definiert werden. Beispiele, für zu betrachtende Themen sind:
  - Gestaltungsprobleme
  - Störungsmanagement, z.B. die Behebung von Störungen, denn nicht jede Störung kann verhindert werden.
- Ein Konzept des Mensch-Maschine-Systems sollte entwickelt werden, welches relevante Kernpunkte, z.B. zeitabhängige Leistung, dynamische Umgebung, soziotechnische Umgebung berücksichtigt. Es sollte bedacht werden, dass jedes Modell Vereinfachung erfordert, aber keine relevanten Aspekte verloren gehen.
- Um die Schulung, die Gestaltung und die Bewertung der Sicherheit zu verbessern, sind geeignete Modelle und Taxonomien der Mensch-Mensch-Maschine-Schnittstellen auszuwählen. Konsistente und eine adäquate Einbeziehung von praktischen Erfahrungen, von organisatorischen Faktoren, und kognitiven Aspekten des menschlichen Verhaltens sollten in das Modell der Mensch-Maschine-Schnittstellen eingeschlossen werden.
- Prospektive und retrospektive Analysen, die verschiedene Methoden wie Kausalanalysen, Aufgabenanalysen, ethnografische Analysen, Ereignisanalysen sollten für das System- und Schnittstellenverständnis durchgeführt werden. Dabei ist es wichtig, dass sich die Analysen auf gemeinsame integrierte Modellen und Daten der Mensch-Maschine-Interaktion stützen.
- Diese Methoden und Techniken sollten in einer integrierten Methodologie für spezifische Probleme wie die Gestaltung, Schulung, Sicherheitsbewertung, Unfalluntersuchung etc. anwendbar sein.
- Zur Betrachtung von Mensch-Maschine-Schnittstellen sollten die neuen internationalen und nationalen Normenreihen berücksichtigt werden, insbesondere DIN EN 61511 /18/, ISA S84 /89/ und VDI 2180 /77/.
- Die Messung der Sicherheitsstufen und die Analyse der Sicherheitskulturen mittels Fragebögen und Interviews sollten die Grundlage sein, um den letztendlichen Verbesserungsgrad, der eingeführt werden soll, zu definieren.
- DIN EN 61511 /18/ fordert eine Risikobeurteilung des Prozesses und der Anlage bevor ein Sicherheitssystem benutzt wird. Es muss sichergestellt werden, dass alle relevanten Risiken analysiert, die Sicherheitsfunktionen definiert wurden und dass die Zuverlässigkeit aller Sicherheitssysteme und -funktionen zu einem akzeptablen Gesamtrisiko des Prozesses oder der

Anlage führt. Freigabekriterien in gesetzlichen Vorschriften müssen in diesem Zusammenhang beachtet werden.

- Es gibt verschiedene Stufen in Sicherheitssystemen, die zum Schutz oder zur Minderung vor Gefahren benutzt werden und der Operateur kann ein Teil der Sicherheitsfunktion sein oder nicht.
- Die Risikoanalyse und die Betrachtung des Operateurs als Teil der Sicherheitsfunktion sollte folgendes enthalten:
  - Ausweitung der Analysen und der Sicherheitsanforderungen auf die komplette Sicherheitsanlage: vom Sensor über den Prozessor bis zum Akteur. Es sollen Informationsmodelle verwendet werden, um die Relevanz menschlicher Eigenschaften als Sensor, Prozessor und Akteur für die Mensch-Maschine-Schnittstelle zu erklären.
  - Die Bestimmung von Gefahren und Gefahrensituationen in Risikoanalysen. Die DIN EN 61508 /76/ fordert die Berücksichtigung von menschlichen Faktoren in Risikoanalysen. Dabei sollten beispielsweise Handlungen oder Störungen, die Sicherheitsfunktionen auslösen, Fehler, die bei der Reaktion auf Alarme auftreten, und Fehler, die beim Test und der Instandhaltung des Systems auftreten und die Effizienz des Schutzes reduzieren, berücksichtigt werden.
  - Anforderungen an den Nachweis des resultierenden Risikos auf der Grundlage der Berechnung der Ausfallwahrscheinlichkeit. Dieser Nachweis sollte auf der Grundlage des SIL (Sicherheitsintegritätslevel)-Klassifikationssystems durchgeführt werden. Es sollte besonders beachtet werden, wie die Zuverlässigkeit des Operateurs in der damit in Verbindung stehenden Berechnung der Zuverlässigkeit der Sicherheitsfunktion enthalten ist und welches die maximal benötigte Zuverlässigkeit für menschliche Handlungen bei dieser Sicherheitsfunktion ist.
- Für die Entscheidung, ob automatische Sicherheitssysteme verwendet werden oder der Operateur Teil der Sicherheitsfunktion sein soll, könnte eine Analyse auf der Grundlage der MABA-MABA-Prinzipien helfen, angemessene Entscheidungen zu treffen. Wenn der Operateur ein Teil der Sicherheitsfunktion ist, sollte sichergestellt sein, dass alle diese Systeme zu den menschlichen Fähigkeiten passen.
- Probleme der Belegschaft, die in Notfallsituationen auftreten können, sollten sorgfältig beachtet werden, wie:
  - Reduktion der Selbstreflektion,
  - Reduktion systematischer Vorgehensweisen,
  - Verlust der Selbstkontrolle,
  - Zunahme der (bewussten) Regelverletzungen,
  - Zunahme des riskanten Verhaltens.

- Die Teile des Gesamtprozesses zur Sicherstellung eines annehmbaren Risikoniveaus sollten die Betrachtung menschlicher Faktoren einschließen und folgendes enthalten:
  - eine systematische Aufgabenanalyse,
  - eine Analyse entsprechend der MABA-MABA-Prinzipien,
  - Aufgabenverteilung entsprechend der MABA-MABA-Prinzipien,
  - die Betrachtung spezieller mit dem Menschen in Verbindung stehende Sicherheitsimplikationen,
  - die Betrachtung der Bedingungen für zuverlässige Leistungen, besonders menschlicher Leistungen.

6.5 Thematische Sitzung 5: Menschliche Faktoren im Alarmmanagement

Menschliche Faktoren und damit verbundene Konzepte werden häufig in Verbindung mit dem Sicherheitsmanagement in Prozessindustrien verwendet. Die zunehmende Informationsdichte durch immer mehr Daten aus dem Prozess und komplexere Systeme stellen neue Anforderungen an die Informationsdarstellung für den Operator. Das Ziel dieser Sitzung war es, zu beschreiben, wie menschliche Faktoren bei der Planung neuer Alarmsysteme einbezogen werden sollten und welche Wege für die Evaluation und Verbesserung bestehender Alarmsysteme existieren. Darüber hinaus sollten Empfehlungen für die hinreichende Unterstützung von Operateuren hinsichtlich Alarmflut, -unterdrückung und -priorisierung gegeben werden.

Die Erfahrung im Bereich Alarmmanagement zeigt, dass oft keine, verspätete oder falsche Reaktionen des Operators auf eingehende Alarme aus dem Prozess erfolgen. Ein risikoadäquates Alarmmanagement kann dem Operateur beim Eingreifen in das System unterstützen. Es führt zu einer Verringerung der Arbeitsbelastung durch Alarmreduzierung und Abweichungen des Produktionsprozesses können frühzeitig erkannt werden. Die NAMUR Arbeitsgruppe 2.9 hat sich in Zusammenarbeit mit der Versicherungswirtschaft mit den Anforderungen an ein Alarmmanagement auseinandergesetzt (NAMUR-Arbeitsblatt NA 102 „Alarm Management“ /46/). Das Arbeitsblatt ist ein Leitfaden für Ingenieure und Operateure von verfahrenstechnischen Anlagen für das Design sowie für die Verwendung und die Wartung von Alarmmanagementsystemen. Darüber hinaus werden für die Hersteller leittechnischer Ausrüstung Hinweise zur funktionalen Erweiterung ihrer Produkte gegeben. Die wichtigsten Erfahrungen der NAMUR Arbeitsgruppe in Bezug auf das Alarmmanagement können unter den folgenden Punkten zusammengefasst werden:

- Eine konsequente Durchführung kostet Zeit und Anstrengung, vor allem in neuen Anlagen.
- Der Anlagenführer ist verantwortlich für die Durchführung. Ebenfalls involviert sind der Anlagenmanager, der Vorarbeiter und der Schichtarbeiter.
- Der Operateur begrüßt eine Alarmreduzierung.
- Das Sicherheitssystem sollte auch ohne Operateureingriff reagieren.
- Sicherheitskritische Alarme haben eine hohe Priorität, obwohl ein Eingriff seitens des Operateurs nicht mehr möglich ist.
- Die Anzahl der Alarme ist abhängig von der Produktionsauslastung.
- Systeminformationen beanspruchen den Operateur. In den meisten Fällen gibt es keine Alarmpriorisierung.
- Alarmmanagement ist ein kontinuierlicher Verbesserungsprozess.

Die Kernaussagen der NA 102 /46/ sind:

- Ein Alarm ist eine Meldung über eine Abweichung der normalen Bedingungen des Prozesses, welche eine unverzügliche Reaktion des Operateurs erfordert.
- Alarme und Meldungen sind Informationsquellen über den Prozess und den Anlagenstatus.
- Die Umsetzung einer Alarmreduktion ist: Alarmunterdrückung, Alarmgruppierung, Filterung bei Alarmgenerierung.
- Die Alarmfrequenz sollte nicht mehr als ein Alarm in 10 Minuten pro Operator im Normalbetrieb betragen (vgl. EEMUA 191 /93/).

(Drahten, H., Alarm management in process industries: aims, experiences, benefits, /102/)

Die gegenwärtig beste Praxis im Hinblick auf Alarmmanagement ist in einem Leitfaden der EEMUA 191: 1999 /93/ beschrieben. Kernanliegen der EEMUA 191 ist es, das Alarmsystem zu einem möglichst hilfreichen Werkzeug für Anlagenfahrer zu machen. Da die menschliche Aufnahmefähigkeit für Informationen beschränkt ist, muss sichergestellt werden, dass sich die Alarmrate einer Anlage in zumutbaren Bereichen bewegt. Die EEMUA 191 /93/ nennt messbare Indikatoren als grobe Richtwerte zur Beurteilung der Leistung eines Alarmsystems, wie die durchschnittliche Alarmrate während Normalbetrieb (maximal 1 Alarm alle 10 Minuten) und Alarme in den ersten 10 Minuten nach einer Störung (weniger als 10). Darüber hinaus sollten Leistungsindikatoren wie beispielsweise die Anzahl und Dauer von ständig auftretenden oder zurückgestellten Alarmen (standing alarms and shelved alarms) und der Nutzen von Alarmen überprüft werden. Das in EEMUA 191 /93/ beschriebene Konzept der Alarmanalyse und -reduzierung erlaubt es bei vielen Anlagen, die Qualität des Alarmsystems mit wenig Aufwand erheblich zu verbessern. Um aber das Prob-

lem der Alarmflut bei Prozessstörungen in den Griff zu bekommen, sind weitere (und häufig komplexe) Maßnahmen erforderlich. So müssen kausale Beziehungen zwischen Alarmen analysiert und Alarme vom aktuellen Zustand der Anlage abhängig gemacht werden. Typische Effekte eines schlechten Alarmmanagements sind: verminderte Wachsamkeit und Vertrauen, gesenktes Situationsbewusstsein, Überlastung des Kurzzeitgedächtnisses des Operators, störende Alarme.

Für jede Anlage sollte es ein schriftlich dokumentiertes Alarmkonzept geben, in dem beschrieben ist, was wann wie alarmiert wird. Das Dokument sollte eine Zuordnungsvorschrift für Alarmprioritäten enthalten, definierte Operateurhandlungen auf Alarme und eine Liste mit Leistungsindikatoren zur Beurteilung des Alarmsystems. Des Weiteren werden Auditprogramme und festgelegte verantwortliche Personen für das Alarmmanagement vorgeschlagen. (Hollender, M., Alarms for operators, /102/)

Es existieren zwei grundsätzliche Probleme im Zusammenhang mit einer starken Zunahme von Alarmen im Kontrollraum: Zum einen kommt es vor allem bei Prozessstörungen häufig zu einer Alarmflut, da eine Ursache eine Vielzahl von kausal miteinander verbundenen Alarmen auslösen kann. Zum anderen kommt es unter normalen Betriebsbedingungen oft zu einer Anhäufung von ständig auftretenden Alarmen. Es besteht die Gefahr, dass die Anlagenfahrer, die in solchen Situationen oft unter großem Stress stehen, überfordert werden und nicht mehr qualifiziert reagieren können. Folglich ist es entscheidend, dem Operateur auch in solchen Situationen zu ermöglichen, seine Arbeitsaufgabe gewissenhaft auszuführen. Dabei spielt die Gestaltung der Mensch-Maschine-Schnittstelle eine entscheidende Rolle. Dafür scheint es wichtig zu sein, Alarmanlagen so zu entwerfen, dass selbst ungeschulte Operateure damit umgehen können. Alarmsysteme sollten so ausgelegt werden, dass bekannte Vorfälle nicht wiederholt werden und dass unbekannte Situationen frühzeitig erkannt werden. Auf diese Art sollten Alarme und Operateureingriffe entsprechend dem zugrunde liegenden unerwünschten Ereignis funktionell bleiben. (Windhorst, J., Alarm management practices in NOVA Chemicals, /102/)

Ein weiteres kontinuierlich auftretendes Problem für Operateure sind anormale Situationen. Eine anormale Situation ist eine Störung oder Serie von Störungen in einem Prozess, die bewirken, dass Anlagenvorgänge von ihrem normalen Betriebszustand abweichen. Es ist die Aufgabe des Betriebsteams, die Ursache für die Situation zu identifizieren und fehlerbehebende Handlungen rechtzeitig und effizient auszuführen. Anormale Situationen nehmen in Abhängigkeit der Komplexität und Dynamik des Prozesses stetig zu, entwickeln sich weiter, verändern sich mit der Zeit und erhöhen damit die Komplexität der Eingriffserfordernisse seitens der Operateure. Die Kosten von anormalen Situationen zu reduzieren, wird für die nächsten Jahre eine Schlüsselherausforderung für viele

Unternehmen werden. Dies erfordert einen mehrdimensionalen Ansatz: Angefangen von einer entsprechenden Managementpolitik über die Kontrolle von Systemeigenschaften und einen breiten Bereich von technologischen Verbesserungen bis hin zur Sicherung der Integration von Geschäftsinformation. (Pandit, P. V., Deploying best practice in managing abnormal situations: Experience from ASM Consortium, /102/)

Aufgrund der intensiven Diskussion in dieser Sitzung, konnten folgende Schlussfolgerungen für die Alarmgestaltung angeleitet werden:

- Gegenwärtig existieren in der Prozessindustrie häufig hohe Alarmraten. Neue intelligente Bauteile sind in der Lage mehr Informationen zur Verfügung zu stellen und führen häufig zu einer Alarmüberlastung.
- Laut Studien in der verfahrenstechnischen Industrie werden über 40% der Ursachen von Störungen menschlichen Faktoren und ungefähr 40% Geräteausfällen zugeschrieben. Jedoch zeigen neue Angaben, dass der menschliche Fehler den höchsten Beitrag zur wirtschaftlichen Bedeutung liefert. Eine Firma schätzt, dass menschliche Fehler mehr als 90% des ökonomischen Verlustes bei Störungen verursachen. So ist die Ausrichtung der Aufmerksamkeit auf menschliche Faktoren auch ökonomisch sinnvoll.
- Ein schlechtes Alarmsystem führt zu verringerter Wachsamkeit und Vertrauen, zu einem herabgesetzten Situationsbewusstsein, zur Überlastung des Kurzzeitgedächtnisses des Operateurs, zur Ablenkung oder Verärgerung.
- Das Ziel des Alarmmanagements ist die Reduzierung der Alarme. Alarmmanagement ist ein kontinuierlicher Verbesserungsprozess
- Die Untersuchung von Alarmen hat gezeigt, dass sehr wenige Alarme zu einer beträchtlichen Anzahl von Alarmsignalen führen können. Eine Verbesserung der Systeme, die diese Alarme verursachen, kann zu einer bedeutsamen Verringerung der Alarmraten führen.
- Ein Alarm ist ein Signal über eine Abweichung der normalen Bedingungen des Prozesses, welche eine unverzügliche Reaktion des Operateurs erfordert. Andere Signale sind Meldungen und keine Alarme. Es sollte darauf geachtet werden, dass Alarme und Meldungen den Operateur nicht überfordern, Alarmprioritäten sind sehr wichtig und der Operateur muss erkennen, dass Alarme eine unverzügliche Reaktion erfordern. Der Zweck eines Alarmsystems ist es, die Aufmerksamkeit des Operateurs auf die Bedingungen der Anlage zu richten, die eine unverzügliche Reaktion oder Handlung erfordern. Jeder Alarm sollte warnen, darstellen und leiten. Jeder Alarm der den Operateur präsentiert wird, sollte nützlich und relevant für ihn sein. Jeder Alarm sollte einen definierten Bedienereingriff haben

und dem Operateur eine angemessene Zeitspanne zur Handlungsausführung gewährleisten.

- Das Wissen der Menschen ist immer begrenzt. Das Alarmmanagement muss auf das Wissen der Belegschaft ausgerichtet sein. Anderer Prioritäten z.B. Kostenreduzierung kann das menschliche Wissen weiter verschlechtern; dieses kann zu überraschenden Fehlern führen z.B. aufgrund der Alterung der Anlage und wegen der Alterung und Verrentung der Belegschaft.
- Gutes Alarmmanagement bereitet durch Störungsentdeckung, Rationalisierung von Problemen und Ursachen sowie der Implementierung von Gegenmaßnahmen, die den Prozess in einen normalen oder sicheren Zustand zurückbringen, auf das Unbekannte vor.
- Schlechtes Alarmmanagement führt zu einer Verschiebung von Bekanntem zu Unbekanntem, zur Verminderung der Fähigkeit, die Wiederholung von bekannten Fällen zu vermeiden, zum Verlust der Robustheit mit Unbekanntem umzugehen; Hauptbeschäftigung der Belegschaft ist z.B. die Alarmflut.
- Aktuelle Beispiele guter Praxis für das Alarmmanagement sind in der EEMUA 191 /93/ zusammengetragen, müssen aber an die DIN EN 61511-1 /18/ (englische Version von 2003) angepasst werden.
- Die Vorteile des Alarmmanagements sind:
  - Abweichungen des Produktionsprozesses können früher erkannt werden, so dass zeitnah einem Trend entgegen gewirkt werden kann und Produktions- oder Qualitätsverluste und das ungeplante Abfahren der Anlage vermieden oder reduziert werden kann.
  - Eine signifikante Reduzierung der Arbeitsbelastung, so dass mehr Zeit für das Prozessmanagement zur Verfügung steht, was zu Qualitäts- und Zuverlässigkeitsverbesserungen führt.
- Das mittlere Management erkennt die Notwendigkeit eines Alarmmanagements, aber benötigt Unterstützung von der obersten Managementebene. Die finanziellen Vorteile müssen dem obersten Management aufgezeigt werden.
- Alarmmanagementsysteme sind notwendig, aber nicht hinreichend, ein holistischer Ansatz ist erforderlich. Erfolgreich ist eine Kombination der Arbeitsprozesse, der Technologie und der Menschen. Vorbeugende Maßnahmen müssen zukünftig über das Alarmmanagement alleine hinausgehen und Methoden und Verfahren einschließen.

Folgende Empfehlungen sind im Hinblick auf menschliche Faktoren im Alarmmanagement abgestimmt worden:

- Jede Anlage mit hohem Gefährdungspotenzial sollte eine definierte Alarmmanagementstrategie, einen Leitfaden für Alarmdesign, eine Liste von Schlüsselindikatoren zur Leistungsbeurteilung, eine verantwortliche Person für das Alarmmanagement und ein Auditprogramm besitzen.
- Neue Alarmsysteme sollten um den Operateur herum gestaltet werden. Die Aufgaben des Operateurs besonders in anormalen Situationen sollten analysiert werden. Es sollte sichergestellt werden, dass ausreichend Ressourcen entsprechend der Operateuraufgaben vor allem in anormalen Situationen vorhanden sind.
- Die Qualität des vorhandenen Alarmmanagementsystems sollte kontinuierlich überwacht, analysiert und verbessert werden. Schlüsselelemente beinhalten: Verbindlichkeit seitens des Managements, ein passendes und adäquates Design, passende Alarmprioritäten, definierte Operateurhandlungen auf Alarme.
- Ein Alarm ist ein Signal über eine Abweichung der normalen Bedingungen des Prozesses, welche eine unverzügliche Reaktion des Operateurs erfordert. Andere Signale sind Meldungen und keine Alarme. Es sollte darauf geachtet werden, dass Alarme und Meldungen den Operateur nicht überfordern, Alarmprioritäten sind sehr wichtig und der Operateur muss erkennen, dass Alarme eine unverzügliche Reaktion erfordern. Der Zweck eines Alarmsystems ist es, die Aufmerksamkeit des Operateurs auf die Bedingungen der Anlage zu richten, die eine unverzügliche Reaktion oder Handlung erfordern. Jeder Alarm sollte warnen, darstellen und leiten. Jeder Alarm der den Operateur präsentiert wird, sollte nützlich und relevant für ihn sein. Jeder Alarm sollte einen definierten Bedienereingriff haben und dem Operateur eine angemessene Zeitspanne zur Handlungsausführung gewährleisten.
- Leistungsindikatoren für ein Alarmmanagement sollten zusammen mit Vergleichswerten entwickelt werden. Alarmraten sollten gemessen werden. Stehende und zurückgestellte Alarme (standing alarms and shelved alarms) sind Leistungsindikatoren, denen zu wenig Aufmerksamkeit geschenkt wird. Der Grad solcher Alarme könnte etwas über die Sicherheitskultur und über die Verträglichkeit ihrer Interaktion aussagen. Die Zweckmäßigkeit von Alarmen für Operateure sollte bewertet werden.
- Aktuelle Beispiele guter Praxis für das Alarmmanagement sind in der EEMUA 191 /93/ zusammengetragen, müssen aber an die DIN EN 61511 /18/ (englische Version von 2003) angepasst werden.

Zusammengefasst kann festgestellt werden, dass der Workshop auf großes Interesse traf. Insgesamt beteiligten sich 160 Teilnehmer aus 32 Ländern an den verschiedenen thematischen Sitzungen. Darunter nahmen Vertreter verschiedener Regierungen, internationaler Organisationen, der Industrie, der Wissenschaft und weiterer fachlich beteiligter Disziplinen teil.

Die Bedeutung des Workshops lässt sich ebenfalls daran erkennen, dass die Ergebnisse in Form eines OECD-Berichtes veröffentlicht werden. Eine besondere Bedeutung kommt den im Workshops entwickelten Schlussfolgerungen und Empfehlungen zu, die nach internationaler Abstimmung Eingang in die OECD Leitprinzipien für die Verhinderung, Bereitschaft für den Fall und Bekämpfung von Chemieunfällen /2/ finden sollen.

6.6 Programm des OECD/CCA-Workshops

Tabelle 9: Workshopprogramm

	Einleitung
D.D	Introduction – Presentation of the discussion document Dr. Babette Fahlbruch (TÜV NORD Systec GmbH & Co Kg, Deutschland)
I.	**Thematische Sitzung I: Arten menschlichen Fehler, Definition von relevanten Begriffen** Chair: Dr. Jochen Uth (Umweltbundesamt (UBA), Deutschland) Rapporteur: Jean-Paul Lacoursiere (Universität von Sherbrooke, Kanada)
I.1	Terms in the context of human factors – Proposed definitions Dr. Babette Fahlbruch (TÜV NORD Systec GmbH & Co Kg, Deutschland)
I.2	Accidents: From human factors to organizational factors Jean-Christophe Le Coze (INERIS, Frankreich)
I.3	Human factors traceability and analysis in MARS Daniele Baranzini (EC, Joint Research Center, Major Accidents Hazards Bureau)
I.4	Review of two Incident databases from the Canadian chemical industry and discussion of human factors related terms/parameters, incident data and opportunities Manuel Marta (NOVA Chemicals Corporation, Kanada)
I.5	The use of storybuilder as an incident analysis tool Joy Oh (Ministerium für Arbeit und Sozialordnung, Niederlande)
II.	**Thematische Sitzung II: Beurteilung von Sicherheitskulturen** Chair: Prof. Dr. Michael Baram (Juristische Universität Boston, USA) Rapporteur: Daniele Baranzini/Maureen Wood (EU, Joint Research Center, Major Accidents Hazards Bureau)
II.1	Challenges and opportunities of assessing safety culture Prof. Dr. Bernhard Wilpert und Dr. Markus Schöbel (Technische Universität Berlin, Deutschland)
II.2	Diagnosis of safety culture: A replication and extension towards assessing “safe” organizational change process Prof. Dr. Gudula Grote (ETH Zürich, Schweiz)
II.3	Safety culture model as basis for improvement P.T.W. Hudson (Universität Leiden, Niederlande)
II.4	The International Safety Rating System „ISRS“ and the „SAMOS“ interview technique Dr. L. Adolph (Det Norske Veritas, Deutschland)
II.5	Improving occupational safety in the Netherlands P. van Wissen (Ministerium für Arbeit und Sozialordnung, Niederlande)

III.	**Thematische Sitzung III: Kompetenz im Thema „Menschliche Faktoren“** Chair: Lee Allford (EPSC Manager Operations, UK) Rapporteur: Oliver Raupach (TÜV NORD Systec GmbH & Co Kg, Deutschland)
III.1	What they should have known: Human factors competencies at different organizational levels Dr. Günter Horn (Ingenieurbüro Horn, Deutschland)
III.2	Inspecting for human factors within the German Major Hazards Ordinance: Examples, experience and future needs Bruno Reddehase (Stattliche Arbeitsaufsichtsbehörde Hannover, Deutschland)
III.3	How to learn human factors competencies at different organizational levels Dr. Gesine Hofinger (Platform Menschen in komplexen Arbeitswelten e.V., Deutschland)
III.4	Human factors related chemical accidents occurred in Korea Seung Kyoo PAK (Amt für Arbeitssicherheit, Korea)
IV.	**Thematische Sitzung IV: Zusammenwirken zwischen Bedienern und Schutzsystemen** Chair: Dr. Christian Jochum (Kommission für Anlagensicherheit (KAS), Deutschland) Rapporteur: Roland Fendler (Umweltbundesamt (UBA), Deutschland)
IV.1	Human error risk management for engineering systems: A methodology for design, safety assessment, accident investigation and training P.C. Cacciabue (EC, Joint Research Center, Major Accident Hazard Bureau)
IV.2	Relevant characteristics of the human system as determining factors for the man-machine-interface in process plants Begoña Hermann (Landesamt für Umwelt, Wasserwirtschaft und Gewerbeaufsicht (LUWG), Deutschland) Dr. Hasso Drahten (Bayer Technischer Service, Deutschland)
V.	**Thematische Sitzung V: Menschliche Faktoren im Alarmmanagement** Chair: Dr. Günter Horn (Ingenieurbüro Horn, Deutschland) Rapporteur: Mark Hailwood (Landesanstalt für Umwelt, Messungen du Naturschutz (LUWG), Deutschland)
V.1	Alarm management in process industries: Aims, experiences, benefits Dr. Hasso Drahten (Bayer Technischer Service, Deutschland)
V.2	Alarms for operators Martin Hollender (ABB Corporate Research, Deutschland)
V.3	Alarm management practices in NOVA Chemicals J. Windhorst (NOVA Chemicals, Kanada)
V.4	Deploying best practice in managing abnormal situations: Experience from the ASM Consortium P.V. Pandit (Honeywell Controls, UK)

7 Gesamtzusammenfassung des Endberichtes

In komplexen Arbeitssystemen wie in Anlagen der verfahrenstechnischen Industrie gewinnt der Faktor Mensch in Bezug auf Management und Tätigkeiten in sicherheitskritischen Anlagen aufgrund der Weiterentwicklung und Veränderungen der Technologien stetig an Bedeutung. Da mögliche beeinflussende Faktoren in komplexen Systemen bisher zwar vielfältig, aber weitgehend unsystematisch betrachtet werden, erschien es notwendig, den Einfluss von menschlichen und organisationalen Faktoren in spezifischen Bereichen detailliert zu bilanzieren und auf dieser Grundlage weiteren Forschung- und Umsetzungsbedarf in den betrachteten Themenfeldern zu ermitteln und wenn möglich, Empfehlungen für die Weiterentwicklung zu formulieren.

Für das Themenfeld **„Arten menschlicher Fehler, Definitionen relevanter Begriffe“** kann insgesamt festgehalten werden, dass es eine Vielzahl von Definitionen von menschlichen und organisationalen Faktoren gibt. Diese unterscheiden sich in Bezug auf ihren Inhalt, ihren Umfang, ihren Detailliertheitsgrad und ihr zugrunde liegendes Verständnis. Ähnlich unübersichtlich verhält es sich bei Definitionen zu menschlichen Fehlern, so beziehen sich einige auf Handlungsfehler des ausführenden Personals, andere beziehen Entscheidungsfehler beispielsweise des Managements mit ein. Auch die Abgrenzung zwischen den beiden Begriffen variiert stark und ist nicht in jedem Fall eindeutig möglich. Die Erstellung einer Systematik erscheint deshalb sehr schwierig und könnte nur mit Hilfe eines allgemein akzeptierten Taxonomiemodells, das sowohl menschliche als auch organisationale Faktoren umfasst, gelingen. Ein solches Modell sollte von den Institutionen entwickelt werden, die für die jeweiligen Ereignisdatenbanken zuständig sind. Für eine Analyse von Ereignissen und deren Dokumentation sind jedoch ein anwendbares Modell und eine praktikable Klassifikation gerade im Sinn der Vergleichbarkeit von Ergebnissen und der Übertragung von Erfahrungen unerlässlich, so dass für diesen Bereich dringender Handlungsbedarf gesehen wird.

Wünschenswert wäre es, wenn die verschiedenen Institutionen sich auf ein gemeinsames Taxonomiemodell, das zwischen individuellen und organisationalen Faktoren unterscheidet, verständigen könnten. Denn bisher sind die unterschiedlichen Angaben über Ursachen im menschlichen Bereich häufig auf Unterschiede in der Ursachenklassifikation und der Untersuchungstiefe zurückzuführen.

In Bezug auf das Themenfeld **„Bewertung von Sicherheitskulturen“** ist zunächst festzustellen, dass die Sicherheitskultur als ein holistisches und ganzheitliches Konzept betrachtet wird, das nicht nur das Verhalten der Mitglieder einer Organisation selbst, sondern aller Mitglieder eines System im weiteren Sinne einschließt, wie beispielsweise einzelne Organisationsmitglieder, Arbeits-

gruppen, die Organisation mit ihren Eigenschaften und Einheiten und besondere Organisationsumwelten, z. B. Aufsichtbehörden sowie Technologien.

Zur Beschreibung und Bewertung von Sicherheitskulturen sind die Identifizierung und die Festlegung von relevanten Schlüsselelementen notwendig. Die Analyse verschiedener Quellen hinsichtlich der Gemeinsamkeiten und Unterschiede in den verwendeten Elementen bzw. Komponenten der Sicherheitskulturen ergab insgesamt 23 Schlüsselelemente.

Das Konzept der Sicherheitskultur ist in verschiedenen Industriebereichen eingeführt und wird als wichtiges Werkzeug zur Verbesserung der Sicherheit in der Prozessindustrie gefördert. Trotz der Verfügbarkeit unterschiedlicher Instrumente zur Bewertung von Sicherheitskultur, bleibt festzuhalten, dass diese nicht alle Ebenen erheben. Die in der Literatur genannten Indikatoren erheben nur Einstellungen und Verhalten und ausgesprochene Werte (espoused values), mit Ihnen wird also eher Sicherheitsklima als Sicherheitskultur erhoben. Indikatoren für zugrundeliegende Normen, Werte und Grundannahmen existieren bislang nicht. Außerdem gibt es für die verfahrentechnische Industrie bislang kein validiertes Instrument zur Bewertung der Sicherheitskultur.

Des Weiteren gibt es keinen Konsens darüber, welche Gruppen bzw. Strukturen die Bewertung umfassen soll, nur den Operateur, Manager, Top-Management oder auch Gruppen außerhalb der Organisation, wie Aufsichtsbehörden und Gesetzgeber (Regelsetzer).

Übereinstimmung hingegen herrscht in der Fachliteratur dahingehend, dass Sicherheitskulturbewertungen regelmäßig wiederholt und zusätzlich nach bedeutsamen Änderungen durchgeführt werden sollten.

Zukünftige Forschungsaktivitäten sollten auf die Methoden- und Verfahrensentwicklung konzentriert werden. Zunächst sollte ein Leitfaden zur Selbstbewertung der Sicherheitskultur für die verfahrenstechnische Industrie in Deutschland entwickelt werden. Dieser Leitfaden sollte sowohl Hinweise für die einzubeziehenden Gruppen, Ebenen und Inhalte als auch über die Erhebung (wie Wiederholungshäufigkeit) und Analyse (wie quantitativ vs. qualitativ oder Geltungsbereich) enthalten. In einem zweiten Schritt sollten die Anwendung und die Umsetzung des Leitfadens in der Praxis anhand von ausgewählten Betrieben überprüft und gegebenenfalls Anpassungen vorgenommen werden.

Für die Beurteilung der Sicherheitskultur ist jedoch ein eher holistischer Ansatz erforderlich, das heißt, Fragebögen sollten zusätzlich durch Beobachtungen, Dokumentanalysen, Interviews oder Gruppenfeedback-Analysen ergänzt werden. Bei einer Überprüfung des oben vorgeschlagenen Leitfadens in ausgewählten Betrieben sollten Ansätze zur Ergänzung einer Befragung entwickelt werden.

Es herrscht Konsens darüber, dass Sicherheitskultur verschieden weit entwickelt sein kann, wie die unterschiedlichen Stufenmodelle zeigen. Unklar bleibt allerdings, wie geeignete Interventionen aussehen sollen, die zu einer Verbesserung oder Förderung der Sicherheitskultur führen. Hier besteht ebenfalls Forschungs- und Entwicklungsbedarf, um zu klären, wie die unterschiedlichen Mitarbeitergruppen am besten in den Veränderungsprozess eingebunden werden sollten und wie eine nachhaltige Verbesserung zu erreichen ist.

Die systematische Aufbereitung der Erkenntnisse zu **„Kompetenz im Thema menschliche und organisationale Faktoren“** gestaltete sich schwierig, da kaum Quellen für die verfahrenstechnische Industrie selbst zur Verfügung standen. Dies kann als Hinweis auf verstärkten Forschungs- und Umsetzungsbedarf gewertet werden.

In der verfahrenstechnischen Industrie wurden als relevant in Bezug auf Kompetenzen im Thema menschliche und organisationale Faktoren folgende Gruppen identifiziert: Regelsetzer, Aufsicht, operationales Management, strategisches Management, Sicherheitspersonal/Sachverständige und Operateure.

Aus der Betrachtung von relevanten Kompetenzfeldern für die Luftfahrt /70/ und für die Kerntechnik /71/ ist erkennbar, dass bereits umfangreiche Inhalte zum Thema menschliche und organisationale Faktoren in Trainingsmodulen vermittelt werden. Für die verfahrenstechnische Industrie sind die dort behandelten Themenfelder (generelle Aspekte, menschliche Leistung und Einschränkung, Sozialpsychologie, leistungsbeeinflussende Faktoren, physikalische Umgebung, Aufgaben, Kommunikation, menschlicher Fehler, und Gefahren am Arbeitsplatz) ebenfalls zu vermitteln, sollten jedoch um die Themen Ergonomie, Krisen- und Human Ressource Management ergänzt werden.

Entsprechend der Empfehlungen des OECD/CCA-Workshops wird vorgeschlagen, die obenstehenden Ergebnisse mittels eines Leitfadens zu präzisieren und zu implementieren.

Im ersten Schritt sollten in diesem Leitfaden die Kompetenzfelder, relevanten Gruppen und jeweils geforderten Kompetenzanforderungen genauer definiert werden.

Da es jedoch nicht nur um die Frage geht, wer welche Kompetenzen benötigt, sondern auch, wie diese erworben werden können, sollte in einem zweiten Schritt im Leitfaden die gruppenspezifischen Kompetenzfelder mit Lernzielen, Ausbildungsinhalten und adäquaten didaktischen Methoden beschrieben werden.

In der Luftfahrt ist der Nachweis der Vermittlung von Kompetenzen im Thema menschliche und organisationale Faktoren eine Anforderung des Regelwerkes. Für die verfahrenstechnische Industrie sollte daher diskutiert werden, inwieweit

eine entsprechende Kompetenzvermittlung als ein Teil der Ausbildung einzuführen bzw. ein entsprechender Kompetenznachweis zu fordern ist.

Auf der Basis der durchgeführten Literaturanalysen zum Forschungsstand der **Schnittstellengestaltung zwischen Bedienern und Schutzsystemen** wird deutlich, dass es nach wie vor viele ungeklärte Fragen gibt, die einer weitergehenden Beschäftigung bedürfen. Inhaltliche Schwerpunkte liegen auf der Funktionsallokation und den Automatisierungsstrategien im Mensch-Maschine-System, insbesondere in nichtbestimmungsgemäßen Systemzuständen.

So kann als Ergebnis festgehalten werden, dass die Ansätze zur Gestaltung der Mensch-Schutzsystem-Schnittstelle bisher nur die direkten Schnittstellen berücksichtigen und unzureichend auf die Schnittstellen zu anderen Operateuren, zur Organisation oder zur Umgebung eingehen, was besonders in Hinsicht auf nichtbestimmungsgemäße Systemzustände verheerende Konsequenzen haben kann. Auf der Grundlage der durchgeführten Analysen wurden zudem vier relevante Konstellationen der Bediener-Schutzsystem-Interaktion identifiziert wurden, die für eine differenzierte aufgaben- und situationsadäquate Gestaltung unbedingt zu berücksichtigen sind. Die konkrete Ausgestaltung der verschiedenen Strategien muss zukünftig für jede Konstellation einzeln erprobt werden und für den spezifischen Einzelfall angepasst werden. Bei der Erprobung ist eine ausreichend große Stichprobenzahl für die verschiedenen Varianten von Aufgaben, Betriebszuständen und Ereignissen sicherzustellen. Hier besteht sowohl Forschungs- als auch Regulierungsbedarf bezüglich der Festlegung detaillierter Anforderungen an Aufgaben, Training sowie Ausbildung der Operateure im bestimmungsgemäßen aber insbesondere auch für den nicht bestimmungsgemäßen Betrieb, um eine Verbesserung der Sicherheitskultur insgesamt zu erreichen.

Aber selbst bei der Betrachtung der Schnittstelle zwischen Mensch und Schutzsystem stellt sich heraus, dass die Systemgestaltung dort nach wie vor Mängel aufweist, die als sicherheitsrelevant einzuschätzen sind. So sollte die Schnittstellengestaltung konsequent auf die MABA-MABA-Prinzipien ausgerichtet sein, um sowohl die Stärken des Menschen angemessen einzusetzen als auch seine Schwächen, wenn notwendig, kompensieren zu können. Hierzu ist es jedoch zukünftig erforderlich, systematische Aufgabenanalysen durchzuführen, die möglichst viele verschiedene Bedingungen und Situationen berücksichtigen, um eine im Sinne der Systemsicherheit optimierte Aufgabenverteilung zwischen Mensch und Technik vorzunehmen.

Darüber hinaus besteht die Notwendigkeit, ein umfassendes Prozessmodell zu erstellen, das alle relevanten Aspekte, wie beispielsweise Zeitabhängigkeit, unterschiedliche Systemzustände oder dynamische Veränderungen des Systemverhaltens, berücksichtigt und beschreibt, so dass dieses Modell die gemeinsame Grundlage für verschiedene Fragestellungen in den Bereichen

Gestaltung, Schulung, Sicherheitsbewertung und Unfalluntersuchung bilden kann. Dieses ist dann unbedingt in der Praxis auf seine Eignung zu erproben und gegebenenfalls weiter zu modifizieren. Dazu ist die konsistente und stimmige Einbeziehung praktischer Erfahrungen, organisatorischen Faktoren sowie kognitiven Aspekte des menschlichen Verhaltens insbesondere für Störfallsituationen unerlässlich.

Ein weiteres Problem bzgl. der Mensch-Maschine-Schnittstelle besteht in der Auswahl und Festlegung geeigneter Modelle, Taxonomien und Analysemethoden. Deshalb erscheint es auch hier sinnvoll, verschiedene Methoden und Instrumente, wie beispielsweise prospektive und retrospektive Analysen, miteinander zu kombinieren, wenn sichergestellt werden kann, dass ihnen eine gemeinsame Modellvorstellung und Datenbasis der Mensch-Maschine-Interaktion zugrunde liegt, um ein umfassendes System- und Schnittstellenverständnis zu erreichen. Diese Methoden und Techniken sollten in einer integrierten Methodologie für spezifische Probleme wie die Gestaltung, Schulung, Sicherheitsbewertung, Unfalluntersuchung etc. anwendbar sein.

Außerdem erscheint es notwendig, Regeln für Notfälle aufzustellen und die Operateure für Notfälle systematisch zu schulen.

Bezüglich des Themenfeldes **„menschliche und organisationale Faktoren im Alarmmanagement“** zeigten die Analysen, dass es angesichts weiter steigender Komplexität von Systemen und Prozessen auch zukünftig erforderlich sein wird, die Operateure über mögliche Probleme mit Hilfe eines Melde- und Alarmsystems zu informieren.

Die konsequente Anwendung eines gut durchdachten und gut geplanten Alarmmanagements ist deshalb unerlässlich, um die Anzahl und Häufigkeit von Alarmen und Meldungen zu reduzieren, ohne damit die Sicherheit der Anlage bzw. eine sichere Fahrweise zu gefährden. Es hat sich immer wieder gezeigt, dass ein intelligentes Alarmmanagement dazu führt, dass sich der Operateur besser auf seine wesentliche Aufgabe, nämlich die Prozessführung konzentrieren kann und nicht von „unnötigen Alarmen“, eigentlich richtiger Meldungen, abgelenkt wird. Doch die Frage, wie ein intelligentes Alarmmanagementsystem in der verfahrenstechnischen Industrie aussehen müsste, ist so pauschal weder zu beantworten, noch erscheint sie sinnvoll.

Da die benötigten Komponenten, die in einem erfolgreichen Alarmmanagementsystem realisiert werden sollten, bekannt sind, besteht bezüglich der Alarmgestaltung hauptsächlich Umsetzungsbedarf unter Berücksichtigung spezifischer System- und Situationsbedingungen. Die entwickelten Gestaltungslösungen sollten jedoch grundsätzlich auf ihre Angemessenheit und Eignung für verschiedene Betriebszustände geprüft werden.

Die durchgeführten Analysen zeigen deutlich, dass das Alarmmanagement keine einmalige Aufgabe, sondern ebenfalls ein wichtiger Bestandteil eines kontinuierlichen Verbesserungsprozesses des Gesamtsystems ist. Deshalb muss das Alarmmanagementsystem regelmäßig überprüft und wenn möglich, optimiert werden, um einerseits negative Auswirkungen von Alarmen aufzudecken und andererseits Schwachstellen in der Anlage zu identifizieren. So kann mit der Beseitigung von Schwächen im Alarmsystem und in der Anlage eine deutliche Reduzierung der Alarmmenge erzielt werden. Bezüglich geplanter Veränderungen am Alarmsystem müssen ebenfalls definierte Verfahren, mit denen die vorgeschlagenen Änderungen vollständig analysiert, ihre Folgen abgeschätzt und durchgeführte Änderungen dokumentiert werde, entwickelt und empirisch erprobt werden. Dazu ist es aber dringend notwendig, validierte Evaluationsmethoden für Alarmmanagementsysteme zu entwickeln und die Ergebnisse aus den Evaluationen von Alarmmanagementsystemen entsprechend zu dokumentieren.

Insgesamt kann festgestellt werden, dass es in allen analysierten Themen dieses Projektes mehr oder weniger dringenden Forschungsbedarf bezüglich der verwendeten Konzepte, Modelle, Methoden und Verfahren gibt, der in Zukunft zu bearbeiten sein wird.

Weiterhin konnte bezogen auf die verfahrenstechnische Industrie ein beachtlicher Umsetzungsbedarf vorhandener Erkenntnisse und Empfehlungen insbesondere bei der Mensch-Maschine-Schnittstelle des Alarmmanagements und der Bewertung von Sicherheitskultur ermittelt werden. Zusammengefasst kann festgestellt werden, dass menschliche und organisationale Faktoren in allen behandelten Themengebieten entscheidende Einflussfaktoren darstellen, die zur Erhöhung der Systemsicherheit beitragen können.

8 Literatur

/1/ Working Group on Chemical Accidents (2006). Preparation of a workshop on human factors in chemical accidents and incidents. ENV/JM/ACC(2006)5. Proceeding at the 16th meeting of the working group on chemical accidents, to be held on 19-20 October 2006 in Varese, Italy.

/2/ OECD (2003). Leitprinzipien für die Verhinderung, Bereitschaft für den Fall und Bekämpfung von Chemieunfällen. Verfügbar unter: http://www.oecd.org/dataoecd/35/35/31188928.pdf [01.10.2007].

/3/ OECD (2005). Report of the OECD Workshop on Lessons Learned from Chemical Accidents and Incidents. ENV/JM/MONO(2005)6. Proceedings at the joint meeting of the chemicals committee and the working party on chemicals, pesticides and biotechnology committee to be held on 21-23 Juni 2004, Karlskoga, Sweden.

/4/ OECD/CCA (2007). OECD/CCA-Workshop on human factors in chemical accidents and incidents. Proceedings at the OECD/CCA Workshop to be held on 8-9 May 2007, Potsdam, Germany. Verfügbar unter: http://www.umweltbundesamt.de/anlagen/OECD_Workshop_Proceedings_070605.pdf [01.10.2007].

/5/ Fahlbruch, B. (2007). Zwischenbericht. Einfluss menschlicher Faktoren auf Chemieunfälle. TÜV NORD SysTec GmbH & Co. KG.

/6/ Reason, J. (1997). Managing the risks of organizational accidents. Aldershot: Ashgate.

/7/ Major Accident Hazards Bureau (MAHB). Major Accident Reporting System (MARS). Verfügbar unter: http://mahbsrv.jrc.it/mars/Default.html [01.10.2007].

/8/ Zentrale Melde- und Auswertestelle für Störfälle und Störungen in verfahrenstechnischen Anlagen (ZEMA). Verfügbar unter: http://www.infosis.bam.de/zema/zema_search_fs.php [01.10.2007].

/9/ Chemical Safety and Hazard Investigation Board (CSB). Verfügbar unter: http://www.csb.gov/ [01.10.2007].

/10/ Nuclear Regulatory Commission (NRC). Verfügbar unter: http://www.nrc.gov [01.10.2007].

/11/ HSE (n.d). Core topic 3: Identifying human failures. Verfügbar unter: http://www.hse.gov.uk/humanfactors/comah/core3.pdf [01.10.2007]

/12/ Reason, J. (1995, 13-14 June). Safety management: The concept of latent failures. In J. Reason (Ed.), Safety Management & Latent Failures (pp. 1-11). Manchester.

/13/ Reason, J. (1990). Human error. Cambridge: Cambridge University Press.

/14/ HSE (2005). Inspectors Toolkit: Human factor in the management of major accident hazards. Verfügbar unter: http://213.212.77.20/humanfactors/comah/toolkit.pdf [01.10.2007].

/15/ Health and Safety Executive (1999). HSG48. Reducing error and influencing behaviour. London: HMSO

/16/ ISO/TC 159 (2006). Terminology. Unpublished paper

/17/ VDI 4006-1. Menschliche Zuverlässigkeit - Ergonomische Forderungen und Methoden der Bewertung, November, 2002.

/18/ DIN EN 61511-1. Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware, Mai 2005.

/19/ van Vuuren, W. (1998). Organisational failure: An explonatory study in the steel industry and the medical domain (pp. 1-149). Eindhoven: Eindhoven University of Technology - Proefschrift 1998.

/20/ HSE (n.d.). Humans and risk. HSE Human Factors Briefing Note No. 3. Verfügbar unter: http://www.hse.gov.uk/humanfactors/comah/03humansrisk.pdf [01.10.2007]

/21/ Hollnagel, E. (2005). The Elusiveness of “Human Error”. Verfügbar unter: http://www.ida.liu.se/~eriho/HumanError_M.htm [01.10.2007].

/22/ Amalberti, R. (2001). The Paradoxes of almost totally safe transportation systems. Safety Science, 37, 109- 126.

/23/ Lourens, P. F. (1989). Error analysis and application in transportation systems. Accident Analysis & Prevention, 21(5), 419-426.

/24/ Leplat, J. (1986). Human errors in new technologies: Methods of analysis. In H. Raum & W. Hacker (Eds.), Optimierung geistiger Arbeitstätigkeiten. Referate des V. Dresdner Symposiums zur Arbeits- und Ingenieurspsychologie.

/25/ Rasmussen, J. (1980). What can be learned from human error reports? In K. D. Duncan, M. M. Gruneberg, & D. Walls (Eds.), Changes in Working Life (pp. 97-113). Chichester: Wiley.

/26/ Rauterberg, M. (1996). Why and What can we learn from human errors? In A. F. Özok & G. Salvendy (Eds.), Advances in Applied Ergonomics.

Proceedings of the 1st International Conference on Applied Psychology, ICAE '96, Istanbul, May 21.24, 1996 (pp. 827-830). Istanbul, West Lafayette: USA Publishing.

/27/ Duffey, R. B. & Saull, J. W. (2003). Errors in Technological Systems. Human factors and Ergonomics in Manufacturing, 13(4), 279-291.

/28/ Zapf, D., Brodbeck, F. C., Frese, M., Peters, H., & Prümper, J. (1992). Errors in working with office computers: A first validation of a taxonomy for observed errors in a field setting. International Journal of Human-Computer Interaction, 4(4), 311-339.

/29/ Shaban, R. Z., Wyatt Smith, C.M., Joy Cumming, J. (2004). Uncertainty, Error and Risk in Human Clinical Judgement: Introductory Theoretical Frameworks in Paramedic Practice. Journal of Emergency Primary Health Care (JEPHC), 2, Issue 1-2.

/30/ Shappell, S. A., Wiegmann, D.A. (2003). Human Error and General Aviation Accidents: A Comprehensive, Fine- Grained Analyses Using HFACS. Verfügbar unter: http://www.hf.faa.gov/docs/508/docs/gaFY04 HFACSrpt.pdf [01.10.2007].

/31/ Helmreich, R. L. (2000). On error management: lessons from aviation. Verfügbar unter: http://bmj.com/cgi/content/full/320/7237/781#BIBL [07.01.2005].

/32/ Bove, T. (2002). Development and Validition of a Human Error Management Taxonomy in Air Traffic Control. Doctoral Dissertation at University of Roskilde.

/33/ Yemelyanov, A. M. (2004). Toward a System Approach to Human Error Investigation. Proceedings of the Human factors and Ergonomics Society 48th Annual Meeting. Denver, CO: 20- 24 September 2004, pp. 2436-2440.

/34/ Klumb, P. L. (1994). Attention, action, absent-minded aberrations: A behaviour-economic approach. Doctoral Dissertation at Technische Universität Berlin.

/35/ U.S.Department of Labor. Occupational Safety and Health (2007). IX. Definitions and acronyms. Human error. Verfügbar unter: http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=DIRECTIVES&p_id=3589#IX [01.10.2007]

/36/ Singleton, W. T. (1973). Theoretical approaches to human error. Ergonomics, 16(6), 727-737.

/37/ Rasmussen, J. (1993). Perspective on the concept of human error. Paper presented at Society for Technology in Anesthesia Conference “Human Performance and Anasthesia Technology”, New Orleans, February 1993.

/38/ Moore, D. A. (2003). A Simplified Risk- Based Approach For Analyzing Human factors. In Hazards XVII- Process safety- Fulfilling our responsibilities, Symposium Series No. 149 (pp. 537- 548). Rugby, UK: IChemE.

/39/ Abu- Khader, M. M. (2004). Impact Of Human Behaviour On Process Safety Management In Developing Countries. In Proceedings of the Trans ICemE, Part B, Process Safety and Environmental Protection, 82 (B6), 431-437.

/40/ Leplat, J., & Rasmussen, J. (1984). Analysis of human errors in industrial incidents and accidents for improvement of work safety. Accident Analysis & Prevention, 16(2), 77-88.

/41/ ICNPO- Conferenence Report. (1994). First International Conference on HF-Research in Nuclear Power Operations (ICNPO). 31 Oktober bis 2 November, Berlin.

/42/ Singleton, W. T. (1972). Techniques for determining the causes of error. Applied Ergonomics, 3(3), 126-131.

/43/ AHRQ Agency for Healthcare Research and Quality (2007). Glossary. Available under: http://psnet.ahrq.gov/glossary.aspx? [01.10.2007].

/44/ Rasmussen, J. (1987). Approaches to the Control of the Effects of Human Error on chemical plant safety. Roskilde: Riso National Laboratory.

/45/ Groeneweg, J. (1992). Controlling the controllable. The management of safety. Leiden: DSWO Press.

/46/ Namur- Worksheet NA 102. Alarmmanagement. AK 2.9, Dezember 2005.

/47/ HSE (1998). Management of alarm systems. Verfügbar unter: http://www.hse.gov.uk/research/crr_pdf/1998/CRR98166.pdf [01.10.2007]

/48/ Swain, A.D., Guttman H.E. (1983). Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final report. (NUREG/CR-1278). Washington DC: U.S. Nuclear Regulatory Commission.

/49/ Schein, E. H. (1985). Organizational culture and leadership. San Francisco: Jossey-Bass.

/50/ IAEA. (1998). Developing safety culture in nuclear activities. Practical suggestions to assist progress. In Safety Reports Series No.11. Vienna: International Atomic Energy Agency.

/51/ Lardner, R. (2003). Safety Culture Application Guide. PRISM FG1. The Keil Centre.

/52/ HSL Report: Bell, J. & Healey, N. (2006). The causes of major hazard incidents and how to improve risk control and health and safety management: a review of the existing literature. Health & Safety Laboratory. HSL/2006/117.

/53/ HSE (1996). The contribution of attitudinal and management factors to risk in chemical industry. HSE Contract Research Report No. 81/1996. Verfügbar unter: http://www.hse.gov.uk/research/crr_pdf/1996/CRR96081.pdf [01.10.2007].

/54/ Fahlbruch, B. (2000). Vom Unfall zu den Ursachen: Empirische Bewertung von Analyseverfahren. Berlin: Mensch und Buch Verlag.

/55/ Gordon, R., Flin, R. & Mearns, K. (2005). Designing and evaluating a human factors investigation tool (HFIT). Safety Science, 43, 147-171.

/56/ U.S. Coast Guard (2005). DoD HFACS. Department of Defense Human Factors Analysis and Classification System. A mishap investigation and data analysis tool. Verfügbar unter: http://www.uscg.mil/safety/pdf_files /hfacs.pdf [12.10.2007].

/57/ Wilpert, B., & Fahlbruch, B. (2004). Safety culture: Analysis and intervention. In C. Spitzer, U. Schmocker, & V. N. Dang (Eds.), Probabilistic safety assessment and management (Vol. 2, pp. 843-849). London: Springer.

/58/ Olive, C., O'Connor, M. & Mannan, M.S. (2006). Relationship of safety culture and process safety. Journal of Hazardous Materials, 130, 133-140.

/59/ OECD (2003). OECD Guidance on Safety Performance Indicators. Verfügbar unter: http://www.oecd.org/dataoecd/60/39/21568440.pdf [11.01.2007].

/60/ INSAG. (1991). Safety culture. Vienna: International Atomic Energy Agency (Safety Series No. 75-INSAG-4).

/61/ INSAG. (2002). Key practical issues in strengthening safety culture. In INSAG-15. Vienna: International Nuclear Safety Advisory Group.

/62/ Responsible Care (n.d.). Verfügbar unter: http://www.cefic.be/Files/Publications/rcreport2004.pdf [11.01.2007].

/63/ Internationale Länderkommission Kerntechnik (2005). ILK-Stellungnahme zum Umgang der Aufsichtsbehörde mit den von den Betreibern durchgeführten Selbstbewertungen der Sicherheitskultur. atw 2005/5, p.317-322.

/64/ The Keil Centre (2001). Safety Culture maturity model. HSE Offshore Technology Report 2000/049.

/65/ MaTSU. (1999). Summary guide to safety climate tools. In Offshore Technology Report 1999/063. Health and Safety Executive. Available under: http://www.hse.gov.uk/RESEARCH/otopdf/1999/oto99063.pdf [13.04.2007].

/66/ Wilpert, B., Büttner, T., Otto, S., Fahlbruch, B., Schöbel, M., Niehoff, J., & Rieger, M. E. (2003). Selbstbewertung und Förderung von Sicherheitskultur im KKW (Abschlussbericht/Final Report. Reaktorsicherheitsforschung-Vorhaben-Nr.: 1501255). Forschungsstelle Systemsicherheit der Technischen Universität Berlin.

/67/ Hudson (1991). Prevention of accidents involving hazardous substances: The role of the human factor in plant operation. OECD-Workshop Tokyo, 22nd - 26th April 1991.

/68/ Kadri, S.H. & Jones, D.W. (2006). Nuturing a strong process safety culture. Process Safety Progress, 25/1, 16-20.

/69/ U.S. Chemical Safety and Hazard Investigation Board (2007). Investigation report. Refinery explosion and fire. Report No.2005-04-I-TX.

/70/ IAEA. (2001). The operating organization for nuclear power plants: safety guide. Vienna: International Atomic Energy Agency (IAEA).

/71/ Commission Regulation (EC) No 2042/2003 of 20 November 2003 on the continuing airworthiness of aircraft and aeronautical products, parts and appliances, and on the approval of organisations and personnel involved in these tasks (Text with EEA relevance). Official Journal L 315 , 28/11/2003 P. 0001 – 0165.

/72/ Störfall-Verordnung-12.BImSchV (2000). Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes. Verfügbar unter: http://www.gesetze-im-internet.de/bundesrecht/bimschv_12_2000/gesamt.pdf [24.10.2007].

/73/ Richtlinie 96/82/EG des Rates vom 9. Dezember 1996 zur Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen (“Seveso II-Richtlinie“). Verfügbar unter: http://europa.eu.int/comm/environment/seveso/ und http://mahbsrv.jrc.it [25.09.2007].

/74/ DIN EN 61511- 2. Funktionale Sicherheit- Sicherheitstechnische Systeme für die Prozessindustrie- Teil 2: Anwendung zur Anwendung des Teils 1, Mai 2005.

/75/ DIN EN 61511- 3. Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheitsintegritätslevel, Mai 2005.

/76/ DIN EN 61508 (2002). Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 0: Funktionale Sicherheit und die IEC 61508. Frankfurt am Main: Deutsche Kommission Elektrotechnik Elektronik Informationstechnik.

/77/ VDI/VDE 2180- 1. Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (Entwurf), Oktober 2005.

/78/ NE 031. Anlagensicherung mit Mitteln der Prozessleittechnik. AK 4.5, Juli 2006.

/79/ Parasuraman, R. & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. Human factors, 39, 230-253.

/80/ Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A Model for Types and Levels of Human Interaction with Automation. IEEE Transactions on Systems,Man, and Cybernetics, 30(3), 286-297.

/81/ Endsley, M., & Kiris, E. (1995). The out-of-the-loop performance problem and level of control in automation. Human factors, 37(2), 381-394.

/82/ Sheridan, T.B. (2000). Function allocation: algorithm, alchemy or apostasy? International Journal of Human-Computer Studies, 52, 203-216.

/83/ Manzey, D. (2005). Arbeit in Mensch-Maschine Systemen 1-2. Vorlesung an der TU-Berlin. Verfügbar unter: http://www.gp.tu-berlin.de/AOPsychologie/Studium/material/ws0506m/A&O_I_10_1.pdf [11.01.2007].

/84/ Wickens, C. D., & Hollands, J. G. (2000). Engineering psychology and human performance (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

/85/ Endsley, M. (1996). Automation and situation awareness. In: Parasuraman, R. & Mouloua, M. (eds.), Automation and human performance. Theory and applications. Mahwah: Erlbaum.

/86/ Lorenz, B., Di Nocera, F., Röttger, S., & Parasuraman, R. (2002). Automated fault management during simulated space flight. Aviation, Space, and Environmental Medicine, 73, 886-897.

/87/ Hollnagel E., Bye, A. (2000): Principles for Modelling Function Allocation. In International Journal of Human-Computer Studies, 52 (2), p. 253-265.

/88/ SFK (2005). Statusbericht des Arbeitskreises Human Factor.SKK-GS-46. Verfügbar unter: http://www.sfk-taa.de/berichte_reports/ berichte_sfk/sfk_gs_46.pdf [24.10.2007].

/89/ ANSI/ISA S84 (2004). Functional safety: Safety instrumented systems for the process industry sector, called S84 herein.

/90/ IFSN - Interdisziplinäre Forschungsgruppe für soziale Nachhaltigkeit (2002). Projekt: Wissenschaftliche Beteiligung sowie Informationsdarstellung zu dem Vorhaben „Human Factors“, Abschlussbericht. Verfügbar unter: http://www.sfk-taa.de/berichte_reports/andere_ dokumente/abschlussbericht_uni_oldenburg.pdf [Stand: 11.01. 2007].

/91/ HSE (2000). Besserer Umgang mit Alarmen. HSE Informationsblatt Nr. 6. Verfügbar unter: http://www.sfk-taa.de/berichte_reports/andere_ dokumente/hse_umgang%20mit%20alarmen.pdf [21.05.2007].

/92/ HSE (n.d.). Alarm handling. HSE information Sheet- Chemical Sheet No. 9. Verfügbar unter: http://www.hse.gov.uk/humanfactors/comah/ 09alarms.pdf [11.01.2007].

/93/ EEMUA (1999, 2007). Alarm Systems: A Guide to Design, Management and Procedurement. EEMUA Publication No 191. The Engineering Equipment and Materials Users Association: London.

/94/ VDI/VDE 3699- 1. Prozessführung mit Bildschirmen – Begriffe, Mai 2005.

/95/ VDI/VDE 3699- 2. Prozessführung mit Bildschirmen – Grundlagen, Mai 2005.

/96/ IEC 73 (1990). Colours of pushbuttons and their meanings. NY: International Electrotechnical Commission.

/97/ DIN 2403. Kennzeichnung von Rohrleitungen nach dem Durchflussstoff, März 1984.

/98/ Smith, W. H., Howard, C. R., & Foord, A. G. (2003). Alarms Management – Priority, Floods, Tears or Gain?. Verfügbar unter: http://www.4-sightconsulting.co.uk/Current_Papers/Alarms_Management/alarms management.html [13.03.2003].

/99/ Dunn, D. G. & Sands, N. P. (2003). ISA-SP18- Alarm systems Management and design guide. Verfügbar unter: http://www.equistar.com/TechLit/Tech%20Topics/Equistar%20Industry% 20Papers/Alarm_Systems_Management.pdf. [11.01.2007].

/100/ Honeywell (2006). Alarm Management. Verfügbar unter: http://hpsweb.honeywell.com/Cultures/enUS/Products/ControlApplications/AlarmManagement/default.htm [11.01.2007].

/101/ Nimmo, I. (2002). It's time to consider Human factors in Alarm Management. Verfügbar unter: http://www.mycontrolroom.com/sitedata/articles/archive/Human%20Factors%20in%20Alarm%20Management.pdf [11.01.2007].

/102/ UBA (2007). OECD/CCA-Workshop über Menschliche Faktoren in Verbindung mit Chemischen Unfällen und Ereignissen – OECD/CCA Workshop on Human Factors in Chemical Accidents and Incidents. Verfügbar unter: http://www.umweltbundesamt.de/anlagen/oecd-cca-workshop.html [01.10.2007].

/103/ Uth, H.-J. & Wiese, N. (2004). Central collecting and evaluating of major accidents and near-miss-events in the Federal Republic of Germany - results, experiences, perspectives. *Journal of Hazardous Materials*, *111*, 139-145.

/104/ Heuer, I.-G. (2007). Untersuchung psychischer Belastungen am Arbeitsplatz. Eine Inspektionsmethode zu Human Factors in Betriebsbereichen nach der Störfall-Verordnung? Technische Überwachung, 48(10), S.43-48.

9 Anhang I Menschliche Faktoren in Ereignisdatenbanken

9.1 Major Accident Reporting System (MARS)

Tabelle 10: Beschreibung der “Ursache Mensch” in der MARS Datenbank /7/

MARS Database		
Cause Human		
No.	Description	Frequency
1	accidental inversion	1
2	act of negligence	2
3	arson (sabotage action), inadequate safe-guarding	1
4	checking erroneously	1
5	confusion	1
6	control error, failure to control	1
7	defective information system	1
8	defective work permit system	1
9	disregard of the risk	1
10	erroneous manoeuvring	1
11	erroneous mixture	1
12	erroneous operation	1
13	external manipulation	1
14	failure of supervision	1
15	failures were not noticed	1
16	forgotten, human error of omission	2
17	handling error	1
18	hazards underestimated	1
19	human error during repair / maintenance	3
20	inadequate maintenance works	1
21	inadequate operation procedures	2
22	inadequate plant design	3
23	inadequate procedures	1
24	inadequate process analysis	1
25	Inadequate safety education of operators	1
26	inadequate training/instruction	1
27	inappropriate action	1
28	inappropriate design of plant/equipment/system	1
29	incorrect operation	1
30	ineffective control	1
31	instruction wasn’t followed by the operator	1
32	instructions have not been respected	1
33	insufficient maintenance procedures	1
34	insufficient operational procedures	4
35	insufficient testing/inspection procedures	1
36	insufficient training	3

MARS Database		
Cause Human		
No.	Description	Frequency
37	interchange	1
38	lack of coordination	1
39	lack of maintenance	1
40	loose of control	1
41	loss of operational process control	1
42	malicious act	1
43	mistake (of the operator)	4
44	misunderstanding	1
45	not completely degasified	1
46	not fastened	1
47	not informed	1
48	operation against regulations	1
49	operator error	10
50	operator's mistake during demolition of installation	1
51	over-charge	1
52	overfilling	1
53	overpressurization	1
54	procedures were not fully applied	1
55	safety procedures were not suitable	1
56	storage mistakes	1
57	terroristic action (sabotage).	2
58	too long delay in reacting	1
59	untimely (wrongly) opened	1
60	violation of procedures	1
61	wrong connection	1
62	wrong handling / (manipulation)	4
63	wrong inertization	1
64	wrong loading	1
65	wrong manipulation	1
66	wrong mixing operation	1
67	wrong performance of a venting operation	1
68	wrong removal	1
69	wrongly operated	1
70	wrongly set rupture pressure	1
71	wrongly shut	1
72	wrongly supplied	1
	Sum	100

9.2 Nuclear Regulatory Commission (NRC)

Tabelle 11: NRC Kodierungsschema /10/

Categories	Areas	Details
T Training	T1 Initial T2 Continuing/requalification T3 On-the-job training	100 Training LTA 101 Training process problem 102 Individual knowledge LTA
	T4 Simulator training	103 Simulator training LTA
P Procedures and Reference Documents	P1 General operating P2 Abnormal/off normal/alarm condition P3 Emergency (EOPs & ERPs) P4 Reactivity control P5 Maintenance/modification P6 Surveillance/calibration/test P7 Chemical/ radiochemical P8 Refueling P9 Administrative P10 Licensing Documents P11 Special P12 Other	110 No procedure/reference documents 111 Procedure/reference document technical content LTA 112 Procedure/reference document contains human factors deficiencies 113 Procedure/reference document development and maintenance LTA
F Fitness for Duty	F1 Drugs F2 Alcohol F3 Mental/emotional F4 Fatigue F5 Unknown/other	120 Testing LTA 121 Assessment LTA 122 Behavioral observation LTA 123 Self-declaration LTA 124 Training missing/LTA 125 Work hour control 126 Task design/work environment 127 Circadian factors/individual differences 128 Non-compliance 129 Impairment
O Oversight	O1 Oversight and control	130 Inadequate supervision/ command 131 Management expectations or directions LTA

Categories	Areas	Details
R Problem Identification and Resolution	R1 Problem identification	140 Problem not completely or accurately identified 141 Problem not properly classified or prioritized 142 Operating experience (OE) review LTA 143 Tracking/trending LTA 144 Audit/self-assessment/effectiveness review LTA
	R2 Problem evaluation	145 Causal development LTA 146 Evaluation LTA
	R3 Problem resolution	147 Individual corrective action LTA 148 Action not yet started or untimely 149 No action planned
	R4 Corrective action program R5 Safety conscious work environment	150 Programmatic deficiency 151 Willingness to raise concerns LTA 152 Preventing and detecting retaliation LTA
C Communication	C1 Oral C2 Written	160 No communication/information not communicated 161 Communication LTA 162 Communication equipment LTA
H Human-System Interface (HSI) and Environment	H1 HSI components/equipment	170 HSI or availability/quality LTA
	H2 Simulator	171 Simulator fidelity LTA 172 Simulator use LTA
	H3 Physical work environment	173 Physical conditions LTA

Categories	Areas	Details
W Work Planning and Practices	W1 Work planning and coordination	180 Scheduling and planning LTA 181 Inadequate staffing/task allocation 182 Work package quality LTA 183 Pre-job activities LTA 184 Tag outs LTA
	W2 Work practices	185 Procedural adherence LTA 186 Failure to take action/meet requirements 187 Action implementation LTA 188 Work practice or craft skill LTA 189 Recognition of adverse condition/questioning attitude LTA 190 Failure to stop work/non-conservative decision making 191 Team interactions LTA 192 Work untimely 193 Non-conservative action 194 Housekeeping LTA 195 Logkeeping or log review LTA 196 Independent verification/plant tours LTA
	W3 Awareness/ attention	197 Self-check LTA 198 Worker distracted/interrupted

9.3 Berichte des Chemical Safety Board (CSB)

Beispielberichte mit menschlichem Beitrag aus der CSB Unfalldatenbank:

1. **Fire at Formosa Plastics Corporation, Point Comfort, Texas, October 6, 2005**

- A worker driving a fork truck towing a trailer under a pipe rack backed into an opening between two columns to turn around.
- When the worker drove forward, the trailer caught on a valve protruding from a strainer in a propylene piping system.
- The trailer pulled the valve and associated pipe out of the strainer, leaving a 1.9 -inch diameter opening.
- Pressurized liquid propylene (216 psig) rapidly escaped through the opening and partially vaporized creating both a pool of propylene liquid and a rapidly expanding vapor cloud.
- Control room operators saw the vapour cloud on a closed circuit television and began to shut down the unit.
- Outside operators tried unsuccessfully to reach and close manual valves that could stop the release.
- The vapor cloud ignited.
- A large pool fire burned under the pipe rack and the side of an elevated structure that supported a number of vessels, heat exchangers, and relief valves.
- The fire was extinguished about five days after the start of the incident.

2. **Kaltech Industries Group, Inc. Borough of Manhattan, New York April 25, 2002**

A chemical reaction caused an explosion when the [nitric] acid was combined with lacquer thinner from another container.

Root Causes:

- There was no compiled list of hazardous chemicals present in the facility.
- Containers of wastes and certain chemicals onsite were not labeled.
- Employees received no formal training on the hazards of specific chemicals in the workplace.
- Material safety data sheets were unavailable to the workforce.
- Waste materials were mixed without being identified or characterized, and no effort was made to determine compatibility among materials.
- Employees received no formal training on proper hazardous waste management practices.

3. West Pharmaceutical Services Dust Explosion and Fire Kinston, NC, January 29, 2003

Root Causes:

- West Pharmaceutical Services, Inc., did not perform an adequate engineering assessment of the use of powdered zinc stearate and polyethylene as antitack agents in the rubber batchoff process.
- The company's engineering management systems did not ensure that relevant industrial fire safety standards were consulted.
- The company's management systems for reviewing MSDSs did not identify combustible dust hazards.
- The hazard communication program at the Kinston facility did not identify combustible dust hazards or make the workforce aware of such.

10 Anhang II Types of Human Error, Definition of Related Terms

10.1 Human Factors, Definitions of General Terms

Human factors

“Human factors refer to environmental, organisational and job factors, and human and individual characteristics, which influences behaviour at work in a way which can effect health and safety” /14/, p.10 according to /15/.

“The term “human factor” is often used in a negative context (equating it to human error). However, humans are often the only means for effectively responding to abnormal situations since they have the capability to reason, and then to override automatic reactions of machines. Humans have the capacity to forecast action, integrate complex and fuzzy information, and understand how to address unusual situations based on experience and training.” /2/, p.55

“Human factors involve designing machines, operations and work environments so that they match human capabilities, limitations and needs (and, therefore, is broader than concerns related to the man-machine interface). It is based on the study of people in the work environment (operators, managers, maintenance staff, and others) and of factors that generally influence humans in their relationship with the technical installation (including the individual, the organisation and the technology).” /2/, p.180

Human performance

“All aspects of human action relevant to the safe operation of a hazardous installation, in all phases of the installation from conception and design, through operation, maintenance, decommissioning, and shutdown“ /2/, p.180.

10.2 Types of Human Error, Definitions of Related Terms

Error

“Mismatch between the user’s goal and the response of the system. Errors can include navigation errors, syntax errors, conceptual errors, etc” /16/, p. 35.

Human error

“In this regard, it should be recognised that humans will, on occasion, fail and the majority of accidents are in some part attributable to human error, meaning human actions or inactions which unintentionally exploit weaknesses in equipment, procedures, systems and/or organisations” /2/, p. 55.

“Human errors are not limited to operator errors but may occur at different points in the hierarchy of the enterprise including, for example, at the level of those responsible for maintenance, management of change or permit to work systems, or at the level supervisors and management. Examples of human failures, in addition to operator errors, can involve: problems with transmission of knowledge, especially when experienced specialists retire; the complexity of the system, including process design and engineering; the ageing of plants and related repairs, without adequate maintenance and inspection; and the need to cope with changes in organization or technology, including automation.” /2/, p. 134

“Human error / working error / erroneous action / error, i.e. all human actions which exceed defined acceptance limits” /17/, p. 3.

“Human error / mistake: Commission or omission which results in unintended consequence” /18/, p. 18.

Human failure and human error

“A human error is an action or decision which was not intended, which involved a deviation from an accepted standard and which led to an undesirable outcome´. Human failure refers to errors AND violations (i.e. non-compliance with rules or procedures).” /14/, p. 83

Human failure

”refers to errors made by those at the sharp end of incident causation that have directly triggered the incident” /19/, p.9. According to the HSE definition it is /14/ “important to remember that human failures are not random; there are patterns to them […]” p. 83.

There are three different types of human failures (unsafe acts) that may lead to major accidents /14/, p. 11:

1. **Unintentional errors:**

“Errors (slips/lapses) are “actions that were not as planned” (unintended actions). These can occur during a familiar task e.g. omissions like forgetting to do something, which are particularly relevant to repair, maintenance, calibration or testing. These are unlikely to be eliminated by training and need to be designed out. “

2. **Mistakes**

“Mistakes are also errors, but errors of judgement or decision-making (“intended actions are wrong”) - where we do the wrong thing believing it to be right. These can appear in situations where behaviour is based on remembered rules or familiar procedures or unfamiliar situations where decisions are formed from

first principles and lead to misdiagnoses or miscalculations. Training is the key to avoiding mistakes."

3. Intentional errors:

"Violations differ from the above in that they are intentional (but usually well-meaning) failures, such as taking a short-cut or non-compliance with procedures e.g. deliberate deviations from the rules or procedures. They are rarely wilful (e.g. sabotage) and usually result from an intention to get the job done despite the consequences. Violations may be situational, routine, exceptional or malicious."

"A deliberate breach of rules and procedures […] /20/, p. 3"

"An error that occurs when an action is taken which contravenes known operational rules, restrictions and/or procedures. The definition of violations excludes actions taken to intentionally harm the system, i.e., sabotage."/14/, p. 83

In the literature there are various definitions of human errors as the following examples show:

"The fundamental semantic problem is that the term "human error" has at least three different denotations, so that it can mean either the cause of something, the event itself (the action), or the outcome of the action." /21/, p. 1:

"Human error "as cause: "The oil spill was caused by human error". Here the focus is on the action (the "human error") as the alleged cause of the observed outcome (the oil spill).

"Human error "as event or action: "I forgot to check the water level". Here the focus is on the action or process itself, whereas the outcome or the consequence is not considered. […]

„Human error "as consequence: "I made the error of putting salt in the coffee". Here the focus is on the outcome, although the linguistic description is of the action. […] A more serious example is the use of the term "latent human error". This implies, wrongly, that one or more "human errors" are hidden somewhere in the system in the system and that they have yet to manifest themselves. The intended meaning is rather that the system hides one or more latent consequences of a "human error" that already have occurred" /21/, p.1. In industry usually, only errors having non acceptable consequences (i.e. outside the field of safety operations, as defined by procedures, instructions and safety analyses) are labelled 'errors' On the other hand, psychologists define error as an erroneous act, whatever its consequences, or the level at which it is detected and recovered. /22/, S. 112.

"Rasmussen, Duncan, and Leplat (1987) defined human errors as an act that is counterproductive with respect to the person's (private or subjective) intentions or goals. A group of experts at the OECD defined human error as behaviour, or

its effects, which lead a system to exceed acceptable limits (Nicolet, 1987). For Mashour (1974), error is the deviation of actual performance from the desired performance of criterion. Kruglanski and Ajzen (1983) described error as the type of experience a person might have following an encountered inconsistency between a given hypothesis, conclusion, or inference, and a firmly held belief." /23/, p. 420f.

"Human error is a feature of human activity: it describes that type of activity that causes the controlled system to diverge further than the tolerated field of variation […]. Human error is an ambiguous expression that must not lead to a uni-causal conception of error but encourage the search for the multiple determining factors in its production. The goal of the analysis of human error will be to discover these determining factors." /24/, p. 126.

"How are faults and errors defined? Basically they are defined as causes of unfulfilled purposes […] human errors can be compared with intermittent faults in an electronic system. For such faults, you will often stick to the deterministic explanation and look for external causes such as noise interference. " /25/, p. 98f

"If a system performs less satisfactorily than it normally does - because of a human act - the cause will very likely be identified as a human error." /26/, p. 827

"We define an error as the integrated accidental causation of an accident, injury, or death, whether or not there are multiple contributions, systems, error types, or persons involved." /27/, p. 279.

"There are three elements to an action-theory-based definition of an error: (a) errors only appear in goal-oriented action; (b) an error implies non-attainment of a goal; (c) an error should have been potentially avoidable." /28/, p. 313f.

"Defining error as a 'failure of planned actions to achieve their desired goal' […] /29/, p. 4 according to /13/.

"Errors represent the mental or physical activities of individuals that fail to achieve their intended outcome." /30/, p. 1.

"…error can be defined as action or inaction leading to deviation from team or organisational interventions" /31/, p. 781.

"Any action (or inaction) that potentially or actually results in negative system effects given the situation that other possibilities were available. This includes any deviation from operating procedures, good working practice or intentions. There are several benefits of this definition. First, the definition of human error is neural with regard to any question of blame. Second, an error does not need to involve any system consequences. This is in concordance with the principle that an error should be judged on the basis of the underlying processes and not the

product. Third, an action or inaction can only be labelled as an error if another alternative was available. Finally, the definition accepts several different criteria or standards to which the performance can be compared, namely the standards operating procedures, good working practice or simply the actor's intentions." /32/, p. 22

"Human error is considered here as any action or failure to act by a human being in the process of his activity, which violates understood standards or acceptable boundaries of behaviour (Kotik and Yemelyanov, 1985; Miller and Swain, 1986) The notion of error is not necessarily associated with guilt, the consequences of the error or the presence or absence of intention." /33/, p. 2437.

"[…] errors as phenomena which are closely related to the correct execution of the respective action, i.e., the two are regarded as two sides of the same coin (e.g., Reason, 1979; Fromkin, 1980; Wehner & Stadler, in press). As a consequence, and in contrast to other disciplines such as engineering, psychological error research deals with both, the description and causal analysis of errors, with their phenotype and genotype (cf. Becker et al., 1994)." /34/, p. 3.

"[…] any human action that exceeds some limit of acceptability (i.e. an out- of-tolerance action) where the limits of human performance are defined by the system." /35/

"Errors are connected with goals and purposes. An individual is always aiming towards some objective and has not yet got there. As soon as he achieves one objective he turns his attention to another one thereby deliberately perpetuating or recreating a state of error […] error can be defined as a transgression of a rule." /36/, p. 727.

"Errors are, basically, defined as being human acts which are judged by somebody to deviate from some kind of reference act. This reference, however, is not stable but depends on the circumstances of the judgement. […] In consequence, the perception of an act as being an error depends on the identity of the judge and the point in time of judgement. That is the concept of ´human error´ is subjective and varies with time. In addition the definition of error appears to be changing with the nature of the work environment in question." /37/, p. 1

"...departure from acceptable or desirable practice on the part of an individual that can result in unacceptable or undesirable results" /38/, p. 538; /39/, p. 432.

"[…] human errors as instances of man-machine-misfits, i.e., instances when human variability is not within the span acceptable for successful task performance. Variations in performance become human errors only in an ´unkind´ environment which does not allow immediate correction. This means that to characterize human ´errors´, one has to determine the variability of human

behaviour and there acceptance limits for variation which hold for the work situation. Generally, human errors are defined in terms of faulty, external task element and data are collected correspondingly." /40/, p. 82

"[…] any failure in a system may be seen as human error" /45/, p. 10.

To organize these different understandings and perspectives on human error and human factors it is suggested to classify them according to task, action, consequences and organizational aspects:

1. **Task related definitions**

Omission: „failure to act at all", „what is not done", "failing to do the right thing" /23/, p. 419; /42/, p. 126, /43/ according to /13/

Comission: „the correct function at the wrong time", „what is done", doing something wrong" /23/, p. 419; /42/, p. 126, /43/ according to /13/

2. **Action related definitions**

Terms: slips, lapses, mistakes

„Errors as failure of planned actions to achieve their desired ends" /6/, p. 71.

„The plan is adequate, but the action fail to go as planned" /6/, p. 71.

„The actions may conform exactly to the plan, but the plan is inadequate to achieve its intended outcome" /6/, p. 71.

3. **Consequence related definitions**

Violation: "deviation from safe operating practice" /29/, p.6 according to /13/,

"the failure to apply a good rule" /29/, p.6 according to /13/.

Mismatch: „errors considered as occurrences of man-task mismatches" /44/, p. 11.

4. **Definitions related to organizational aspects**

Terms: latent failures, performance shaping factors (PSFs), general failure types

„Errors as described by Reason relates to the difference in the active or latent nature of error" /29/, p. 6.

"Active errors occur at the point of contact between a human and some aspect of a larger system (e.g., a human-machine interface). They are generally readily apparent (e.g., pushing an incorrect button, ignoring a warning light) and almost always involve someone in the frontline. Latent errors (or latent conditions), in contrast, refer to less apparent failures of organizations or design that contributed to the occurrences of errors or allowed them to cause harm." /43/ according to /13/

"Unsafe acts and situations do not just occur. They are generated by mechanism acting in an organisation. …Sometimes those mechanisms result from decisions taken high in the organisation, thereby causing many unsafe acts. … These mechanisms are called General Failure Types (GFTs)." 11 GFTs were identified as follows /45/, p. 151:

- hardware defects
- inappropriate design
- poor maintenance management
- poor operating procedures
- error-enforcing conditions
- poor housekeeping
- incompatible goals
- communication failures
- organizational failures
- inadequate training
- inadequate defences

10.3 Terms Relevant for Incident Investigation and Documentation

1. **Error of commission**

which are „the correct function at the wrong time", „what is done" and „doing something wrong" /23/, p. 421; /41/, p. 126; /43/ according to /13/ can be subsumed under lapses (of memory)

2. **Error of omission**

which are „failure to act at all", „what is not done" and „failing to do the right thing" /23/, p.421; /41/, p. 126; /43/ according to /13/ can be subsumed under slips (of action)

3. **Human error**

"In this regard, it should be recognized that humans will, on occasion, fail and the majority of accidents are in some part attributable to human error, meaning human actions or inactions which unintentionally exploit weaknesses in equipment, procedures, systems and/or organizations" /2/, p.55.

4. **Unintentional errors:**

slips/lapses are "actions that were not as planned" (unintended actions).

These can occur during a familiar task e.g. omissions like forgetting to do something, which are particularly relevant to repair, maintenance, calibration or

testing. These are unlikely to be eliminated by training and need to be designed out." /14/, p. 11

"**Mistakes** are also errors, but errors of judgment or decision-making ("intended actions are wrong") - where we do the wrong thing believing it to be right. These can appear in situations where behavior is based on remembered rules or familiar procedures or unfamiliar situations where decisions are formed from first principles and lead to misdiagnoses or miscalculations. Training is the key to avoiding mistakes." /14/, p. 11

5. **Intentional errors:**

"**Violations** differ from the above in that they are intentional (but usually well meaning) failures, such as taking a short-cut or non-compliance with procedures e.g. deliberate deviations from the rules or procedures. They are rarely willful (e.g. sabotage) and usually result from an intention to get the job done despite the consequences. Violations may be situational, routine, exceptional or malicious." /14/, p. 11

6. **Active error**

which relates to human error: „ […] active failures are made by those at the sharp end of incident causation (e.g. control room operators, maintenance personnel, the pilot who shuts down the perfectly healthy engine in the incident description). Failures made at the sharp end generally lead to direct consequences and the one making the failure is therefore also likely to experience the consequences" /19/, p. 11, according to /13/.

7. **Latent error**

which are mainly organizational errors: „Latent errors … are made at the blunt end by those whose activities are removed in both time and sharp end of incident causation (e.g. high level decision makers, designers, the CAA in the incident description). These latent failures create the conditions for active failures to be made" /19/, p. 11, according to /13/.

8. **Organizational culture**

"a pattern of basic assumptions-invented, discovered, or developed by a given group as it learns to cope with its problems of external adaptation and internal integration that has worked well enough to be considered valid and therefore to be thought to new members as the correct way to perceive, think, and feel in relation to those problems" /49/, p. 9.

9. **Qualification**

"The existence of physical, mental, and personal qualifications for tasks with specific requirements, whereby it is essential to dispose of capabilities (physical as well as psychological) and skills (behavior learned and trained) to react according to the requirements" /17/, p. 4.

10. Safety culture

“Safety culture is an amalgamation of values, standards, morals and norms of acceptable behavior. These are aimed at maintaining a self-disciplined approach to the enhancement of safety beyond legislative and regulatory requirements. Therefore, safety culture has to be inherent in the thoughts and actions of all the individuals at every level in an organization. The leadership provided by top management is crucial. Safety culture applies to conventional and personal safety as well as nuclear safety. All safety considerations are affected by common points of beliefs, attitudes, behavior, and cultural differences, closely linked to a shared system of values and standards.” /50/, p. 3

11. Safety climate

“the workforce’s attitudes and perceptions at a given place and time. It is a snapshot of the state of safety providing an indicator of the underlying safety culture of an organization.” /51/, p. 1

12. Training

“Organized education which is designed to increase and maintain the physical and psychological performance capabilities of human beings” /17/, p. 4.

13. Work load

“The entirety of all external conditions and requirements in the working system, which could influence a person physically and/or psychologically /17/, p. 2f.

14. Work stress

“sum of those external conditions and demands in the work system which act to disturb a person’s physiological and/or psychological state” /16/, p. 116.

10.4 Terms Relevant for Other Sessions of the Workshop

15. Alarm

“Indication requiring immediate response by the operator for reasons of safety. The response may be, for example, manual intervention, increased watchfulness or initiation of further investigation.” /46/, p. 6

16. Alarm flooding

“Situation in which alarms occur faster than they can be perceived and processed by the operator” /46/, p. 6.

17. Alarm management

“Alarm management systems support the operator in avoiding and controlling abnormal conditions” /46/, p. 6.

18. **Alarm priority**

“Classification of alarms according to their importance (e.g. seriousness of consequences and urgency)” /46/, p. 6.

19. **Alarm rate**

“Number of alarms that occur per unit of time” /46/, p. 6.

20. **Behavior**

“**skill-based behavior**

Behavior mostly related to frequent tasks. Only a small degree of conscious thinking activity is required.

rule-based behavior

Behavior mostly related to less-familiar tasks, which are based on the experience and capabilities of the person in question. The behavior is the result of comparing the information with familiar patterns or rules on a if-then-basis.”

knowledge-based behavior

Behavior mostly related to new tasks, whereas familiar patterns and rules cannot be applicated directly. Requires a high degree of conscious thinking.” /17/, p. 4f.

21. **Critical alarm**

“Safety critical alarms are distinguishable from other operational alarms. For critical alarms, the expected operator action is documented. The state of all critical alarms is always visible. Critical alarms are tested on some plant-defined frequency.” /47/, p. 217

22. **Human reliability**

”Which refers to the absence of human errors: The capability of human beings to complete a task under given conditions within a defined period of time and within the acceptance limits.” /17/, p. 4

23. **Ergonomics**

“The area of ergonomics with the purpose of designing working conditions adapted to human beings. The discipline which deals with the design and handling of machines as well as with working environments so that these match human capabilities and limitations” /17/, p. 3.

24. **Man-machine-system (MMS)**

“The combinations and the total of interactions between human beings and operational means during the work“ /17/, p. 3.

25. Message

“Indication or report of an occurrence i.e. transition from one discrete status to another (according to VDI/VDE 3699). Note: The term “message” or “notification” is used in the literature both as a generic and a particular term. In this worksheet, the term is used for those messages that do not necessitate an immediate response from the operator”. /46/, p. 7.

26. Performance shaping factors

”In modeling human performance for PRA, it is necessary to consider those factors that have the most effect on performance. …Some of these performance shaping factors (PSFs) are external to the person and some are internal.

The external PSFs include the entire work environment, especially the equipment design and the written procedures or oral instructions. The internal PSFs represent the individual characteristics of the person – his skills, motivations, and the expectations that influence his performance.” /48/, p.2-5

27. Safety function

“function to be implemented by an SIS, other technology safety related system or external risk, reduction facilities, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event” /18/, p. 24.

28. Safety instrumented system (SIS)

“instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final elements (s)” /18/, p. 25.

29. Safety life cycle

“necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use” /18/, p. 26.

30. Task analysis

“Analytical process employed to determine the specific behaviors required of people when operating equipment or doing work (ISO 9241-5:1998). Note: The task analysis is not a risk assessment of the workplace according to legal requirements” /16/, p. 102.

11 Anhang III Schlüsselelemente der Sicherheitskultur nach INSAG (/60/, S.5ff):

Selbstverpflichtung, sich für die Sicherheit und die Verbesserung der Sicherheitskultur einzusetzen: “Selbstverpflichtung der Unternehmensleitung, sich für die Sicherheit und die Verbesserung der Sicherheitskultur einzusetzen, ist die erste und entscheidende Bedingung, um herausragende Sicherheitsleistung zu erringen. Das bedeutet, dass Sicherheit (und besonders kerntechnische Sicherheit) von der Unternehmensleitung klar und eindeutig an die erste Stelle der Anforderungen gesetzt wird und dass es absolute Klarheit über die Sicherheitsziele der Organisation gibt. Jedoch bedeutet wahre Selbstverpflichtung zur Verbesserung der Sicherheit mehr als das Verfassen eines Unternehmensziels und der Betonung, wie wichtig Sicherheit ist, in Reden von Führungskräften. Obwohl dies entscheidende Schritte sind, bemerken doch die meisten Personen sehr schnell Unterschiede zwischen wohl gewählten Worten und der Realität. Selbstverpflichtung bedeutet nicht nur, Führung auszuüben, sondern auch daran mit der Belegschaft zu arbeiten, die Bedeutung der Sicherheitsziele der Organisation in das Tagesgeschäft zu übersetzen Daraus ergibt sich der erkennbare Beleg, dass wirkliche Bemühungen unternommen werden. Das beinhaltet die echte Zuordnung von Zeit und Ressourcen für Sicherheit und erfordert, dass die Unternehmensleitung geschult ist und so die notwendige Kompetenz in Sicherheitsfragen haben.” /60/, S.5.

Das Vorhandensein und Einhaltung von Vorschriften und Verfahrensanweisungen (Gebrauch von Prozeduren): “Managementsysteme erfordern eindeutige schriftliche Unterlagen, die geeignet sind, alle Aspekte nukleare und radiologischer Sicherheit zu kontrollieren. Jedoch ist es ein großer Unterschied, ob man herausragende Unterlagen auf dem Papier hat oder ob man Unterlagen hat, die von allen Mitarbeitern verstanden und konsistent und bewusst angewandt werden. Die Anzahl und das Ausmaß der Prozeduren müssen ausgewogen sein. Sie sollten die wichtigsten Risiken identifizieren und behandeln sowie klar verständlich und von Relevanz für die Benutzer sein. Insbesondere sollten die Regeln und Prozeduren für die Belegschaft, durch Training verstärkt, eindeutig die Gründe für bestimmte Anforderungen hervorheben, nur dann werden diese der Relevanzüberprüfung durch den Operateur standhalten, wenn er vollständig zu ihrer Nutzung verpflichtet ist. so relevant für den Nutzer sind, wenn In anderen Worten, ist es entscheidend, dass die Wahrnehmung der Mitarbeiter von Risiken entsprechend den an sie als notwendig und relevant gestellten Anforderungen ist. Wenn Unterlagen nicht geschätzt werden, kann eine Praxis von “Abkürzungen und Umgehungen” Einzug nehmen. Das könnte zu einer weiteren Abwertung von

Sicherheitsstandards führen, weil Umgehungen von Anforderungen, die nicht primär Sicherheitsanforderungen sind, schnell zu einer Kultur führen können, in der sogar entscheidende und fundamentale Sicherheitsprozeduren nicht länger als unantastbar gelten. Als wichtiger Schluss gilt, dass leicht verständliche Prozeduren für die Arbeit vorhanden sein sollten. Diese sollten so gestaltet sein, dass die direkt vor Ort genutzt werden können." /60/, S. 6.

Die in Bezug auf Sicherheit konservative Entscheidungsfindung: "INSAG-4 [1] bezieht sich auf eine hinterfragende Grundhaltung und eine strikte und umsichtige Herangehensweise. Systeme, die überprüft sind und auf einem gestaffelten Sicherheitssystem basieren sowie durch prozedurale Anforderungen unterstützt werden, schützen Mitarbeiter und die Öffentlichkeit vor radiologischen Gefahren. Daher ist es leicht für die Mitarbeiter, die Einstellung zu gewinnen, dass sichere Bedingungen durch andere geschaffen werden sowie dass Ereignisse aus anderen Anlagen Ausnahmen sind und in der eigenen Anlage nicht eintreten können. Deshalb ist das wichtig, dass jeder, der in Zusammenhang mit Sicherheit steht, immer an die möglichen Konsequenzen, wenn Sicherheit nicht die höchste Priorität hat, erinnert wird. Die meisten Ereignisse in der Kerntechnik sind eingetreten, weil jemand ohne die notwendige Umsicht oder ohne konservative Entscheidungsfindung gehandelt hat. Tatsächlich ist es wichtig, dass eine Anforderung für jeden Einzelnen und jedes Team existiert, innezuhalten und die Sicherheit zu bedenken bevor eine Arbeit begonnen oder eine Prozedur umgesetzt wird. Es gibt verschiedenen Methoden, wie das STAR-Prinzip (stop, think, act, review). Sie haben alle eines gemeinsam: Die Notwendigkeit einer konservativen Herangehensweise in Sicherheitsfragen durch die Mitarbeiter bei der Überprüfung des Situationsverständnisses (ggf. Suche nach zusätzlicher Information) und bei der Annahme, dass der schlechteste Fall eintritt. Eine konservative Herangehensweise ist nicht immer einfach, besonders wenn es einen Handlungsdruck gibt, hier müssen die Prioritäten der Organisation eindeutig und akzeptiert sein. Um eine solche Kultur zu entwickeln und zu fördern, sollten Mitarbeiter gelobt werden, wenn sie aus Zweifeln an Folgen für die Sicherheit die Arbeit stoppen oder Änderungen nicht vornehmen. " /60/, S. 7

Die Offenheit, auch scheinbar unbedeutende Vorkommnisse und Beinahe-Ereignisse zu melden (Berichtskultur): "Fehler und Beinahe-Ereignisse werden von Organisationen mit einer guten Sicherheitskultur als Lektionen angesehen, die zur Verhinderung von ernsteren Ereignissen genutzt werden können. Es herrscht so ein gewisser Druck, dass alle Ereignisse mit Lernpotenzial berichtet und auf ihre Ursachen hin analysiert werden sowie dass zeitnahes Feedback zu den Ergebnissen und Maßnahmen sowohl an die beteiligten Arbeitsgruppen als auch an andere in der Organisation oder in der Industrie, die mit demselben Problem konfrontiert werden könnten, gegeben wird. Diese horizontale Kommunikation ist besonders wichtig. Ebenfalls sehr wichtig sind Beinahe-

Ereignisse, da sie eine größere Auswahl und Umfang von Informationen zum Lernen bieten. Um das zu erreichen, müssen alle Mitarbeiter bestärkt werden, auch kleinere Anliegen zu berichten. Hier erwächst die wichtige Frage nach „schuldzuweisungsfreiem“ Berichten. Wenn Mitarbeiter Beinahe-Ereignisse berichten sollen, dann müssen sie überzeugt sein, dass diese Berichte wertgeschätzt werden und dass sie und ihre Kollegen nicht dafür bestraft oder diszipliniert werden, dass sie sie erstellt haben. Natürlich kann es Situationen geben, die Maßnahmen in Bezug auf eine Person als Ergebnis eines Ereignisses erfordern wie beispielsweise eine mutwillige Handlung oder eine wissentliche Abweichung von einer Regel, die als praktikabel, verständlich und korrekt gilt. Unter Umständen wird eine Nachschulung notwendig. Schwieriger wird es, wenn ein gewissenhafter Mitarbeiter wiederholt Fehler begeht, die nicht durch Coaching oder Nachschulung korrigiert werden können. Jedoch bei einer guten Berichtskultur wird akzeptiert, dass es ein unakzeptabler Fehler ist, sicherheitsrelevante Aspekte nicht zu berichten. Eine gute Berichtskultur wird von den Mitarbeitern als „gerecht“ angesehen und basiert auf einer Vertrauensatmosphäre. Dieser offene und reflektierte Ansatz bei Berichten und Folgemaßnahmen birgt Implikationen für die Aufsichtsbehörden. Beispielsweise könnten sie versucht sein, auf die größere Anzahl berichteter “Fehler” eines Betreibers aufgrund eines solchen Systems zu reagieren. Es ist absolut notwendig, dass eine ausgewogene Haltung eingenommen wird, denn Überreaktionen könnten Entwicklungen gefährden, die langfristig zu einer wirklichen und nachhaltigen Verbesserung der Sicherheit führen.” /60/, S. 8

Ablehnung von unsicheren Handlungen und Bedingungen: “Fast alle Ereignisse von industriellen und radiologischen Unfällen, Störfällen, Beinahe-Ereignissen bis hin zu sicherheitsrelevanten Fehlern beginnen mit einer unsicheren Handlung oder unakzeptablen Anlagenbedingung oder –prozess. Letztere sind häufig latent und blieben unentdeckt oder wurden als “üblich oder Praxis” angesehen und deshalb ignoriert. Anschließend kommt es zu einem weiteren signifikanten Fehler in der Kombination mit einem weitern Problem. Die Minimierung von bestehenden latenten Defiziten bei Arbeitspraktiken oder Anlagenbedingungen ist daher notwendig, um ernstere Ereignisse zu vermeiden. Die Minimierung von latenten Defiziten erfordert Wissen bei Mitarbeitern und Fremdfirmenmitarbeitern darüber, warum es spezifische Sicherheitssysteme und Anforderungen gibt und über die sicherheitstechnische Bedeutung jedes Anlagenteils. Sie müssen nicht nur entsprechend qualifiziert und erfahren in ihren Bereichen sein, sondern auch darin bestärkt werden, potenziell unsichere Praktiken in Frage zu stellen und Defizite zu identifizieren, wann und wo auch immer sie mit ihnen konfrontiert werden. In Ergänzung zum Wissen über die Sicherheitsbedeutung von Anlage, Systemen und Prozeduren müssen sie dabei unterstützt werden, Vertrauen zu entwickeln, dass sie andere anzweifeln können, wenn sie Defizite der Sicherheit beobachten. Dieses muss

auf eine konstruktive Art geschehen und mit Lob für sicheres Verhalten kombiniert werden. Aufsichtsbehörden sollten sich ebenso darüber im Klaren sein, warum Sicherheitssysteme und Anforderungen des Anlagenmanagements vorhanden und warum sie wichtig sind. Aufsichtsbehörden müssen besonders vorsichtig vergewissern, dass ihre Vorgaben zur Korrektur von Defiziten nicht kontinuierliche Verbesserungen der Sicherheitskultur behindern. Beispielsweise ist es notwendig, dass die Mitarbeiter noch „im Besitz" ihrer Prozeduren sind und sie als geeignet für ihren Zweck ansehen. Das Nichtanzweifeln, besonders von Managern und Führungskräften, führt nicht nur dazu, dass bestimmte beobachtete Verhaltensdefizite nicht eliminiert werden, sondern führt auch zu einer Kultur, in der Fehler, Oberflächlichkeit und Defizite zur Norm werden. Das wir sehr gut durch den Ausspruch verdeutlicht „tolerieren heißt validieren". /60/, S. 9.

Der Wille sich weiter zu verbessern und zu lernen (Lernende Organisation): "Wenn eine Organisation aufhört mit Hilfe von Benchmarks und der Identifikation von best practices nach Verbesserungen und neuen Ideen zu suchen, dann besteht die Gefahr eines Rückschritts. Eine lernende Organisation ist in der Lage, die Ideen, Energien und Anliegen auf allen Ebenen der Organisation anzuzapfen. Sicherheitsverbesserungen werden erreicht, in dem sichergestellt wird, dass die Vorteile der Verbesserungen weitflächig von Mitarbeitern und Arbeitsgruppen wahrgenommen werden und das zu noch größerer Selbstverpflichtung und Identifikation mit dem Verbesserungsprozess der Sicherheitskultur führt. Idealerweise beteiligen sich alle Mitarbeiter daran, proaktiv Verbesserungsvorschläge zuzusteuern, und werden darin bestärkt, sich bewusst zu werden, was Weltklasse in der Sicherheit für ihre Arbeit bedeutet. Sie beteiligen sich nicht nur, weil sie dazu überredet wurden, sondern weil sie es wollen. Dafür muss ihnen die Gelegenheit gegeben werden, ihre Arbeit mit der anderer zu vergleichen, damit ihnen klar wird, was zur Excellenz in ihrem Arbeitsgebiet führt. Um ein Gefühl für Erfolg zu erhalten, müssen sie in die Lage versetzt werden, ihre identifizierten Verbesserungen mit offensichtlicher Verstärkung und Rückendeckung durch das Management immer dann auszuführen, wenn es sicher und sinnvoll für sie ist. Es ist notwendig Mechanismen zu installieren, die einen Transfer von Erfahrungen und Ideen in die Organisation ermöglichen. Es erscheint ebenfalls notwendig, das es formale Monitoring- und Feedbacksysteme für das Management gibt, so dass es über die Effektivität der eingeführten Verbesserungen informiert ist und damit garantiert ist, dass die Organisation im Gedächtnis behält, warum und wie Verbesserungen gemacht wurden. Obwohl sich Mitarbeiter häufig anfangs auf Arbeitssicherheit und Fragen der Anlagenbedingungen konzentrieren, führt Beteiligung und Selbstverpflichtung am Verbesserungsprozess wahrscheinlich zu einem breiteren Verständnis von Belangen der nuklearen Sicherheit und der Umwelt und zu größeren Geschäftsvorteilen durch die Förderung einer Kultur der

aktiven Beteiligung und Teamarbeit. Nützlich sind Vergütungssysteme, die das Personal bestärken, Verbesserungsideen zu liefern. Entweder können Teams belohnt werden oder Sachprämien können für gute Leistungen gewährt werden. Jedoch zeigt die Erfahrung, dass solche Vergütungssysteme mit der Zeit an Impetus verlieren und weniger effektiv werden. Nachhaltiger sind solche Ansätze, die die Mitarbeiter bestärken, im Team zu arbeiten und kontinuierlich nach Verbesserungen zu suchen, in dem sie einzelne Handlungen identifizieren, um die Sicherheit in ihrem Arbeitsgebiet zu erhöhen." /60/, S. 10f..

Zugrundeliegende Fragen: Kommunikation, klare Prioritäten und Organisation): "Zusätzlich zu den oben genannten spezifischen Aspekten gibt es Grundvoraussetzungen, die alle Fragen untermauern. Die erste stellt die Etablierung einer guten Kommunikation über Sicherheitsfragen dar. Dazu gehören die drei Elemente der Kommunikation: Übertragung, Aufnahme, Bestätigung. Verschiedene Methoden können nützlich sein, von mündlichen Teambriefings bis hin zur geeigneten schriftlichen Sicherheitskommunikation. Allerdings gibt es keinen Zweifel, dass face-to-face-Kommunikation mit hoher Sichtbarkeit von Managern und Führungskräften an den Arbeitsplätzen den größten Effekt hat. Es gibt Belege, dass selbst wenn Manager belegen können, dass sie eine sicherheitsrelevante Nachricht übermittelt haben, Mitarbeiter diese nicht als adäquate für sie bedeutende Information wahrgenommen haben. Das bedeutet wiederum, dass die Art der Übermittlung ungeeignet war, dass es ungenügende Klarheit gab oder dass die Nachricht nicht bei den Empfängern willkommen war. Deshalb ist eine Überprüfung wichtig, nicht nur, ob die Nachricht übermittelt wurde, sondern auch, dass sie erhalten und verstanden wurde und auch dementsprechend gehandelt wird. Es ist ebenfalls wichtig, dass gesichert ist, dass die Kommunikation mit den Aufsichtsbehörden nach denselben Prinzipien durchgeführt wird. Die zweite Grundvoraussetzung ist, dass ein Realitätssinn über Erreichbares und die benötigte Zeitspanne erhalten wird. Viele Sicherheitsprogramme wurden wegen fehlender Übereinstimmung hinsichtlich ihrer Ziele verzögert. Die Schlüsselvoraussetzung scheint hier Prioritätensetzung zu sein. Das Aufstellen von Verbesserungswunschlisten, die aufgrund fehlender Übereinstimmung der Prioritäten nicht ausgeführt oder nur teilweise implementiert wurden, verfehlen nicht nur wirkliche Verbesserung sondern verstärken auch Zynismus und ein Gefühl der Überladung mit Initiativen und resultieren letztendlich in einem Verlust der Dynamik im Prozess der Sicherheitserhöhungen. Es ist wichtig, dass in der Diskussion mit Mitarbeitern und Fremdfirmenmitarbeitern realistische Ziele und Zeitspannen gesetzt werden und dass die Bemühungen diese zu erreichen, mit den richtigen Ressourcen ausgestattet werden. Pläne zur Erhöhung oder Verbesserung müssen priorisiert werden, mit Feedback zu Aufsichtsbehörden und Mitarbeitern, darüber warum bestimmte Aktivitäten zur Umsetzung ausgewählt wurden, während andere nicht dieselbe Priorität erhielten. Ein wichtiger Weg, Bedeutung zu signalisieren und ein

Vehikel für die Veränderung einzusetzen, ist die Entwicklung eines Plans zur Sicherheitserhöhung. Damit dieser effektiv ist, muss er Prioritäten enthalten, alle Veränderung von Prioritäten reflektieren (d.h. ein lebendiges Dokument sein) und besonders wichtig von den Mitarbeitern entwickelt und geteilt sein. Es ist auch notwendig, dass in einem solchen Plan Erfolgsmessungen identifiziert sind und er eindeutig in Bezug auf Zeithorizonte und Verantwortlichkeiten ist. Die dritte Grundvoraussetzung ist, dass Klarheit über die Organisationsstruktur und Zuständigkeiten erreicht und beibehalten wird. Mitarbeiter müssen wissen, was ihre Aufgabe in der Organisation ist und wie ihre Fähigkeiten und ihr Wissen eingesetzt wird, um die Ziele zu erreichen und zu erhalten. Alle Mitglieder eines Teams müssen den von den anderen Mitgliedern erwarteten Input kennen und respektieren sowie den der anderen, die mit ihnen zusammenarbeiten, wie Fremdfirmenmitarbeiter. Dies ist in Perioden schneller Organisationsveränderung besonders wichtig. ” /60/, S. 11f.f.

12 Anhang IV Screening-Verfahren zur Selbstbewertung der Sicherheitskultur/66/:

Im Folgenden wird beispielhaft ein Screening-Verfahren zur Selbstbewertung der Sicherheitskultur aus /66, S.199f/ dargestellt.

		stimmt gar nicht	stimmt wenig	stimmt teil teils	stimmt ziemlich	stimmt völlig	für mich nicht zutreffend
1	Ich finde es wichtig, auf unerwartete Ereignisse vorbereitet zu sein.	O	O	O	O	O	☐
2	Ich habe schon vom Erfahrungsaustausch mit Fachleuten anderer Institutionen profitiert.	O	O	O	O	O	☐
3	Es ist mir leicht möglich auf die Erfahrungen von ehemaligen Kollegen oder Vorgängern zurückzugreifen.	O	O	O	O	O	☐
4	Meine Arbeit wird geschätzt.	O	O	O	O	O	☐
5	Bei der Auswertung unserer Erfahrungen berücksichtigen wir Einflüsse der Technik, der Organisation u. des Menschen gleichermaßen.	O	O	O	O	O	☐
6	Ich sage es Vorgesetzten, wenn sie sich irren.	O	O	O	O	O	☐
7	In meiner Abteilung werden die technischen Komponenten regelmäßig durch Unabhängige auf ihre Sicherheit geprüft.	O	O	O	O	O	☐
8	Ich beteilige mich an der Überarbeitung von Prozeduren, mit denen ich arbeite.	O	O	O	O	O	☐
9	Mir ist bewusst, dass Routine gefährlich sein kann.	O	O	O	O	O	☐
10	Wenn sich jemand gefährdend verhält, schreite ich sofort ein.	O	O	O	O	O	☐
11	Ich nehme regelmäßig an Schulungen teil, um meine Aufgaben nach neuestem Stand von Wissenschaft und Technik ausführen zu können.	O	O	O	O	O	☐
12	Ich habe jederzeit die Möglichkeit, auch bei der Kraftwerksleitung meine Sicherheitsbedenken zu äußern.	O	O	O	O	O	☐
13	Ich kann mich auf die Unterstützung erfahrener Kollegen verlassen, wenn ich Hilfe benötige.	O	O	O	O	O	☐
14	Meine Leistungen werden regelmäßig In jährlichen Mitarbeitergesprächen besprochen und ausgewertet.	O	O	O	O	O	☐

		stimmt gar nicht	stimmt wenig	stimmt teil teils	stimmt ziemlich	stimmt völlig	für mich nicht zutreffend
15	Ich bin an der Analyse von Störungen, Befunden und Fehlern beteiligt.	O	O	O	O	O	☐
16	In den betriebsinternen Veröffentlichungen und im Intranet werden Fragen der Anlagensicherheit diskutiert	O	O	O	O	O	☐
17	Ich melde sicherheitsrelevante Mängel und Gefahren sofort.	O	O	O	O	O	☐
18	Ich achte sehr auf eine vollständige Dokumentation.	O	O	O	O	O	☐
19	Fällt mir eine Schwachstelle im Regelwerk oder den Betriebshandbüchern auf, so bemühe ich mich um deren Korrektur.	O	O	O	O	O	☐
20	In der Zusammenarbeit mit Mitarbeitern von Fremdfirmen beachten wir spezielle Betriebsanweisungen.	O	O	O	O	O	☐
21	Ich weiß genau, wofür ich verantwortlich bin.	O	O	O	O	O	☐
22	Unsere Anlage ist gut gepflegt.	O	O	O	O	O	☐
23	Ich habe die Möglichkeit, eigene Erfahrungen weiterzugeben.	O	O	O	O	O	☐
24	Über meinen Arbeitsplatz hinaus, achte ich auf Ordnung und Sauberkeit.	O	O	O	O	O	☐
25	Meine Leistungen werden korrekt beurteilt.	O	O	O	O	O	☐
26	Wir sind offen im Umgang mit externen Experten.	O	O	O	O	O	☐
27	Ich selbst hinterfrage meine Handlungen, ob sie dem sicheren Betrieb der Anlage dienen.	O	O	O	O	O	☐
28	Ich fühle mich von meinen Vorgesetzten gut informiert	O	O	O	O	O	☐
29	Die Einhaltung der Sicherheits- und Strahlenschutzvorschriften ist bei all meinen Tätigkeiten problemlos möglich.	O	O	O	O	O	☐
30	Alle externen Vertragspartner sind an unsere Sicherheitsbestimmungen gebunden.	O	O	O	O	O	☐

		stimmt gar nicht	stimmt wenig	stimmt teil teils	stimmt ziemlich	stimmt völlig	für mich nicht zutreffend
31	Störungen werden eingehend untersucht.	O	O	O	O	O	☐
32	Ich kann jederzeit alle erforderlichen Meldewege nutzen.	O	O	O	O	O	☐
33	In jährlichen Notfallübungen wird die Zusammenarbeit mit dem regionalen Katastrophenschutz geprobt.	O	O	O	O	O	☐
34	Es ist deutlich erkennbar, dass unser Unternehmen erheblich in die Sicherheit investiert.	O	O	O	O	O	☐
35	Ich bin an der Auswertung von Sicherheitsprüfungen der Anlage beteiligt.	O	O	O	O	O	☐
36	Ich kann leicht mit Kollegen aus den verschiedensten Bereichen der Anlage in Verbindung treten, um Informationen einzuholen.	O	O	O	O	O	☐
37	Ich kann auch mit trivialen Fragen zu meinen Vorgesetzten gehen, ohne befürchten zu müssen, mich zu blamieren.	O	O	O	O	O	☐
38	Wir arbeiten mit Gutachterteams offen zusammen.	O	O	O	O	O	☐
39	Wenn Kollegen den Arbeitsplatz wechseln möchten, werden die Gründe mit den Vorgesetzten besprochen.	O	O	O	O	O	☐
40	Ich unterstütze die Arbeit der Sicherheitsbeauftragten aktiv.	O	O	O	O	O	☐
41	Meine Vorschläge zur Verbesserung der Sicherheit werden von meinen Vorgesetzten gefördert.	O	O	O	O	O	☐
42	Gravierende private Probleme werden von meinen Vorgesetzten ernst genommen.	O	O	O	O	O	☐
43	Mitarbeiter, welche die Sicherheit durch ihre Einstellungen und Ihr Verhalten aktiv fördern, werden durch Vorgesetzte gewürdigt.	O	O	O	O	O	☐
44	Externe Mitarbeiter werden von mir oder meinen Kollegen ausführlich eingewiesen.	O	O	O	O	O	☐
45	Meine Vorgesetzten fördern das sichere Handeln der Mitarbeiter.	O	O	O	O	O	☐
46	Spreche ich mit Anderen über fachliche Dinge, so achte ich darauf, dass es keine Missverständnisse gibt.	O	O	O	O	O	☐

		stimmt gar nicht	stimmt wenig	stimmt teil teils	stimmt ziemlich	stimmt völlig	für mich nicht zutreffend
47	Bei der Analyse von Fehlhandlungen werden keine Schuldzuweisungen vorgenommen.	O	O	O	O	O	☐
48	Die Arbeit externer Mitarbeiter wird von uns kontrolliert.	O	O	O	O	O	☐
49	Technik und menschliches Verhalten sind gleichrangige Bestandteile bei der Bewertung der Sicherheit in unserer Anlage.	O	O	O	O	O	☐
50	Trotz sehr hoher Sicherheitsstandards in unserer Anlage hinterfrage Ich unseren Arbeitsalltag kritisch.	O	O	O	O	O	☐
51	Für spezielle Fragen und Probleme habe ich bisher meistens einen Experten im Werk gefunden, der mir weiterhelfen konnte.	O	O	O	O	O	☐
52	Für tiefer gehende Sicherheitsanalysen gibt es in unserem Werk detaillierte Regeln und Anweisungen.	O	O	O	O	O	☐
53	Bei Konflikten zwischen Produktions- und Sicherheitszielen haben die Sicherheitsziele Vorrang.	O	O	O	O	O	☐
54	Ich achte auf potentielle Gefahren für Andere.	O	O	O	O	O	☐
55	In Sicherheitsfragen gehen meine Vorgesetzten mit gutem Beispiel voran.	O	O	O	O	O	☐
56	Ich melde jede Auffälligkeit meinem Vorgesetzten.	O	O	O	O	O	☐
57	Es gibt ein klares mit Prioritäten versehenes Programm zur Erhöhung der Sicherheit.	O	O	O	O	O	☐
58	Ich kenne alle Anweisungen, die sich auf meinen Aufgabenbereich beziehen im Detail.	O	O	O	O	O	☐

13 Anhang V Namur Empfehlung 31 / DIN EN 61511

Im Folgenden werden einige wichtige Punkte aus der NAMUR Empfehlung 31 „Anlagensicherung mit Mitteln der Prozessleittechnik“ sowie der DIN EN 61511 “Funktionale Sicherheit – Sicherheitstechnische Systeme in der Prozessindustrie“ dargestellt.

13.1 Namur Empfehlung (Namur Recommendation) 31: Empfehlungen für Schutzeinrichtungen (5.2, /88/)

Im Einzelnen werden festgelegt:

- Aufgabenstellung, Schutzaufgabe
- Funktion der PLT-Schutzeinrichtung
- Technische Ausführung (Prinzip)
- Art und Häufigkeit der regelmäßigen Funktionsprüfung
- sonstige organisatorische Maßnahmen

Bei der Festlegung der PLT-Schutzeinrichtung sind zwei Punkte zu beachten: die durch die PLT-Schutzeinrichtung mindestens zu erreichende Risikoreduzierung und die sicherheitsbezogene Verfügbarkeit der PLT-Schutzeinrichtung.

Grundanforderung:

Die PLT-Schutzeinrichtungen der Klasse A sind so auszulegen und zu betreiben, dass bei Auftreten eines als Wahrscheinlich anzunehmenden passiven Fehlers in den Schutzeinrichtungen dennoch die Lösung der Schutzaufgabe gewährleistet ist.

Bei der Auslegung der PLT-Schutzeinrichtung muss daher deren sicherheitsbezogene Verfügbarkeit so gewährleistet werden, dass bei Auftreten eines passiven Fehlers das Risiko unter das Grenzrisiko (RGrenz) auf ein verbleibendes (RV) reduziert wird.

Die sicherheitsbezogene Verfügbarkeit von PLT-Schutzeinrichtungen hängt ab von

- der Ausfallrate infolge passiver Fehler,
- der mittleren Zeit für Erkennung und Beseitigung passiver Fehler und
- dem Redundanzgrad der PLT-Schutzeinrichtung.

Die folgenden wichtigen Grundsätze sind bei der Planung und Errichtung von PLT-Schutzeinrichtungen der Klasse A zu beachten:

- Bewährte und zuverlässige Geräte- und Installationstechnik ist zu verwenden. Die PLT-Schutzeinrichtung ist einfach und übersichtlich aufzubauen.

Fehlerauswirkungen (Beispielsweise Folgefehler in der PLT-Schutzeinrichtung) sind möglichst durch geeignete Fehlerfortpflanzungssperren zu begrenzen.

- Schädliche Einflüsse durch Umgebungs- und Produkteigenschaften wie: Vibration, Stoß, statische Kräfte infolge Verspannung, Temperatureinwirkung, Korrosion, Verschmutzung, Abnutzung, elektromagnetische Einwirkungen (z. B. durch Blitz, Netzverschmutzung, Störungen im Netz, Störspannungen aus Netz usw.), sind zu berücksichtigen.
- Das Ruhesignalprinzip ist möglichst anzuwenden und Fail-Safe-Eigenschaften von Betriebsmitteln auszunutzen (z. B. Stellglied mit Federrückstellung in die sichere Lage u. ä.).
- Werden Betriebs- und Überwachungseinrichtungen als Elemente von PLT-Schutzeinrichtungen mitbenutzt, dann gilt: Vorrang der Schutzfunktion vor anderen Funktionen und Auslegung der gemeinsam genutzten Elemente nach den Maßstäben der Schutzeinrichtung.
- Die Messung der Prozesssicherungsgrößen, die Verarbeitung und das Wirksam werden der Schutzfunktion muss der Schutzaufgabe entsprechend ausreichend genau und ausreichend schnell erfolgen. Die Messbereiche der Prozesssicherungsgrößen müssen so gewählt werden, dass eine hinreichende Auflösung gewährleistet ist. Grenzwerte sollen einen solchen Abstand von den Messbereichsendwerten haben, dass bei Messfehlern innerhalb der zulässigen Toleranz eine sichere Auflösung gewährleistet ist.
- Die korrekte Einstellung der Grenzwerte ist gegen unbeabsichtigte Verstellung zu schützen.
- Das selbsttätige Wiedereinschalten nach Auslösen der Schutzfunktion ist in der Regel zu sperren.
- Alle wichtigen Komponenten der PLT-Schutzeinrichtung sind in der Dokumentation, vor Ort, im Schaltraum und in der Messwarte als PLT-Schutzeinrichtung zu kennzeichnen, damit eine besondere Aufmerksamkeit bezüglich dieser Einrichtungen bei allen Eingriffen in der Anlage erreicht wird.

Zur Aufdeckung passiver Fehler sind Funktionsprüfungen erforderlich. Es sind gemeinsam mit dem Betreiber Prüfanweisungen zu erstellen, in denen Art und Umfang der wiederkehrenden Prüfungsmaßnahmen zusammengestellt sind. Die Prüfanweisung muss Angaben zu Sollzustand und Sollverhalten der Schutzeinrichtung sowie eine Beschreibung der zu prüfenden Eigenschaften und Funktionen enthalten. Dazu gehören insbesondere Angaben über Grenzwerte und Messbereiche, über sonstige zu prüfende Spezifikationsmerkmale, wie Stellzeiten von Ventilen, Verzögerungszeiten für Auslösesignale oder ähnliche für die Erfüllung der Sicherungsaufgabe wichtige Eigenschaften. Der Prüf-

ablauf ist in einer dem Prüfpersonal verständlichen Form, z. B. Check-Liste, zu beschreiben. Die Prüfanweisung ist zwischen dem Betreiber und der PLT-Fachabteilung abzustimmen. Die Grenzwerte werden von dem Betreiber der Fachabteilung schriftlich vorgegeben.

Der Prüfzyklus wird in der Sicherheitsbetrachtung festgelegt. Wegen unterschiedlicher Verfügbarkeiten kann es erforderlich sein, Teile einer Schutzeinrichtung häufiger zu prüfen als andere. Falls keine vergleichbaren Erfahrungen vorliegen, ist der Prüfabstand zunächst angemessen kurz zu wählen. Zeigt sich bei den Prüfungen eine ausreichende sicherheitsbezogene Verfügbarkeit, kann der Prüfabstand mit zunehmender Betriebszeit verlängert werden. In Analogie zu geltenden einschlägigen technischen Richtlinien soll die Prüfung der gesamten PLT-Schutzeinrichtung (vom Sensor bis zum Aktor) mindestens einmal pro Jahr erfolgen. (Quellen: AD-Merkblatt A6, TRbF).

Prüfungen sollen außerdem vorgenommen werden nach längeren Stillstandzeiten und Instandhaltungsarbeiten an der PLT-Schutzeinrichtung. Prüf-, und Instandhaltungsmaßnahmen an PLT-Schutz- oder PLT-Schadensbegrenzungseinrichtungen

sind zu dokumentieren (vergleiche § 6 (2) StörfallV). Insbesondere sind die Funktionsprüfungen mit wenigstens folgenden Angaben zu dokumentieren:

- Bezeichnung des Prüfobjektes,
- Prüfbefund mit detaillierten Angaben über beseitigte Fehler,
- Datum der Prüfung,
- Unterschrift des Prüfers,
- Unterschrift des Betreibers.

13.2 Aussagen und Anforderungen in der DIN EN 61511 /18/ bis 3 /84, 85/ bzgl. Operatorhandlungen, Berücksichtigung menschlicher und organisationaler Faktoren und deren SIS-Schnittstellen

DIN EN 61511 - Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie

Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware

Teil 2: Anleitungen zur Anwendung des Teils 1

Teil 3: Anleitung für die Bestimmung des erforderlichen Sicherheits-Integritätslevel

13.2.1 DIN EN 61511-1

13.2.1.1 Kap. 1 Anwendungsbereich

Insbesondere… fordert sie (die Norm),

- dass der Entwurf sicherheitstechnischer Funktionen menschliche Verhaltensweisen berücksichtigt;
- stellt sie keinerlei direkte Anforderungen an die einzelnen Anlagenfahrer oder Mitarbeiter der Instandhaltung.

13.2.1.2 Kap. 3.2.72 sicherheitstechnisches System (SIS)

Anmerkung 5: Wenn eine Handlung eines Menschen Teil eines SIS ist, dann muss die Verfügbarkeit und Zuverlässigkeit dieser Handlung in der Spezifikation der Sicherheitsanforderungen festgelegt und in der Berechnung der Leistung des SIS eingeschlossen werden.

13.2.1.3 Kap. 5.2.2.2 Kompetenz der Mitarbeiter

In die Beurteilung der Kompetenz müssen mindestens folgende Gesichtspunkte einbezogen werden:

a) technisches Wissen, Ausbildung und Erfahrung bezogen auf die prozesstechnische Anwendung
b) technisches Wissen, Ausbildung und Erfahrung bezogen auf die eingesetzte Technologie (z.B. elektrische, elektronische oder programmierbare elektronische Technologie)
c) technisches Wissen Ausbildung und Erfahrung bezogen auf die Sensoren und Aktoren
d) sicherheitstechnisches Wissen (z.B. über Sicherheitsanalysen)
e) Kenntnis der gesetzlichen und behördlichen Anforderungen
f) ausreichende Management- und Führungsqualitäten für die jeweilige Aufgabe im Sicherheitslebenszyklus
g) das Verständnis für die möglichen Folgen eines Ereignisses
h) den Sicherheits-Integritätslevel der sicherheitstechnischen Funktionen
i) die Neuartigkeit und Komplexität einer Anwendung beziehungsweise Technologie

13.2.1.4 Kap. 11.3 Anforderungen an das Systemverhalten bei Entdeckung eines Fehlers

Hängen die oben genannten Maßnahmen davon ab, dass ein Bediener als Reaktion auf einen Alarm besondere Aktionen einleitet (z.B. das Öffnen oder Schließen eines Ventils), dann ist dieser Alarm als Bestandteil des sicherheitstechnischen Systems anzusehen (d.h. unabhängig vom BPCS).

Hängen die oben genannten Maßnahmen davon ab, dass ein Bediener aufgrund eines Diagnosealarms die Instandhaltung beauftragt, ein fehlerhaftes Teil zu reparieren, dann kann dieser Alarm zwar Teil des BPCS sein, muss aber hinsichtlich der Wiederholungsprüfungen und Änderungen wie ein Bestandteil des SIS behandelt werden.

13.2.1.5 Kap. 11.7.1 Anforderungen an die Bediener-Schnittstelle

11.7.1.1

Wenn als Bediener-Schnittstelle des SIS die Bediener-Schnittstelle des BPCS verwendet wird, müssen deren mögliche Ausfälle berücksichtigt werden.

11.7.1.2

Der Entwurf des SIS muss so sein, dass der Bediener bei laufender Anlage so selten wie möglich eine Auswahl treffen oder das System umgehen muss. Wenn das SIS Bedienereingriffe erfordert, dann sind auch Einrichtungen zum Schutz gegen Fehlbedienung vorzusehen.

ANMERKUNG Wenn der Bediener eine bestimmte Auswahl zu treffen hat. dann muss ein Schritt zur Bestätigung vorgesehen werden.

11.7.1.3

Überbrückungsschalter müssen durch Schlüsselschalter oder Passwort gegen unbefugte Betätigung gesichert werden.

11.7.1.4

Die Statusinformation über das SIS, die entscheidend für die Aufrechterhaltung des Sicherheits-Integritätslevels ist, muss als Teil der Bediener-Schrittstelle abgebildet werden. Zu dieser Information darf gehören:

- wo sich der Prozess in seinem Ablauf befindet;
- eine Anzeige für die Auslösung der SIS-Schutzfunktion;
- eine Anzeige, ob eine Schutzfunktion überbrückt ist;
- eine Anzeige über automatische Vorgänge, wie beispielsweise, ob sich eine Veränderung bei einem Ausgangsvergleich und/oder der Fehler-Behandlungsroutine ergeben hat;

- Zustand der Sensoren und der Aktoren;
- Meldungen über Energieausfall, wenn davon die Sicherheit betroffen ist;
- Diagnoseergebnisse;
- der Ausfall von Einrichtungen zur Herstellung von Umweltbedingungen, die für den Betrieb des SIS notwendig sind.

11.7.1.5

Die Bediener-Schnittstelle des SIS muss so ausgeführt werden, dass Änderungen an der Anwendungssoftware des SIS verhindert werden. Zur Übermittlung von Sicherheitsinformationen vom BPCS zum SIS sollten Systeme verwendet werden, mit denen das BPCS in bestimmte Variablen des SIS schreiben kann. Dazu sollten Einrichtungen oder Prozeduren verwendet werden, die bestätigen, dass die richtigen Daten übertragen und vom SIS empfangen wurden und dass die Sicherheitsfunktionalität des SIS nicht beeinträchtigt wurde.

ANMERKUNG 1 Wenn Auswahlen oder Überbrückungen im BPCS festgelegt und der zugehörige Datenbereich auf das SIS heruntergeladen wird, dann kann ein Versagen des BPCS die Fähigkeit des SIS in Frage Stellen, auf Anforderungen zu reagieren. Wenn dies vorkommen kann, ist das BPCS sicherheitsbezogen.

ANMERKUNG 2 In Chargen-Prozessen können mit Hilfe des SIS je nach verwendetem Rezept unterschiedliche Sollwerte oder logische Verknüpfungen ausgewählt werden. In diesem Fall kann die Auswahl über die Bediener-Schnittstelle getroffen werden.

ANMERKUNG 3 Die Bereitstellung fehlerhafter Daten durch das BPCS an das SIS darf die Sicherheit nicht beeinträchtigen.

13.2.2 DIN EN 61511-2

13.2.2.1 Kap. 8.2.1 Anforderungen an die Gefährdungs- und Risikoanalyse

Bei der Betrachtung der Anforderungshäufigkeit kann es in schwierigen Fällen notwendig sein, eine Fehlerbaumanalyse durchzuführen. Dies ist oft dann erforderlich, wenn schwerwiegende Auswirkungen als Folge gleichzeitiger Ereignisse auftreten (beispielsweise wenn Entspannungssammelleitungen nicht für den „worst case“-Fall einer Entspannung aller angeschlossenen Leitungen ausgelegt sind). Eine Abschätzung ist erforderlich, ob Fehler des Bedienungspersonals in die Liste der Ereignisse, die eine Gefährdung verursachen können, aufgenommen werden müssen, sowie die anzusetzende Häufigkeit solcher Ereignisse, Ein Fehler des Bedienungspersonals kann als Anforderung in vielen

Fällen dann ausgeschlossen werden, wenn eine Handlung einem Genehmigungsverfahren unterliegt oder Verriegelungsmechanismen vorgesehen sind, die eine unabsichtliche Handlung verhindern. In Fällen, in denen die Anforderungshäufigkeit mit Hilfe einer Handlung des Bedienungspersonals reduziert wird, ist ebenso Sorgfalt erforderlich. In welchem Maße dies berücksichtigt werden kann, hängt davon ab, wie schnell die erforderliche Handlung durchgeführt werden muss und wie komplex die erforderlichen Aufgaben sind. Wenn ein Operator eine Handlung infolge eines Alarms durchführen soll und die angenommene Risikoverminderung größer als 10 ist, ist die Auslegung des Gesamtsystems entsprechend DIN EN 61511-1 erforderlich. Das System, das die Sicherheitsfunktion ausführt, würde in diesem Falle aus dem Sensor, der die gefährliche Bedingung feststellt, der Darstellung des Alarms, dem Bedien eingriff und der vom Operator verwendeten Einrichtung zur Unterbindung der Gefährdung bestehen. Es bleibt anzumerken, dass eine Risikoverminderung um einen Faktor kleiner als 10 angenommen werden kann, ohne dass gemäß DIN EN 61511 vorgegangen wenden muss. Im Falle solcher Annahmen sollte man die Gesichtspunkte menschlichen Handelns sorgfältig berücksichtigen. Bei jeder Inanspruchnahme eines Alarms für eine Risikoreduzierung sollte die erforderliche Antwort auf den Alarm beschrieben und dokumentiert werden, dass ausreichend Zeit für den Bediener zur Durchführung des erforderlichen Eingriffs zur Verfügung steht und dass der Bediener für die erforderlichen Eingriffe ausgebildet ist.

13.2.2.2 Kap. 11.2.6 Rolle und Einfluss des Bedienpersonals

Das Bedienungspersonal, das Instandhaltungspersonal, die Meister und die Betriebsleitung spielen alle eine Rolle bei dem sicheren Betrieb einer Anlage. Menschen machen jedoch gelegentlich Fehler oder sind nicht imstande, eine Aufgabe auszuführen, geradeso wie Geräte und Einrichtungen einer Fehlfunktion oder einem Ausfall unterworfen sein können,

Die menschliche Leistung ist deshalb ein Element des Systementwurfs. Die Mensch-Maschine-Schnittstelle ist besonders wichtig bei der Übermittlung des Zustands des SIS an das Bedienungs- und Instandhaltungspersonal.

Die Analyse der menschlichen Zuverlässigkeit erkennt Bedingungen, die Menschen zu Fehlern veranlassen, und liefert Schätzwerte für Fehlerraten, die auf statistisch aufbereiteten Vergangenheitswerten und Verhaltensstudien beruhen. Einige Beispiele menschlicher Fehler, die zu einem Sicherheitsrisiko in Chemieanlagen beitragen können, sind:

- versteckte Planungsfehler;
- Fehler im Betrieb (beispielsweise falscher Sollwert);

- fehlerhafte Instandhaltung (beispielsweise Ersatz eines Ventils durch ein anderes mit einem falschen Ausfallverhalten);
- Fehler bei der Kalibrierung, beim Prüfen oder bei der Interpretation von Ausgabewerten leittechnischer Systeme;
- fehlerhafte Reaktion im Notfall.

13.2.2.3 Kap. 11.7.1 Anforderungen an die Bediener-Schnittstelle

Hier werden für Videobildschirme, Anzeigetafeln und Drucker als Schnittstelle im SIS konkrete Anforderungen gestellt.

Beispiele:

Wenn während Notfallsituationen eine Handlung des Bedienungspersonals erforderlich ist, dann sollten die Update- und Bildwiederholraten der Anzeige für das Bedienungspersonal entsprechend der Spezifikation der Sicherheitsanforderungen ausgeführt sein.

Zum SIS gehörende Videobildschirme sollten klar als solche erkennbar sein, um so Unklarheiten oder die Möglichkeit einer Verwechslung für den Bediener in einer Notfallsituation zu vermeiden,

Anzeigetafeln sollten so angeordnet sein, dass das Bedienungspersonal leichten Zugang hat.

Anzeigetafeln sollten so angeordnet sein, dass das Bedienungspersonal nicht durch die Anordnung der Drucktaster, Lampen, Anzeigegeräte und anderer Informationen verwirrt wird, Schalter zum Abschalten verschiedener Anlagenteile oder Einrichtungen, die gleich aussehen und gemeinsam angeordnet sind, können dazu führen, dass in einer Notfallsituation ein Bediener unter Stress die falsche Einrichtung abschaltet. Schalter zum Abschalten sollten körperlich getrennt und ihre Funktion gekennzeichnet werden.

Die Anzeige sollte so geplant werden, dass die Daten von farbenblinden Bedienern erkannt werden können, Beispielsweise können Zustände mit roter oder grüner Farbe und zusätzlich durch normale oder inverse Darstellung angezeigt werden.