

UMWELTFORSCHUNGSPLAN DES  
BUNDESMINISTERIUMS FÜR UMWELT,  
NATURSCHUTZ UND REAKTORSICHERHEIT  
- Wirkungen von Umweltbelastungen auf Ökosysteme -

Forschungsbericht 298 94 309  
UBA-FB 000140/1



**Strategien zur Verhinderung  
von Fehlbedienungen  
in verfahrenstechnischen  
Anlagen**  
- Abschlußbericht -

von

**Begoña Hermann**, EcoTeam GmbH, Trier

**Uwe Dülsen**, Schwedt/Oder

**Klaus Kämpf**, Prognos GmbH, Basel

**Rainer Müller**, Leipzig

**Kerstin Tschiedel**, Schwedt/Oder

im Auftrag des Umweltbundesamtes

Diese TEXTE-Veröffentlichung kann bezogen werden bei  
**Vorauszahlung von DM 20,-- (10,26 Euro)**  
durch Post- bzw. Banküberweisung,  
Verrechnungsscheck oder Zahlkarte auf das

Konto Nummer 4327 65 - 104 bei der  
Postbank Berlin (BLZ 10010010)  
Fa. Werbung und Vertrieb,  
Ahornstraße 1-2,  
10787 Berlin

Parallel zur Überweisung richten Sie bitte  
eine schriftliche Bestellung mit Nennung  
der **Texte-Nummer** sowie des **Namens**  
und der **Anschrift des Bestellers** an die  
Firma Werbung und Vertrieb.

Der Herausgeber übernimmt keine Gewähr  
für die Richtigkeit, die Genauigkeit und  
Vollständigkeit der Angaben sowie für  
die Beachtung privater Rechte Dritter.  
Die in dem Bericht geäußerten Ansichten  
und Meinungen müssen nicht mit denen des  
Herausgebers übereinstimmen.

Herausgeber: Umweltbundesamt  
Postfach 33 00 22  
14191 Berlin  
Tel.: 030/8903-0  
Telex: 183 756  
Telefax: 030/8903 2285  
Internet: <http://www.umweltbundesamt.de>

Redaktion: Fachgebiet III 1.2  
Dr. Hans-Joachim Uth

Berlin, Februar 2001

# Berichts-Kennblatt

1. Berichtsnummer UBA-FB	2.	3.
4. Titel des Berichts	Strategien zur Vermeidung von Fehlbedienungen in verfahrenstechnischen Anlagen	
5. Autor(en), Name(n), Vorname(n) Hermann, Begoña; Düslen, Uwe, Kämpf, Klaus; Müller, Rainer; Tschiedel, Kerstin	8. Abschlußdatum September 2000	9. Veröffentlichungsdatum
6. Durchführende Institution (Name, Anschrift) Hauptauftragnehmer: Prognos GmbH, Dovestr. 2-4, 10587 Berlin  Unterauftragnehmer: Ecoteam GmbH, Olewiger Straße 62, 54295 Trier; Uwe Düslen; Jamikow Rainer Müller, Leipzig; Kerstin Tschiedel, Stolpe	10. UFOPLAN-Nr. 298 94 398	11. Seitenzahl 184
7. Fördende Institution (Name, Anschrift) Umweltbundesamt Postfach 33 00 22 D-14191 Berlin	12. Literaturangaben 194	13. Tabellen und Diagramme 11
15. Zusätzliche Angaben	14. Abbildungen 29	
16. Kurzfassung	<p>Mit höherer Zuverlässigkeit automatischer Anlagensteuerungen steigt der Anteil menschlicher Fehlhandlungen als Störfallursache in verfahrenstechnischen Anlagen. Daraus resultiert eine zunehmende relative Bedeutung menschlicher Zuverlässigkeit für die Vermeidung bzw. Beherrschung von nicht-bestimmungsgemäßen Betriebszuständen. Der Bereich technischer Zuverlässigkeit ist inzwischen weitgehend optimiert worden; als wichtiger Handlungsbereich zur Verbesserung der Anlagensicherheit verbleibt noch die systematische Optimierung der menschlichen Zuverlässigkeit.</p> <p>Im Rahmen des Forschungsprojekts wurden Vorschläge zur besseren Berücksichtigung des "Human Factors" erarbeitet. Hierzu wurden Methoden zur Darstellung der an einen Bediener gestellten Anforderungen (zum Vergleich mit den objektiven Leistungsgrenzen des Menschen) entwickelt und anhand konkreter Anlagen getestet.</p> <p>Es wurden bestehende Vorschriften, Regeln und Instrumente (z.B. Sicherheitsmanagementsysteme) zur Berücksichtigung des Human Factor analysiert und Vorschläge zu deren Weiterentwicklung erarbeitet.</p> <p>Als Hilfsmittel für die betriebliche Praxis wurde ein "Leitfaden zur Berücksichtigung der Human Factor-Aspekte in verfahrenstechnischen Anlagen" entwickelt.</p>	
17. Schlagwörter	Human Factor, Bediensicherheit, Fehlbedienung, Bedienkonzeption, Störfall, Verfahrenstechnische Anlagen, Chemische Industrie	
18. Preis	19.	20.

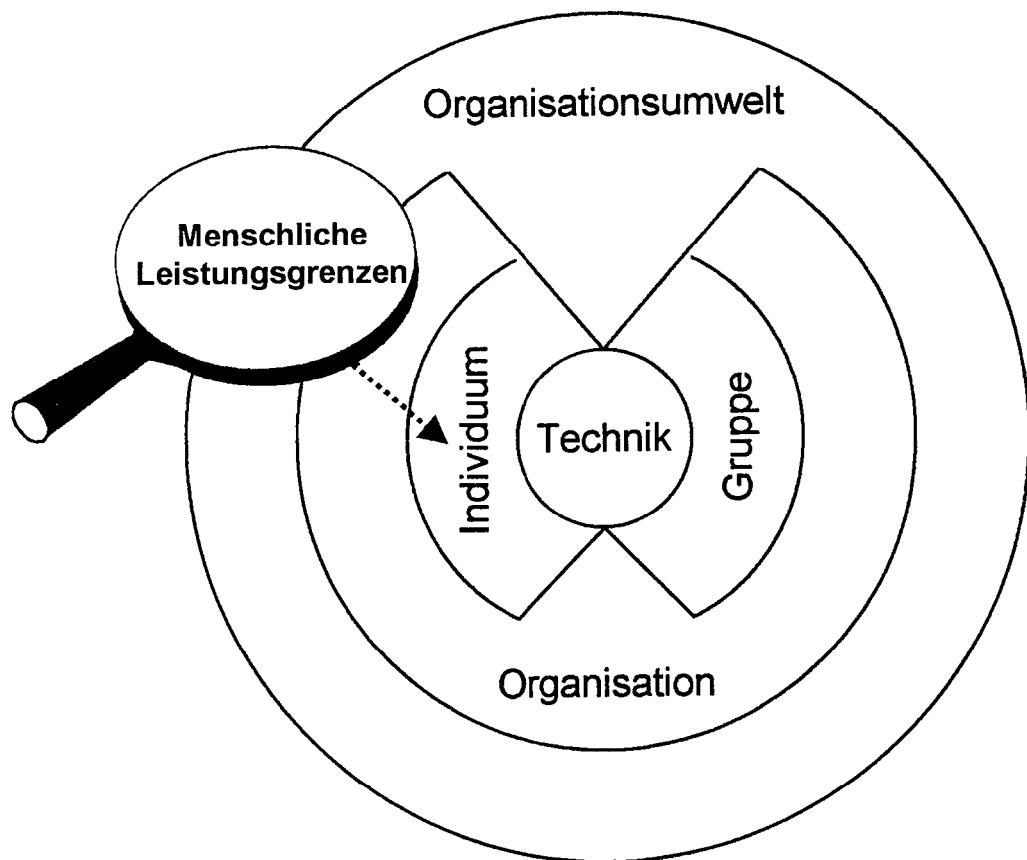
# Report Cover Sheet

1. Report No. UBA-FB	2.	3.
4. Report Title Strategies to prevent operational errors in chemical plants		
5. Autor(s), Family Name(s), First Name(s) Hermann, Begoña; Düslen, Uwe, Kämpf, Klaus; Müller, Rainer; Tschiedel, Kerstin		8. Report Date September 2000
		9. Publication Date
6. Durchführende Institution (Name, Anschrift) Main Contractor: Prognos GmbH, Dovestr. 2-4, D-10587 Berlin  Subcontractors: Ecoteam GmbH, Olewiger Straße 62, D-54295 Trier; Uwe Düslen; D-Jamikow Rainer Müller, D-Leipzig; Kerstin Tschiedel, D-Stolpe		10. UFOPLAN-Ref. No. 298 94 398
		11. No. of Pages 184
		12. No. of References 194
7. Sponsoring Agency (Name, Address) Umweltbundesamt Postfach 33 00 22 D-14191 Berlin		13. No. of Tables, Diagrams 11
		14. No. of Figures 29
15. Supplementary Notes		
16. Abstract  As a consequence of the improved reliability of automatic plant regulating systems, the relative importance of operational errors as an incident cause is increasing, resulting in a growing relative importance of human reliability for the avoidance or control of unforeseen operating conditions. Technical reliability has been further improved in recent years. Therefore, systematic optimisation of human reliability remains a pending issue to improve the safety of plants.  In the course of this research project, recommendations for an improved consideration of human factor were derived. In order to achieve this goal, new methods to represent the requirements to be met by operators (compared with the objective human limits) were developed and tested at existing plants.  Existing regulations, rules, and instruments (e.g safety management systems) aimed at taking into account the human factor were analysed and recommendations for their further development were derived.  A „Guide for the consideration of human factor-related aspects in chemical plants“ was elaborated as an aid for the corporate practice.		
17. Keywords  Human factor, operational safety, operational error, operating concept, accident, chemical plants, chemical industry		
18. Price	19.	20.

## Inhalt

Inhaltsverzeichnis	1
Kurzfassung	4
Executive Summary (engl. Übersetzung der Kurzfassung)	9
1. Einleitung	13
2. Abgrenzungen und Definitionen	16
3. Technische, organisatorische und personenbezogene Faktoren	19
4. Beispielhafte Regelungen in Unternehmen	22
4.1 Allgemeine Erkenntnisse aus den Gesprächen zum Umgang der Unternehmen mit dem Thema "Bediensicherheit"	122
4.2 Besonderheiten in den einzelnen befragten Unternehmen	24
5. Analyse vorhandener Regelwerke im Hinblick auf Bediensicherheit	28
5.1 Verordnungen und Richtlinien	28
5.2 Internationale Regelungen	33
5.3 Technische Normen und Richtlinien der Verbände	39
5.4 Bediensicherheit in der internationalen Normung	41
6. Bestand und Lücken bestehender Instrumente zur Berücksichtigung des Human Factors	43
7. Entwicklung einer Methodik zur prüfbaren Darstellung der Bedienkonzeption	63
7.1 Vergleich und Bewertung verschiedener Notierungsformen	64
7.1.1 Demonstrationsbeispiel kontinuierlich arbeitende Anlagen	69
7.1.2 Demonstrationsbeispiel Batch-Anlagen	77
7.2 Analyse und Bewertung der Aussagen zur Bediensicherheit in vorhandenen Sicherheitsanalysen	81
7.3 Ergänzung von in Sicherheitsanalysen vorgelegten Störfallszenarien hinsichtlich der Bedienanforderungen	82

7.4	Besonderheiten hochgradig automatisierter Anlagen	83
7.5	Statische Prüfung der dargestellten Bedienkonzeptionen hinsichtlich der gleichen Zahl von Sicherheitsbarrieren für mögliche Ereignisketten	84
7.6	Dynamische Prüfung	84
7.7	Ergebnisse der Praxistests	85
7.7.1	Demonstrationsbeispiel kontinuierlich arbeitende Anlagen	85
7.7.2	Demonstrationsbeispiel Batch-Anlagen	96
8.	Möglichkeiten zur Integration der Ergebnisse in betriebliche Managementsysteme	125
8.1	Schnittstelle Mensch – Organisation	125
8.2	Integrierte Managementsysteme (IMS)	126
8.3	Managementhandbücher – Tote Papieransammlung oder aktives Steuerungsinstrument?	130
8.4	Berücksichtigung des Human Factor im Sicherheitsmanagementsystem (SMS)	135
8.5	Weiterführende Literatur zu Kapitel 8	151
9.	Möglichkeiten zur Umsetzung der Human Factor-Aspekte	153
10.	Zusammenfassung und Schlußfolgerungen	159
	Begriffsdefinitionen	166
	Literatur	168
Anhang	Einschlägige Normen	180



"Die Leistung des Menschen beim Umgang mit der Technik wird u.a. durch psychologische und physiologische Gesetzmäßigkeiten [...] beeinflußt"  
(Wilpert et al.: Analyse von sicherheitsrelevanten Ereignissen in verfahrenstechnischen Anlagen. UBA-Text 79/98)

## Kurzfassung

Die Vermeidung von Fehlbedienungen – also die Berücksichtigung des Human Factors – hat in der Kerntechnik und in der Flugverkehrstechnik bereits eine längere Tradition. Im Zusammenhang mit verfahrenstechnischen Anlagen dagegen tauchen die Schlüsselbegriffe im Umfeld von Human Factors zwar zunehmend häufiger auf, haben jedoch noch nicht in den einschlägigen Regelwerken und den üblichen Prüfungsabläufen bei Planung, Bau und Betrieb von Anlagen tatsächlich Einzug gehalten.

Aus der mit höherer Zuverlässigkeit von automatischen Anlagensteuerungen steigende Anteil menschlicher Fehlhandlungen als Störfallursache resultiert eine zunehmende relative Bedeutung menschlicher Zuverlässigkeit für die Vermeidung bzw. Beherrschung von nicht-bestimmungsge-mäßen Betriebszuständen. Der Bereich technischer Zuverlässigkeit ist in den vergangenen Jahren weiter optimiert worden, so daß die ebenso systematische Optimierung der menschlichen Zuverlässigkeit als Handlungsbereich für Verbesserung der Anlagensicherheit noch verblieben ist.

Eine solche – an den menschlichen Leistungsgrenzen orientierte – Verbesserung der Zuverlässigkeit der Bediener verfahrenstechnischer Anlagen spielt jedoch nicht nur zur Vermeidung von Störfällen, sondern im Hinblick auf Anlagenverfügbarkeit und Produktqualität auch im Normalbe-trieb eine wichtige Rolle.

Die physiologischen und psychologischen Aspekte menschlicher Leistungsfähigkeit werden dabei als eingebettet in das technische System und die Organisationsumwelt begriffen. Der Bediener wird hier nicht als "Risikofaktor" gesehen, dessen Unzulänglichkeit es durch technische Sicherungsmaßnahmen weitmöglichst zu kompensieren gilt. Vielmehr steht sein kreatives Potential im Vordergrund, das ihm – unter der Voraussetzung, daß er nicht überfordert wird – die flexible und angemessene Reaktion auf sämtliche Bedienanforderungen ermöglicht.

Ausgehend von den Ergebnissen des BMU/OECD-Workshops "Human Performance in Chemical Process Safety: Operating Safety in the Context of Accident Prevention, Preparedness, and Response" (1997) und des Arbeitskreises "Bediensicherheit" der Störfallkommission (weitergeführt als "AK Human Factor") wurden im Rahmen des Forschungsprojekts

### *"Strategien zur Verhinderung von Fehlbedienungen in verfahrenstechnischen Anlagen"*

Vorschläge zur besseren Berücksichtigung des Human Factors erarbeitet. Der vorliegende Be-richt dokumentiert die Ergebnisse.

Dieses Vorhaben wurde durch das Umweltbundesamt im Rahmen des Umweltforschungsplanes des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit (BMU) gefördert (FKZ 298 94 398).

Die **Ziele** des Projekts sind:

- Die Förderung eines Problembewußtseins im Hinblick auf die Vermeidung von Fehlbedienungen bei den maßgeblichen Akteuren (Anlagenplaner und -bauer, Betreiber, Behörden).
- Die Entwicklung von Methoden zur Erfassung der an einen Bediener gestellten Anforderungen (zum Vergleich mit den objektiven Leistungsgrenzen des Menschen).
- Die Analyse bestehender Vorschriften, Regeln und Instrumente zur Berücksichtigung des Human Factor und die Erarbeitung von Vorschlägen zur Weiterentwicklung.
- Die Prüfung der Möglichkeiten zur Integration von Human Factor-Aspekten in bestehende betriebliche Managementsysteme.
- Die Erstellung eines "Leitfadens zur Berücksichtigung der Human Factor-Aspekte in verfahrenstechnischen Anlagen" als Hilfsmittel für die betriebliche Praxis. Hierbei steht die praxisgerechte Aufbereitung bestehender theoretischer Aufarbeitungen zum Thema Human Factor im Vordergrund.

Zur Sicherstellung des Praxisbezugs der Arbeiten wurde eine breite **Einbindung der Fachöffentlichkeit** angestrebt. Dies umfaßte

- Die Beteiligung eines Beirats aus externen Experten verschiedener Richtungen zur Begleitung des Projektverlaufs. Die Mitglieder des projektbegleitenden Beirats stammen aus den Bereichen Arbeitsschutz und Arbeitssicherheit, Anlagenbau, Anlagenüberwachung, Versicherungswesen, Recht und Arbeitnehmervertretung.
- Die Erarbeitung und praktische Prüfung der Methoden zur Erfassung der an einen Bediener gestellten Anforderungen erfolgte anhand konkreter Anlagen in Zusammenarbeit mit zwei Industriepartnern.
- Es erfolgte ein regelmäßiger Austausch mit dem Arbeitskreis "Human Factor" der Störfallkommission.
- Im Rahmen eines "UBA-Fachgesprächs" am 25. Mai 2000 beim Umweltbundesamt wurden die Ergebnisse einer breiteren Fachöffentlichkeit präsentiert und zur Diskussion gestellt.

Die wichtigsten **Ergebnisse** sind:

Obwohl Bediensicherheit zunehmend in das Bewußtsein der Unternehmen der chemischen Industrie gelangt, erfolgt die Umsetzung der zahlreichen vorliegenden Erkenntnisse noch zögerlich. Offenbar mangelt es an einer geeigneten Kommunikation zwischen den mit Human Factor-

Aspekte beschäftigten Ergonomen und Arbeitspsychologen einerseits und den technisch ausgebildeten Anlagenplanern und Betriebsleitern andererseits.

Ausgehend von der Beobachtung, daß es zahlreiche theoretische Erkenntnisse zur besseren Berücksichtigung des Human Factor gibt, die jedoch in der Praxis erst teilweise Einzug gefunden haben, gilt es zunächst, das Problembewußtsein bei den entscheidenden Akteuren zu wecken. Ferner sind entsprechende Hilfsmittel für die betriebliche Praxis bereitzustellen.

Hierzu wurde im Rahmen des Projekts ein "Leifaden zur Berücksichtigung der Human Factor-Aspekte in verfahrenstechnischen Anlagen" als in sich geschlossene Unterlage – vorgelegt als Materialband zu diesem Abschlußbericht – entwickelt.

Der Leitfaden besteht aus zwei Teilen:

1. Einer Darstellung der Leistungen und Leistungsgrenzen des Menschen. Hierbei steht die praxisgerechte Aufarbeitung vorhandenen Wissens im Vordergrund.
2. Checklisten zur Prüfung der Human Factor-Aspekte als Hilfsmittel für die betriebliche Praxis. Die Checklisten decken die wesentlichen betrieblichen Planungsbereiche ab (Anlagendesign, Leitwertengestaltung, Personalauswahl etc.).

Die menschlichen Leistungsgrenzen des Bedieners beziehen sich dabei im wesentlichen auf die drei Schritte Informationsaufnahme – Informationsverarbeitung – Informationsumsetzung. Neben den Anforderungen an Anlage und Betrieb zur Berücksichtigung der menschlichen Leistungsmöglichkeiten wird auf die Veränderung dieser Leistungsfähigkeit in Störsituationen eingegangen.

Üblicherweise wird der bedienende Mensch über das planmäßige Fahren einer verfahrenstechnischen Anlage im Normalbetrieb hinaus zum Beherrschung unvorhergesehener Situationen eingesetzt. In der Regel erfolgt keine Prüfung der an den Bediener gestellten Anforderungen hinsichtlich ihrer Erfüllbarkeit im Hinblick auf die physiologischen und psychologischen Leistungsgrenzen des Menschen.

*Die Bilanzierung der Ausführbarkeit von Bedienanforderungen scheint das zentrale Problem der Erhöhung der Bediensicherheit zu sein.*

Ein wesentliches Ziel dieses Vorhabens war die Entwicklung von Methoden zur Erfassung und Bewertung der an den Bediener gestellten Anforderungen als Hilfsmittel für Anlagenplaner und -betreiber, sowie ggf. als Prüfunterlage für den Vollzug.

Kontinuierliche und diskontinuierliche (Batch-)Prozesse erfordern dabei unterschiedliche Ansätze. Dies liegt insbesondere daran, daß kontinuierliche Fließgutprozesse mit vergleichsweise wenig Personal, aber viel Prozeßleittechnik betrieben werden. Batch-Prozesse hingegen werden häufig bedienungsintensiv in Vielzweckanlagen mit geringem Automatisierungsgrad betrieben.

Für **kontinuierliche Prozesse** wurden verschiedene Notierungsformen der Bedienkonzeption unter Betrachtung konkreter Anlagen auf ihre Anwendbarkeit untersucht. Dabei zeigte sich, daß die möglichen Eingriffe der Bediener in Gefahrensituationen in Form eines "Störungskompensationsgraphen" (ausgehend von den im Rahmen des PAAG-Verfahrens herausgearbeiteten betrieblichen Gefahrenquellen) erfaßt werden können. Durch die graphische Darstellung kann die Gesamtübersicht über die Sicherheitssituation wesentlich verbessert werden. Es ist notwendig, die Bedienereingriffe, die Möglichkeit des Unterlassens eines Eingriffes durch den Bediener und die Wirkung des Notabfahrsystems in einer gemeinsamen Darstellung zusammenzuführen. Damit wird übersichtlich und vollständig deutlich, unter welchen Bedingungen bzw. infolge welcher Bedienfehler noch "Dennoch-Störfälle" möglich sind. Eine solche (oder eine vergleichbare) Darstellung könnte Eingang in die untergesetzlichen Regelwerke finden.

Insgesamt wurde deutlich, daß ein erheblicher Arbeitsaufwand notwendig ist, Bedienabläufe vorzusehen (zu konstruieren). Die Betrachtung der gängigen Praxis der Anlagenplanung zeigt, daß alle Abläufe, die bei der Planung detailliert vorausgedacht werden, bei hochgradig automatisierten Anlagen in technische Lösungen zur Anlagensicherung eingehen (Notabschaltung, automatische Umschaltung auf Reserve u.ä.).

In **Batch-Anlagen** kann schon der Normalbetrieb zu Bedienerüberlastung führen. Deshalb beginnt die Darstellung der Bedienkonzeption in jedem Fall zunächst mit dem Normalbetrieb. Durch eine graphische Darstellung mit vertikaler Zeitachse und horizontal aufgetragenen räumlichen Abständen der Bedienorte können die raum-zeitlichen Abläufe für den Normalbetrieb einer Batchanlage (die mehrere parallel betriebene Reaktoren oder sonstige Apparate umfassen kann) visualisiert werden. Es können auf diese Weise Beginn, Dauer und Ort der Bedienhandlung dargestellt und Konflikte durch gleichzeitige Anforderungen identifiziert werden. Diese Darstellung erlaubt dem Betreiber eine bedienerorientierte Produktionsplanung und die Identifikation ggf. zur Entlastung des Bedieners erforderlicher Teilautomatisierungen oder sonstiger (technischer oder organisatorischer) Unterstützung.

Allerdings genügen die vorliegenden Rezeptanweisungen gewöhnlich nicht als Grundlage, da sie nicht alle erforderlichen Informationen enthalten. Beispielsweise sind häufig nicht alle zu beobachtenden Meßwerte zu entnehmen. Für den nicht-bestimmungsgemäßen Betrieb fehlen die erforderlichen Informationen zur Darstellung der Anforderungen an den Bediener erst recht. Damit eine derartige Darstellung möglich wird, sind die Gefahrenanalysen durch entsprechende Informationen über das erwartete Verhalten des Bedieners in Störsituationen zu ergänzen.

Langfristig sind für das Zusammenspiel zwischen Anlagenplaner, Betreiber und Aufsichtsbehörde verbindliche Regelungen zur besseren Vorsorge gegen Fehlbedienung wünschenswert. Insbesondere folgende Aussagen sollten in solche Regelungen eingehen:

- Es sollte gefordert werden, daß in den Sicherheitsbetrachtungen eine Auseinandersetzung mit der Bedienkonzeption (nach einem der in diesem Bericht dargestellten oder einem alternativen Verfahren) erfolgt.

- Es sollten über die Einzelfehlerbetrachtung hinaus auch Handlungsketten betrachtet werden.
- Die Handlungs- bzw. Ereignisketten sind zur besseren Erkennbarkeit potentieller menschlicher Fehlerquellen grafisch darzustellen.

## Executive Summary

Prevention of operational errors – i.e. consideration of the human factor – is not a recent issue: it has a long tradition in aviation and nuclear technology. Human factor-related topics in chemical plants are becoming more frequent in recent years, but they are usually not included in regulations and verification processes connected with the planning, construction and operation of plants.

As a consequence of improved reliability of automatic plant regulating systems, the relative importance of operational errors as a cause for accidents is increasing, thus resulting in a growing relative importance of human reliability for the avoidance or control of unforeseen operating conditions. Technical reliability has been further improved in recent years. Therefore, systematic optimisation of human reliability remains a pending issue to improve the safety of plants.

Improving operator's reliability at chemical plants – by taking into account human limits – is crucial not only with respect to the prevention of major accidents, but as well with regard to plant availability and product quality under regular operating conditions.

Physiologic and psychological aspects of human performance are considered to be embedded in the technical system and the organisational environment. The operator is not regarded as a „risk factor“, whose lack of capacity has to be compensated for by adequate technical safety measures. On the contrary, the focus lies on his creative potential, which enables him – provided he can cope with the situation – to react flexibly and properly to all operating requirements.

On the basis of the results of the BMU/OECD workshop "Human Performance in Chemical Process Safety: Operating Safety in the Context of Accident Prevention, Preparedness, and Response" (1997) and the working group "Operational Safety" of the Incident Prevention Commission (resumed as "AK human Factor ") within the course of the research project

*"Strategies to prevent operational errors in chemical plants "*

recommendations were made to allow for an improved consideration of human factor. The present report documents the results.

This project was funded by the German Federal Environmental Agency in the course of the Environmental Research Programme of the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU) (project number: 298 94 398).

The principal **objectives** of the project are:

- To promote the awareness for human factor aspects among the relevant persons and institutions (plant designers and constructors, plant operating companies, and authorities) with a view to avoiding operational errors.
- To develop new methods to determine the requirements to be met by operators (compared with the objective human limits).
- To analyse existing rules and instruments aimed at taking into account the human factor and to derive recommendations for their further development.
- To check the options to include human factor aspects in existing corporate management systems.
- To develop a „Guide for the consideration of human factor-related aspects in chemical plants" as an aid for corporate practice. The guide should take into account existing theoretical studies on the human factor and should have a practical approach.

In order to ensure a practical approach, a broad involvement of **experts** was striven for, including

- The involvement of an interdisciplinary advisory board, which consists of extern experts, to accompany the project. The members of the advisory board represent various fields of specialisation, such as working safety, industrial safety, plant design, process control, insurance, law and employee representation.
- The elaboration and the practical check of the methods to determine the requirements to be met by operators, which was done on the basis of existing plants, in co-operation with two industrial partners.
- Periodic information exchange with the working group "Human Factor" of the Incident Prevention Commission.
- The results were presented to and discussed by a wide range of experts during the "UBA Expert Talks" on 25 May, 2000, held at the Federal Environmental Agency in Berlin.

The main results can be resumed as follows:

Chemical companies are increasingly aware of the importance of operating safety. Nevertheless, this has not resulted in an implementation of the numerous existing findings. Apparently, there is a lack of communication between ergonomists and work psychologists specialised in operational safety issues on the one hand and plant designers and plant managers – with a technical background – on the other hand.

Based upon the observation that there are numerous theoretic findings which could allow for a better consideration of human factor but have only partially been included in practice, there is a need to raise the awareness of the problem among the involved persons. In addition, adequate tools should be developed for corporate practice.

In order to achieve this goal, a "Guide for the consideration of human factor-related aspects in chemical plants" was worked out – as a separate volume – in the course of this project.

This guide consists of two parts:

1. A description of human performance and its limits. Available knowledge was reviewed, pointing out its practical implications.
2. Checklists to verify human factor aspects as a tool for corporate practice. These checklists cover the essential corporate planning areas (plant design, control room design, staff selection, etc.).

The operator's performance limits concern basically the following three steps: information assimilation – information processing – information implementation. In addition to the requirements for the plant to take into account human capability, performance variations during incidents are considered.

Operators are usually expected to operate chemical plants not only under normal conditions but also under exceptional circumstances. As a rule, there is no check of the requirements to operators, so as to ascertain whether the requirements can be met with regard to physiologic and psychological limits.

*The assessment of the practicability to meet operational requirements seems to be the main problem for the improvement of operational safety.*

One of the basic goals of this project was to develop methods to determine and assess the requirements to operators as an aid for plant designers and operators, and possibly as a document for the legal execution.

Different approaches are required for continuous and discontinuous (batch) processes. This is due to the fact that continuous processes in general involve fewer operating staff, but many process control engineering systems. Batch processes are usually run in multi-purpose installations with a low degree of automation, thus requiring more staff.

Several representation forms for the operating concept of **continuous processes** were analysed. Existing plants were involved in order to check practicability. It turned out that possible operator interventions in dangerous situations could be represented as a "incident compensation graphs" (based on existing hazard analyses, which were identified in the course of the so-called "PAAG

process"). Graphic representation can considerably contribute to improve the overview of the security system. It is necessary to include the operators intervention, the possibility of an omitted operator intervention and the effects of emergency shut-down system in a single representation. By this means it is possible to ascertain under which conditions certain incidents, which occur although they are very improbable and can reasonably be excluded, may occur. Such a representation (or a comparable representation) could be required by law.

The study showed that a considerable amount of work is required in order to think ahead operating steps. The analysis of the current plant design practice shows that all operating steps which are considered in detail during the planning result in technical solutions to improve plant safety (emergency shut-down, automatic switch to the reserve, etc.).

In **batch plants**, even normal operating conditions may lead to situations which cannot be coped with by the operator. For this reason, representation of the operating concept starts by describing normal operating conditions. Graphic representations where time is plotted against spatial distances of operating places (on the horizontal axis) can help to visualise operating steps of a batch plant (which can comprise several parallel running reactors) and its time and spacial dimensions during normal operating conditions. This helps to represent start, duration and places of each operating step and to identify conflicts due to simultaneous requirements. This representation allows the plant operating company to take into account the operator when planning production and to identify automatisation (or other technical or organisational measures) needed to support the operator.

Nevertheless, the standard recipe instructions can normally not be taken as a basis for such a representation of the operating concept because they do not include all required informations. For instance, usually not all measured values which have to be controlled are mentioned. In case of unforeseen operating conditions, the essential informations which are needed to represent the operating requirements are missing. To make possible such a representation, risk analyses have to be completed by adequate informations about the operator's expected reaction in case of an incident.

In the long run, binding regulations should be worked out to improve the co-operation between plant designers, operators and the competent authorities, thus lowering the risk of human error. The following statements should be included in such regulations:

- Safety considerations should include an analysis of the operating concept (this can be done using one of the methods described in this study or an alternative approach).
- The analysis should go beyond consideration of single errors. Chains of actions should also be analysed.
- Chains of actions and events should be represented graphically to facilitate the identification of potential human error sources.

## 1. Einleitung

Die Vermeidung von Fehlbedienungen, also die Berücksichtigung der **Human Factors** (HF) hat in der Kerntechnik und der Flugverkehrstechnik bereits eine längere Tradition. Im Zusammenhang mit verfahrenstechnischen Anlagen dagegen tauchen die Schlüsselbegriffe im Umfeld von HF zwar zunehmend häufiger auf, ohne jedoch bereits in Regelwerken und den üblichen Prüfabläufen bei Planung, Bau und Betrieb einer Anlage tatsächlich Einzug gehalten zu haben. Es lässt sich dies auch anhand der von Reason (1990) dargestellten Entwicklung der Sicherheitswissenschaft darlegen (Frank 1994, S. 27):

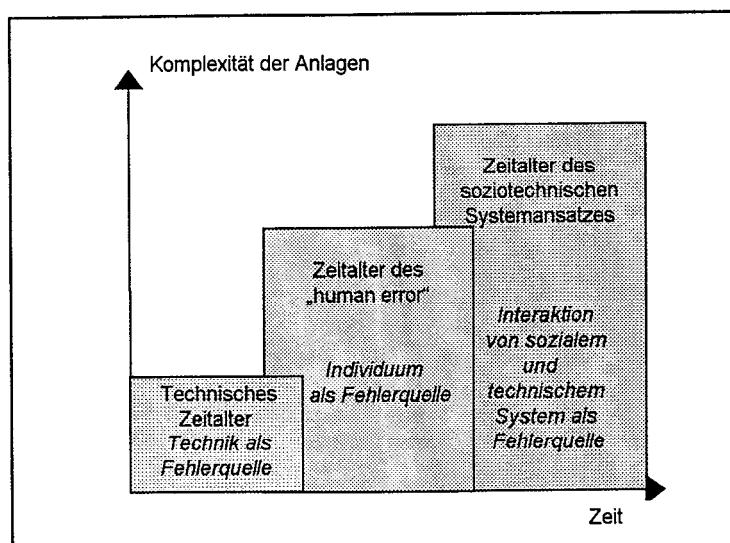


Abb. 1-1: Paradigmenwechsel in der Sicherheitsforschung (Wilpert 1995, S. 70)

### (a) Technische Phase (bis ca. 1930)

In dieser Phase ging man davon aus, daß Technikversagen als wichtigste Fehlerquelle anzusehen sei. So ging es in erster Linie um Unfallvermeidung durch Optimierung technischer Komponenten. In einer Maximierung des Ausbaus technischer Barrieren gegen Systemzusammenbrüche und unerwünschte Anlagenzustände versuchte man, Sicherheit und Zuverlässigkeit zu erhöhen. Man merkte dann aber doch sehr schnell, daß die menschliche Erfindungsgabe in Verbindung mit Fehlhandlungen selbst hochgezüchtete technische Barrieren umgehen konnte. Daraus:

### (b) Phase menschlicher Fehlhandlungen (bis ca. 1980)

In dieser Phase nahm man an, daß Individuen wichtige Fehlerquellen seien. Daher investierte man vornehmlich in den besagten „Faktor Mensch“: Auswahl der Geeigneten, Kompetenzerweiterung, Trainings, Fachprüfungen vor allem der Operateure waren angezeigt. Wachsende

Einsicht, daß angesichts zunehmender Komplexität der Anlagen ein ausschließliches Abheben auf entweder technische oder menschliche Teilkomponenten unbefriedigend bleiben muß, läutete die nächste Phase ein:

### (c) Soziotechnische Phase (seit ca. 1980)

Diese Phase wird von der Erkenntnis geleitet, daß eine komplexe Interaktion sowohl technischer als auch menschlicher, sozialer, managerialer und organisationaler Faktoren des gesamten Systems als Mitverursacher auffälliger Stör- und Unfälle betrachtet werden muß. Der soziotechnische Systemansatz geht davon aus, daß jede Organisation, jedes System aus zwei Subsystemen (soziales und technisches) besteht, deren zielgerichtete Interaktion erst den Erfolg (Produktqualität, Sicherheit, Zuverlässigkeit) garantiert. Die Entwicklungsphasen der Anlagensicherheit führten damit von der „Unfallfreiheit“ über die „Fehlerfreiheit“ bis zum heutigen Leitgedanken der „Zuverlässigkeit“.

Handlungsleitender Kerngedanke des soziotechnischen Systemansatzes, z.B. wenn es darum geht, im Interesse von Sicherheit und Zuverlässigkeit Maßnahmen zu treffen, ist

- die **gemeinsame** Optimierung beider Subsysteme – des technischen und des sozialen Subsystems.

Der steigende Anteil menschlicher Fehlhandlungen als Störfallursache ist nach den Entwicklungsphasen als „zunehmende relative Bedeutung menschlicher Zuverlässigkeit“ (Schäffler 1994, S. 193) zu verstehen. Der Bereich technischer Zuverlässigkeit ist in den vergangenen Jahren zunehmend optimiert worden, so daß die ebenso systematische Optimierung der menschlichen Zuverlässigkeit als Handlungsbereich für die Anlagensicherheit noch verblieben ist. Handlungsbereiche früherer Phasen sind dabei nicht entbehrlich geworden, sondern sollen ergänzt werden, hin zum Ziel einer ganzheitlichen Anlagensicherheit.

Ausgehend von den Ergebnissen des BMU/OECD-Workshops "Human Performance in Chemical Process Safety: Operating Safety in the Context of Accident Prevention, Preparedness, and Response" (1997) und des Arbeitskreises "Bediensicherheit" der Störfallkommission sollen im Rahmen des Forschungsprojekts "Strategien zur Verhinderung von Fehlbedienungen in verfahrenstechnischen Anlagen" des Umweltbundesamtes Vorschläge zur besseren Berücksichtigung des Human Factor erarbeitet werden.

Im Rahmen dieses Projekts werden prioritär primäre Bedienfehler (Fehlbedienung im Normalbetrieb im Sinne der Störfallvorsorge) betrachtet. Es geht dabei nicht darum, Fehlbedienung als Produkt von Nachlässigkeit, Unzulänglichkeit oder Inkompetenz des Bedieners zu begreifen. Im Zentrum steht vielmehr die Frage, warum die Leistungsgrenzen des Bedieners überschritten wer-

den und wie in der Bedienkonzeption einer Anlage vorbeugend diesen Leistungsgrenzen entsprochen werden kann.

Die **Ziele** des Projekts sind:

- Die Förderung eines Problembewußtseins bei allen Beteiligten.
- Die Entwicklung von Methoden zur Erfassung der an einen Bediener gestellten Anforderungen (im Vergleich mit den objektiven Leistungsgrenzen des Menschen).
- Die Analyse bestehender Vorschriften, Regeln und Instrumente zur Berücksichtigung des Human Factor und die Erarbeitung von Vorschlägen zur Weiterentwicklung.
- Die Prüfung der Möglichkeiten zur Integration von Human Factor-Aspekten in bestehende betriebliche Managementsysteme.
- Die Erstellung eines "Leitfadens zur Berücksichtigung der Human Factor-Aspekte in verfahrenstechnischen Anlagen" als Hilfsmittel für die betriebliche Praxis. Hierbei steht die praxisgerechte Aufbereitung bestehender theoretischer Aufarbeitungen zum Thema Human Factor im Vordergrund.

Zur Sicherstellung des Praxisbezugs der Arbeiten wurde bereits im Verlauf des Projekts eine breite Einbindung der Fachöffentlichkeit angestrebt. Dies umfaßte

- Die Beteiligung eines Beirats aus externen Experten verschiedener Richtungen, der den Projektverlauf begleitet. Die Mitglieder des projektbegleitenden Beirats stammen aus den Bereichen Arbeitsschutz und Arbeitssicherheit, Anlagenbau, Anlagenüberwachung, Versicherungswesen, Recht und Arbeitnehmervertretung.
- Die Erarbeitung der Methoden zur Erfassung der an einen Bediener gestellten Anforderungen erfolgte in Zusammenarbeit mit zwei Industriepartnern.
- Den regelmäßigen Austausch mit dem Arbeitskreis "Human Factor" der Störfallkommission.
- Die Präsentation und Diskussion der Ergebnisse mit einer breiteren Fachöffentlichkeit im Rahmen eines "UBA-Fachgesprächs" am 25. Mai 2000 beim Umweltbundesamt.

Allen Beteiligten sei an dieser Stelle für ihr ehrenamtliches Engagement, das wichtige Impulse für das Vorhaben lieferte, gedankt.

## 2. Abgrenzungen und Definitionen

Die multidisziplinäre Ausrichtung der HF-Forschung hat entscheidend dazu beigetragen, daß gleiche Begriffe unter unterschiedlichem Verständnis verwendet werden:

- **Arbeitspsychologen** verstehen unter HF eher individualpsychologische Dispositionen (Motivation, Locus of control, individuelles Problemlöseverhalten, Stressverhalten, Kommunikation, psychosoziale Stabilität, Belastungsgrenzen, Kognitionen).
- **Arbeitswissenschaftler** betonen die Arbeitsbedingungen (Schichtdienst, Pausenregelungen, Bezahlung) und die direkte Arbeitsumwelt (Arbeitsraum, Lichtverhältnisse, Klima, ergonomische Arbeitsplatzgestaltung, Teamarbeit, Regelung von Verantwortlichkeiten, Verhalten der Vorgesetzten).
- **Planende und Sicherheitsingenieure** setzen Human Factor mit Human Error gleich und fokussieren ihr Konzept zu HF im wesentlichen auf fehlertolerante Technik.

Daraus folgend richten sich ihre Interventionen und Optimierungen auf unterschiedliche Ansatzpunkte (Qualifizierung, Personalentwicklung, Lernen nach lerntheoretischen Erkenntnissen versus Ergonomie versus fehlertolerante Technik).

Diese personenbezogenen, organisatorischen und technischen Faktoren der HF sollen unter dem Blickwinkel ganzheitlicher Anlagensicherheit zu einer systematischen Strategie zur Verhinderung von Fehlbedienung führen, wobei strenggenommen die fehlertolerante Technik nichts mit der Vermeidung von Fehlbedienung zu tun hat, sondern lediglich mit der Begrenzung ihrer Auswirkungen, bzw. mit der Verringerung der Eintrittswahrscheinlichkeit einer Störung durch Fehlbedienung.

Dort, wo schon sinnvolle Verbindungen zwischen den einzelnen Erkenntnisbereichen erkennbar sind, setzt sich die Überzeugung durch, daß der „menschliche Faktor“ nicht nur ein Potential für Fehler, sondern auch ein **Potential für Erkenntnis** ist. Das Erfahrungswissen des Bedieners wird dann beim Anlagendesign, bei der Gestaltung der eingesetzten Technik, bei der Optimierung der Anlagensicherheit, mitberücksichtigt.<sup>1</sup> Es ist jedoch noch keineswegs so, daß sich die Beteiligung des Bedienpersonals am Anlagendesign durchgesetzt hätte.

Dabei sollte seit den grundlegenden Ausführungen von Reason zum „Human Error“ (1990) klar geworden sein, daß sich lediglich die Kategorie „**aktive Fehler**“ auf direkte Fehlbedienung des Operators bezieht, nicht aber die Kategorie „**latente Fehler**“, die einem System innewohnen können und erst im Zusammenwirken mit anderen Faktoren bemerkbar werden. Sie sind im wesentlichen auf Auslegung, Instandhaltung, Organisation und Management zurückzuführen, also auf das Handeln von Personen, die nicht unmittelbar in den Prozeß eingreifen.

<sup>1</sup> Als positives Beispiel ist hier das Projekt "Sicherheit durch organisationales Lernen (SOL)" der Forschungsstelle Systemsicherheit zu nennen (UBA-Text 98/79).

## Definitionen „Human Factors“

1. „HF sind diejenigen Faktoren, die generell den Menschen beim Umgang mit der technischen Anlage beeinflussen. Leistungsbeeinflussende Faktoren sind **Technik, Organisation, Person**“ (vgl. Becker 1991, bzw. FSS 1997).

Eine Definition, die auch die überbetriebliche Ebene einschließt (sprich Behörden und Gutachter) verwendet die Forschungsstelle Systemsicherheit (FSS):

2. „Human Factors sind all jene Handlungsmöglichkeiten auf unterschiedlichen Systemebenen, die einzeln oder interaktiv einen Beitrag zur Steigerung oder Minderung der Effektivität, Sicherheit und Zuverlässigkeit sowie der befriedigenden Nutzung eines soziotechnischen Systems liefern“ (Frank und Wilpert 1994).

Hier wird also bereits auf Handlungsansätze abgestellt und nicht mehr allein auf sicherheitsbeeinflussende Faktoren.

Weitere Definitionen sind im wesentlichen bereits durch die zuvor genannten abgedeckt:

3. „HF are environmental, organisational and job factors and human and individual characteristics which influence behaviour at work in a way which can affect health and safety“ (Health and Safety Executive, Großbritannien).

Der unter 1. genannte Faktor „Person“ wird hier als „menschliche und individuelle Merkmale“ spezifiziert.

Wenn auch die individuellen Eigenschaften der Person als Einflußfaktor durchaus erkannt werden, so wird dieser Bereich in der Fachdiskussion als Handlungsansatz eher nicht wahrgekommen. Die sogenannten „**subjektiven**“ **Faktoren** (Motivation, Kommunikationsfähigkeit, Sozialverhalten, Konzentrationsfähigkeit) werden im allgemeinen nicht als dem HF-Konzept zugehörig betrachtet, da sie sich einem „**objektiven**“ **Zugang** (= Erkennen und Beseitigen) verweigerten (vgl. hierzu Eisgruber 1997, S. 5). Daß dies der Ingenieur so sieht („people are the weakest link in our safety system“), ist von seinem eigenen Fachverständnis her durchaus nachvollziehbar. Ob der Arbeitspsychologe hierzu jedoch nicht eine ganz andere Sichtweise hat, soll in diesem Bericht noch diskutiert werden.

Schon im Vorgriff auf die an späterer Stelle festgestellten Lücken und Mängel im Umgang mit dem Thema „human factors“ soll hier darauf hingewiesen werden, daß in diesem Projekt der Schwerpunkt des Vorgehens auf dem **Individuum** – eingebunden in die Gruppe, die Organisation und die Organisationsumwelt (siehe Abbildung auf Seite 3) – liegt. Selbst wenn die Ansicht geteilt würde, daß die subjektiven Faktoren kaum Interventionsansätze bieten könnten, so sind die physiologischen, psychischen und psychosozialen Merkmale und Grenzen des Menschen vor allem bei komplexen verfahrenstechnischen Anlagen doch als Ausgangspunkt für die Bedienkonzeption heranzuziehen. Dies wird aktuell – vor allem für den Fall gefahrdrohender Betriebssituationen,

in denen schnelles, ausschließlich richtiges Verhalten gefordert wird – nicht ausreichend berücksichtigt.

#### **Definition „Bediensicherheit“, „Mensch-Maschine-Schnittstelle“**

Unter Bediensicherheit wird im allgemeinen verstanden, daß ein bedienender Mensch die ihm zugesagten Bedienhandlungen verläßlich und richtig ausführt.<sup>2</sup>

Bezog sich die Bediensicherheit unter dem Gesichtspunkt des Arbeitsschutzes zunächst nur darauf, daß die Maschine den Bediener nicht verletzte, so wird derselbe Begriff heute mit einer neuen, zweiten Bedeutung verwendet, nämlich im gleichen Zusammenhang wie das HF-Konzept mit seinen drei Aspekten: Technik, Organisation und Person, so daß die Begriffe „HF-Konzept“ und „Bedienkonzept“ nicht klar abgrenzbar sind.

Ähnliches gilt für den Begriff „Mensch-Maschine-Schnittstelle“ (M-M-S). Das M-M-System bezeichnet den Umgang des Menschen mit der technischen Einrichtung (Schäffler 1994). Die Aufarbeitung der M-M-S deckt im wesentlichen die Interaktionsprobleme der Einflußfaktoren auf die Anlagensicherheit nach dem HF-Konzept auf. Man versucht, den Betrachtungskonflikt „**Risikofaktor Mensch**“ versus „**Sicherheitsfaktor Mensch**“ durch die Betrachtung der Schnittstelle aufzuarbeiten.

Wie all diese Ausführungen zeigen, geht es bei der Betrachtung der Human factors, der Bediensicherheit, der Mensch-Maschine-Schnittstelle im wesentlichen um das Aufdecken von Fehlern für/in Gefahrensituationen.

---

<sup>2</sup> Die Unterlassung erforderlicher Bedienhandlungen ist demnach auch eine Fehlbedienung. Die Bereiche Wartung und Instandhaltung werden **nicht** mit den Begriffen „Human Factor“, „Bediensicherheit“ oder „Mensch-Maschine-Schnittstelle“ erfaßt.

### 3. Technische, organisatorische und personenbezogene Faktoren

Allen verschiedenen Ausprägungen des HF-Konzeptes/Verständnisses ist gemeinsam, daß **technische, organisatorische und personenbezogene Einflußfaktoren** auf die Mensch-Maschine-Schnittstelle unterschieden werden. Unter diesen drei Faktorenbereichen wird verstanden (Christiandl 1992):

#### Technische Faktoren:

- Sicherheitstechnische Auslegung der Anlage derart, daß sie möglichst unempfindlich gegen menschliche Fehler ist und sich aus menschlichem Fehlverhalten keine gravierenden nachteiligen Auswirkungen auf die Anlagensicherheit ergeben können.
- Ein dem Menschen angepaßter Automatisierungsgrad von Sicherheits- und Betriebsfunktionen.
- Eine dem Menschen angepaßte Technik zur sicheren Überwachung der Betriebszustände.
- Eine dem Menschen angepaßte Technik zur Erkennung und Beherrschung von Störungen und Störfällen.
- Instandhaltungsfreundlichkeit von Systemen.
- Ergonomische Gestaltung der Arbeitsplätze, der Arbeitsmittel und der Arbeitsumgebung.
- Simulatoren zum Training selten auftretender Anforderungen.

#### Organisatorische Faktoren:

- Eine dem Menschen angepaßte Betriebs- und Ablauforganisation mit eindeutigen Festlegungen von Aufgaben, Verantwortlichkeiten und Befugnissen des Personals.
- Dem Menschen angepaßte Betriebsordnungen
  - Wartungs- und Schichtordnung
  - Instandhaltungsordnung
  - Strahlenschutzordnung
  - Alarmordnung
  - Brandschutzordnung
  - Erste-Hilfe-Ordnung.
- Dem Menschen angepaßte Betriebsanweisungen zur Durchführung des Normalbetriebs und für Reparatur und Wartung, zur Beherrschung von Störungen und Störfällen.
- Motivationsmaßnahmen des Managements
- Sicherheitskultur

**Personenbezogene Faktoren:**

- Qualifikation (Ausbildung, Schulung, Training)
- Eignung (Mitarbeiterauswahl)
- Motivation (Arbeitsbedingungen, Sicherheitskultur)
- Zuverlässigkeit.

Die Forschungsstelle Systemsicherheit (FSS) drückt HF als Schalenmodell aus, wodurch Aufbau und Abhängigkeiten deutlich werden (vgl. Abbildung 3-1).

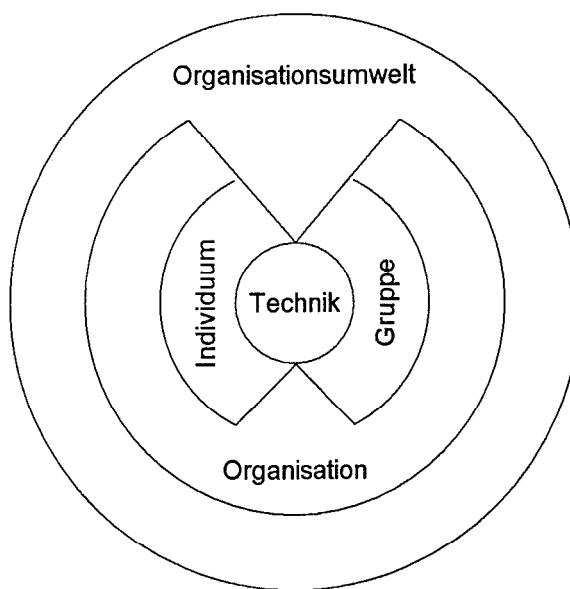


Abb. 3-1: Die fünf Subsysteme des soziotechnischen HF-Ansatzes (aus: Miller et al. 1997, S. 2)

Zu den bisher genannten Einflußfaktoren Technik, Organisation und Person/Individuum werden hier also zwei weitere ergänzt:

Gruppe: Dort werden gruppenspezifische Einflußfaktoren wie Gruppendruck und soziale Arbeitsbedingungen angesiedelt.

Organisationsumwelt: Dieses Subsystem bezeichnet alles das, was außerhalb der Organisation zur Zielgröße „Sicherheit“ beiträgt: Fremdfirmen, Gutachter, Aufsichtsbehörden

Die Zusammenhänge zwischen den drei Hauptfaktorenbereichen werden in der Literatur häufig über das Informationsmodell dargestellt (siehe z.B. Eisgruber 1997), das von den Aufgaben des Menschen ausgeht:

**Wahrnehmen** (Informationsaufnahme) → **Denken** (Verarbeitung) → **Handeln** (Informationsumsetzung)

und daraus das Arbeitsgebiet „Human Factors“ ableitet (vgl. Abbildung 3-2).

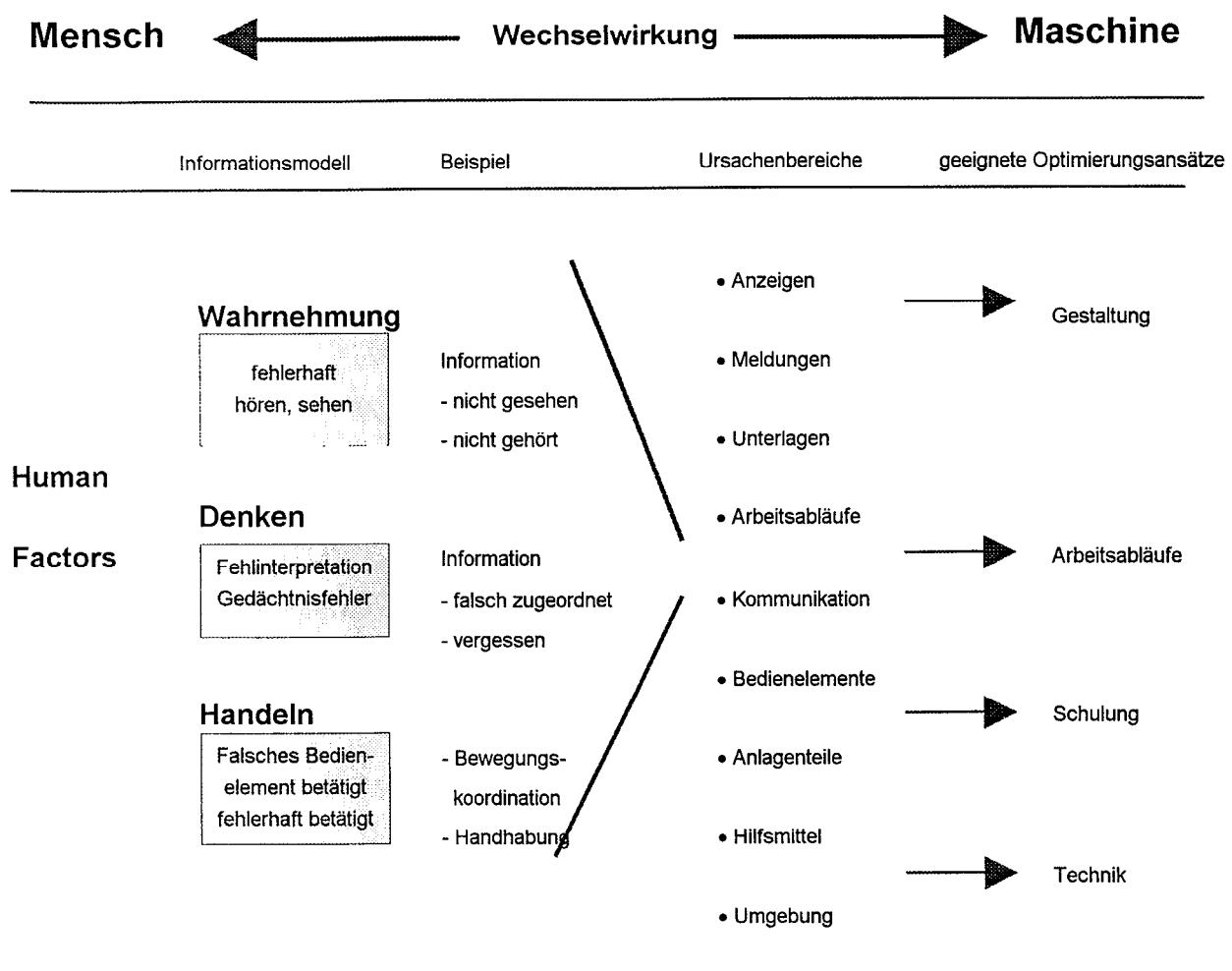


Abb. 3-2: Arbeitsgebiet: „Human Factors“ (aus: Eisgruber 1997, S. 4)

## 4. Beispielhafte Regelungen in Unternehmen

Das Thema „Vermeidung von Fehlbedienung“ gewinnt erst in jüngerer Zeit Bedeutung in den Unternehmen der Chemischen Industrie. Viele Bereiche der Human Factors tauchten zwar immer einmal implizit in den Sicherheitsphilosophien, in Werkrichtlinien, in den internen Schulungsinhalten der Unternehmen auf, wurden jedoch kaum systematisch unter der Zielsetzung „Bediensicherheit“ verfolgt. Um in Rahmen des Projektes möglichst aktuelle Entwicklungen in den Unternehmen zu erfassen, wurden Gespräche mit für die Anlagensicherheit Verantwortlichen in großen Chemieunternehmen geführt.

Nachfolgend sind allgemeine Erkenntnisse aus den Unternehmen (Kapitel 4.1) sowie jeweilige Besonderheiten aus den Einzelunternehmen (Kapitel 4.2) zusammengestellt.

### 4.1 Allgemeine Erkenntnisse aus den Gesprächen zum Umgang der Unternehmen mit dem Thema „Bediensicherheit“

Aus den durchgeführten Gesprächen wurde insbesondere deutlich, daß Unternehmen, die überwiegend **kontinuierliche Anlagen** betreiben, einen anderen – in der Regel weniger expliziten – Umgang mit dem Thema „Bediensicherheit“ zeigen als die Unternehmen, die eher Batch-Anlagen oder Vielzweckanlagen betreiben (vgl. Tab. 4-1). Dies liegt grundsätzlich darin begründet, daß Konti-Anlagen mit wenig Personal, aber viel **Prozeßleittechnik (PLT)** gefahren werden, Vielzweckanlagen dagegen mit viel Bedienungsaufwand und wenig (teurer) Automatisierungstechnik.

In keinem der befragten Unternehmen konnte festgestellt werden, daß bei der Planung der Anlage explizit geprüft wird, ob der Bediener die an ihn gestellten Anforderungen nach der Fahrvorschrift nach menschlichen oder sogar individuellen Leistungsgrenzen überhaupt erfüllen kann. Zwar kommt es vor, daß eine verantwortliche Person im Verlauf der Planungsphase die Fahrvorschrift in ein Ablaufschema übersetzt und damit bildlich zumindest extreme Überlastungen des Bedieners in bestimmten Produktionsphasen erkennen kann, doch erfolgt bereits dies nicht regelmäßig oder nach unternehmensinternen Maßgaben (Richtlinien, Vorschriften o.ä.). Wenn es überhaupt geschieht, dann auch nur für den bestimmungsgemäßen Betrieb. In keinem Gespräch konnte erkannt werden, daß die Unternehmen in irgendeiner Phase der Planung oder des Betriebes genauer die Bedienanforderungen im nicht-bestimmungsgemäßen Betrieb erfassen oder gar bewerten nach „ausführbar“ oder „nicht ausführbar“.

Die Bedienkonzeption als Teil der Sicherheitskonzeption ist in den befragten Unternehmen eher als grobe Leitlinie erkennbar, aber weniger in konkreten Vorschriften. Diese umfaßte bisher überwiegend Schulung in fachlicher Hinsicht, nicht jedoch z.B. in psychologischer (Umgang mit Stress/Umgang mit Ermüdung) oder kommunikativer Hinsicht (Gruppenatmosphäre, Austausch im Team).

Tab. 4-1: Unterschiede zwischen Batch-Anlagen und Konti-Anlagen mit Bedeutung für die Strategie zur Vermeidung von Fehlbedienung (z.T. in Anlehnung an BVCT 1999)

Konti-Anlage	Batch-Anlage
<ul style="list-style-type: none"> <li>– wenige Mitarbeiter</li> <li>– hoher Automatisierungsgrad/hoher PLT-Aufwand</li> <li>– hoher Stoffdurchsatz</li> <li>– Bedienung und Beobachtung in zentralen Leitwarten</li> <li>– überwiegend spezialisiertes Personal (<u>nur</u> Meßwarte oder <u>nur</u> in der Anlage)</li> <li>– Arbeitsintensität über größere Zeiträume (→ Problem der Unterforderung) entweder sehr groß oder sehr klein</li> <li>– sehr große Anlagen- und Bedienbereiche pro Bedienperson</li> <li>– komplexe Vernetzung (Beeinflussung durch vor- und nachgeschaltete Bereiche)</li> <li>– Der Bediener muß bei einer Störung oft sehr schnell, ohne Möglichkeit der Rücksprache mit dem Schichtleiter reagieren</li> </ul>	<ul style="list-style-type: none"> <li>– hoher Bedienungsaufwand</li> <li>– geringer Automatisierungsgrad</li> <li>– geringe Kapazität</li> <li>– Bedienung und Beobachtung vor Ort bzw. in unmittelbarer Nähe der Meß- und Stellorte</li> <li>– gleichwertige Arbeitsaufgaben in der Anlage und am Bedienplatz</li> <li>– Arbeitsintensität eher gleichmäßig</li> <li>– gut überschaubare, begrenzte Anlagen</li> <li>– Beeinflussungen durch vor bzw. nachgeschaltete Bereiche sind meist nicht gegeben</li> <li>– Der schrittweise Prozeß erlaubt auch in kritischen Situationen in der Regel noch Kommunikationsphasen</li> </ul>

Noch sehr wenig angesprochen werden die menschlichen Faktoren

- physiologische Leistungsgrenzen,
- Reaktionsmuster in Notfallsituationen,
- Gruppendynamik,
- Umgang mit dem Hierarchiegefüge.

In den Gesprächen wurde aber zunehmend die Erkenntnis geäußert, daß die **Arbeitsatmosphäre** und das **zwischenmenschliche Verhältnis** zwischen Betriebsleitung und Betriebspersonal für ein zuverlässiges Bedienverhalten für wichtig gehalten wird. Es wurden auch Zielvorstellungen wie „Identifikation mit dem Betrieb“ geäußert, die die Zuverlässigkeit der Mitarbeiter mitbeeinflussen. Die Erkenntnis hat jedoch noch nicht dazu geführt, daß in diesem Bereich gezielt interviewt, analysiert oder gefördert wird. Ansätze hierzu finden sich lediglich in dem noch recht neuen Begriff „**Sicherheitskultur**“.

Generell ist in den Gesprächen deutlich geworden, daß das Thema „**Bediensicherheit**“ zwar zunehmend bewußter als Planungs- und Strategiebereich im Rahmen der Anlagensicherheit erkannt wird, daß jedoch echte Vorschriften, insbesondere zum systematischen Umgang mit dem

Faktor Mensch noch weitgehend fehlen. Lediglich im Nacharbeiten von Ereignissen sind vielversprechende Ansätze zur Verbesserung der Bediensicherheit erkennbar.

## 4.2 Besonderheiten in den einzelnen befragten Unternehmen

### Unternehmen 1

Dieses Unternehmens betreibt eher große Anlagen, mit hohen Stoffdurchsätzen und hohem Automatisierungsgrad. Es erfolgt bisher kein systematischer Zugang zur Bediensicherheit. Bediensicherheit ist im wesentlichen Angelegenheit des einzelnen Betriebes – nicht die der zentralen Sicherheitsabteilung. Gezielte Maßnahmen zur Verbesserung der Bediensicherheit sind:

- Aus- und Weiterbildung,
- Einbau manueller Schaltvorgänge, um die Aufmerksamkeit des Bedieners zu erhalten,
- Simulationstrainings (Simfactory): Bisher erst testweise eingeführt, wird wohl zukünftig vor allem von jüngeren Mitarbeitern stärker genutzt werden,
- in Einzelfällen: Einschaltung des Betriebspyschologen,
- Herausgabe von „Learning lessons“: Dort werden konzernweit Hintergründe von sicherheitsrelevanten Ereignissen erläutert, um daraus für zukünftiges Sicherheitsverhalten zu lernen.

Ansonsten erfolgt keine weitere Beschäftigung mit dem Thema. Die Grundtendenz geht eher in Richtung weiter zunehmender Automatisierung, mit dem Ziel, daß der Bediener allenfalls noch kleinere Ereignisse durch Fehlbedienung hervorrufen kann.

Problematisiert wurde im Gespräch die hohe Anzahl von gesetzlich notwendigen **Betriebsanweisungen** (ca. 30 bis 50 pro Betrieb). Es erfolgt bisher jedoch keine zentrale Sichtung der Betriebsanweisungen, um sie z.B. auf Durchführbarkeit zu prüfen.

Auf Nachfrage könnte man es sich durchaus vorstellen, daß es sinnvoll ist, die Bedienanforderungen in geeigneter Form darstellbar zu machen.

### Unternehmen 2

Bediensicherheit ist für die Vielzweckanlagen dieses Unternehmens, in denen mit derselben Anlagenkonfiguration wechselnde (in einer Anlage bis zu 20-25) Rezepturen gefahren werden, ein wichtiges Thema. Deshalb findet sich in den unternehmensinternen Hinweisen zur Anlagenplanung auch ein expliziter Bereich „Bediensicherheit“.

Das Unternehmen hat 1997 ein internes Programm „Sicheres Verhalten“ aufgelegt, das im Oktober 1999 aktualisiert wurde. Dieses Programm besteht aus fünf Bausteinen:

1. Die Befragung (Zwei Fragen werden gestellt: als erstes sind die Tätigkeiten, von denen im eigenen Arbeitsbereich Gefährdungen ausgehen können, zu nennen; als zweites sind die Werkzeuge und Hilfsmittel, die gefährlich sein können, zu nennen).
2. Die Auswertung (Alle Fragebögen eines Betriebes oder einer Abteilung werden ausgewertet nach genannten Schwerpunktgefahrenbereichen und ggf. unterschiedlichen Sichtweisen von Gefahren).
3. Die Projektgruppe (Neben Sicherheitsfachkräften und Betriebsleitern sind hier auch das Bedienpersonal und Arbeitnehmervertreter eingebunden).
4. Das Kurzgespräch (Der Betriebsleiter oder der Betriebssicherheitsbeauftragte führt Kurzgespräche mit dem Mitarbeiter über ausgewählte Gefahrenpunkte).
5. Das Review (Regelmäßige Rückschau, inwieweit das Programm zu verbessern ist).

Das Programm ist inzwischen in den meisten Betrieben des Unternehmens durchgeführt worden. Ansonsten wird großer Wert auf gut geschultes Personal und klare Produktionsvorschriften gelegt. Auf Nachfrage wurde es als sinnvoll bezeichnet, durch eine geeignete Dokumentationsform den Ort kritischer Bedienhandlungen erkennen zu können. Bei den Vielzweckanlagen eignet sich das **Rohrleitungs- und Instrumentenschema** (R-I-Schema nach DIN 28004 bzw. DIN 19227) jedoch nach Ansicht unserer Gesprächspartner eher nicht dafür.

### Unternehmen 3

Der unternehmensinternen Richtlinie „Sicherheitsmaßnahmen bei der Änderung in und an Anlagen, Arbeitsweisen und Verfahrensabläufen sowie bei der Durchführung von Instandhaltungsarbeiten“ sind implizit Hinweise zur Bediensicherheit zu entnehmen. Unter anderem werden in Form einer Beispielsammlung ggf. sicherheitsrelevante Arbeitsweisen/Verfahrensabläufe beschrieben, die nach einem bestimmten Schema genauer zu prüfen sind. Darüber hinaus wird in jüngerer Zeit zunehmend bei sicherheitsbedeutsamen Ereignissen eine systematische Ereignisanalyse durchgeführt, die die drei HF-Bereiche

- personenbezogene Faktoren,
- organisatorische Faktoren und
- technische Faktoren

systematisch und umfassend erfaßt.<sup>3</sup>

Wie Unternehmen 1 läßt auch Unternehmen 3 „Lern- und Erfahrungsreports“ erstellen, wodurch alle Mitarbeiter aus geschehenen Ereignissen sicherheitsgerechtes Verhalten lernen sollen. Daraus werden dann auch angepaßte Schulungspläne zusammengestellt. So ergab sich aus bestimmten Ereignistypen für das Jahr 1999 das Schwerpunktthema „Handhabung hochaktiver Substanzen.“

<sup>3</sup> Das Unternehmen war an dem UBA-Projekt „SOL – Sicherheit durch organisationales Lernen“ beteiligt.

Ein Ansatz zu einer prüfbaren Darstellung der Bedienanforderung besteht in der Kennzeichnung einer sicherheitsgerichteten Wartenfahrerfunktion durch "(Z)", die in den Gesprächen zur Sicherheitsanalyse speziell problematisiert werden muß. Die Darstellung erlaubt jedoch noch nicht das Erkennen gleichzeitiger Bedienanforderungen und berücksichtigt auch nicht Handlungsanforderungen in nicht-bestimmungsgemäßen Situationen.

#### Unternehmen 4

Das Unternehmen betreibt zahlreiche große Anlagen mit großen Stoffumsätzen und hohem Vernetzungsgrad verschiedener Anlagen. Der Automatisierungsgrad der Anlagensteuerung ist hoch.

Der Sicherheit wird unternehmensweit ein hoher Stellenwert zugemessen. Dabei steht der Arbeitsschutz im Vordergrund. Es gibt eine Reihe von Sicherheitsprogrammen, in die teilweise auch Fremdfirmen eingebunden sind. Hier ist insbesondere das ausgefeilte Berichtssystem zum Lernen aus Erfahrungen mit Unfällen und Störungen zu nennen, das auch **Beinahe-Ereignisse** und **Ereignisse ohne negative Folgen** umfaßt. Ziel des Berichtssystems ist die Identifikation von Schwachstellen zur Erhöhung der Arbeits- und Anlagensicherheit sowie der **Anlagenverfügbarkeit**. Die Meldungen erfolgen freiwillig, weitgehend formlos und anonym. Die erarbeiteten Erfahrungsberichte sind allen Werken des Unternehmens zugänglich. Die Akzeptanz seitens der Mitarbeiter ist hoch, das Berichtssystem wird allgemein als nützlich und sinnvoll angesehen.

Es werden unternehmensweit sicherheitsbezogene Ziele definiert, deren Erreichung über ein Bonussystem für die Mitarbeiter gehaltsrelevant ist.

Hinsichtlich der Bedienung der Anlagen ist festzuhalten: Aufgrund des hohen Vernetzungsgrades im Produktionsverbund laufen in der Warte Anforderungen verschiedener Anlagen (einschl. Wasserversorgung und Reststoffverbrennung) zusammen. Im Alltag steht für das Bedienungspersonal im Vordergrund, die Anforderungen der verschiedenen Anlagen in Einklang zu bringen. Das Augenmerk richtet sich dabei insbesondere auf die Zielgröße Produktqualität, sowie auf die Anlagenverfügbarkeit. Dabei befindet sich das Bedienungspersonal im Spannungsfeld zwischen Anlagenverfügbarkeit und Sicherheit, wobei die Sicherheit letztlich Vorrang hat.

Besondere Streßsituationen für das Bedienungspersonal ergeben sich aus An- und Abfahrvorgängen, Änderungen der Prozeßparameter und nicht-bestimmungsgemäßen Betriebszuständen. Komplexere planmäßige Vorgänge sollten aus Sicht des Bedienungspersonals möglichst nicht nachts durchgeführt werden.

Insgesamt kann festgehalten werden, daß in dem Unternehmen eine weitreichende Sicherheitskultur gepflegt wird. Das Thema "Bediensicherheit" im Sinne dieser Untersuchung bleibt als solches jedoch weitgehend ausgeklammert.

### Schlußfolgerungen aus der Betrachtung der Einzelfälle

- Unternehmen, die überwiegend kontinuierliche Anlagen betreiben, zeigen in der Regel weniger expliziten Umgang mit dem Thema "Bediensicherheit" als Betreiber von Batch- oder Vielzweckanlagen.
- In der Regel erfolgt keine Prüfung der an den Bediener gestellten Anforderungen hinsichtlich der Erfüllbarkeit (im Hinblick auf menschliche Leistungsgrenzen).
- Das Thema "Bediensicherheit" gelangt zunehmend in das Bewußtsein der Unternehmen der chemischen Industrie. Allerdings erfolgt die Umsetzung der Erkenntnisse in der Praxis noch zögerlich. Vielversprechende Ansätze zur Verbesserung der Bediensicherheit existieren in der nachträglichen Aufarbeitung von Ereignissen.
- Die Instrumente zur Vermeidung von Störfällen/Störungen sind identisch mit den Instrumenten zur Gewährleistung der Produktqualität und der Anlagenverfügbarkeit. Erst im Augenblick des Eintritts einer Störung muß die klare Priorität bei Arbeitsschutz und der Vermeidung von Emissionen liegen.
- Es existiert eine Fülle von Regelungen, die sich in zahlreichen Betriebsanweisungen für das Bedienungspersonal niederschlägt. Es ist darauf zu achten, daß diese nicht mit dem Abheften als erledigt betrachtet werden. Wichtig ist auch die regelmäßige Revision der Betriebsanweisungen: Sie sind in Gesamtheit regelmäßig zu sichten auf Vollständigkeit, Redundanz und Widerspruchsfreiheit. Es ist stets nur die aktuelle Version vorzuhalten.

## 5. Analyse vorhandener Regelwerke im Hinblick auf Bediensicherheit<sup>4</sup>

### 5.1 Verordnungen und Richtlinien

#### EG-Richtlinie 96/82/EG zur Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen ("SEVESO II-Richtlinie") vom 9. Dezember 1996

In Artikel 7 der Richtlinie ("Konzept zur Verhütung schwerer Unfälle) ist unter anderem ausgeführt: "Mit dem vom Betreiber vorgesehenen Konzept ... soll durch geeignete Mittel, Organisation und Managementsysteme ein hohes Schutzniveau für Mensch und Umwelt sichergestellt werden". Bediensicherheit ist damit als Bestandteil der menschlichen Faktoren unter Organisation und Management subsummiert. In Artikel 8 und 9 wird von "Sicherheitsmanagement" gesprochen, das genauso die Bediensicherheit implizit enthält. Die nach Umsetzung der Seveso II-Richtlinie in der neuen Störfall-Verordnung neuzfassenden StörfallVwV sollten deshalb explizit auf den Aspekt Bediensicherheit eingehen.

#### Störfallverordnung (Zwölfta Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes – 12. BImSchV)

Die Änderung der Störfallverordnung vom 20. September 1991 durch Verordnung vom 26. April 2000 dient der Umsetzung der Seveso-II-Richtlinie in nationales Recht. In der neuen Störfallverordnung heißt es unter § 6 Absatz 1 :

*"Der Betreiber hat zur Erfüllung der sich aus § 3 Abs. 1 oder 3 ergebenden Pflichten über die in den §§ 4 und 5 genannten Anforderungen hinaus [...]"*

3. *die erforderlichen sicherheitstechnischen Vorkehrungen zur Vermeidung von Fehlbedienungen zu treffen,*
4. *durch geeignete Bedienungs- und Sicherheitsanweisungen und durch Schulung des Personals Fehlverhalten vorzubeugen."*

Es ist derzeit noch nicht absehbar, wann und in welcher Form die bestehenden Verwaltungs vorschriften zur alten Störfall-Verordnung an die novellierte Störfall-Verordnung angepaßt werden.

<sup>4</sup> Die nachfolgenden Ausführungen basieren teilweise auf einer vom Umweltministerium Brandenburg in Auftrag gegebenen Studie (Beiträge zur Störfallvorsorge im Land Brandenburg, Müller 1998). Die Autoren danken dem Land Brandenburg für die Erlaubnis zur Verwendung der Ergebnisse im Rahmen dieser Untersuchung.

In den alten Verwaltungsvorschriften fehlt es an Hinweisen oder einer Anleitung (vergleichbar einer technischen Regel), was unter der in der alten Störfall-Verordnung geforderten "Sicherung gegen Fehlbedienung" zu verstehen ist und wie man dazu vorgeht.

Die logische Konsequenz ist, daß es bisher praktisch keine Sicherheitsanalyse gibt, in der die Sicherung gegen Fehlbedienung konkret und belastbar dargestellt ist, und daß diese Frage bei der behördlichen Prüfung der Sicherheitsanalyse de facto keine Rolle spielt.

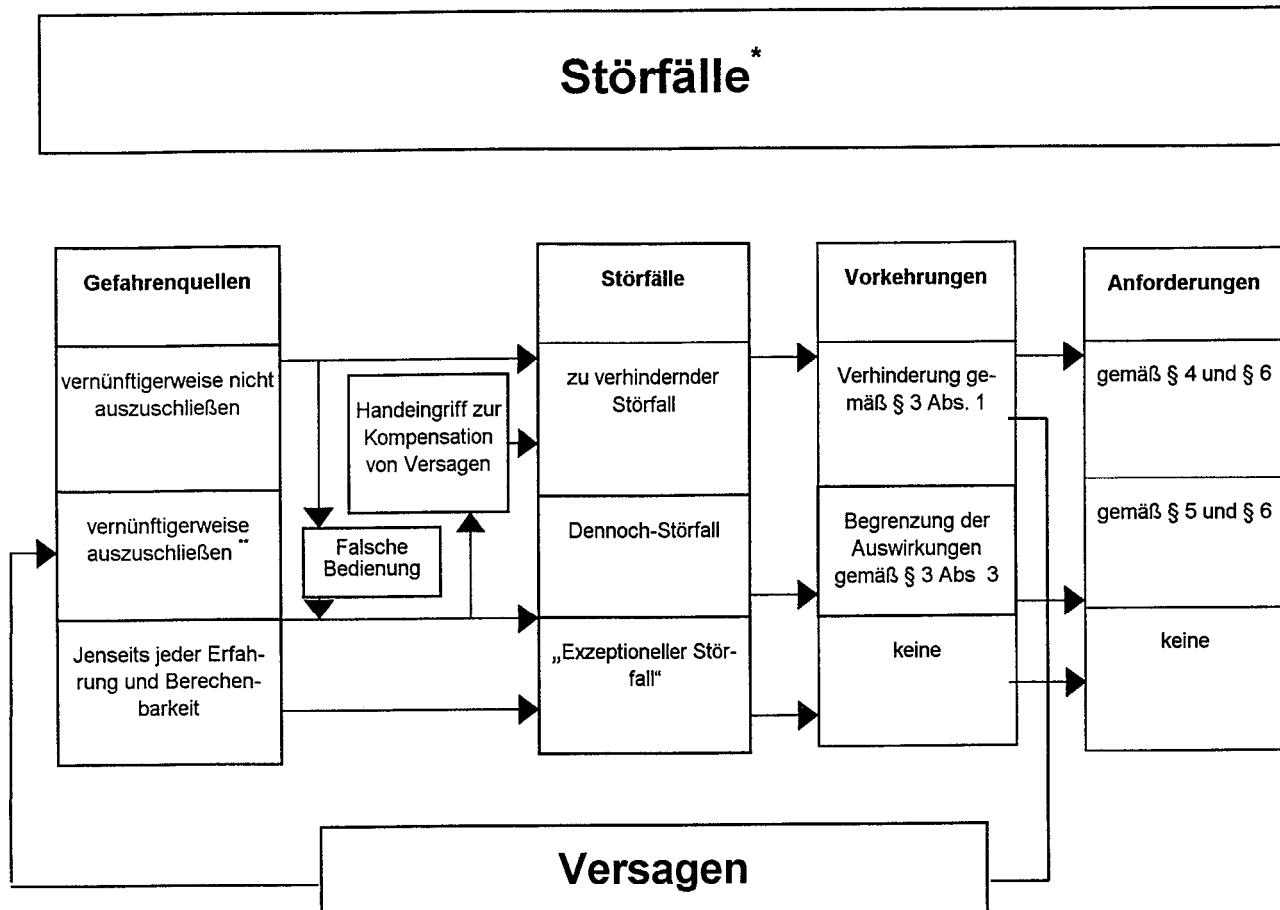
Ein Antrag des Landes Brandenburg im Unterausschuß Anlagensicherheit des Länderausschusses für Immissionsschutz (LAI), bei der Prüfung von Sicherheitsanalysen verstärkt nach der Darlegung einer Bedienkonzeption zum Nachweis der Sicherung gegen Fehlbedienung zu fragen, wurde abgelehnt, da ohne eine verbindliche oder akzeptierte Handlungsanleitung zum methodischen Vorgehen kein Vollzug möglich sei. Der Unterausschuß "Anlagensicherheit" des Länderausschusses für Immissionsschutz hat deshalb in seiner 19. Sitzung am 16./17. Dezember 1997 den Wunsch nach einem entsprechenden Leitfaden artikuliert (Tagesordnungspunkt 8.1).

Bedarf zur Präzisierung der Vorkehrungen gegen Fehlbedienung besteht auch nach der Novellierung der Störfallverordnung. Die Ergebnisse dieses Projekts können Anregungen dazu liefern (siehe Kapitel 9).

#### Klassifikation der Störungen und Störfälle (vgl. Abbildung 5-1)

Das deutsche Störfallrecht unterscheidet nach 12. BlmSchV § 3 Abs. 1 in „vernünftigerweise nicht auszuschließende Störfälle“, zu denen Maßnahmen zur Verhinderung vorzusehen sind und nach § 3 Abs. 3 „vernünftigerweise auszuschließende Störfälle, für die Maßnahmen zur Begrenzung der Auswirkungen vorzusehen sind“ (vgl. Abb. 4). Im Gesetzes- und Regelwerk sind diese zwei parallele Zweige. Durch die Bedienung entstehen Übergänge zwischen diesen beiden Zweigen:

- Einerseits können durch vermeidbare Bedienfehler (abhängig von Motivation, Qualifikation, Training usw.) Störungen, die nur einen zu verhindernden Störfall nach sich ziehen sollten, in einen vernünftigerweise ausgeschlossenen Störfall überführt werden.
  - Andererseits kann durch den Bedieneingriff der vernünftigerweise auszuschließende Ausfall einer Sicherheitseinrichtung kompensiert werden. Qualifizierte und aufmerksame Bedienung kann einen sich anbahnenden Dennoch-Störfall in einen zu verhindernden Störfall überführen.
- In diesem Sinne sollte der Mensch im Störfallrecht sowohl als „Risikofaktor“ wie auch als „Sicherheitsfaktor“ berücksichtigt werden.



\* erweitert nach AK-Dennoch-Störfälle der SFK

\*\* nicht für möglich gehalten = nicht daran gedacht

Abb. 5-1: Störfälle im Sinne der StörfallV (Müller 1998)

Die bisherige 2. StörfallVwV geht an anderen Stellen auf die Automatisierungseinrichtungen ein. Es entsteht deutlich der Eindruck, daß Bedienung bei automatisierten Anlagen als Hand-Automatik-Umschaltung zu Regelkreisen und Steuerketten gesehen wurde. Solche Informationsstrukturen werden normalerweise dekomponiert entworfen, dabei wird die Bedienbarkeit des jeweils betrachteten einzelnen Informationskanals gesehen. Die objektiven Probleme des möglichen Informationsverarbeitungsbedarfs durch die Gleichzeitigkeit von Bedienanforderungen wird bisher nicht gesehen. Diese unvollständige Betrachtungsweise schließt noch ein anderes Problem ein: Durch den Einzug der Mikrorechentechnik in die Automatisierungsausrüstungen stieg die Zuverlässigkeit der Geräte rapide an. Die Fahrweise eines Regelkreises von Hand zur Überbrückung von Geräteausfällen ist dadurch **keine typische Bedienhandlung** mehr, also kein geübtes und abrufbares Verhaltensmuster.

Wichtig ist, daß sich die Erkenntnis durchsetzt, daß die Bedienkonzeption nicht nur dem Normalbetrieb standzuhalten hat, sondern insbesondere auch im Störbetrieb den Bediener nicht an seine menschlichen Leistungsgrenzen bringt (⇒ Informationsüberlauf, ⇒ Gleichzeitigkeitsproblem).

## Weitere immissionsschutzrechtliche Regelungen

- Verordnung über **Immissionsschutz- und Störfallbeauftragte** (5. BlmSchV): Hinsichtlich der geforderten Fachkunde (vgl. § 7 in Verbindung mit Anhang II) findet sich kein Hinweis auf notwendige Kenntnisse zur Vermeidung von Fehlbedienung. Vom Störfallbeauftragten wird lediglich ein Teilespekt, nämlich Kenntnisse zur betrieblichen Sicherheitsorganisation gefordert.
- Verordnung über das **Genehmigungsverfahren** (9. BlmSchV): In den in § 4 geforderten Antragsunterlagen ist die Darstellung der Bedienkonzeption oder des Konzeptes zur Vermeidung von Fehlbedienung nicht (auch nicht indirekt) aufgeführt. Sie ist allenfalls unter dem Begriff „Angaben über die organisatorischen Vorkehrungen“ zur Störfallvorsorge (vgl. § 4b der 9. BlmSchV) zu erahnen.
- Verordnung zum Schutz vor gefährlichen Stoffen (**Gefahrstoffverordnung**, GefStoffV): Die GefStoffV dient explizit dem Schutz von Mensch und Umwelt gegen stoffbedingte Schädigungen. Sie fordert insofern zahlreiche Schutzmaßnahmen, die direkt oder indirekt auf die Vermeidung von Fehlern bzw. eine Begrenzung ihrer Auswirkungen beim Umgang mit Gefahrstoffen abzielen: Kennzeichnungspflicht (§§ 6 bis 9), Verpackung (§ 10), Sicherheitsdatenblatt (§ 14), Betriebsanweisung (§ 20).

## Leitgrundsätze für den Chemieunfall, Verhütung, Vorsorge und Bekämpfung herausgegeben von der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung OECD/GD (92)43

Unter B.5.44 ist ausgeführt: „Besondere Aufmerksamkeit sollte der Rolle der Human Factors in der Unfallverhütung in genehmigungsbedürftigen Anlagen zukommen, da anerkannt werden muß, daß gelegentlich menschliches Versagen auftreten kann und daß die Mehrzahl der Unfälle irgendwie auf menschliche Fehler zurückzuführen sind. Darunter verstehen wir menschliches Handeln, das unbeabsichtigt Schwachpunkte in Ausrüstung, Verfahren, Systemen und/oder der Organisation ausnutzt.“

- ➔ Bei der Planung aller Konstruktions-, Entwicklungs-, Betriebs-, Wartungs-, Stilllegungs- und Abbauphasen einer genehmigungsbedürftigen Anlage sollte der Betreiber das mögliche Auftreten menschlichen Versagens ins Auge fassen, damit seine Auswirkungen abgemildert werden können.
- ➔ Der Human Factor sollte bei Erkennung und Bewertung von Gefährdungen mitberücksichtigt werden.
- ➔ Der Human Factor, einschließlich der positiven und negativen Aspekte des menschlichen Verhaltens, gilt für alle Beschäftigten einer genehmigungsbedürftigen Anlage, einschließlich Geschäftsführung und Fremdfirmen.

Die OECD-Expertengruppe für Chemieunfälle aktualisiert die Leitgrundsätze in Auswertung des Workshops München 1997. Themen sind dabei:

- Menschliche Zuverlässigkeit generell
- Sicherheitskultur
- Entwurf gefährlicher Anlagen einschließlich Konzepte zur inhärenten Sicherheit
- Bedienpraxis und -prozeduren
- Bedienerqualifikation und -fähigkeiten
- Regulierung und Zustimmung
- Interne und externe Kommunikation.

(Beschluß des 8. Treffens, Paris, 2. bis 4.12.98).

**Gesetz über die Durchführung von Maßnahmen des Arbeitsschutzes zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Beschäftigten bei der Arbeit (Arbeitsschutzgesetz – ArbSchG)**

Um Irrtümern vorzubeugen ist festzustellen, daß der Begriff "Bediensicherheit" im Arbeitsschutz bisher anders gebraucht wurde als bei der Störfallvorsorge, nämlich im Sinne von Schutz vor Verletzungen durch sich bewegende Teile einer zu bedienenden Maschine. Deshalb liefert das gleiche Stichwort für die hier zu behandelnde Thematik nur indirekt Beiträge.

### TRGS 300 – Sicherheitstechnik

Die TRGS 300 (in der Fassung vom 15. April 1995)<sup>5</sup> beschreibt eine Methode zur systematischen Sicherheitsbetrachtung an Anlagen, bei Verfahren und Arbeitsverfahren mit technischen Arbeitsmitteln. Sie soll als Basisregel für Gremien gelten, die sich mit der Weiterentwicklung sicherheitstechnischer Regeln befassen.

In den Sicherheitsgrundsätzen findet sich jedoch wiederum nur die allgemeine Anforderung „Sichern gegen Fehlhandlungen“. Anhang 2 der TRGS 300 konkretisiert zwar etwas diese allgemeine Anforderung („Anwendung ergonomisch/psychologisch geeigneter Arbeitsmethoden“, „Benutzerfreundliche Anordnung von Funktionselementen“, „Betriebsanweisungen/-unterweisungen unter besonderer Berücksichtigung von An- und Abfahrvorgängen, Probefahrt etc.“, „Sicherstellung von Ausbildung, Schulung und Training“).

- In den ausgearbeiteten Beispielen dazu fehlen genauere Vorstellungen, wie diese Anforderungen auszufüllen sind.

<sup>5</sup> Vgl. R 27 der Schriftenreihe der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin.

## 5.2 Internationale Regelungen

### Frankreich

In Frankreich wurde die Seveso II-Richtlinie durch den Erlass (Arrêté) vom 10. Mai 2000 implementiert. Dieser schreibt die Einführung von Maßnahmen zur Verringerung des Unfallrisikos und zur Minimierung der potentiellen Auswirkungen eines Störfalls vor. Dazu muß der Anlagenbetreiber

- eine Politik zur Vermeidung von Unfällen definieren und umsetzen und deren Erfüllung durch Kontrollen sicherstellen
- das Personal angemessen schulen und
- Sicherheitsmanagementsysteme einführen.

Es ist ein der Präfektur vorzulegender Sicherheitsbericht zu erstellen sowie Studien über potentielle Gefahren durchzuführen. Das Sicherheitsmanagementsystem muß Informationen zu

- Maßnahmen zur Schulung des Personals
- Organisatorische Maßnahmen
- Identifizierung und Bewertung der Risiken
- Prozeduren für alle Betriebsphasen (Wartung, Anfahren, Betrieb, usw.)
- Management von betrieblichen Veränderungen
- Notfallpläne
- Unfällen und Störfällen

enthalten.

Durch den Erlass werden die Anforderungen der Seveso II-Richtlinie erfüllt. Der menschliche Faktor wird darin nicht explizit berücksichtigt, sondern implizit als Bestandteil des Sicherheitssystems betrachtet.

### Großbritannien

Die COMAH-Regelungen (Control Of Major Accidents and Hazards Regulations) vom 11. März 1999 traten am 1. April 1999 in Kraft und implementierten die Seveso-II-Richtlinie. Es wird dabei zwischen sogenannten „lower tier“ und „upper tier“ Anlagen unterschieden. Maßgeblich dafür sind die Mengen gelagerter und verarbeiteter gefährlicher Stoffe.

Bei „Lower tier“ Anlagen muß der sichere Betrieb der Anlage nachgewiesen werden. Außerdem müssen die zuständigen Behörden (Environmental Agency und Health and Safety Executive, HSE) über die Aktivitäten sowie über die Mengen gefährlicher Stoffe, die in der betreffenden Anlage gelagert, produziert und behandelt werden, informiert werden. Ein Unfallvorsorgekonzept

mit definierter Organisation und Plänen muß den zuständigen Behörden zur Genehmigung vorgelegt werden.

„Upper Tier“ Anlagen müssen denselben Anforderungen genügen und darüber hinaus einen Sicherheitsbericht und einen Notfallplan vorlegen, lokale Behörden und Notdienste informieren und Anweisungen für die Anwohner über das Verhalten bei Störfällen vorbereiten.

Neben diesen Bestimmungen der COMAH muß die HSE zur Erfüllung der Seveso II-Richtlinie eine Störfall-Datenbank erstellen. Der Aspekt der Bediensicherheit wird in den COMAH-Regelungen erwähnt (Schedule 2, Regulation 5(3)). Darin heißt es:

*„Folgende Punkte sollten bei den Sicherheitsmanagementsystemen berücksichtigt werden:*

*(...)*

*(c) Bediensicherheit – Annahme und Umsetzung von Prozeduren und Anweisungen für einen sicheren Betrieb, einschließlich der Wartung von Anlagen, Prozessen, Betriebsmaterial und Stillstandphasen.“*

Die Anforderungen der COMAH-Regelung werden in einem Bewertungshandbuch (Assessment Manual) präzisiert und das allgemeine Prinzip „Unfallrisiken sollten identifiziert, um alle nötigen Maßnahmen zur Vorbeugung und zur Minimierung etwaiger Konsequenzen getroffen werden“ zu operationalisieren.

Der Human Factor wird im COMAH Safety Report Assessment Manual (Part 2, Chapter 3 - Predictive Aspects, Criterion 3.1.1) explizit als Beurteilungskriterium genannt: „*Es sollte sicher gestellt werden, daß HF bei der Risikobewertung berücksichtigt wurden.*“ Ferner heißt es:

*„Das Betriebspersonal ist ein wichtiger Bestandteil von Sicherheitssystemen. Es kann aber auch infolge eines Bedienfehlers einen Störfall auslösen. Die Rolle, die das Anlagenpersonal bei der Kontrolle von Risiken und Gefahren spielt, sollte individuell festgestellt werden und die Folgen eines Fehlers bei der Ausübung der Kontrollfunktion analysiert werden, so daß eine Priorität der unterschiedlichen Funktionen abgeleitet werden kann.“*

*Zum Beispiel kann der Betriebsplan vorsehen, daß ein Angestellter gewisse Aktionen nach dem Auslösen eines Alarmsignals unternimmt. In diesem Fall müssen im Rahmen der Risikoanalyse Annahmen über die Wahrscheinlichkeit einer Fehlbedienung getroffen werden. Diese Aufgabe kann kritisch sein, falls ein hohes Maß an menschlicher Zuverlässigkeit vorausgesetzt werden muß, um die Risiken so gering wie möglich zu halten. In diesem Fall können automatische Kontroll- und Schutzmechanismen erforderlich sein, um die Abhängigkeit vom Human Factor zu reduzieren. Die nötige Redundanz und Diversität muß im System vorhanden sein, damit die erforderliche Zuverlässigkeit erreicht werden kann. Diese wird von den zu erwartenden Gefahren und Risiken abhängen.“*

*Das Bedienpersonal muß gut ausgebildet, kompetent und motiviert sein. Die Anlage muß so konzipiert sein, daß menschliche Fehler (routinemäßige unbeabsichtigte Fehler, Fehlentscheidungen und Nichtbeachten der Regeln) minimiert werden.“*

Weiterhin finden sich im Bewertungshandbuch folgende Anweisungen:

- Kriterium 3.3.2: "Die Methoden zur Evaluierung der Risiken müssen offen gelegt werden. Insbesondere muß die Methodik zur Bestimmung von Wahrscheinlichkeiten oder Sequenzen von Ereignissen (inklusive Identifizierung und Analyse des HF) beschrieben werden."
- Kriterium 3.4.1: "Der Sicherheitsbericht sollte beweisen, daß Ereignisse und Kombinationen von Ereignissen, die zu grösseren Unfällen führen könnten, systematisch identifiziert wurden. Alle denkbaren Unfallursachen sollten betrachtet werden. Einsichten, die bei der Analyse von Störfällen und Unfällen gewonnen werden, können dafür eine gute Basis darstellen. Wenn eine Folge oder Kombination von Ereignissen zu einem grösseren Unfall führen können – z.B. wenn ein automatisches Isoliersystem versagt und der Bediener nicht angemessen auf das Alarmsignal reagiert –, sollten die möglichen Auswirkungen dieses Fehlverhaltens auf die Anlage und auf die betrieblichen Systeme zur Vorbeugung, Warnung und Bekämpfung von Unfällen analysiert werden. Ziel dieser Untersuchung ist es, zu entscheiden, ob die Zuverlässigkeit des automatischen Systems ausreicht. Der Mensch sollte nicht nur als Beteiligter, sondern auch als Initiator von Unfällen betrachtet werden, z.B. das Laden falscher Reaktionsmittel in einen Batch-Reaktor, oder falsche „Operating Procedures“, die zu einer Einleitung in Fließgewässer führen."
- Kriterium 3.4.3: "Annahmen über die Zeit, die das Bedienpersonal braucht, um auf Störfälle angemessen zu reagieren, müssen begründet werden."
- „Im Sicherheitsbericht muß erkennbar sein, daß sichere Arbeitsabläufe (Operating Procedures) für alle vorsehbaren Bedingungen etabliert und dokumentiert sind.“

In ergänzenden Regelwerken (Assessment Manual) finden sich detaillierte Angaben zur Operationalisierung. Dabei wird der HF als ein wichtiges Element behandelt.

## Korea

Das koreanische Gesetz für Industrielle Sicherheit und Gesundheit (Industrial Safety and Health Act) von 1990 wurde zuletzt in Januar 2000 novelliert. Bei der zweiten Novelle (1994) wurden sogenannte Managementsysteme zur Sicherstellung der Prozeßsicherheit (PSM) eingeführt. Das Gesetz trat am 1.1.1996 in Kraft und entspricht etwa den europäischen Regelungen zur Implementierung der Seveso-II-Richtlinie. Die Betreiber von gefährlichen Anlagen müssen dem Arbeitsministerium regelmäßig Prozeßsicherheitsberichte zukommen lassen.

### Die Sicherheitsberichte umfassen

- Prozeßsicherheitsinformationen (detaillierte Angaben zu den chemischen Prozessen, inklusive Fließdiagramme und verwendete Chemikalien),
- eine Gefahrenanalyse,
- Pläne und Richtlinien für den sicheren Betrieb sowie
- Notfallpläne.

Die Risikoanalyse beinhaltet Checklisten, Baumdiagramme und andere Methoden zur Erfassung und Bewertung bestehender Gefahren. Dazu gehört auch eine explizite Human-Error-Analyse.

Pläne für den sicheren Betrieb enthalten klare Anweisungen und Ablaufpläne für alle betrieblichen Prozesse (Inbetriebnahme, Management von Prozeß- und Betriebsveränderungen), Schulungen und Audits sowie Anweisungen für die Ermittlung etwaiger Unfallursachen.

Im Rahmen der Notfallpläne müssen die betroffenen Ressourcen, das Kommunikationssystem und die Bildungs- und Schulungsmaßnahmen beschrieben werden.

Das Arbeitsministerium kann nach Überprüfung des Sicherheitsberichts weitere Maßnahmen oder eine Änderung des bestehenden Sicherheitsmanagementsystems verfügen.

## Niederlande

Die Seveso-II-Richtlinie wurde 1999 mit der Verabschiedung einer Verordnung (Besluit risico's zware ongevallen, BRZO) umgesetzt. Zentraler Bestandteil dieser Verordnung ist der in Holland traditionell angewendete Ansatz der quantitativen Risikobewertung. Auf der Basis der so gewonnenen Erfahrungen wurden somit die Risikotoleranzkriterien in eine gesetzliche Basis eingebunden.

Bei der quantitativen Risikobewertung wird der menschliche Faktor berücksichtigt, indem er als mögliche Unfallursache betrachtet wird und dem Eintreten eines Störfalls aufgrund einer Fehlbedienung eine Wahrscheinlichkeit zugeordnet wird. Die Wahrscheinlichkeiten werden aufgrund von Statistiken berechnet. (Beispielsweise wird die Wahrscheinlichkeit berechnet, daß der Bediener in einem Zeitraum von einem Jahr vergißt, ein Ventil zu schließen). Sind die so ermittelten Wahrscheinlichkeiten und die sich daraus ergebenden Risiken zu hoch, dann müssen Maßnahmen getroffen werden, um das Risiko auf ein akzeptables Maß zu reduzieren.

Das Gesetz verlangt auch von den Anlagenbetreibern die Vorlage eines Berichtes, in dem die Strategie zur Vermeidung von Unfällen aufgezeigt werden muß. Ein Bestandteil davon ist das Sicherheitsmanagementsystem. Im Sicherheitsbericht des Betreibers muß nachgewiesen werden, daß das Unternehmen den Sicherheitsanforderungen entspricht. Dabei müssen die Risiken und die entsprechenden Maßnahmen zu deren Bewältigung beschrieben werden.

Das Sicherheitsmanagementsystem muß Sicherheitsanalysen für alle Betriebsphasen (Inbetriebnahme, Anfahren, Wartung, usw.) beinhalten und sich anerkannter Beurteilungsmethoden (Fehleranalyse mit Baumdiagrammen, Prozeßsicherheitsanalysen, Risikoanalysen) bedienen. Außerdem müssen Arbeitsabläufe und Anweisungen entworfen werden, die die Betriebssicherheit – auch bei Wartungen und in Arbeitspausen – sicherstellen.

Eine Prüfung der Anlagen in Hinblick auf den HF wird nicht explizit im Gesetz verlangt. Dieser Aspekt wird jedoch von den zuständigen Behörden in der Praxis überprüft.

## Schweiz

Die schweizerische Störfallverordnung vom 27. Februar 1991 stützt sich auf das Umweltschutzgesetz vom 7. Oktober 1983 und auf das Gewässerschutzgesetz vom 8. Oktober 1971. Das Ziel der Störfallverordnung ist der Schutz der Bevölkerung und der Umwelt vor schweren Schädigungen durch Störfälle, welche beim Betrieb von Anlagen entstehen können.

Im Vergleich zu den in Deutschland geltenden Gesetzen wird die Eigenverantwortung der Anlagenbetreiber stärker betont. Dieser soll geeignete technische, organisatorische und personelle Maßnahmen treffen, um einen sicheren Betrieb zu garantieren.

Der Betreiber muß einen Bericht über die möglichen Sicherheitsrisiken und die getroffenen Sicherheitsmaßnahmen sowie gegebenenfalls – auf Anforderung der Behörde – eine Risikoermittlung erstellen. Die Behörde kann nach Prüfung dieser Unterlagen zusätzliche Sicherheitsmaßnahmen verfügen. Somit wird sichergestellt, daß der Betreiber der Anlage alle Maßnahmen zur erfolgreichen Störfallvorsorge getroffen hat.

Weiterhin muß der Betreiber Störfälle unverzüglich bekämpfen, den Behörden melden und die Konsequenzen schriftlich festhalten (Störfallbewältigung). Ein weiteres Ziel ist die Verbesserung der Information der Öffentlichkeit, um die bestehenden Risiken bewußter und verständlicher werden zu lassen.

In Bezug auf den HF schreibt die Verordnung lediglich vor, daß der Anlagenbetreiber „genügend und geeignetes Personal einsetzen und es im Hinblick auf die Verhinderung, Begrenzung und Bewältigung von Störfällen ausbilden“ soll.

Das Bundesamt für Umwelt, Wald und Landschaft (BUWAL) hat Handbücher mit branchenspezifischen Checklisten erstellt, in denen die Anforderungen an die Bediensicherheit operationalisiert werden.

## USA

Die Clean Air Act von 1990 sieht die Verabschiedung von Gesetzen über Prozeßsicherheit sowie das Aufstellen von Sicherheitsplänen vor. Diese Vorgabe wurde durch die

- Process Safety Management (PSM-)Richtlinie der Occupational Safety and Health Administration (OSHA) und die
- Risk Management Plan (RMP-)Richtlinie der Environmental Protection Agency (EPA)

Anfang der 90er Jahre erfüllt.

1992 wurde die PSM-Verordnung verabschiedet, die das Eintreten von Störfällen verhindern und die Auswirkungen eventueller Störfälle minimieren sollte. Sie sieht das Bereitstellen von Informationen (Process Safety Informations, PSI) über die Gefahren der verwendeten Chemikalien, Technologien und Anlagen vor.

Die Mitarbeiter und die von ihnen gewählten Vertreter sollen bei der Ausarbeitung von Sicherheitsplänen beteiligt werden und Zugang zu den Risikoanalysen haben. Die Schulungen

des Personals sollen sich schwerpunktmäßig mit den spezifischen Gesundheits- und Sicherheitsrisiken befassen und regelmäßig wiederholt werden.

Operating Procedures müssen schriftlich verfaßt sein und klare Anweisungen für den sicheren Betrieb der Anlage enthalten. Für jeden Verfahrensschritt müssen die durchzuführenden Teilaufgaben und die Grenzen für den sicheren Betrieb, Sicherheits- und Gesundheitsaspekte sowie die Sicherheitssysteme aufgeführt und erläutert werden, so daß eine sichere Arbeitsweise auch unter besonderen Bedingungen garantiert werden kann.

Es sind Notfallpläne zu erarbeiten. Darüber hinaus enthält die Process Safety Management Richtlinie Bestimmungen über Maßnahmen bei Inbetriebnahme und Veränderungen der Anlage und Untersuchungen nach Störfällen (Unfallforschung) vor. Die Prozeßrisiken müssen im Rahmen von Process Hazards Assessments (PHA) evaluiert werden.

Die Process Safety Management Richtlinie gilt als ergebnisorientiert, da die Ziele definiert werden, aber nicht genau vorgeschrieben wird, wie diese Ziele erreicht werden sollen. In Bezug auf Bediensicherheit heißt es: „Die PHA soll den menschlichen Faktor (...) berücksichtigen.“ Dies wird auch in der Praxis überprüft. In den Compliance Guidelines and Enforcement Procedures wird zum Beispiel die Untersuchung folgender Aspekte vorgeschlagen:

- die Schnittstellen Bediener/Prozeß und Bediener/Equipment
- die Anzahl und die Häufigkeit der Aufgaben, die ein Bediener erfüllen muß
- Erweiterte oder abweichende Einsatzpläne
- die Klarheit und Einfachheit von Kontrollanzeigen
- Automatische Instrumente vs. manuelle Prozeduren
- Bediener-Feedback
- Klarheit von Signalen und Codes.

Alle Betreiber von Anlagen, in denen gefährliche Substanzen hergestellt, verarbeitet oder eingesetzt werden, müssen einen Risk Management Plan (RMP) aufstellen. Die möglichen Risiken müssen identifiziert und bewertet werden. Ein sicherer Betrieb der Anlage soll durch Entwurf, Wartung und Betrieb gewährleistet und die Folgen eventueller Störfälle minimiert werden.

RMP's sollen mögliche Freisetzungen gefährlicher Chemikalien vorbeugen bzw. deren Folgen minimieren und ein schnelles und effizientes Handeln bei Störfällen ermöglichen. RMP's bestehen aus drei Bausteinen:

- Eine Risikobewertung („Hazard Assessment“) muß durchgeführt werden, um potentielle Auswirkungen von Freisetzungen gefährlicher Stoffe zu bewerten. Die Risikobewertung muß den örtlichen Katastrophenschutzämtern, der Öffentlichkeit und anderen Dritten zur Verfügung gestellt werden.
- Das Vorsorgeprogramm („Prevention Program“) soll Sicherheitsmaßnahmen, Wartungs- Monitoring- und Schulungsmaßnahmen enthalten.

- Im Rahmen eines obligatorischen Notfallplans („Emergency Response Program“) müssen die Anlagenbetreiber einen Plan ausarbeiten, in dem die spezifischen Aktionen zum Schutze der Menschen und der Umwelt bei Störfällen zu beschreiben sind. Die Schulung des Personals und die Information der Öffentlichkeit sowie der lokalen Katastrophenschutzämter sind vorgeschrieben.

Folgende Elemente betreffen den Human Factor:

- Die PHA erfordert vom Arbeitgeber eine Analyse der Bedienerschnittstelle und der damit verbundenen Risiken.
- Operator Procedures: Der Betreiber muß aufgabenspezifische „procedures“ für jede Betriebsphase (Anfahren, Normalbetrieb, Notfall, Ausschalten) ausarbeiten und implementieren. Die normalen Betriebsintervalle und –grenzwerte müssen definiert und die Konsequenzen eventueller Abweichungen erläutert werden.
- Schulung des Bedienpersonals (Operator Training).

Risk Management Plan und Process Safety Management enthalten zahlreiche Überschneidungen, so daß die Erfüllung beider Anforderungen in der Praxis simultan durchgeführt wird. Diese Vorgehensweise wird auch von den Behörden unterstützt: Untersuchungen einer bestimmten Anlage, die im Rahmen von Risk Management Plan oder Process Safety Management durchgeführt wurden, werden gegenseitig anerkannt. Während das PSM primär arbeitsschutzorientiert ist, steht beim RMP der Umweltschutz im Vordergrund. Die Bestimmungen aus Risk Management Plan und Process Safety Management werden durch Bestimmungen auf verschiedenen Verwaltungsebenen präzisiert und ergänzt.

### 5.3 Technische Normen und Richtlinien der Verbände

Im Auftrag des Landes Brandenburg wurde 1998 die Ergiebigkeit von technischen Normen und Richtlinien der Industrie- und Ingenieurverbände zur Sicherung gegen Fehlbedienung untersucht (Müller 1998). Die Sichtung ergab folgende Ergebnisse:

#### Einschlägige Normen

##### Normen zur Regelung des "Bedienens" im Sinne dieser Thematik

Es gibt kaum Regelungen, die auf den bedienenden Menschen und seinen Beitrag zur Anlagensicherheit, insbesondere unter dem Blickwinkel seiner physiologisch gegebenen Grenzen, eingehen. Es gibt eine breite Palette, die die möglichst günstige Präsentation der Anlage auf den Bedienelementen regeln. Diese Präsentation bemüht sich, ergonomische Gesichtspunkte zu berücksichtigen, eine Bilanzierung der dem Menschen zumutbaren Informationsmenge findet dabei nicht statt.

- Da überwiegend Prozeßleittechnik als Mittel zur Bedienung benutzt wird, sollten die von der Automatisierungstechnik herkommenden Normen einbezogen werden.
- Hinsichtlich der zu betrachtenden Grenzen des Menschen sollten die Normen zur Anlagedarstellung einbezogen werden, da man nur daraus das Übersichts- und Gleichzeitigkeitsproblem erkennen kann.

Im Anhang sind die einschlägigen Normen aufgelistet und kurze Inhaltsangaben eingefügt.

### **Normen zur Softwaredokumentation**

Als weitere Gruppe sind Normen zur Programmdokumentation aus der Informationsverarbeitung heranzuziehen, da die Bedienungsanweisungen letzten Endes Regelungen der Informationsverarbeitung durch den Menschen darstellen (vgl. u.a. DIN 66230, DIN 66231, DIN 66232, DIN 66234)

Weiterhin sollen Normen erwähnt werden, deren Titel eine Beziehung zur Bediensicherheit im hier gebrauchten Sinne vermuten lässt, die sich aber statt dessen auf den Schutz des bedienenden Menschen vor Verletzungen durch die Maschinentechnik beziehen (vgl. u.a. DIN 31 000, DIN 31001)

### **Normen zur "Bediensicherheit" bei der Instandhaltung**

Darüber hinaus gibt es Normen, die im Zusammenhang mit "Bediensicherheit" zu Wartung und Instandhaltung Bedeutung haben (vgl. DIN 33409, DIN 33410).

### **Aus der Untersuchung der Normen mit Bezug „Bediensicherheit“ wurden folgende Schlussfolgerungen gezogen:**

Die Darstellung der Informationen aus einer Anlage ist gut und detailliert geregelt. Die Aufnahmemöglichkeit des Menschen gegenüber diesem Informationsangebot ist jedoch unzureichend berücksichtigt. Darauf geht nur DIN 33 414 ein. Mit dem Begriff "Dimensionalität" wird dort auch ein erster Ansatz zur Berücksichtigung des Gleichzeitigkeitsproblems bei der Informationserfassung und -bewertung durch einen Menschen gemacht. Trotzdem fehlt auch dort die Angabe einer Grenze für den Informationsüberlauf im Menschen. Der Denkprozeß im bedienenden Menschen wird in dieser Norm tiefgreifend beschrieben. Die Handlungsempfehlungen hinsichtlich der Sicherheit störfallrelevanter Anlagen bleiben jedoch hinter den Wünschenswerten zurück.

- Das vorliegende Normenwerk deckt die Sicherheitsbedürfnisse, die sich aus der Betrachtung der Bedienkonzeption für den Störbetrieb ergeben und sich in der Forderung nach Verhütung von Informationsüberlauf im Bediener bei parallelen Informationsverarbeitungsforderungen widerspiegeln, nicht ab.

### VDI/VDE-Richtlinien

VDI-Richtlinien zum Thema Anlagensicherheit, Prozeßleitwarten (vgl. VDI/VDE 2180, VDI/VDE 3541, VDI/VDE 3542, VDI/VDE 3546, VDI 4003) geben zum Thema Bediensicherheit keine anderen Aussagen als die Normen.

### NAMUR-Empfehlungen (Normen-Arbeitsgemeinschaft Meß-und Regeltechnik der chemischen Industrie)

Die NE 31 „Anlagensicherung mit Mitteln der Prozeßleittechnik“ geht u.a. ein auf die Klassifizierung von Prozeßleitsystemen und Fehlern. Sie beinhaltet eine Anleitung zum Entwurf und zur Instandhaltung (Funktionsprüfung) sicherer Prozeßüberwachungs- und -sicherungssysteme, sie betont in gewissem Ausmaß einkanalige Sicherungssysteme und weist einen klaren Bezug zur Störfall-Verordnung auf.

- Die NE 31 zielt u.a. auf die Sicherstellung von Warninformationen an den Bediener, sie beinhaltet jedoch keine Aussagen über die Verarbeitungsmöglichkeiten der Informationen durch den Bediener.

## 5.4 Bediensicherheit in der internationalen Normung<sup>6</sup>

In den 60er Jahren begann man damit, zur Erhöhung der Bediensicherheit bestimmte Aspekte der Betätigung zu standardisieren. Problem war damals und ist es noch heute, daß das Thema von verschiedenen Gremien – selbst wenn sie nur einem Normenausschuß angehören – aus unterschiedlicher Sicht und mit unterschiedlichen Ergebnissen behandelt wird.

Auch wenn Normen zunächst keinen verbindlichen Charakter haben, so schafft es doch große Schwierigkeiten, wenn im globalen Handel einzelne Anlagenkomponenten verschiedener Hersteller nicht abgestimmt sind über eine Standardisierung durch Normen. Wenn der Bediener dann in kritischen Situationen beispielsweise mit unterschiedlichen Kodierungsprinzipien konfrontiert ist und Fehler macht, so ist das zwar menschliches Versagen, aber nicht unbedingt das des Bedieners.

Aus der Sicht von Hinz (1997) ist für den Komplex Bediensicherheit ein „human-centred system design“ erforderlich, an denen jedoch zusätzliche Disziplinen zu beteiligen sind. Hierzu sei eine Umstrukturierung der Normenorganisation unumgänglich. Grundlegend sind Standardisierungen der Kodierung, also der zur Repräsentation der Anlage verwendeten Darstellungsform.

<sup>6</sup> In Anlehnung an Hinz, in: OECD 1997.

Die IEC 73 und IEC 447 Basic and safety principles regeln seit kurzem auch die bildschirmgestützte Prozeßführung und können als Grundlage für die Auslegung eines M-M-Systems direkt angewandt werden.

Die ISO 10075 (ergonomic principles related to mental work load) beschreibt ausführlich die Aspekte psychischer Arbeitsbelastung.

Die Lücke soll derzeit als deutsche Vorbereitung für die ISO-Arbeit durch einen Normentwurf zu den zu berücksichtigenden kognitiven Funktionen des Menschen ausgefüllt werden.

Die derzeit vorbereitete ISO 11064 soll in sieben Teilen die Berücksichtigung kognitiver Funktionen bei der Wartenauslegung ermöglichen.

Die EU-Richtlinie 90/270/EWG zur Arbeit an Bildschirmplätzen hat indirekt auch einen begünstigenden Effekt auf die Bediensicherheit.

### **Schlußbemerkungen zur Berücksichtigung von Maßnahmen zur Vermeidung von Fehlbedienung im bestehenden Regelwerk**

Strategien zur Vermeidung von Fehlbedienungen werden im wesentlichen erst seit den 80er Jahren thematisiert und diskutiert. Berücksichtigt man den üblichen Entstehungszeitraum von Normen, die seit verbindlicher Einführung des europäischen Binnenmarktes zunächst auf europäischer Ebene abzustimmen sind, bevor sie in deutsche Normen aufgenommen werden, und berücksichtigt man zusätzlich die noch weitgehend fehlende interdisziplinäre Ausrichtung einer eindeutig interdisziplinären Fragestellung, so verwundert es nicht, daß noch wenig detailliertere Ausführungen zum Thema Fehlbedienung im Regelwerk zu finden sind.

## 6. Bestand und Lücken von Instrumenten zur Berücksichtigung des Human Factors

In vielen Bereichen ist man längst dabei, geeignete Erfassungs-, Durchführungs- und Prüfinstrumente zu entwickeln, wie die nachfolgende Zusammenstellung zeigt:

Tab. 6-1: Instrumente im Zusammenhang mit Human Factors

Instrument	Zweck	Inhalt	Quelle
Ablaufplan	Prüfung des Arbeitsschutzes bei An- und Abfahrvorgängen von Chemieanlagen	Liste der Arbeitsschritte zur Analyse menschlichen Fehlverhaltens	Hauptmanns 1994
RISIVE	Beurteilung der Lage der Arbeitssicherheit in einem Betrieb	<p>Interviewleitfaden mit 108 Fragen zu den Bereichen</p> <ul style="list-style-type: none"> <li>– Unternehmen</li> <li>– Fertigkeiten, Fähigkeiten und Kenntnisse des Personals</li> <li>– Arbeitsbedingungen</li> <li>– Arbeitsgruppenkultur</li> </ul>	Rüegsegger 1995
SAM	Beurteilung der Sicherheitskultur eines Unternehmens	Erhebung von Merkmalen mit Hilfe von Leitfragen	Künzler 1995
BIGL	Bewertung der Bediensicherheit von Leitwarten	<p>Erfassung und Bewertung der Merkmale menschengerechter Gestaltung von Leitwarten nach den Einflußgrößen:</p> <ol style="list-style-type: none"> <li>1. Anzeigen</li> <li>2. Bedienelemente</li> <li>3. Umgebungsbedingungen</li> <li>4. Arbeitsorganisatorische Bedingungen</li> </ol>	Windel 1993

Instrument	Zweck	Inhalt	Quelle
Fragebogen zur Sicherheitsdiagnose (FSD)	Erfassung der psychischen Belastung in einer Gefahrensituation	<p>Es werden sicherheitskritische psychische Belastungen erfaßt:</p> <ul style="list-style-type: none"> <li>- Aufmerksamkeitsverteilung</li> <li>- wahrgenommenes Zeitbudget</li> <li>- widersprüchliche Anforderungen</li> <li>- Gefahr als Stressor</li> <li>- Über- und Unterforderung</li> </ul>	Graf Hoyos, in: Richter 1998
International Safety Rating (ISR)	Organisations- und Managementaudit	<p>Meß- und Bewertungsinstrument nach 20 Prüflementen, u.a.:</p> <ul style="list-style-type: none"> <li>- Analyse von Arbeitsplatz und Arbeitsauftrag</li> <li>- Analyse von Unfällen und Ereignissen</li> <li>- Beschäftigtentraining</li> <li>- Gruppenarbeit</li> </ul>	International Loss Control Institute, 1986
Human Reliability Analysis (HRA)	Abschätzung der menschlichen Zuverlässigkeit	Hauptkennzeichen ist die Benutzung quantitativer Daten zur Bestimmung der Zuverlässigkeit	Giesa 1995, in: Monteau 1995
Online-Trainingssystem für Bediener-schulungen	Kenntnisse zum Verhalten in gefahrdrohenden Situationen in Fertigkeiten übertragen	<ul style="list-style-type: none"> <li>- An- und Abfahrvorgänge</li> <li>- schnelle Abfahrvorgänge in gefahrdrohenden Situationen</li> <li>- Verbesserung der Reaktionen in Fehler-, Stör- und Abfahrvorgängen</li> </ul>	Schmidt 1997, in: OECD 1997

Instrument	Zweck	Inhalt	Quelle
Sicherheit durch organisationales Lernen (SOL)	Lernen aus Betriebserfahrung	Systematische Ursachenanalyse nach Störungen/Störfällen mit schriftlichem Berichtssystem oder DV-gestützter Dokumentation entsprechend dem soziotechnischen HF-Systemansatz	Miller et al. 1997, in: OECD 1997 bzw. UBA-Text 98/79
PRAP (nach TERROS)		Zwang zur formalisierten Notierung einer Steuerungsaufgabe (auch an den Menschen gerichtete Steuerungsaufgaben) mit der automatisierten Prüfung auf Vollständigkeit und Widerspruchsfreiheit	Müller 1987 (Interkama 92)
R-I-Schema nach DIN 19227	Dokumentation der Bedienaufgaben	Darstellung der Bedienkonzeption nach der Form des Rohrleitungs- und Instrumenten-Schemas	Müller 1991 (IFAC Zürich und 8. Workshop der BG Chemie)
VISUA	Unterstützung und Entlastung des Betriebspersonals bei der Wahrnehmung seiner Aufgaben	Technische Betriebsführungs-, Instandhaltungs-, Dokumentationsmanagements-, Schulungs- und Informationssysteme mit grafischer Benutzerführung (⇒ Vermeidung von Widersprüchen und Redundanzen in den Dokumentationen).	Stuhrmann, in: OECD 1997

Einer gewissen Systematik folgen diese Instrumente jedoch nur innerhalb ihres bezweckten Teilbereiches, nicht aber vor dem gesamten soziotechnischen System der Human Factors.

Für das Gesamtsystem sind folgende Komplexe auf Lücken/Mängel zu prüfen:

Komplex 1: Beschreibung des Menschen mit den spezifischen Merkmalen seiner Leistungsfähigkeit und seiner physiologischen, psychischen und psychosozialen Leistungsgrenzen

- Komplex 2: Darstellungsinstrumente
- für die Bedienkonzeption
  - für die Leitwartengestaltung
- Komplex 3: Erfassungsinstrumente / Prüfinstrumente zur Bedienkonzeption unter dem Blickwinkel der „Strategie zur Vermeidung von Fehlbedienung“ (d.h. nicht unter Kriterien des Arbeitsschutzes)
- Komplex 4: Bewertungsmaßstäbe, -hilfen

### **Komplex 1 – Kenntnis der Leistungsgrenzen des Menschen**

Den Anlagenplanern und den Leitwartengestaltern sind die physiologischen und psychologischen Leistungsgrenzen des Menschen häufig nicht in ausreichendem Maße bewußt, so daß sie bereits bei der Planung Überforderungen des Bedieners einbauen, die dann spätestens bei nicht bestimmungsgemäßen Betriebszuständen als Fehlbedienung zutage treten. Wesentliche Probleme sind:

- Leistungsgrenzen des Menschen hinsichtlich gleichzeitiger Informationen,
- Leistungsgrenzen hinsichtlich Informationsverarbeitungskapazität und
- unerwartete und ungewollt ablaufende Reaktionsmuster des Menschen unter Stress.

### **Physiologische Leistungsgrenzen**

**Tab. 6-2: Physiologische Leistungsgrenzen des Menschen**  
(aus: Bergmann 1984)

<b>Physische und psychologische Kennwerte des Menschen (Richtwerte)</b>	
kleinstes Sehdetail	1,6'
Flimmerverschmelzungsfrequenz	20...60 Imp/s
gehörschädigender Lärm	90 dB
Kanalkapazität	0,2...12 bit/s
quasi parallel überwachbare Meßstellen	300...400
quasi parallel handhabbare Informationen	7 !
simultan steuerbare Regelkreise	3

Keineswegs alle von der Psychologie und der Physiologie zu gewinnenden Aussagen über die menschlichen Leistungsgrenzen haben Bedeutung für die hier behandelte Thematik:

- Die Werte über Greifweiten und Kräfte haben in der Arbeitsgestaltung und in einschlägigen Normen Berücksichtigung gefunden.
- Das kleinste Sehdetail wird bei der Planung der Relationen von Betrachtungsabstand und Instrumenten(Skalen-) oder Schriftgröße auf dem Bildschirm berücksichtigt.
- Die Flimmerverschmelzungsfrequenz liefert einen unteren Grenzwert für die Arbeitsfrequenz der Bildschirme und ist bei deren Konstruktion hinreichend berücksichtigt. Im Interesse von Schonung und Komfort wird dabei ein angemessener Abstand gewahrt.

Die Kanalkapazität im Sinne der Informatik ist für die Bedienerbelastung wichtig, es gibt aber bisher keine praktikablen Ansätze, die Arbeitsaufgaben als Informationsraten zu erfassen.

Wesentlich für alle Betrachtungen ist die auch in DIN IEC 423 niedergelegte und relativ gut gesicherte Erkenntnis, daß die Teilbarkeit der menschlichen Aufmerksamkeit auf  $7 \pm 2$  "Psychologische Einheiten" (siehe DIN IEC 423) begrenzt ist. Berücksichtigt man, daß bei der Übernahme einer Regelungsaufgabe ständig Soll- und Istwert verglichen werden müssen, so ergibt sich daraus näherungsweise die Grenze von 4 gleichzeitig von Hand fahrbaren Regelkreisen.

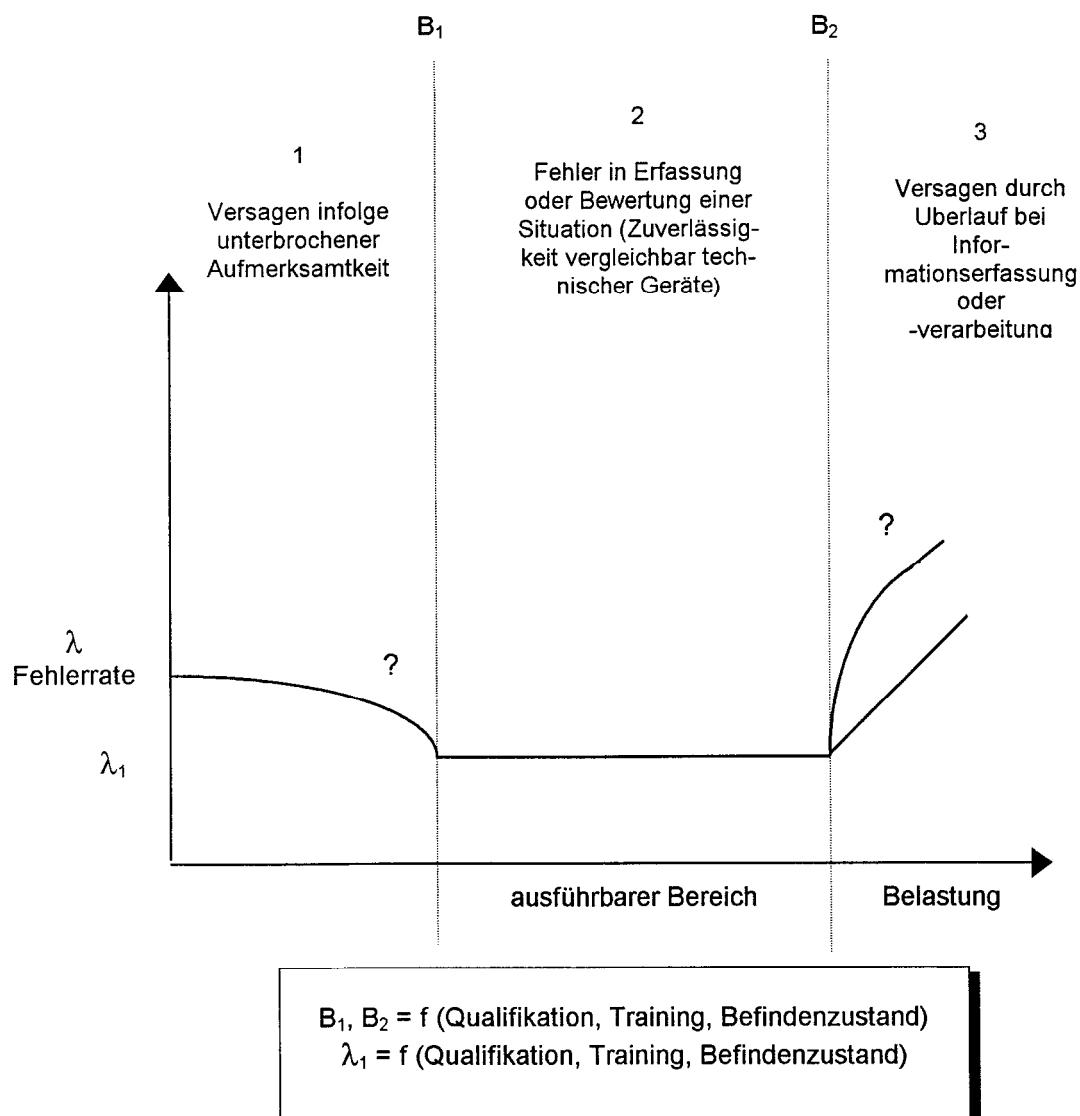
Die Zahl der einem Wartenfahrerarbeitsplatz zuordnenbaren Meßstellen ist kein Grenzwert. Bei den in der Verfahrenstechnik üblichen Relationen von Signalhäufigkeit und Bedürfnissen des Prozesses hinsichtlich der Zeiten, in denen auf ein Signal die notwendige Reaktion erfolgt, hat sich dies als grober Erfahrungswert herausgestellt.

Letztlich ist von der in Handlung umzusetzenden Informationsdichte die Handlungsfähigkeit des Bedieners abhängig (vgl. Abb. 6-1).

- Es gibt den (mit 2 gekennzeichneten) mittleren Bereich, in dem ein Mensch **optimal handlungsfähig** ist. Allen Beteiligten ist klar, daß es eine Menge von Anforderungen gibt, die die menschliche Leistungsfähigkeit überschreiten. Fallen mehr Aufgaben an, als erledigbar sind, so müssen immer Aufgaben unerledigt bleiben, die dann als Fehler zu zählen sind.
- Dementsprechend steigt also im Bereich 3 die Fehlerrate rapide an. Hat der Mensch „stahlharte“ Nerven, so kann er weiter die mögliche Aufgabenmenge erledigen, lediglich aus deren Überschreitung ergibt sich eine ansteigende Fehlerquote. Dieses theoretisch denkbare Verhalten tritt in der Praxis kaum auf. Gewöhnlich verliert der Mensch bei Überforderung die Nerven. Dadurch ist die Fehlerquote nicht vorhersehbar. Das kann bis zur völligen Handlungsfähigkeit führen.
- Daraus ergibt sich, daß das Überschreiten dieser oberen Belastungsgrenze schon in der Planung vermieden werden muß. Selbstverständlich hängt der Betrag dieser Belastungs-

grenze von Training, Qualifikation und Kondition ab. Trotzdem bleibt die Forderung nach der Bilanzierung der in einer Bedienkonzeption gedachten Bedienanforderungen, um sicherzustellen, daß diese die Belastungsgrenze nicht überschreiten.

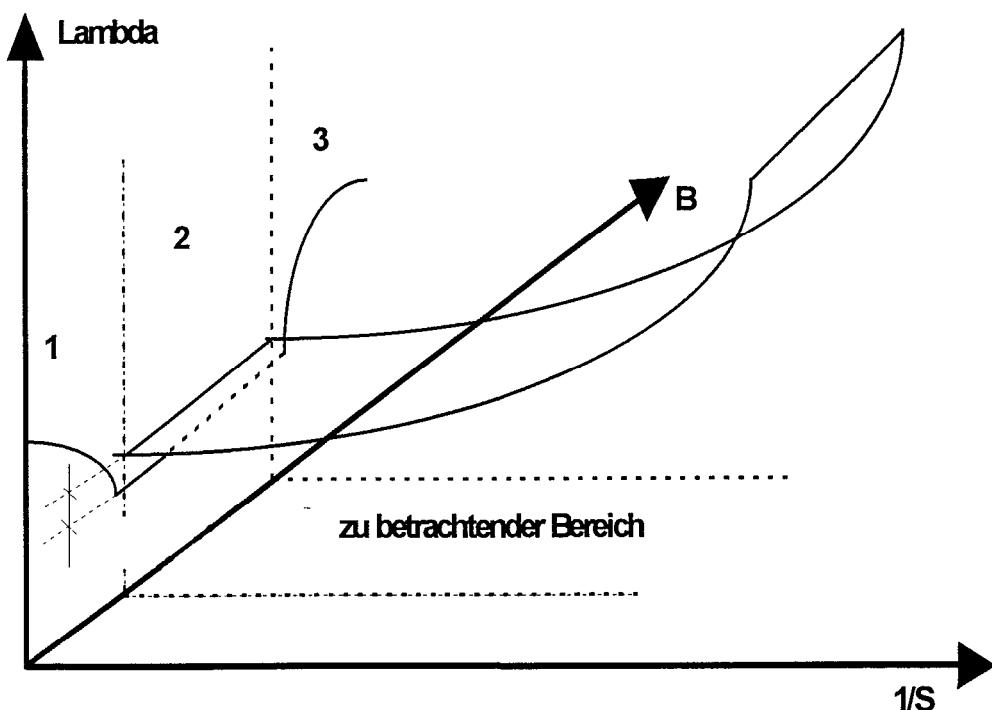
Nicht gleichermaßen geläufig ist das Versagen des Menschen bei **Unterforderung**. Sinkt die Be-anspruchung unter einen Grenzwert, so schweift er mit seinen Gedanken ab, und hat es dabei nicht im Griff, rechtzeitig wieder auf die Aufgabe zurückzukommen. Unterforderung führt also ebenfalls zu einem unvorhersehbaren Ansteigen der Bedienfehler.



Aufgabe: Beschränkung der Bedieneranforderungen auf Bereich 2

Abb. 6-1: Bedienzuverlässigkeit und Fehlerraten eines Bedieners (aus: Müller 1995)

Der Einfluß der Sicherheitskultur auf die Belastungsgrenzen und die erreichbare Zuverlässigkeit ist in Abbildung 6-2 bildlich aufgezeigt (vgl. UBA-Text 61/97, S. 228). Das dargestellte Verhalten ist der günstigste asymptotische Wert, der bei optimalen Umfeld-Voraussetzungen erreicht wird. Faßt man das Umfeld mit dem Begriff „Sicherheitskultur“ zusammen und stellt sich vor, dafür eine quantifizierbare Maßeinheit zu haben, so kommt man zur Darstellung der Abbildung 6-2 (große Werte von  $1/S$  bedeuten schlechte Sicherheitskultur).



Lambda	Fehlerrate
B	Belastung
S	Maß für die Sicherheitskultur

$\text{Lambda}(1/S = 0) \approx \text{Physiologische Leistungsgrenze des Menschen}$   
(asymptotisch)

Abb. 6-2: Fehlerrate eines Bedieners (aus: Müller 1997)

## Psychische Leistungsgrenzen

Neben der Gefahr des Informationsüberlaufes, die in physiologischen Grenzen des Menschen begründet ist, muß der Planer und das Führungspersonal der Anlage auch die psychologischen Besonderheiten des Menschen in der Notfallsituation berücksichtigen, um angemessene Erwartungen an ihn zu stellen. Nach Experimenten von Dörner (1980) ist das Verhalten des Menschen in Notfallsituationen durch bestimmte Reaktionsmuster gekennzeichnet, die erheblich von dem üblicherweise geschulten „normalen“ Verhalten des Bedieners abweichen.

**Tab. 6-3: Psychologische Merkmale des Menschen unter Stress**

<b>Verhalten des Menschen in Notfallsituationen (zusammengefaßt aus Dörner 1980)</b>
<ul style="list-style-type: none"><li>— Selbstreflektionen (= Rekapitulieren und Analysieren des eigenen vergangenen Handelns und Denkens) reduzieren sich.</li><li>— Geplantes, systematisches Vorgehen reduziert sich.</li><li>— Mit steigender Fehlerzahl wächst das Anwenden von Stereotypen, d.h. derselbe (falsche) Gedankengang wird wieder und wieder ausgeführt.</li><li>— Mit zunehmender Fehlerzahl sinkt die Selbstkontrolle; man merkt gar nicht mehr, daß die Pläne, die man hatte, gar nicht mehr ausgeführt werden.</li><li>— Man will die Gefahrensituation (zu) schnell hinter sich bringen; man überlegt nicht mehr, welche Umstände zu beachten sind, bevor Entscheidungen getroffen werden.</li><li>— Steigendes Risikoverhalten / Kampf statt Flucht; man will die Gefahrensituation „um jeden Preis“ meistern.</li><li>— Zunehmende Regelverstöße; das Ziel heiligt die Mittel. Es ist nicht mehr wichtig, was verboten ist und was erlaubt ist.</li><li>— Verhaltensziele werden weniger konkret; es kommt mehr und mehr zu unverbundenen Einzelhandlungen.</li></ul>

Geht man die Analysen von Störfallereignissen durch, so finden sich in fast allen Fällen mindestens mehrere dieser Reaktionsmuster. Aus diesen Erkenntnissen ist u.a. folgende Schlußfolgerung zu ziehen:

In der Notfallsituation muß der Bediener auf ein „programmiertes“ Reaktionsinventar zurückgreifen können. Intellektuelles Durchdenken kann unter Stress von ihm nicht erwartet werden.

Das heißt, Schulungen, die ausschließlich die kognitive Verarbeitung ansprechen, genügen nicht als Vorbereitung auf die Notfallsituation. Der Bediener muß über Simulationstrainings an die Verfügbarkeit von Handlungsmustern herangeführt werden. Diese Erkenntnis ist nicht neu, wie wir u.a. aus der Pilotenausbildung wissen. Sie findet jedoch noch kaum Niederschlag in der Ausbildung des Bedienpersonals verfahrenstechnischer Anlagen. Erste Schritte sind in einigen Unternehmen erkennbar, doch werden sie noch in keiner Weise konsequent umgesetzt.

Das Einzelfehlertoleranzprinzip, wie wir es aus der Störfall-Verordnung oder aus sonstigen Risikobetrachtungen kennen, mag auf den Bereich technischer Fehler anwendbar und sinnvoll sein, es paßt aber nicht für den Bereich der menschlichen Fehler.

Aus den Experimenten von Dörner ist ableitbar, daß die Wahrscheinlichkeit eines menschlichen Fehlverhaltens sich exponentiell mit jedem gemachten Fehler erhöht. Ist der erste Fehler erst einmal gemacht, folgen ein zweiter und dritter mit hoher Wahrscheinlichkeit. Auch vor diesem Hintergrund ist die systematische Erfassung der Bedienanforderungen vor allem für nicht-bestimmungsgemäße Anlagenzustände von hoher sicherheitsrelevanter Bedeutung.

### Komplexe 2 und 3 – Darstellungs- und Prüfinstrumente

Grundvoraussetzung für die Prüfbarkeit der Bedienkonzeption ist eine geeignete Darstellungsform. In einigen Bereichen liegen hier erste Ansätze vor, in einigen Bereichen haben die betroffenen Unternehmen interne Instrumente entwickelt, in einigen Bereichen sind noch keine Ansätze erkennbar. Um sowohl intern im Unternehmen wie extern durch Behörde oder Sachverständige die Strategie zur Vermeidung von Fehlbedienung prüfen zu können, bedarf es jedoch eines einheitlichen und für die jeweilige Art des Betriebes vollständigen Darstellungsinstrumentariums:

Tab. 6-4: Entwicklungsstand zu Darstellungs- und Prüfinstrumenten zur Bediensicherheit

Bereich der Bedienkonzeption	Darstellungsform	Bewertung der derzeit verfügbaren Instrumente
<b>I. Technische Faktoren</b>		
1. Fehlerverzeihende Technik	<ul style="list-style-type: none"><li>• Bildliche Darstellung der Wartenfahrerfunktionen im Produktionsablauf</li></ul>	Ansätze in einzelnen Unternehmen vorhanden, jedoch noch unvollständig und noch ungeeignet als Prüfgrundlage

Bereich der Bedienkonzeption	Darstellungsform	Bewertung der derzeit verfügbaren Instrumente
2. Eine dem Menschen angepaßte Technik zur Beherrschung von Störungen	<ul style="list-style-type: none"> <li>• Bildliche Darstellung von Handeingriffsmöglichkeiten in den Prozeß</li> <li>• Systematische Gefahrenanalyse zu denkbaren Fehlbedienungen mit Darstellung der Technikreaktion</li> <li>• Darstellung der Alarmklassifizierungen im konkreten Betrieb</li> </ul>	<p>Erfolgt derzeit nicht systematisch</p> <p>Erfolgt derzeit nicht systematisch</p> <p>Erfolgt derzeit nicht systematisch</p>
3. Eine dem Menschen angepaßte Technik zur sicheren Überwachung der Betriebszustände und zur Erkennung von Störungen → ergonomische Gestaltung der Arbeitsplätze	<ul style="list-style-type: none"> <li>• BIGL-Darstellungs-, Prüfungs- und Bewertungsinstrument für die Leitwarten gestaltung (Anzeigen, Bedienelemente, Umgebungsbedingungen und arbeitsorganisatorische Bedingungen)</li> </ul>	Anwendung nicht bekannt
<b>II. Organisatorische Faktoren</b>		
1. Eine dem Menschen angepaßte Betriebs- und Ablauforganisation	<ul style="list-style-type: none"> <li>• Aufbauorganisation in Diagrammform</li> </ul>	Form zu allgemein, nicht aussagekräftig
2. Sicherheitskultur	<ul style="list-style-type: none"> <li>• Ablauforganisation als Betriebsanweisungen</li> </ul>	Als Prüfunterlage geeignet. Betriebsanweisung zur Beherrschung von Störungen fehlt weitgehend
3. Sicherheitsmanagement	<ul style="list-style-type: none"> <li>• SAM-Erhebungsinstrument mit Leitfragen</li> <li>• LUA-Projekt 1999</li> </ul>	Wird es angewendet? (z.B. im Rahmen der Öko-Auditierung) Allgemein verfügbar? Wie wird es verbreitet?

Bereich der Bedienkonzeption	Darstellungsform	Bewertung der derzeit verfügbaren Instrumente
<b>III. Personenbezogene Faktoren</b>		
1. Qualifikation	• Schulungen, Trainings werden nicht personenbezogen in abrufbarer Form dokumentiert	Nicht ausreichend
2. Eignung/Mitarbeiterauswahl	• Persönlichkeitstests	Werden nicht angewandt
3. Motivation	• Belastungstests	Werden nicht angewandt
	• Test „kommunikative Fähigkeiten“	Werden nicht angewandt
	• Systematische Erfassung der Mitarbeiterbeteiligung in Sicherheitsfragen	Erfolgt nicht

### Grundsätze zur Darstellung der Bedienanforderungen

In der Informatik wurde zur rechnerischen Behandlung der Erledigung von Informationsströmen die **Bedientheorie** entwickelt. Unglücklicherweise ergibt sich hier eine Überschneidung der Begriffe: Bedientheorie behandelt das Erledigen (Bedienen) von Forderungen.

Die Bedientheorie bezeichnet Signale, die eine Handlung erfordern, als Forderungen und ihr zeitliches Aufeinanderfolgen als Forderungsstrom. Die Instanz, die die Forderungen erledigt – im vorliegenden Fall der Anlagenfahrer –, wird als Bedienknoten bezeichnet. Die Forderungen werden im Detail nacheinander erledigt. Deshalb muß es vorgeschaltet einen Wartenraum für die ankommenden Forderungen geben. Dem entspricht das Kurzzeitgedächtnis des Anlagenfahrers mit der wiederholt diskutierten begrenzten Teilbarkeit der Aufmerksamkeit.

Für den Anlagenfahrer ist der Prozeß mit seiner Instrumentierung eine Forderungsquelle. Indem er Forderungen erledigt, wirkt er als Forderungssenke. Aufgaben, die er – z.B. wegen Überbeanspruchung – übersieht, sind abgewiesene Forderungen. Aufgaben, die in der für den Prozeß zulässigen Zeit erledigt werden müssen, sind ungeduldige Forderungen. Nicht in der Zeit erledigte ungeduldige Forderungen werden zu abgewiesenen Forderungen. Aus diesen beiden kann sich ein Strom nicht bedienter Forderungen, d.h. nicht erledigter Aufgaben ergeben, der zu gefährlichen Zuständen des Prozesses führen kann. Das Ziel ist daher, den Strom nicht bedienter Forderungen bei Null zu halten.

Abbildung 6-3 zeigt die bedientheoretische Modellierung eines Anlagenfahrers.

Die Bedientheorie beschreibt nur die Mengenströme der Forderungen. Falsche Bearbeitung von Forderungen – Bedienfehler im eigentlichen Sinne – sind damit nicht darstellbar. Alle in Folge des Informationsüberlaufs nicht bedienten (unerledigten) Forderungen sind für den gesteuerten Prozeß (die Anlage) als Bedienfehler wirksam.

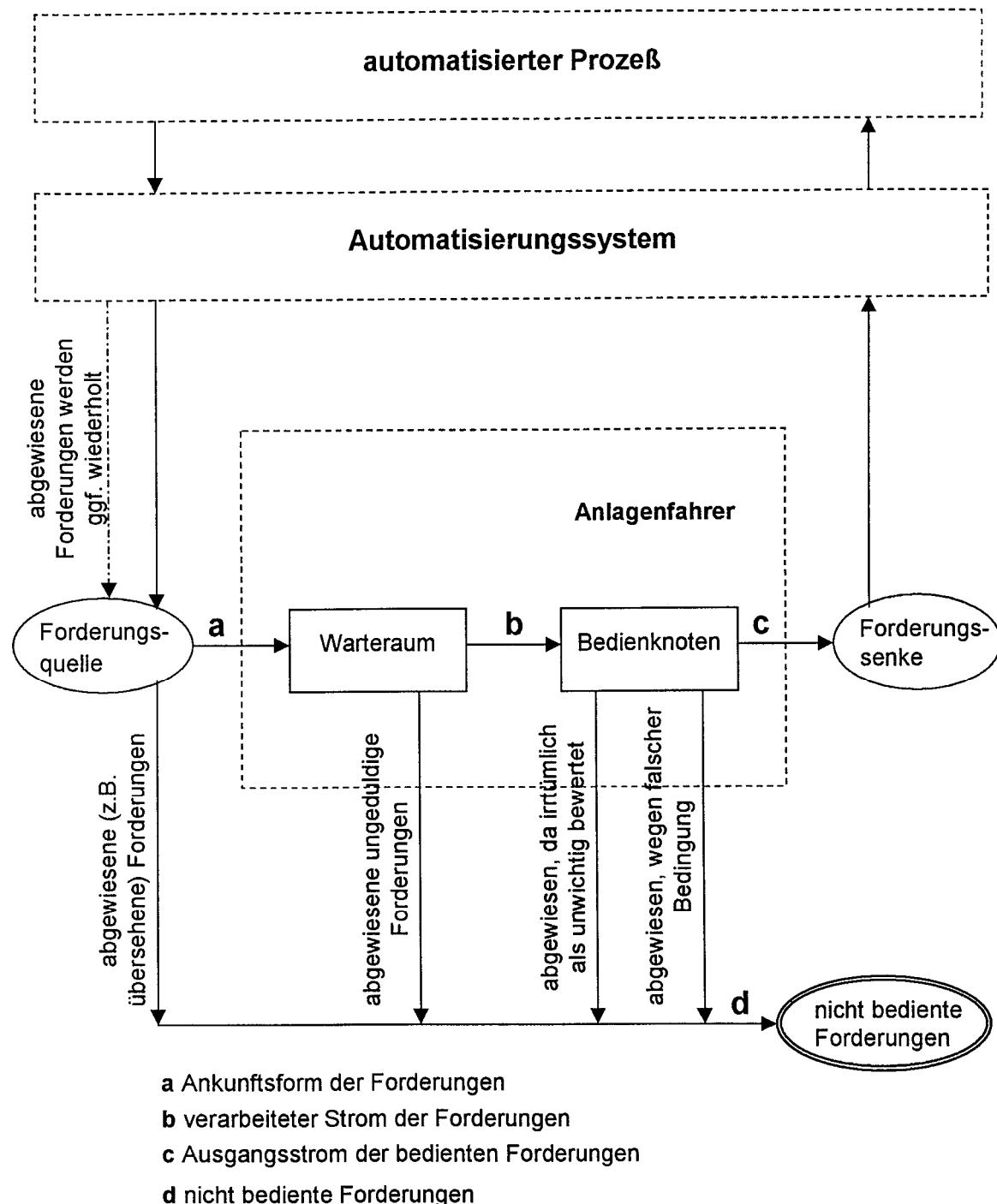


Abb. 6-3: Bedientheoretisches Modell eines Anlagenfahrers (Müller 1995)

Ziel jeder Bedienkonzeption für einen Anlagenfahrer muß es sein, Verluste durch unerledigte Forderungen zu vermeiden. In diesem Zusammenhang ist daran zu erinnern, daß es für die Informationen keinen Erhaltungssatz wie für Masse und Energie gibt: Nicht wahrgenommene oder nicht verarbeitete Informationen verschwinden im Überlauf und sind damit wertlos.

Erfolgt keine Reaktion des Bedieners auf eine Forderung, kann es sein, daß aus dem Prozeß mit seiner Automatik erneut Forderungen kommen (gestrichelte Linien in Abb. 6-3).

Fehlentscheidungen des Bedieners wirken sich als Abweisen von Forderungen aus.

Die komplizierten Vorgänge bei zweistufigen Alarmen und bei übergeordneten automatischen Notabschaltungen wurden in Abbildung 6-3 nicht dargestellt. Es wird vorausgesetzt, daß die technischen Konzepte zum Abweisen von Bedienfehlern unvollständig sind.

Abbildung 6-4 erweitert das bedientheoretische Modell für das Zusammenspiel aus gesteuertem Prozeß, Prozeßleitsystem und Anlagenfahrer. Ein großer Teil der Forderungen wird planmäßig immer durch das Prozeßleitsystem erledigt. Daneben gibt es sicherheitsrelevante Anforderungen, die sich grundsätzlich an den Anlagenfahrer wenden. Weiterhin gibt es vorübergehende Anforderungen durch Ausfall einzelner Komponenten des Prozeßleitsystems, Signalströme und Verzweigungen. Das Überbrücken von Teilausfällen ist durch die Signalanwahl im Sinne der beabsichtigten Hand-Automatik-Umschaltung gekennzeichnet.

Abweichend von der prinzipiellen Darstellung in Abbildung 6-3 unterscheidet sich eine reale Situation in folgendem:

- Der Bediener arbeitet parallel zu einem Automatisierungs- oder Prozeßleitsystem
- Nur ein Teil der Informationsströme ist sicherheitsrelevant.
- Es gibt Automatisierungsstrukturen, zu denen kein Handeingriff vorgesehen ist.
- In gewissem Umfang können angezeigte Informationen auf dem Bildschirm oder Instrument "warten", bis sie wahrgenommen werden.
- Der Bediener kann Informationen anwählen.
- Es ist nicht sichergestellt, daß der Bediener, wenn sicherheitsrelevante Informationen und sein (innerer) Warteraum mit unwichtigen Informationen teilweise oder ganz besetzt ist, seinen Warteraum unverzüglich für die sicherheitsrelevanten Informationen frei machen kann.

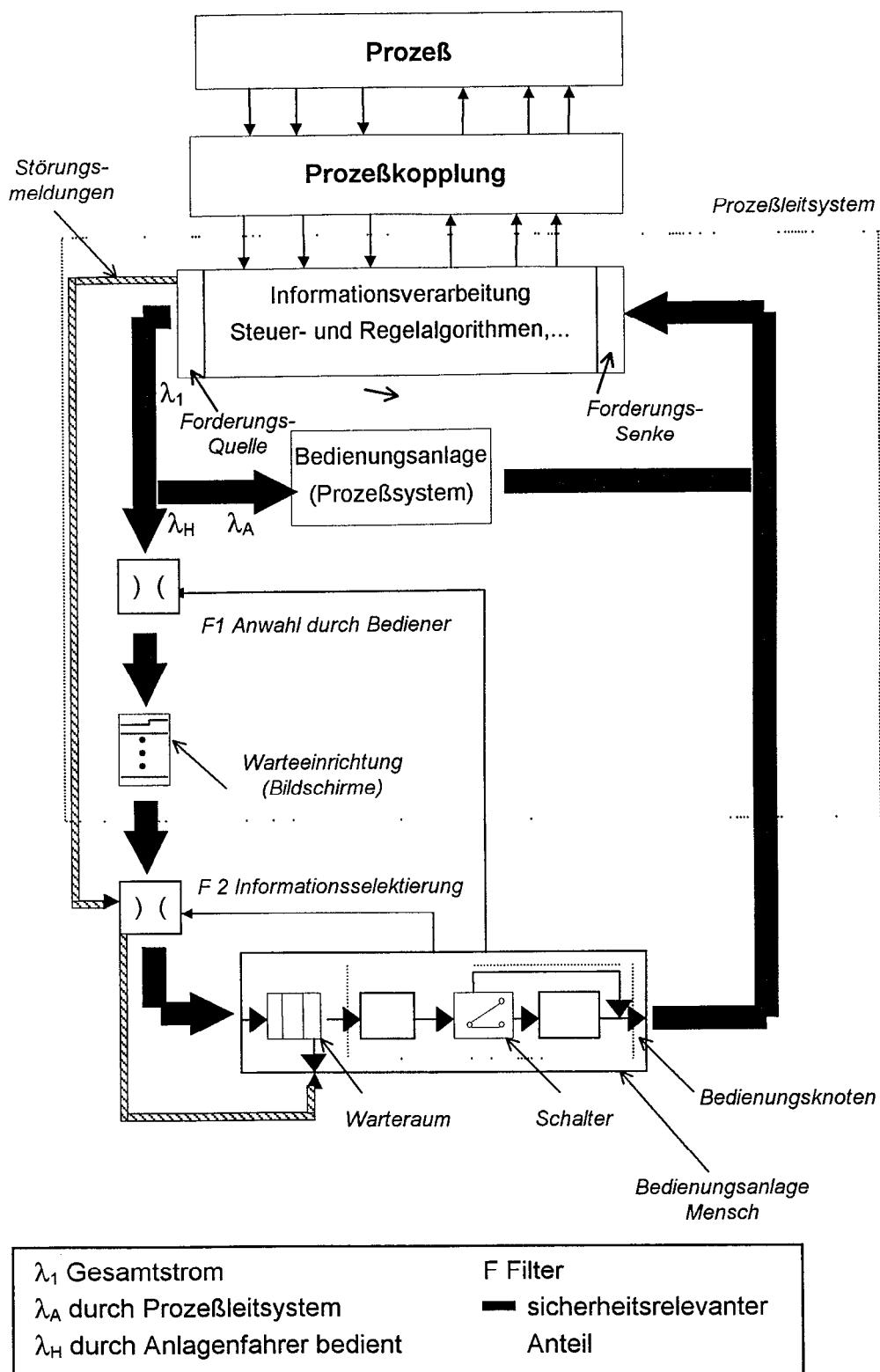


Abb. 6-4: Modell der Tätigkeit eines Bedieners als Bedienungssystem (Müller 1995)

In Abbildung 6-4 ist deshalb der Informationsstrom (Forderungsstrom) auf 3 Teilströme aufgeteilt, nämlich:

- (sicherheitsrelevante) Störungsmeldungen, die dem Bediener zwingend (unabhängig von seiner Anwahl) zugeführt werden.
- Informationen, für die der Bediener wählen kann, ob er sich einschalten will, oder ob er es der Automatik überläßt.
- Informationen, zu denen kein Handlungseingriff vorgesehen ist (Regelkreise, die für den Menschen zu schnell sind, zwingende Notabschaltung).

In der Abbildung sind deshalb mit F1 und F2 Auswahlmöglichkeiten für die Weiterleitung von Informationen dargestellt. Außerdem ist eingezeichnet, daß man durch die Art der Alarmgestaltung bemüht ist, die wichtigen sicherheitsrelevanten Informationen unabhängig von der Wahl des Bedieners an die der Verarbeitung nächste Stelle seines Warteraums zu bringen.

Weiterhin ist in Abbildung 6-4 dargestellt, daß angestrebt wird, im Bedarfsfalle begonnene, nicht sicherheitsrelevante Aufgaben liegen zu lassen und durch den eingezeichneten Schalter zu umgehen.

Betrachtet man ein Prozeßleitsystem als Netz von Informationsverarbeitungseinheiten, so ist selbstverständlich, daß neben der Rechenkapazität der einzelnen Einheit auch die Datenströme zwischen den Einheiten in Relation zu den technischen Grenzen bilanziert werden müssen. Man spricht gewöhnlich von einer Ressourcenbilanzierung. Ein bedienender Mensch ist funktionell mit einer informationsverarbeitenden Recheneinheit vergleichbar. Konsequenterweise ist er in die Ressourcenbilanzierung quasi gleichberechtigt einzubeziehen.

Durch die Leistungssteigerung der technischen Recheneinheiten sind deren Grenzen heute so weit weg, daß die Bilanzierung aus der Planungspraxis verschwindet. Die Leistungsfähigkeit des Menschen kann nicht gleichermaßen steigen, deshalb ist für ihn die Bilanzierung mehr denn je zu fordern.

Es ist also zu prüfen, ob seine Informationsverarbeitungsgeschwindigkeit zur Erledigung einer Forderung ausreicht und ob die Gesamtmenge der Forderungen aufgenommen und verarbeitet werden kann.

Die möglichen Hand-Automatik-Umschaltungen werden jeweils einzeln betrachtet und einzeln konzipiert. Allen Beteiligten ist klar, daß das nur für notwendige Reaktionszeiten sinnvoll ist, die vom Menschen bewältigt werden könnten. Nicht gleichermaßen selbstverständlich ist, darüber hinaus die Menge der gleichzeitig auftretenden Anforderungen zu betrachten.

Ausführbarkeit von Bedienkonzeptionen  
– Bilanzierung der Bedienerbelastung –

Reaktionszeiten  
Einzelkanal

+

Gleichzeitigkeit von  
Anforderungen

Ziel: keine unerledigten Forderungen (kein Überlauf)

Probleme:

- \* Entwurf des Handeingriffs bisher nur für Einzelkanäle  
(ungenügende Betrachtung der Gleichzeitigkeit)
- \* Notierung der Bedienaufgaben (z.B. im RI-Schema)

Akzeptiert man, daß die einem Anlagenfahrer zugesetzte Bedienkonzeption hinsichtlich ihrer Ausführbarkeit bilanziert werden muß, so ist es eine unerlässliche Voraussetzung, die Bedienaufgaben darzustellen. Zunächst einmal muß man sich Klarheit darüber verschaffen, welche Aussagen für eine Bedienstrategie notwendig sind.

### Aussagen zur Bedienstrategie

Bedienorte	Warte, örtlich, Reparaturschalter
Bedienmittel	Knöpfe, Tastatur, Hebel, Handräder
Bedientiefe	Struktur, Parameter
Bedienzeitpunkte	zyklisch, ereignisorientiert
Bedienberechtigung	durch Anlagenfahrer      für Instandhaltung für Inbetriebsetzung für Verfeinerung
Kontrolle der Bedienberechtigung	wiederholte Eingabefehler führen zur Informationsverweigerung
Bedienkontrolle	Registrierung (Protokollierung) der Eingriffe
Bedienungsalgorithmen	Betriebsvorschriften der Anlage
Beratungsmittel für Bedienhandlungen	Expertensysteme
-----	
Reaktion des Bedieners auf die Eigenüberwachung des Automatisierungssystems durch das Herausfiltern der handlungsauslösenden Signale	

Es ist üblich, die Informations- und Steuerfunktionen eines Prozesses in einem Rohrleitungs- und Instrumenten (RI-)Schema nach DIN 28004 oder DIN 19227, Blatt 1, darzustellen. Wenn man die sichere Ausführung von Bedienkonzeptionen herbeiführen will, muß man einen Weg suchen,

auch die Bedienaufgaben vergleichbar darzustellen. Abbildung 6-5 zeigt ein einfaches Beispiel. Dabei ist noch gesondert zu diskutieren, ob eine solche Darstellung von Bedienfunktionen zusätzlich im gleichen RI-Schema unterzubringen ist oder ob man aus Gründen der Übersichtlichkeit eine extra Darstellung entwickeln muß. Eine verbale Darstellung der Bedienfunktionen müßte grundsätzlich in den Betriebsbeschreibungen abgelegt sein.

Die Bilanzierung der Ausführbarkeit von Bedienkonzeptionen scheint das ungelöste zentrale Problem der Erhöhung der Bediensicherheit zu sein.

Unabhängig davon gibt es einige qualitativ bekannte Regeln, die besser umzusetzen sind. Dazu gehört u.a. die Alarmkultur. Bleiben Alarne über technische Mängel der Anlage längere Zeit anstehen, obwohl aus irgendwelchen Gründen der Betrieb trotzdem weitergeführt wird, so entsteht daraus eine unbewußte, aber tiefgreifende Entwertung jeder Alarmmeldung im Bewußtsein des Anlagenfahrers. Auch darin zeigt sich ein Planungsmangel. Entweder sind die als Gefahren gemeldeten Zustände für den Weiterbetrieb nicht wirklich gefährlich – dann wäre im Entwurfsstadium eine andere Darstellungsart zu suchen – oder der Betrieb wird trotz bestehender Warnmeldungen über gefährliche Zustände hinaus weitergeführt. Dann muß man Fragen zur Verantwortung der Betriebsführung stellen.

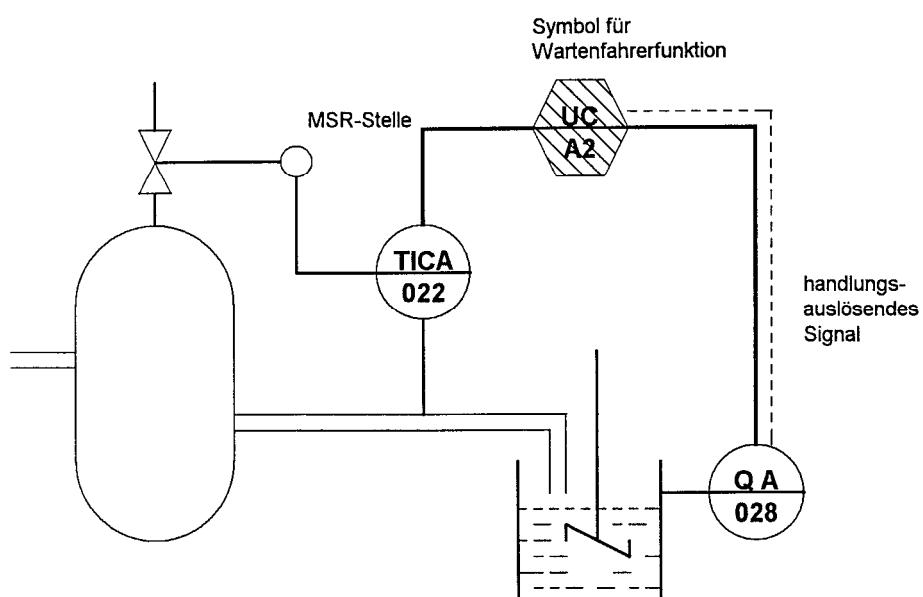


Abb. 6-5: Notierung von Bedienforderungen (aus: Müller 1997)

Frey und Mitarbeiter prägten zur Zusammenfassung derartiger Effekte den Begriff „gelernte Sorglosigkeit“. Dieser viel weiterführende Effekt sollte unter dem Blickwinkel Managementsysteme an anderer Stelle weiterverfolgt werden.

### Disziplinierte Arbeitsplatzgestaltung

Alarmkultur

Begrenzung der aktiven Alarmzahl: Umschaltung auf Gruppenalarm

Alarmspezifik an Handlungsmöglichkeiten orientiert

Als Anforderungen an die Darstellungsform der Bedienerbelastung – soll sie als Basis zur Prüfung der Bedienkonzeption dienen – sind festzuhalten:

- Die Art der Bedienanforderung muß erkennbar sein (Informationsaufnahme oder Handlung/Schaltung).
- Die Anzahl gleichzeitig ankommender Signale/Informationen muß erkennbar sein.
- Die Darstellungsform/Symbolik sollte sich an bestehende/bekannte Darstellungsformen anlehnen (z.B. RI-Schema).
- Die Darstellungsmöglichkeiten sollten auch die Bedienerbelastungen in nicht-bestimmungsgemäßen Betriebszuständen abbilden können.
- Die Detaillierungstiefe sollte je nach prinzipieller Funktion des Bedieners (Konti- versus Batch-Anlagen) variieren können. Für die Entscheidung über die Darstellungstiefe sind operationale Kriterien zu entwickeln.

### Komplex 4 – Bewertungsmaßstäbe/Bewertungshilfen

Sind schon in den Darstellungs- und Prüfinstrumenten deutliche Lücken und Unzulänglichkeiten erkennbar, so gilt dies für Bewertungsmaßstäbe im besonderen. Dies ist vor allem darin begründet, daß an die Sicherheit verfahrenstechnischer Anlagen kaum ein allgemeingültiger Maßstab zu legen ist. Dies gilt bereits für die technische Absicherung und ebenso für die Absicherung gegen Fehlbedienung, denn verfahrenstechnische Anlagen sind im allgemeinen individuelle Anlagen und nur sehr bedingt miteinander vergleichbar. Prüfinstrumente sind jedoch nur dann eine Hilfe zur Verbesserung der Anlagensicherheit, wenn sich auch Schlußfolgerungen (sprich: Bewertungen) daraus ziehen lassen.

Das zuvor genannte Hindernis für die Entwicklung allgemeingültiger Bewertungsmaßstäbe darf deshalb nicht dazu führen, daß sich der Bewertung der Bediensicherheit gar nicht erst genähert wird. Hinsichtlich physiologischer Leistungsgrenzen sollten relativ klare Bewertungsmaßstäbe festgelegt werden können. Hinsichtlich anderer HF-Bereiche (Qualität von Bedienungsanweisungen, des Sicherheitsmanagements u.ä.) sollten zumindest möglichst konkrete Bewertungshinweise möglich sein, die die unterschiedlichen, in verfahrenstechnischen Anlagen vorzufindenden Umstände berücksichtigen.

## Hürden zur Umsetzung der Erkenntnisse

Bei der Sichtung der Publikationen zu HF und Bediensicherheit kann leicht festgestellt werden, daß zwischen den beteiligten Expertengruppen (Arbeits- und Organisationspsychologen auf der einen Seite und Sicherheitsingenieuren und Anlagenplanern auf der anderen Seite) eine nur sehr begrenzte Kommunikation besteht

Wenn Müller (1995) feststellt, daß § 6 der 12. BImSchV zwar als prinzipielle Forderung im Raum steht, sich jedoch nirgendwo eine Anleitung zum Handeln, eine Regel, findet, so ist dies seiner Ansicht nach „Ausdruck dafür, daß das Problem nicht ingenieurtechnisch aufgearbeitet ist und daß aus der Ingenieurpsychologie die dort vorhandenen Grundlagen nicht zu umsetzbaren Regeln entwickelt sind.“

Ein zweites Problem ist die teilweise nicht in die Breite entwickelte „**positive Irrtumskultur**“: Fehler werden versteckt, statt daß sie systematisch aufgearbeitet werden und daraus gelernt wird. Zwar deuten zahlreiche Veröffentlichungen auf diesen Aspekt explizit hin, und es wurden bereits Methoden zur systematischen Ursachenanalyse entwickelt (z.B. SOL). Sie haben jedoch in manchen Unternehmen noch keinen Einzug gefunden in die üblichen Betriebsabläufe.

Es mag zwar der Wunsch und die Empfehlung sein, die Suche nach dem Schuldigen aufzugeben und statt dessen systematisch die Fehlerursachen aufzuarbeiten und entsprechende Schlußfolgerungen daraus zu ziehen, es entspricht jedoch noch lange nicht der Kultur in den meisten Betrieben. Dazu wäre es notwendig, allen Beteiligten (Management, Schichtleiter, Bediener, Wartungs- und Instandhaltungspersonal, Sicherheitsingenieur und Anlagenplaner und nicht zuletzt auch der Aufsichtsbehörde) eine andere Einstellung zu vermitteln. Beginnen könnte man beispielsweise mit einer neuen Aufarbeitung gemeldeter Störfälle, bei der die Ursachensuche nicht mit dem Ergebnis „Fehlbedienung“ endet, sondern tiefer geht und auch die Vernetzung mehrerer Fehlerquellen und eine Differenzierung aktiver und latenter Fehler aufdeckt. Unternehmensintern sind solche Aufarbeitungen bereits feststellbar, sie werden jedoch noch nicht einer größeren Fachöffentlichkeit als Informationsquelle zur Verfügung gestellt.

Eine weitere Hürde liegt in dem Irrtum begründet, Information könne nicht verloren gehen. Tatsächlich kann Information im ungünstigen Fall irreversibel verloren gehen.

Die Umsetzung der Erkenntnisse wird auch all zu oft durch die menschliche Ignoranz gegenüber Erkenntnissen, die nicht aus dem eigenen Arbeits- und Erfahrungsfeld stammen, vermindert. Dem Problem Fehlbedienung begegnet der Sicherheitsingenieur vorzugsweise (bzw. allein) mit der Weiterentwicklung fehlertoleranter Technik. Daß parallel dazu auch mit dem Menschen und seiner unmittelbaren Umgebung zu arbeiten ist, kommt ihm kaum in den Sinn. Dies zeigt schon die Tatsache, daß bei Sicherheitsgesprächen im Rahmen einer Anlagenplanung Arbeitspsychologen nur in den seltensten Fällen anzutreffen sind.

Alle genannten Hürden können jedoch nicht systematisch angegangen werden, solange eine grundlegende Voraussetzung fehlt:

Es fehlt eine Dokumentationsmethodik für die Bedienkonzeption, die eine Prüfbarkeit überhaupt erst ermöglicht.

Die Dokumentation muß neben den Bedienhandlungen im Normalbetrieb insbesondere auch die erforderlichen Bedienhandlungen im Störbetrieb, konsequent für alle erkannten anlagenbezogenen Gefahren, erkennbar machen. Erst dann ist es möglich zu identifizieren, wo menschliche Leistungsgrenzen überschritten werden und wo im einzelnen Schulungen und Trainings oder auch Änderungen des Anlagendesigns anzusetzen haben.

Dieses Forschungsvorhaben soll hierzu einen Beitrag liefern. Damit die zu erstellenden Methoden und Materialien, die im Rahmen des Projektes entwickelt bzw. zusammengezustellt werden, am Ende in der Praxis eingesetzt werden, muß den Bedenken der Betreiber verfahrenstechnischer Anlagen ausreichend begegnet werden:

- Qualität verfügbarer Materialien: zuviel, zu kompliziert, zuviel Zeitbedarf
- Unklare Zusammenhänge zwischen den einzelnen Strategiefeldern Technik, Organisation und Person
- Uneinheitlichkeit in Art und Umfang der Dokumentationen
- Befürchtungen, ein neues (überflüssiges?) Regelungsfeld („Vorkehrungen gegen Fehldienungen“) zu öffnen
- keine ausreichende Differenzierung von Anlagen- bzw. Verfahrenstypen.

In diesem Forschungsvorhaben wurden mehrere Darstellungsmöglichkeiten anhand von Praxisbeispielen getestet und jeweils mit ihren Vor- und Nachteilen gegenübergestellt.

## 7. Entwicklung von Methodiken zur prüfbaren Darstellung der Bedienkonzeption

### Vorbemerkung

In Kapitel 6 wurde herausgearbeitet, daß die Menge der Informationen oder Informationsströme mit der Grenze der menschlichen Leistungsfähigkeit kollidieren kann. Zur Prüfung der Bedienkonzeption einer Anlage soll eine Notierungsform (Darstellung der Bedienkonzeption) erarbeitet werden, welche die Anforderungen an den Bediener den menschlichen Leistungsgrenzen prüfbar gegenüberstellt.

Die Abbildung<sup>1</sup> 7-1 zeigt die Einflüsse auf die Leistungsfähigkeit eines Bedieners und verdeutlicht den Bilanzquerschnitt, auf den die Methoden zur prüfbaren Darstellung der Bedienkonzeption hinsichtlich der Informationsströme abzielen.

Abbildung 6-3 in Kapitel 6 zeigt das bedientheoretische Modell eines Anlagenfahrers. Ankommende Forderungen sind dadurch gekennzeichnet, daß bestimmte Reaktionszeiten, also Zeiten bis zur Erledigung, einzuhalten sind. Der Prozeß hat eine begrenzte zeitliche Toleranz, in der Gegenmaßnahmen zu einer sich anbahnenden Störung noch wirksam sein können. Werden die zulässigen Wartezeiten überschritten, so stellt das in dem hier betrachteten Zusammenhang einen unzulässigen Zustand für den gesteuerten Prozeß dar. In der Sprache der Bedientheorie verläßt eine ungeduldige Forderung unerledigt den Wartezeitraum.

Ziel jeder Bedienkonzeption für einen Anlagenfahrer muß es sein, Verluste durch unerledigte Forderungen zu vermeiden.

In diesem Zusammenhang ist daran zu erinnern, daß es für die Informationen keinen Erhaltungssatz wie für Masse und Energie gibt:

- Nicht wahrgenommene oder nicht verarbeitete Informationen verschwinden im Überlauf.
- Fehlentscheidungen des Bedieners wirken sich als Abweisen von Forderungen aus.
- Erfolgt keine Reaktion des Bedieners auf eine Forderung, kann es sein, daß aus dem Prozeß mit seiner Automatik erneut Forderungen – in der Regel weitere bzw. andere – kommen.

Die komplizierten Vorgänge bei zweistufigen Alarmen und bei übergeordneten automatischen Notabschaltungen werden in Abbildung 6-3 nicht dargestellt, um die Verständlichkeit nicht zu belasten. Es wird vorausgesetzt, daß die technischen Konzepte zum Abweisen von Bedienfehlern unvollständig sind, so daß die richtige und aufmerksame Bedienung für die Anlagensicherheit wichtig ist.

<sup>1</sup> Die Abbildungen und Tabellen zu diesem Kapitel befinden sich am Ende des Kapitels (Seiten 99ff)

## 7.1 Vergleich und Bewertung verschiedener Notierungsformen

Will man eine Notierungsform für die Bedienkonzeption entwickeln, so ist es angebracht, diese an eine bestehende und eingeführte Notierungsform aus der Verfahrens-Anlagen-technik zu knüpfen. Nachfolgend werden verschiedene Möglichkeiten diskutiert und auf ihre Anwendbarkeit geprüft.

### **Bedienfunktionen-Schema**

Nach dem Vorschlag von Bergmann und Müller (Müller, R. 1991 und Müller, R. 1992) sollen, vergleichbar der Darstellung von MSR- oder PLT-Funktionen in einem Rohrleitungs-Instrumenten-Schema (RI-Schema) nach DIN 28004 oder DIN 19227, zeitunabhängig die möglichen Informationsverarbeitungsknoten und ihre Verbindung zu Meßgebern und Stellgliedern dargestellt werden (Abbildung 6-5 in Kapitel 6). Ein solches Bedienfunktionenschema liefert die notwendige Übersicht, welche Informationsaufnahme und -verarbeitung dem Bediener zugeordnet ist, aber noch ohne Berücksichtigung der Zeiten, in denen diese Informationen verarbeitet werden müssen.

Abweichend von den früher publizierten Vorschlägen wird für die Bedienfunktion ein auf der Spitze stehendes Quadrat, oder bei mehr Zeichenbedarf für die Beschriftung ein Rhombus vorgeschlagen.<sup>2</sup> Während die meisten Regelkreise nur eine Meßgröße mit einer Stellgröße verknüpfen, ist für den Bediener typisch, viele Informationen zueinander in Beziehung zu setzen. Die Zahl der Wirkungslinien zu den Bedienstellen ist deshalb sehr viel größer als für die MSR-Funktionen. Man kann aber von einem Bediener nicht die Beherrschung vieler Informationsverknüpfungen verlangen, wenn man schon davor zurückschreckt, diese Verknüpfungen überhaupt darzustellen.

Die Darstellung der Bedienfunktion über das Symbol für Handeingriff am Stellglied hinaus ist notwendig, da für die Bedienhandlungen oft mehrere Informationen zu verknüpfen sind.

Hierbei ist vorläufig die Betrachtung auf die Schemata der Anlagenplanung ausgerichtet. Die üblicherweise praktizierte Darstellung von Ausschnitten aus RI-Schemata auf den Bedienungs-Bildschirmen wird (noch) nicht betrachtet.

Für diese Darstellung sind zwei Varianten denkbar:

1. Eintragung der Bedienfunktionen in das RI-Schema
2. Separates Bedienschema mit Bedienfunktionen.

Für die erste Variante spricht, daß man für das Bedienschema nahezu alle MSR-Stellen mit Anzeige- oder Alarmfunktion braucht. Andererseits gibt es gewöhnlich mehr Signalverknüpfungen zur Bedienung als für die Regelung und Steuerung. Die Aussagefähigkeit des

<sup>2</sup> Das ursprünglich publizierte Sechseck wurde inzwischen in DIN 19227 für Prozeßrechnerfunktionen vergeben.

RI-Schemas zu den Automatisierungsfunktionen wird dabei durch die mit den vielen Signalverknüpfungen des Bedienschemas einhergehende Unübersichtlichkeit gemindert.

Bei der zweiten Variante müssen alle Symbole für Meß- und Stellglieder in dem separaten Schema noch einmal dargestellt werden. Zu Zeiten der rechnergestützten Zeichnungs erstellung sollte eine solche partielle Kopie des RI-Schemas kein Problem sein.

Entscheidend für die Wahl der Variante ist die Notwendigkeit der Beurteilung von Wechselwirkungen zwischen Automatik und Bedienung.

Bei vielen Anlagen ist zu erwarten, daß es nur ganz wenige im RI-Schema darzustellende Funktionen gibt, die keine Bedeutung für die Bedienung haben. Solche Funktionen sind in der Regel ausschließlich maschinenorientiert, wie z.B. Informationen zur Identifikation von Wartungsbedürfnissen und zur Störungsanalyse.

Welche der beiden Varianten die geeigneter ist, soll nachfolgend anhand von ausgearbeiteten praktischen Beispielen geprüft werden.

### **Bedienfunktionen im RI-Fließbild für ein von der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin publiziertes Beispiel**

Von der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) wurden als Regelwerk Rw 27 Beispiele für systematische Sicherheitsbetrachtungen nach TRGS 300 publiziert. Bevor reale Praxisbeispiele untersucht werden, sollen einige Überlegungen an einem solchen, als mustergültig anzusehenden Beispiel demonstriert werden.

Die Abbildungen 7-2 und 7-3 (RI-Schemata mit eingetragenen Bedienfunktionsstellen für Rohstoffversorgung und Reaktor) zeigen die in die Fließbilder des Beispiels aus Rw 27 von den Autoren dieses Berichtes eingezeichneten Bedienfunktionen. Bei der Benutzung dieses Beispiels muß man berücksichtigen, daß dieses Beispiel an der TRGS 300 und nicht an weiterführenden Betrachtungen zur Bediensicherheit orientiert ist.

#### Kommentar zu den eingetragenen Bedienstellen

Die Gliederungsnumerierung der Prozeßbeschreibung in Rw 27 wurde als "Schritt des Produktionsplanes" übernommen. Die Schritte 10, 11, 12 werden durch Grenzwert- oder Zeitschalter ausgelöst.

Es wurden nur von der Warte auszuführende Bedienfunktionen und die für die Bedienung von der Warte aus relevanten Rückmeldungen des örtlichen Anlagenpersonals eingetragen. Die Schemata enthalten zusätzlich örtliche Meßstellen, die für Störungsbeseitigung durch Reparaturen hilfreich sind.

Folgende Noteingriffsfunktionen, die in der Verfahrensbeschreibung keine Erwähnung

fanden, wurden zusätzlich definiert:

- N 2.01 Überfüllalarm B 1
- N 4.01 Überfüllalarm B 3
- N 1.01 Mangelalarm Kühlwasserzufluß
- N 1.04 Stromaufnahme oder Drehzahl des Rührwerkes nicht normal
- N 1.20 Temperaturalarm Notkühlung (automatisch gesteuert + Alarm)
- N 1.19 Absperren aller Leitungen bei Druckanstieg.

Das Schema für den Reaktor enthält auch eine Grenzwertfunktion (GO 1.21), die keinen Alarm enthält und die in keine Verarbeitung eingebunden ist. Die Beobachtungsmöglichkeit zur Kontrolle eines örtlichen Noteingriffs wird in dem für die TRGS 300 interessierenden Zusammenhang nicht angesprochen.

Die Notfunktion N 1.04 muß außer dem unmittelbaren Stelleingriff einen nicht dargestellten Ablaufplan auf weitere Stelleingriffe auslösen.

Die Funktion PIC 1.17 sollte um einen Alarm ergänzt werden, da die Kontrolle des Druckes durch den Bediener in der Verfahrensbeschreibung dargelegt ist. Damit ergibt sich ohne nennenswerten Aufwand diversitäre Redundanz zu FIC-A 1.14.

#### Bewertung des Beispiels

Die ganze Philosophie der MSR-Stellen im Fließbild ging von Anlagen mit kontinuierlichen Fließgutprozessen, d.h. überwiegend mit Regelungen, aus. Für die Regelungen ist typisch, daß gewöhnlich nur eine Prozeßvariable zu betrachten ist. Die dem Prozeß innewohnenden Wechselwirkungen zwischen den einzelnen physikalischen Größen müssen weder abgebildet noch verarbeitet werden, es ist gerade die ausschlaggebende Eigenschaft der Regelung, Einflüsse aus solchen Wechselwirkungen, die im Prozeß intern wirken, zu kompensieren. D.h., es sind kaum Verbindungen in der Automatik zwischen den einzelnen Regelkreisen notwendig und darzustellen.

Bei binären Steuerungen muß der ganze technische Ablauf in der Steuerung abgebildet werden. Dafür sind andere Beschreibungen, wie Petri-Netze (standardisiert als Funktionsplan nach DIN 40719 oder IEC 60848), Prozeßablaufplan (siehe unten) o. ä. eingeführt. Die MSR-Stellen im RI-Fließbild sind dabei nur geeignet, die Prozeßkopplung der Steuerung deutlich zu machen.

Dieses Problem wird in den Abbildungen 7-2 und 7-3 indirekt deutlich. Die Darstellung wird nahezu erdrückt von der Einzeichnung der vom Menschen wahrzunehmenden Verknüpfungen zwischen den MSR-Stellen und von den Konnektoren, die die Signalverknüpfungen über die einzelnen Blätter der Darstellung hinweg zeigen.

Die Konsequenz aus dieser Betrachtung und diesem Beispiel ist: Nur wenn Regelungen dominieren, hat man ausreichend Aussichten, die nötige Übersicht im RI-Schema zu behalten. Dominieren Steuerungen, z.B. für die Abläufe eines Chargenprozesses, ist das

Bedienfunktionen-Schema weniger geeignet, es bleibt vorwiegend den kontinuierlichen Fließgutprozessen vorbehalten.

### **Darstellung der Bedienaufgaben als Prozeßablaufplan**

Der Prozeßablaufplan (PRAP) wurde zur Notierung von Steuerungsaufgabenstellungen als Verständigungsmittel zwischen Verfahrenstechnologen und Automatisierungstechnikern entwickelt. Dabei wurden folgende Ziele verfolgt:

- Durch den Zwang zu einer detaillierten formalisierten Notierung wird die Aufgabenstellung frei von Interpretationsmöglichkeiten unscharfer Angaben.
- Durch die Prüfbarkeit auf Vollständigkeit und Widerspruchsfreiheit werden die meisten Fehler und Lücken der Aufgabenstellung aufgedeckt.

Für die Erarbeitung stand das Softwarewerkzeug TECAD aus dem System TEPROS<sup>3</sup> zur Verfügung, das die Prüfalgorithmen und die automatische Erzeugung von Listen der Operationsvariablen (Befehle) und Zustandsvariablen (Meldungen) einschließt.

Die Beseitigung des Interpretationsspielraumes und die Prüfung der Aufgabenstellung führte beim Steuerungsentwurf zur Verkürzung der Inbetriebsetzungszeiten um Faktoren 3 bis 10, weil bei der Inbetriebsetzung soviel weniger Korrekturnotwendigkeiten (ändern von Verknüpfungen, Umklemmen) gegenüber mit herkömmlichen Methoden geplanten Steuerungen auftraten (Graul und Krause 1987) und (Müller, R. 1987).

Üblicherweise zerlegt man für den Prozeßablaufplan den Gesamtprozeß in Teilprozesse (TP)<sup>4</sup>, so daß handliche Darstellungen auf einem Blatt entstehen. Diese Teilprozesse werden dann durch Koppelvariablen verknüpft.

Zur Demonstration der Methode wurde wieder das Beispiel 3 aus der o. g. Schrift Rw 27 der BAuA herangezogen.

Dabei kann man sich folgende Teilprozesse vorstellen:

- TP 1 Bereitstellung Monomer 1
- TP 2 Bereitstellung Starter
- TP 3 Bereitstellung Monomer 2
- TP 4 Reaktor vorbereiten und füllen
- TP 5 Reaktion durchführen
- TP 6 Störungsanalyse Ventil
- TP 7 Störungsanalyse Pumpe

<sup>3</sup> Firma Automatisierung in Verwaltung und Industrie, Schwarze Pumpe (URL [www.avinet.de](http://www.avinet.de))

<sup>4</sup> „Teilprozeß“ ist ein Begriff des Softwaresystems TECAD für einen Teil einer Ablaufbeschreibung.

- TP 8 Störungsanalyse Druck
- TP 9 Störungsanalyse Dichtheit

...

Die Abbildungen 7-5 und 7-6 zeigen die Prozeßablaufpläne für die TP 1 und 2, die Tabellen 7-1 bis 7-4 verdeutlichen die hinsichtlich der negierten Variablen noch nicht bearbeiteten, vom Programm automatisch erzeugten Variablenlisten.

Zweifellos ist diese Art der Darstellung mühsam, der Erkenntnisgewinn hinsichtlich unge- nauer Vorgaben ist aber beträchtlich. Zur Illustration dieser Aussage wird wieder das Beispiel aus Rw 27 herangezogen. Dort gibt es Befehle, die auf die Bodenarmatur des Behälters 1 und die Pumpe 1 verzweigt werden, obwohl es zu beiden Stellgliedern getrennte Rückmeldungen gibt. Die Diagnosemöglichkeiten auf technische Störungen, wenn nach einer Betätigung nur eine der beiden Rückmeldungen kommt, wird in Rw 27 nicht erörtert. Zeichnet man einen Prozeßablaufplan, wird man von dem Zeichenprogramm gezwungen, die beiden Rückmeldereaktionen getrennt zu betrachten. Für die Bedienung, d.h. für Aktionen, gibt es keine Gleichzeitigkeit. Diese gibt es nur für Zustände. Wenn gefordert wird, Ventile (V 1.07 und V 2.03) zu betätigen und gleichzeitig die Pumpe P1 zu starten, muß das im Detail nacheinander erfolgen.

Dieses Werkzeug wurde für den Entwurf binärer Steuerungen erarbeitet. Der Ablauf ergibt sich dabei aus den erreichten Zuständen. Deshalb ist weder die Menge der vom Bediener gleichzeitig wahrzunehmenden Signale noch der Zeitablauf unmittelbar darstellbar. Für den Zeitablauf ist in dem Softwarewerkzeug eine Hilfe enthalten: Zu jedem Block ist ein Feld erklärender Text programmiert.

Im PRAP für den TP 1 wurden die angenommenen Zeiten für den Ablauf der einzelnen Schritte eingetragen.

Bisher ist unklar, ob ein Bediener eine angestoßene Aktivität, z.B. "Ventil xy öffnen" im Auge behält, und damit seinen begrenzten Speicherplatz belastet, bis das Ziel der Operation, d.h. z.B. "Ventil offen" erreicht ist, oder ob er nach Anstoßen der Aktivität seinen Speicherplatz frei macht und sich der nächsten Forderung zuwendet.

Geht man davon aus, daß der Mensch die angestoßene Operation bis zum Erreichen des Zielzustandes verfolgt, bietet der PRAP eine gute Möglichkeit zur Kontrolle der Gleichzeitigkeit, weil man dann nur ein Fenster mit sieben Aktivitäten (siehe hierzu auch Kapitel 6) über den PRAP zu schieben braucht. Mehr, als in dem Fenster unterzubringen ist, kann ein Bediener nicht ausführen. Daraus ergeben sich z.B. Zeiten für die Durchführung von Bedienabläufen, die man mit den für den Prozeß zulässigen Zeiten vergleichen kann.

An dieser Stelle wird diese Hypothese nicht weiterverfolgt, da noch psychologische Grund- satzforschung erforderlich ist, um zu klären, ob ein bedienender Mensch eine angestoßene Maßnahme bis zu ihrem Abschluß im Auge behält.

### 7.1.1 Demonstrationsbeispiel kontinuierlich arbeitende Anlagen (kontinuierlicher Fließgutprozeß)

#### Erfassung der Zeitabhängigkeit und Gleichzeitigkeit von Bedienanforderungen

Die u.a. in DIN IEC 56(SEC)423 niedergelegte und relativ gut gesicherte Erkenntnis, daß die Teilbarkeit der menschlichen Aufmerksamkeit auf  $7 \pm 2$  "psychologische Einheiten"<sup>5</sup> begrenzt ist, ist auch die gegenwärtig nahezu einzige anwendbare Bewertungsgröße für die Verarbeitungsmenge der Informationen, die der Mensch durch akustische oder optische Signale erhält und die er gleichzeitig und sicher in akustische Signale wandeln bzw. weiterleiten oder in manuelle Handlungen umsetzen kann.

Unter der Voraussetzung, die Zahl 7 als Grenze möglicher gleichzeitiger Aufmerksamkeit als gesicherte Größe anzusehen, und unter Vernachlässigung der Frage, ob manchen Aufgaben mehrere "psychologische Einheiten" entsprechend DIN IEC 56(SEC)423 zuzuordnen wären, wurde ein Balkendiagramm zur Erfassung des Ablaufes von Bedienabläufen entworfen (Abbildung 7-7).

Dabei wird für alle Vorgänge eine Zeit angesetzt, die in der Regel geschätzt werden muß. In einigen Fällen ist sie durch die Laufzeit von Stellgliedern, bei denen die Rückmeldung des Erreichens der gewünschten Position abzuwarten ist, gut bekannt.

Das Balkendiagramm geht davon aus, daß die achte Aktivität erst begonnen werden kann, wenn eine der vorangegangenen sieben abgeschlossen ist.

Das im Abbildung 7-7 skizzierte Beispiel wurde auf der Basis interner Bedienanweisungen eines petrochemischen Werkes erarbeitet. Als wesentliche Darstellungsformen für die Darstellung der Bedienhandlungen sind **Betriebsvorschriften (BV)** und **Betriebshandbücher** üblich.

Anhand einer Betriebsvorschrift einer Chemieanlage, die als kontinuierlicher Fließgutprozeß (Definition nach Müller, R. 1979) arbeitet, soll untersucht werden, inwieweit bei der Beschreibung der Bedienerhandlungen das "Gleichzeitsproblem" berücksichtigt wurde.

Erschwerend für die Betrachtung ist, daß auffällig viele Befehle in der vorliegenden Betriebsvorschrift nicht abschließend aufgeführt sind, sondern auf weitere Betriebsvorschriften (siehe nachfolgendes Beispiel) verweisen. Auch ist zu beachten, daß der Bediener die Möglichkeiten des Zugriffs auf die Verweisstellen haben muß, die elektronisch oder auf Papier vorliegen können.

<sup>5</sup> Eine psychologische "Einheit" ist die Inanspruchnahme eines Informationskanals

### Beispiel 1: Ausfall Rührwerk (1. Kristallisator) nach BV 985

- Nimm beide (parallelen) Reaktoren gemäß BV (985 Teil 2, Seiten 9, 10)<sup>6</sup> auf "Halten".  
In der BV zum "Halten"<sup>7</sup> beider Reaktoren wiederum ist festgelegt
  - informiere gemäß BV 981, daß Reaktor auf Halten geht.
- Entleere Apparat bis Gasphase bzw. Abriß Pumpe
  - entspanne
  - und restentleere Behälter gemäß BV (Nr. 985 Teil 2, Seite 4).
- Lasse Störungsursache beseitigen und nimm Apparat gemäß BV (Nr. 985 Teil 1, Seite 20) in Betrieb.
- Starte Reaktoren gemäß BV (Nr. 985 Teil 1, Seite 24).

Die beiden letzten Punkte sind allerdings nicht in einer zeitlichen Zwangfolge mit der Störungsabwehr verbunden. Es kommt aber deutlich zum Ausdruck, daß es sich bei der Formulierung der Anweisungen nicht um abschließende, d.h. eindeutige Befehle handelt.

Die Betriebsvorschriften sind als Original in Papierform in der Meßwarte abgelegt. Zusätzlich sind sie über die Bildschirme aufrufbar. Die untersuchte Betriebsvorschrift ist nach technischen Betriebseinheiten aufgegliedert. Die betrachtete Betriebseinheit (BE) enthält eine Reaktionsstufe mit zwei parallelen Reaktoren gleicher Bau- und Wirkungsart mit einer nachfolgenden mehrstufigen Kristallisation. Daneben ist der Umgang mit den für den Prozeßablauf erforderlichen Hilfsstoffen und Energien beschrieben. Im Einzelnen ist im Inhaltsverzeichnis aufgeführt:

#### Inbetriebnahme

- Inbetriebnahme von Hilfsstoffen und Energie
- Inbetriebnahme der Anlage
- Normalbetrieb
  - mit: Abweichungen von Normalbetrieb

#### Außerbetriebnahme

- Außerbetriebnahme der Anlage
- Spülung des Systems
- Außerbetriebnahme von Hilfsstoffen und Energie
- Störungen und deren Beseitigung
  - mit: Ausfall von Rührwerken
  - Ausfall von Regelventilen
  - technische Störungen
  - wichtige technische Noteingriffe
    - Ausfall von Roh- und Hilfsstoffen sowie Energien
    - havariemäßige Außerbetriebnahme

<sup>6</sup> Sämtliche in den Beispielen 1 und 2 in Klammern gesetzte Hinweise sind in der BV nicht mit aufgeführt

<sup>7</sup> "Halten" ist ein Zustand, bei dem die Anlage unter bestimmten technischen Parametern, wie Temperatur, Druck, Füllstand o. ä. verharrt

Im Weiteren soll zunächst das Kapitel **Störungen und deren Beseitigung** und hierbei die beiden Störungsarten:

- technische Ausfälle von Ausrüstungen (Rührwerke, Regelventile)
- Ausfall von Roh- und Hilfsstoffen sowie Energien

betrachtet werden.

Zu diesen Störungsarten kann postuliert werden:

- Das Eintreten dieser Störungen kann vom Bediener nicht beeinflußt werden.
- Der Bediener wird zu (Abwehr-)Handlungen gezwungen.

Da der Begriff Bediener hier noch in "Örtlichen Anlagenbetreuer" (ÖAB), der vor Ort agiert, und Meßwartenfahrer (MWF) zu unterteilen ist, muß die vorstehende Aussage in folgender Form konkretisiert werden:

- Das Eintreten dieser Störungen wird dem MWF über technische Kommunikationsmittel (Meßwartenbildschirmtechnik und akustischer Alarm) zur Kenntnis gebracht.
- Das Eintreten dieser Störungen kann vom Bediener (ÖAB und MWF) nicht verhindert werden und zwingt ihn zu Handlungen.
- Es kann eine Kommunikation zwischen mehreren Bedienern notwendig werden, zum Beispiel zwischen MWF als Überwacher der Maßnahme und ÖAB als vor Ort Handelnder.

Unter der Berücksichtigung, daß näherungsweise die Belastungsgrenze des Bedieners neben der ständigen Überwachung von Soll- und Ist-Werten durch die Übernahme von vier von Hand gefahrenen Regelkreisen liegt, ist zu erwarten, daß der MWF diese Grenze schnell erreicht haben kann, wenn Anlagenstörungsmeldungen reihenweise einlaufen. Dies gilt insbesondere bei vernetzten Anlagen, wo üblicherweise eine Apparatestörung Störungen in weiteren nachgeschalteten (abhängigen) Anlagen(teilen) nach sich zieht. Erfahrungsgemäß ist es unerheblich, wieviele Meßstellen dem Bediener bzw. einem Bedienplatz an sich zugeordnet sind. Bei kontinuierlichen Fließgutprozessen ist sicher zu berücksichtigen, daß an dem Punkt, wo mit Wahrscheinlichkeit die Belastungsgrenze des Bedieners überschritten wird, durch den Anlagenplaner die "sichere Endlage" aller geregelten Stelleinrichtungen vorgesehen ist, d.h. übergeordnetes automatisches Not-Abfahren erfolgt.

Derartige unter der Überschrift "Ausfall von Roh- und Hilfsstoffen und Energien" zu einem havariemäßigen Abfahren der Anlage führenden Handlungsabläufe sind "nicht vernünftigerweise auszuschließende Störfälle" (vgl. Abbildung 5-1 in Kapitel 5), für die durch Unterbrechung des Betriebes Vorsorge getroffen wird, da ein Bediener solche Störungsursachen nicht kompensieren kann.

Ein Versagen der gefahrlosen Endlage und Nachhelfen von Hand wird bei der Komplexität der hier betrachteten Anlage nicht in Betracht gezogen.

### Beispiel 2: Petrochemische Anlage

#### Technische Beschreibung

Die betrachtete petrochemische Anlage ist nach den erforderlichen technischen Vorstufen zur Produktanmischung mit zwei parallel geschalteten gleichartigen Reaktoren ausgerüstet. Diese Reaktoren sind als Rührwerksbehälter ausgeführt. Unter Zuführung von Luft erfolgt eine exotherme Reaktion, die im Ergebnis unter Beachtung der verströmten Luft ein Dreiphasengemisch erzeugt. Die flüssige Phase wird mit dem Feststoff am Reaktorboden abgezogen und strömt in einen nachgeschalteten 1. Kristallisator, in welchen für eine Nachoxidation Luft eingeblasen wird. Aufgrund der niedrigeren Temperatur fällt in diesem Behälter weiterer Feststoff aus der Lösung aus.

Die Einströmventile der beiden Zulaufleitungen von den Reaktoren zu dem 1. Kristallisator werden über den Füllstand der Reaktoren gestellt.<sup>8</sup>

Die Meßwarte ist in Bildschirmtechnik (Honeywell TDC 3000) ausgeführt. Es sind insgesamt acht Bildschirme von einer Bedienperson zu betrachten. Die Bilddarstellungen auf allen Schirmen sind frei wählbar. Auf allen Schirmen sind alle Darstellungen aufrufbar.

Die Meßwarte ist zusätzlich mit Kommunikationstechnik ausgerüstet: Telefon, Faxgerät, Wechselsprechanlage.

#### Technische Ausfälle von Ausrüstungen (Rührwerke, Regelventile)

Für die Untersuchung der Handlungsabläufe bei Störungen wird das gleichzeitige Versagen eines (Standregel)-Ventils am Eingang des 1. Kristallisators und des Rührwerkes im 1. Kristallisator angenommen.

Der Ausfall des Standregelventils führt zum "Halten"<sup>8</sup> eines Reaktors. Durch die Kombination des unmittelbar/gleichzeitig ausfallenden Rührwerkes im nachgeschalteten 1. Kristallisator wird das "Halten" der beiden Reaktoren erforderlich.

Da das Standregelventil des Reaktors am Eingang des Kristallisators installiert ist und in Fließrichtung in der Produktleitung in der Reihenfolge "Kugelhahn, Schnellschlußventil, Standregelventil, Kugelhahn" die Absperrorgane angebracht sind, ist bei dieser Störung das "Abfahren" der Reaktoren vermeidbar.

<sup>8</sup> Die komplizierten stofflichen Eigenschaften des strömenden Mediums geben dem Bediener im Falle einer Störung ein besonders schwieriges Problem auf

Aus den Betriebsvorschriften ergeben sich folgende, parallele Handlungsabläufe:

### Ausfall Standregelventil

(Reaktor – Eingang 1. Kristallisator)

- Nimm beide (parallelen) Reaktoren gemäß BV auf "Halten"

- Nimm nachfolgenden Behälter (1. Kristallisator) gem. BV a. B.<sup>9</sup>

- Lasse defektes Regelventil demontieren.  
*Dies ist eine Handlung, die für die Bedienerbelastung unerheblich ist.*

### Ausfall Rührwerk

(1. Kristallisator)

- Nimm beide (parallelen) Reaktoren Gemäß BV auf "Halten"

*Anmerkung:*

- BV zum "Halten" beider Reaktoren:  
Handlungen, die für den 2. Reaktor Vorzunehmen sind, während für den 1. Reaktor gemäß BV noch Handlungen Vorzunehmen sind:
  - Nimm ein Gebläse i. B.<sup>10</sup>
  - hänge die Abgasleitung ab und entspanne sie

- Entleere 1. Kristallisator bis Gasphase

- Entspanne und restentleere Behälter gemäß BV und führe gegebenenfalls (**operative Entscheidung**) Spülung durch

Beide Störungen sind hier gegeneinander gestellt, um vergleichbare Handlungen zu erkennen. In den beiden Kapiteln der BV erscheint der Verweis: BV zum "Halten" beider Reaktoren. Im Einzelnen ist das gleichzeitige "Halten" des 1. und 2. Reaktors in der BV wie folgt zu behandeln:

#### 1. Reaktor

- Informiere, daß *ein* Reaktor auf "Halten" geht
- Senke Durchsatz des Reaktors auf x Nm<sup>3</sup>/h ab
- Nimm einen Seitenabzug durch Betätigen von 2 Regeleinrichtungen a.B.
- Wechsel die Rührergeschwindigkeit
- Senke Durchsatz weiter ab
- Halte Abgaskonzentration ein (gesonderte BV)
- Kontrolliere Arbeitsweise einer Regelung
- Beobachte das Verhalten von 3 Regelungen
- Korrigiere (falls erforderlich) durch Öffnen oder Schließen von Umfahrungen
- Senke Durchsatz auf Null ab
- Schließe Gaszufuhr
- Schließe Produktzufuhr
- Regel den Reaktordruck mit Druck eines nachgeschalteten Apparates

#### 2. Reaktor

- Nimm ein Gebläse i. B.
- Hänge die Abgasleitung ab und entspanne sie
- Informiere, daß 2. Reaktor auf "Halten" geht
- Senke Durchsatz des Reaktors auf x Nm<sup>3</sup>/h ab
- Nimm einen Seitenabzug durch Betätigen von 2 Regeleinrichtungen a.B.
- Wechsel die Rührergeschwindigkeit
- Senke Durchsatz weiter ab
- Halte Abgaskonzentration ein (gesonderte BV)
- Kontrolliere Arbeitsweise einer Regelung
- Beobachte das Verhalten von 3 Regelungen
- Korrigiere (falls erforderlich) durch Öffnen oder Schließen von Umfahrungen
- Senke Durchsatz auf Null ab
- Schließe Gaszufuhr
- Schließe Produktzufuhr
- Regel den Reaktordruck mit Druck eines nachgeschalteten Apparates

<sup>9</sup> In der Betriebsvorschrift verwendete Abkürzung für "außer Betrieb"

<sup>10</sup> In der Betriebsvorschrift verwendete Abkürzung für "in Betrieb"

Es ist nicht erkennbar dargestellt, ob beide Reaktoren und zusätzlich gleichzeitig der Kristallisator bei einem Rührwerksausfall des Kristallisators "gehalten" (Reaktoren) oder abgefahren/entleert (Kristallisator) werden müssen. Da aber bei einem Rührwerksausfall im 1. Kristallisator aus den Reaktoren kein Produkt mehr zugefahren werden kann und der Kristallisator ohne Rührwerk nicht fahrbar ist, muß von Gleichzeitigkeit ausgegangen werden.

Somit kommen als gleichzeitige Handlungen zusätzlich die in der BV "Außerbetriebnahme der Kristallisation" beschriebenen zu denen bei den Reaktoren hinzu. Daneben ist in den Reaktoren eine Mindesttemperatur vorgegeben, die eingehalten werden muß. Bei Unterschreitung dieser Temperatur ist das "Halten" unmöglich und die Reaktoren müssen abgefahren werden, wodurch weitere Handlungen anfallen würden.

Halten 1. Reaktor	Halten 2. Reaktor	Außerbetriebnahme 1. Kristallisator
s. o	s. o.	<p>(Anmerkung: Ist das Rührwerk im Antriebssystem defekt, kann es passieren, daß der 1. Kristallisator nicht mehr entleert werden kann, da sich der Feststoff am Behälterboden absetzt. Die Folge ist eine erhebliche Reihe von Handlungen, die in diesem Beispiel nicht betrachtet werden sollen)</p> <ul style="list-style-type: none"> <li>- Entleere 1. Kristallisator bis zur Gasphase in nachfolgenden Behälter</li> <li>- Fülle den 1. Kristallisator mit Spülflüssigkeit</li> <li>- Entleere die Spülflüssigkeit in nachfolgenden Behälter</li> <li>- Beachte, daß das Rührwerk nicht trocken läuft</li> <li>- Fülle den 1. Kristallisator bis 50% Stand mit Spülflüssigkeit</li> <li>- Entleere die Spülflüssigkeit in nachfolgenden Behälter</li> <li>- Nimm Rührwerk gem. BV 988, BDA 21 a. B. s.u.</li> <li>- Entspanne 1. Kristallisator über PICA in eine Kolonne</li> <li>- Schließe Mantelbeheizung und Begleitheizung</li> </ul> <p>Da die vorstehende Vorschrift nicht abschließend ist, folgen hier noch Anweisungen, die allerdings entfallen, wenn das Rührwerk ausgefallen ist:</p> <ul style="list-style-type: none"> <li>- Überprüfe, ob der Behälter feststofffrei ist</li> <li>- Schalte den Antrieb aus</li> <li>- Beobachte Auslaufvorgang</li> </ul>

Aus den vorstehenden Bedienanleitungen ergibt sich folgende Liste an Bedienhandlungen mit geschätzten Bedienzeiten (die gleichen Handlungen an den Reaktoren sind gesondert aufgeführt):

Bedienhandlungen	Zeiteinheit
1 Informiere, daß ein Reaktor auf "Halten" geht	1
2 Senke Durchsatz des Reaktors auf $x \text{Nm}^3/\text{h}$ ab	10
3 Nimm einen Seitenabzug durch Betätigen einer Regeleinrichtungen a.B.	3
4 Nimm einen Seitenabzug durch Betätigen einer Regeleinrichtungen a.B.	3
5 Wechsel die Rührergeschwindigkeit	2
6 Senke Durchsatz weiter ab	10
7 Halte $\text{O}_2$ –Abgaskonzentration ein	Wiederholungshandlung
8 Halte $\text{CO}_2$ –Abgaskonzentration ein	Wiederholungshandlung
9 Kontrolliere Arbeitsweise einer Regelung	5
10 Beobachte das Verhalten einer Regelung	Wiederholungshandlung
11 Beobachte das Verhalten einer Regelung	Wiederholungshandlung
12 Beobachte das Verhalten einer Regelung	Wiederholungshandlung
13 Korrigiere (falls erforderlich) durch Öffnen oder Schließen von Umfahrungen	5
14 Senke Durchsatz auf Null ab	Handlung und Beobachtung
15 Schließe Gaszufuhr	3 1 1
16 Schließe Produktzufuhr	usw.
17 Regel den Reaktordruck mit Druck eines nachgeschalteten Apparates	
18 Nimm ein Gebläse i. B.	
19 Hänge die Abgasleitung ab und entspanne sie	
20 Informiere, daß 2. Reaktor auf "Halten" geht	
21 Senke Durchsatz des Reaktors auf $x \text{Nm}^3/\text{h}$ ab	
22 Nimm einen Seitenabzug durch Betätigen einer Regeleinrichtungen a.B.	
23 Nimm einen Seitenabzug durch Betätigen einer Regeleinrichtungen a.B.	
24 Wechsel die Rührergeschwindigkeit	
25 Senke Durchsatz weiter ab	
26 Halte $\text{O}_2$ –Abgaskonzentration ein	
27 Halte $\text{CO}_2$ –Abgaskonzentration ein	
28 Kontrolliere Arbeitsweise einer Regelung	
29 Beobachte das Verhalten einer Regelung	
30 Beobachte das Verhalten einer Regelung	
31 Beobachte das Verhalten einer Regelung	
32 Korrigiere (falls erforderlich) durch Öffnen oder Schließen von Umfahrungen	
33 Senke Durchsatz auf Null ab	
34 Schließe Gaszufuhr	
35 Schließe Produktzufuhr	
36 Regel den Reaktordruck mit Druck eines nachgeschalteten Apparates	
37 Entleere 1. Kristallisator bis zur Gasphase in nachfolgenden Behälter	
38 Fülle den 1. Kristallisator mit Spülflüssigkeit	
39 Entleere die Spülflüssigkeit in nachfolgenden Behälter	
40 Beachte, daß das Rührwerk nicht trocken läuft	
41 Fülle den 1. Kristallisator bis 50% Stand mit Spülflüssigkeit	
42 Entleere die Spülflüssigkeit in nachfolgenden Behälter	
43 Überprüfe, ob der Behälter feststofffrei ist	
44 Schalte den Antrieb des Rührwerks aus	
45 Beobachte Auslaufvorgang des Rührwerks	
46 Entspanne 1. Kristallisator über PICA in eine Kolonne	
47 Schließe Mantelbeheizung	
48 Schließe Begleitbeheizung	

## Darstellung störungskompensierender Handeingriffe anknüpfend an das PAAG-Verfahren ("Störungskompensationsgraph")

### Variante 1

Die betrieblichen Gefahrenquellen einer Anlage und die getroffenen Gegenmaßnahmen sind in der entsprechenden Sicherheitsanalyse für die Anlage darzulegen. Bei kontinuierlich arbeitenden Anlagen wurde im Rahmen dieser Untersuchung häufig die Anwendung des PAAG-Verfahrens in den Sicherheitsanalysen vorgefunden.

Zur Darstellung der Bedieneraktivitäten wurde die Idee entwickelt, ausgehend von den Fragestellungen und Ergebnissen des PAAG-Verfahrens einer vorhandenen Sicherheitsanalyse, die möglichen Eingriffe der Bediener in Gefahrensituationen bildlich darzustellen. Eine solche Vorgehensweise kann, da sie auf schon dokumentierte Untersuchungen aufbaut, den erforderlichen Aufwand zur "Bediener-Bilanzierung" reduzieren. Ziel dieser Betrachtungen soll es sein, eine vorhandene Sicherheitsanalyse um ein Bediener-Modul zu erweitern.

Die Darstellung umfaßt die Bediener-Aktivitäten innerhalb folgender drei Ebenen:

1. Normalbetrieb der Anlage
2. gefahrlose Änderung des Betriebes (Anlage außer Betrieb, Teilabschaltungen, Leistungsreduzierungen, Einfrieren)
3. gefährliche Situation (Störung, Störfall)

Mit der Darstellung in den Abbildungen 7-9 und 7-10 wird deutlich, in welchen Situationen die Bediener (Wartenfahrer und Anlagenbetreuer vor Ort) mit welchem Ergebnis eingreifen können und welche Auswirkungen Mangel- oder Fehlbedienungen haben.

Für die Darstellung der Bedienfunktionen wird das vorgeschlagene, auf der Spitze stehende Quadrat verwendet (vgl. Abbildung 7-4). In Erweiterung der verwendeten Symbolik wird die Mangel- oder Fehlbedienung als Ausgang von der unteren Spitze des Quadrates dargestellt.

Zur Vergleichbarkeit mit der in Darstellung der Bedienfunktionen im RI-Schema wurden die schon dort untersuchten Bedienhandlungen Nrn. 3.1 und 3.6 aus der PAAG-Liste (siehe Tabelle 7-6) ebenfalls mit dieser Visualisierungsmethode dargestellt.

### Variante 2

Es kann zur Darstellung der störungskompensierenden Eingriffe der Bediener auch eine Kombination aus Störungsanalyse und Fehlerbaum-Strukturen verwendet werden (Steinbach 1999). Die grundsätzliche Idee besteht in der Visualisierung des Bedienkonzeptes.

Dabei wird auf der Basis von PAAG-vergleichbaren Fragen, die somit auch verfahrenstechnische Verknüpfungen beinhalten, die Wirkung eines oder mehrerer gleichzeitiger Fehler verdeutlicht. Als Fehler wird sowohl technisches als auch menschliches Versagen berücksichtigt.

Es wird in folgenden Schritten vorgegangen:

1. Ausgangspunkt sind die möglichen Alarmierungen (was löst Alarne aus?).
2. Notwendige Gegenmaßnahmen werden aufgezeigt.
  - a) technische Maßnahmen
  - b) organisatorische Maßnahmen (Bedieneraktivitäten)
3. "Kritische Knotenpunkte", das sind mehrfache, ggf. gleichzeitig auflaufende Anforderungen an technische oder organisatorische (Bediener) Maßnahmen, deren "Nicht-Funktionieren" kritische Auswirkungen hat, können erkannt und bewertet werden; erforderliche Modifizierungen des Bedienkonzeptes können abgeleitet werden.
4. Die Anzahl und Wirkung der vorhandenen Sicherheitsbarrieren wird dokumentiert.

Diese Betrachtung wird für die sicherheitsbedeutsamen Ausrüstungen und die dort relevanten Parameter (z.B. Temperatur, Druck, Massenstrom) durchgeführt und bildlich dargestellt. In Abbildung 7-10 findet sich als Beispiel eine solche Darstellung für die Drucküberwachung eines Reaktors.

Soweit Verknüpfungen zwischen verschiedenen Ausrüstungen oder Parametern zu berücksichtigen sind, werden diese durch Konnektoren dargestellt.

In Erweiterung der vorgestellten Darstellungen in den Abbildungen 7-9 und 7-10 ist es erforderlich, sämtliche Verknüpfungsketten für Gefahrensituationen bzw. Prozeßabweichungen innerhalb einer Anlage herauszuarbeiten, mit Konnektoren zu verbinden und die Anforderungen an den Bediener über ein Zeitfenster zu bilanzieren.

### 7.1.2 Demonstrationsbeispiel Batch-Anlagen

In Batch-Anlagen ist der Automatisierungsgrad auch heute noch teilweise sehr beschränkt. Es gibt oftmals keine definierte Anlagenkonfiguration, vielmehr erfolgt in Abhängigkeit vom Produktionsplan die Apparatezusammenstellung und Verrohrung jeweils individuell für die vorgesehene Rezeptur. Da in derartigen Anlagen durchaus 20 bis 30 verschiedene Rezepturen gefahren werden können, werden häufig keine rezeptspezifischen RI-Schemata (zu große Menge, Apparatezusammenstellung kann je nach Gesamtproduktionsplan wechseln) erstellt.

Solche Anlagen werden noch sehr weitgehend per Hand gefahren: z.B. Mengenvorwahl, Temperaturlöschung (Heizung/Kühlung zuschalten/abschalten), Grenzwerteinstellungen, z.T. Einpumpen der Reagenzien aus Fässern oder Einfüllung per Sack über das Mannloch, Anschluß der jeweils benötigten Abluftwäschersysteme usw.

Zwar wird auch bei Batch-Anlagen zunehmend PLT eingesetzt, und Meßwerte können zentral in einer Leitwarte über den Bildschirm beobachtet werden. Der Bediener wird aber auch in Zukunft nicht zum reinen Beobachter werden. Es wird auch weiterhin einzelne Prozeßschritte selbst einleiten, und er wird insbesondere auch weiterhin die jeweilige Apparatekonfiguration für die jeweilige Rezeptur (Anschlüsse von Reaktoren oder sonstigen Apparaten an bestimmte Rohrleitungen – Stoff, Heizung, Kühlung –, an bestimmte Abluftreinigungssysteme) zusammenstellen.

Aus dieser Situation ergibt sich, daß die Bedienkonzeption eigentlich bereits für den Normalbetrieb systematisch durchdacht und in geeigneter Form abgebildet bzw. dokumentiert werden mußte. Der Bediener hat zahlreiche Fehlbedienungsmöglichkeiten, die zu unsicheren Betriebszuständen führen können, so daß schon für den bestimmungsgemäßen Betrieb zu prüfen ist, an welchen Stellen der Bediener ggf. an seine Leistungsgrenzen gelangen und Überforderung nicht ausgeschlossen werden kann.

Trotz dieser besonders großen Bedeutung des Bedieners für die Anlagensicherheit zeigen die existierenden Sicherheitsanalysen keine eingehendere Behandlung der Auswirkungen falscher oder fehlender Bedienhandlungen. Schon gar nicht wird erkennbar, an welchen Stellen ein einzelner Bediener gleichzeitig bzw. innerhalb eines kurzen Zeitraums mehrere Apparate zu bedienen hat. Insofern fehlt derzeit auch für Batch-Anlagen eine Unterlage, aus der die Bedienkonzeption als wesentlicher Teil des sicheren Anlagenbetriebs erkennbar wäre.

### Darstellung des Normalbetriebs

Mit Unterstützung eines größeren Unternehmens, das seine Produktion pharmazeutischer Wirkstoffe und von Laborchemikalien überwiegend in Batch-Anlagen fährt, wurde deshalb im Rahmen dieses Forschungsvorhabens eine Darstellungsform für die Bedienkonzeption entwickelt.

Als Ausgangspunkt der Darstellung dienten die Rezeptanweisungen, aus der die einzelnen Bedienhandlungen hervorgehen. Diese wurden in eine vertikal abfolgende Zeitachse (proportionale Darstellung) übertragen. Tätigkeiten, die parallel an weiteren Apparaturen stattfinden, wurden auch parallel dargestellt. Liegen Apparate, an denen ein Bediener tätig ist, räumlich in größerer Entfernung (oder in einem anderen Stockwerk), so wurde dies durch entsprechenden Abstand zwischen den parallel zu bedienenden Apparaten erkennbar gemacht (Abstand zwischen den Reaktoren R111 und R222 in Abbildung 7-12). Besonders sicherheitsrelevante Bedienschritte werden rot dargestellt. Die einzelnen Bedienhandlungen sind nicht nur mit einem Zeitpunkt markiert, sondern mit der gesamten Zeitdauer der Aktion

(einschließlich notwendiger Beobachtungen). Beobachtungen von z.B. Meßstellen sind generell auch als Bedienaktion aufzunehmen.

Schon diese Darstellung dient

- dem Betreiber zu einer gezielten bedienerorientierten Produktionsplanung (entweder Anpassung des Produktionsplans an bestehende Personalstärke oder umgekehrt Anpassung der Personalstärke an den Produktionsplan),
- dem Betreiber zur Identifizierung notwendiger bedienerentlastender Teilautomatisierungen oder technischer Bedienerunterstützungen,
- der Behörde zum Erkennen der Bedienerbelastung im Normalbetrieb.

Der Betreiber hat – im eigenen Interesse – auch die Möglichkeit, relevante produktqualitäts-sichernde Arbeitsschritte zusätzlich erkennbar zu machen (z.B. durch Blau-Einfärbung). Bei dieser Darstellungsform der Bedienkonzeption geht es im wesentlichen darum, schon die erste Fehlhandlung zu vermeiden, indem man unterhalb des Überforderungsniveaus bleibt.

#### *Exkurs „Überforderungsniveau“*

*Das Problem ist, daß kein allgemeingültiges Niveau definierbar ist, ab dem mit Bediener Überforderung und damit mit Fehlbedienung zu rechnen ist.*

*Die Zahl 7 als menschliche Leistungsgrenze im Sinne der Anzahl der maximal gleichzeitig wahmehm- und verarbeitbaren Informationen stellt eine Obergrenze dar. Für den Normalbetrieb wie auch den Störbetrieb ist ein Puffer einzuplanen, der sicherstellt, daß man von dieser Obergrenze entfernt bleibt.*

*In der Praxis empfiehlt sich schon bei zwei gleichzeitig bzw. parallel geforderten sicherheitsrelevanten Bedienhandlungen mindestens die Diskussion dieser Situation im Rahmen von Sicherheitsgesprächen (vgl. beispielsweise den Zeitpunkt „1 Stunde“ in Abbildung 7-12). Die eingehender Beschäftigung mit ggf. zu stark beanspruchender Bedienerbelastung wird in jedem Fall zu einem besseren Problembewußtsein beitragen.*

Schon bei der Darstellung der Bedienschritte im Normalbetrieb wurde erkennbar, daß die Rezeptanweisung nicht alle notwendigen Informationen hergibt. Es sind ihr häufig nicht alle zu beobachtenden Meßwerte zu entnehmen und es wird nicht ausreichend erkennbar, wie weit der Bediener durch notwendige Meßwertbeobachtungen zeitlich und örtlich beansprucht wird.

#### **Darstellung des Störbetriebs**

Absicht des Forschungsvorhabens war es, die Bedienerbelastung auch für den Störbetrieb beispielhaft darzustellen. Hierzu gab es unter den betrieblichen Unterlagen jedoch keine geeignete Arbeitsgrundlage. Erforderlich sind Informationen darüber, welche Handlungen

vom Bediener bei vorhersehbaren Störungen – gleichgültig ob durch technischen Fehler oder durch Fehlbedienung verursacht – erwartet werden (Wahrnehmung von Meßwertangaben, nachdenken darüber, welche Ursachen den Abweichungen vom bestimmungsgemäßem Betrieb zuzuordnen sind, Schlußfolgerungen ziehen, handeln). Eine solche Dokumentation existiert offensichtlich in den Betrieben derzeit nicht.

Von der Form der Darstellung hätten sich die gleichen Anforderungen wie für den Normalbetrieb ergeben (Abbildung der Bedienschritte in einer Zeitachse). Dadurch wäre z.B. direkt erkennbar, ob dem Bediener überhaupt genügend Zeit zum Reagieren zur Verfügung steht. In der Störsituation ist dabei zusätzlich zu berücksichtigen, daß der Bediener unter Stress andere Reaktionen zeigt und andere Reaktionszeiten benötigt als in der Normalsituation.

Eine solche Darstellung ist letztlich unverzichtbar für eine bedienerfreundliche Anlagenkonzeption, damit der Bediener als Sicherheitsfaktor seine Rolle überhaupt wahrnehmen kann.

Schlußfolgerungen aus der Darstellung der erwarteten Bedienhandlungen (einschließlich Meßwertbeobachtungen, Nachdenken und Kommunizieren mit anderen) in Störsituationen könnten u.a. sein:

- Ausblenden bestimmter Informationen (und Konzentration auf die wesentlichen Informationen) nach Eintritt eines Erstereignisses.
- Anweisung (in der Betriebsanweisung oder durch automatische Fenstereinblendung auf dem Bildschirm), für die Restanlagenbedienung einen zweiten Bediener hinzuziehen (damit er seine volle Aufmerksamkeit der Beseitigung der Ursache einer Störmeldung widmen kann).
- Änderung der Produktionsplanung (zeitliches Entfernen zur Vermeidung von Bedienerüberlastung).
- Änderung des Grenzwertes zur Alarmauslösung (mehr Zeit für die Fehlerwahrnehmung, das Ziehen der Schlußfolgerung und der Reaktion).
- Betriebsanweisung für alle Störereignisse, die menschliche Eingriffe erfordern; ständiges Üben der Handlungsabfolgen.
- Einrichtung zusätzlicher Verriegelungen.

Damit derartige Bedienanalysen möglich werden, sind die Gefahrenanalysen durch entsprechende Informationen zu ergänzen:

- durch notwendige Handlungsabläufe des Bedieners bei sicherheitsrelevanten betrieblichen Störungen,
- durch die Darstellung der gesamten Meldeabläufe bei Eintritt sicherheitsrelevanter Störungen.

## 7.2 Analyse und Bewertung der Aussagen zur Bediensicherheit in vorhandenen Sicherheitsanalysen

### Zitate aus Sicherheitsanalysen hinsichtlich der Aussagen zur Bediensicherheit

Die Forderung der (alten) Störfall-Verordnung) zur Vorsorge durch Sicherung gegen Fehlbedienung besteht schon seit 1980. Trotzdem sind die Aussagen zu dieser Thematik in geprüften und akzeptierten Sicherheitsanalysen so unscharf und global, daß sie in keiner Richtung wirklich belastbar und eine Anleitung zum konkreten Handeln sind. Als Beleg für diese Behauptung wurden in der Tabelle 7-5 Textstellen zu Bediensicherheit aus vorliegenden Sicherheitsanalysen unter Anonymisierung der Betreiber zusammengestellt.

Daneben gibt es einen erheblichen Anteil von Sicherheitsanalysen, die zur Bediensicherheit keine Aussage machen. Über die Quote der Sicherheitsanalysen ohne Aussage wurden keine Untersuchungen angestellt.

### Bewertung der Zitate aus Sicherheitsanalysen

Weitaus die meisten Sicherheitsanalysen bleiben hinsichtlich der Bediensicherheit unkonkret. Allgemein wird beschworen, daß nur qualifiziertes Personal einzusetzen ist oder eingesetzt wird, und es wird unterstellt, daß damit schon die Voraussetzungen für das Vermeiden von Bedienfehlern gegeben seien. Daneben wird grob fahrlässiges Verhalten thematisiert, im allgemeinen ohne auf dessen Vermeidung einzugehen.

Andererseits gibt es Fälle, die unrealistische Behauptungen hinsichtlich der Vorsorge gegen Fehlbedienung enthalten, indem dargestellt wird, das Prozeßleitsystem würde bei allen fehlerhaften Aktionen des Anlagenpersonals Alarne auslösen. An sich wird damit der laut 2. Störfallverwaltungsvorschrift/Mustergliederung/Abschnitt 5 anzustrebende Umfang des Vorausdenkens möglicher Fehler getroffen. Man muß sich aber im klaren sein, daß das Spektrum menschlicher Irrtümer grenzenlos ist, und daß deshalb eine solche Vollständigkeit unrealistisch ist.

Es findet sich kein Beispiel, in dem darauf eingegangen wird, daß dem Handeln des Bedieners Grenzen gesetzt sind, die neben Fahrlässigkeit – d.h. trotz guter Motivation und Qualifikation – zu objektiv begründeten Fehlhandlungen führen. Es finden sich aber Beispiele, die die verbleibenden möglichen Bedienfehler als akzeptierbares Restrisiko einstufen.

Häufig wird der in der Mustergliederung vorgegebene Punkt "Bedienfehler" nur dazu benutzt, Verriegelungs- oder Notabschaltungen darzustellen, ohne unter diesem Gliederungspunkt auf Bedienung wirklich einzugehen.

Hier wurden die Sicherheitsanalysen nur danach betrachtet, was sie unter dem nach der

2. VwV zur Störfallverordnung geforderten Gliederungspunkt "Bediensicherheit" aussagen.

Sicherheitsanalysen, die z.B. die Gefahrenanalyse nach dem PAAG-Verfahren durchgeführt und dargestellt haben, enthalten versteckt unter der Überschrift "Gefahrenquellen" teilweise detaillierte Einzelangaben zu Bedienhandlungen, die aber keineswegs konzeptionell oder bilanzierend zusammengeführt werden. Darauf wurde oben bereits eingegangen.

## 7.3 Ergänzung von in Sicherheitsanalysen vorgelegten Störfallszenarien hinsichtlich der Bedienanforderungen

### Betrachtung von "Dennoch-Störungen"

Entscheidend für den Umfang der Vorsorge-Betrachtungen ist, ob der politische Wille besteht, sog. Dennoch-Störungen (vgl. Abbildung 5-1 in Kapitel 5) bei der Untersuchung der Voraussetzungen zur Bediensicherheit zu betrachten. Das Hauptargument für einen menschlichen Bediener, z.B. im Vergleich zur Automatisierung, ist, daß der Mensch in unvorhergesehenen Situationen noch handeln kann. Damit ist genau der Dennoch-Störfall erfaßt.

In der Vergangenheit hat z.B. der Verband der chemischen Industrie (VCI) oft den Kurs verfolgt, Störungen, die man als "vernünftigerweise auszuschließen" klassifizieren kann – im Weiteren als "Dennoch-Störungen" bzw. "Dennoch-Störfälle" bezeichnet – in Sicherheitsanalysen nicht zu betrachten. Die Auswertung eingetretener Störfälle zeigt, daß sehr wohl solche Dennoch-Störfälle vorkommen. Die Klassifikation "vernünftigerweise auszuschließen" wird der Ursache "nicht daran gedacht" nicht gerecht. Allein dies rechtfertigt auch bei beliebigem Automatisierungsgrad das Verbleiben eines Bedieners.

Diese Argumentation kann den Entwerfer und Entwickler einer Anlage nicht davon befreien, in möglichst großem Umfang vorauszudenken, welche unvorhergesehenen Ereignisse durch den Bediener in ihrer nachteiligen Auswirkung kompensiert werden sollen. Man kann keineswegs voraussetzen, daß der Bediener den gleichen Kenntnisstand über alle möglichen Vorgänge in der Anlage haben kann, wie der Verfahrensentwickler. Die prinzipiell mögliche Reaktion des bedienenden Menschen auf unvorhergesehene Vorgänge ist von vornherein durch den möglichen Kenntnisstand eines Anlagenfahrers eingeschränkt. Die logische Konsequenz ist, daß man vom Verfahrensentwickler das Vorausdenken möglicher Bediensituationen in großem Umfang verlangen muß.

Das Problem ist dadurch besonders erschwert, daß das Spektrum möglicher Dennoch-Störungen grenzenlos ist. Es ist erst noch ein Konsens zu entwickeln, wieweit die Betrachtung zu treiben ist.

Die in Kapitel 7.1 behandelten Darstellungen enthalten einige Details, die das Problem

deutlich machen können. Der Handschalter (HS 2.03) wirkt – wie schon in Abschnitt "Darstellung der Bedienaufgaben im Prozeßablaufplan" erwähnt – parallel auf zwei Stellglieder, nämlich Ventil und Pumpe. Für beide gibt es getrennte Rückmeldungen, nämlich (GOS 2.03) und (SOS 2.04). Kommt nach Betätigung des Handschalters nur eine der beiden Rückmeldungen, ermöglicht das eine Störungsdiagnose, in einem Fall klemmt das Ventil, im anderen liegt ein Fehler im Pumpenantrieb vor. Die Bedienanweisungen des Beispiels gehen auf diese Diagnosemöglichkeiten nicht ein.

In diesem einfachen Fall kann man sich noch vorstellen, daß der Anlagenfahrer sich die Diagnosekombination selbst überlegen kann. Es gibt in realen Anlagen sicher viele Konstellationen, bei denen die Diagnoseschlußfolgerungen die Möglichkeiten des Anlagenfahrers überschreiten. Unabhängig vom Kenntnisstand muß man auch berücksichtigen, daß unter Stress die Fähigkeit zum analytischen Denken nahezu verschwindet. Viele dokumentierte Störfälle belegen das Verschwinden des richtigen analytischen Denkens in Störsituationen. Unter Stress kann der Mensch bekanntlich nur vorbereitete und gelernte Algorithmen aufrufen.

Dieses kleine Beispiel zeigt, wie wichtig das Vorausdenken zu ziehender Schlußfolgerungen durch den Verfahrensentwickler ist. Der Zwang zu einer formalisierten Notierung der Abläufe wird eine wesentliche Hilfe zum Aufdecken notwendiger Informationskombinationen sein.

## 7.4 Besonderheiten hochgradig automatisierter Anlagen

Es wurde deutlich, daß ein erheblicher Arbeitsaufwand notwendig ist, Bedienabläufe vorauszudenken (zu konstruieren). Die Betrachtung der gängigen Entwurfspraxis zeigt, daß alle Abläufe, die bei der Planung detailliert vorausgedacht werden, auch in technische Lösungen zur Anlagensicherung eingehen (Notabschaltung, automatische Umschaltung auf Reserve u.ä.). Das bedeutet, es bleiben praktisch keine durchdachten Abläufe zur ausschließlichen Ausführung durch einen Bediener übrig.

Geht man von dieser Voraussetzung aus, kann man die Bedienerbeanspruchung ganz anders und viel einfacher als bisher betrachtet definieren: Für den Bediener bleiben – neben dem planmäßigen Fahrplan des Normalbetriebes – zur Störungsbekämpfung nur Aufgaben zur Kompensation partieller Geräteausfälle übrig. Diese kann man aber summarisch mit der Ausfallquote der Gerätetechnik erfassen. Daraus folgt das Postulat, die Ausfallquote muß so klein sein, daß unter Beachtung eines Sicherheitsabstandes von der Gesamtzahl der technisch realisierten Schutzfunktionen nicht mehr als sieben (bzw. – mit Blick auf die Vergleichsnotwendigkeit von Grenzwert und Istwert – nicht mehr als vier) gleichzeitig ausfallen.

## 7.5 Statische Prüfung der dargestellten Bedienkonzeption hinsichtlich der gleichen Zahl von Sicherheitsbarrieren für mögliche Ereignisketten

Üblicherweise ist die Bedienmöglichkeit nur eine von mehreren Maßnahmen zur Störungsverhütung. Abbildung 7-13 zeigt ein einfaches Beispiel. Die Überfüllsicherung entspricht der Vorsorge nach § 3 Abs. 1 und § 4 der alten Störfall-Verordnung, die Auffangtasse der Vorsorge nach § 3 Abs. 3 und § 5. Durch die Möglichkeit der Bedienung von Hand kann ein vernünftigerweise ausgeschlossener Dennoch-Störfall ggf. verhindert werden. In diesem Fall gibt es eine Barriere gegen eine zu erwartende Störung und zwei Barrieren gegen einen Dennoch-Störfall oder seine Auswirkungen. Die Anlage hat somit gegenüber der Umwelt drei Sicherheitsbarrieren.

Für die Sicherheit einer Anlage ist es erstrebenswert, daß es für alle denkbaren Störungen die gleiche Zahl Sicherheitsbarrieren gibt. Diese Betrachtung deckt gewöhnlich Lücken in der Sicherheitsvorsorge auf. Danach kann man sich in begründeten Fällen darüber Klarheit verschaffen, ob verschiedene Störungsursachen unterschiedlich gefährlich sind und eine entsprechende Zahl von Sicherheitsbarrieren rechtfertigen.

Anhand einer realen Sicherheitsanalyse, bei der die möglichen Störungsquellen nach dem PAAG-Verfahren aufgelistet wurden (Tabelle 7-6), wird das Verfahren demonstriert (Tabelle 7-5).

Es ist sofort offenkundig, daß gegen verschiedenartige Störungen ganz unterschiedliche Sicherheitsbarrieren vorgesehen werden. Die Tabelle soll mit den leeren Plätzen den Anlagengestalter zum Nachdenken zwingen, ob die jeweilige Störungsmöglichkeit richtig bewertet wurde, oder ob weitere Sicherheitsbarrieren gerechtfertigt sind. Vor dem Hintergrund programmierbarer Prozeßleittechnik fallen gewöhnlich die Kosten eines weiteren Informationskanals nicht mehr ins Gewicht.

## 7.6 Dynamische Prüfung

Die prüfbare Darstellung der Zeitabhängigkeit von Bedienanforderungen als Voraussetzung für die Bewertung des Gleichzeitigkeitsproblems erfordert erheblichen Aufwand, der bisher üblicherweise nicht geleistet wurde. Vor dem Hintergrund der ständig artikulierten Forderungen nach Deregulierung und dem im BlmSchG verankerten Grundsatz der Verhältnismäßigkeit erscheint es bedenklich, die Erbringung eines solchen Aufwandes von Seiten der Behörden durchzusetzen. Unabhängig davon ist eine weitere Entwicklung zur Verbesserung der Bediensicherheit wünschenswert.

Die Entwicklung kann in zwei Linien verlaufen:

- Anstelle des Aufwandes für die Konstruktion von Bedienabläufen sollte der Aufwand

besser in Trainingsanlagen, die die reale Anlage abbilden, gesteckt werden. Über programmierbare Trainingsanlagen, die über Telekommunikation genutzt werden können (z B Bildungsverbund Chemie und Technik Halle, als Gemeinschaftseinrichtung von VCI und IHK) werden solche Lösungen auch für mittelständische Betriebe tragfähig.

- Die Aktivitäten zum Wecken des Problembewußtseins sollen dazu führen, daß Betreiber aus Eigeninteresse sich stärker mit dem Vorausdenken von Bedienabläufen zur Bekämpfung von Störungsszenarien befassen und das auch von ihren Anlagenlieferanten fordern.

## 7.7 Ergebnisse der Praxistests

### 7.7.1 Demonstrationsbeispiel kontinuierliche arbeitende Anlagen

#### Umfang der Untersuchungen

In Analogie zur nach DIN eingeführten MSR-Stelle und PLT-Stelle wird besser der Begriff "Bedienstelle" anstatt des zunächst verwendeten Begriffs "Bedienfunktion" verwendet.

Die Untersuchungen wurden an zwei kontinuierlich arbeitenden Anlagen (kontinuierliche Fließgutprozesse) des Praxispartners (Anlagenbetreibers) durchgeführt:

Anlage	Untersuchungsart
Raffinationsanlage	Bedienstellen-Schema
	Störungskompensationsgraph
Petrochemische Anlage	Balkendiagramm zur Darstellung der Gleichzeitigkeit

#### Bedienstellen-Schema

Der Vorschlag des Bedienstellen-Schemas ging von Voraussetzungen aus, die zum Teil an den betrachteten Anlagen nicht mehr zutreffen. Diese nicht mehr gegebenen Voraussetzungen waren:

- Unterlage für die Übersicht der Bediener sind vereinfachte RI-Schemata,

- ein erheblicher Teil der sicherheitsrelevanten Bedienung ist Hand-Automatik-Umschaltung zur Kompensation von Ausfällen der Automatik.

An der untersuchten Anlage sind, wie unten noch ausführlicher dargelegt, für alle vorausgedachten Störungen der Bedienung übergeordnete Notabschaltsysteme installiert. Die Aufgaben des Bedieners konzentrieren sich darauf, bei einer beginnenden Störung die Zeit bis zum zwangsweisen Notabschalten zu nutzen, um die mit der Notabschaltung einhergehende Produktionsstörung abzuwenden.

Die Zuverlässigkeit der Automatik ist so gestiegen, daß Handeingriffe zur Kompensation von Störungen der Automatik keine Rolle mehr spielen.

Grundlage der Bedienung sind Bildschirmbilder, in denen die für das Bedienstellen-Schema geforderten Informationen in einem Anlagenschema angeordnet dargestellt sind (Abbildung 7-8) Der praktische Betrieb zeigt, daß es gelingt, die Bediener so zu schulen, daß sie ein mentales Modell der Wirkungsverbindungen von den Informationen zu den notwendigen Stelleingriffen entwickeln, so daß aus Sicht des Betreibers die Darstellung der Wirkungsverbindungen nicht erforderlich ist.

Diese Bedienbilder sind unter dem Aspekt der bestmöglichen Platzausnutzung des Bildschirmes entstanden. Damit gehen viele Einschränkungen einher, die bei Vorsorgebetrachtungen nicht zwingend wären. Die parallele Beschäftigung des Betreibers mit der später näher ausgeführten Vorzugsvariante führte dazu, daß das Bedienstellen-Schema nicht weiter verfolgt wurde.

#### **Balkendiagramm zur Darstellung der Gleichzeitigkeit**

Ziel der Untersuchungen war die Klärung, ob die betrachtete Anlage so mit technischen Mitteln ausgerüstet ist, daß eine Überlastung des Bedieners (Meßwartenfahrers) durch eine Vielzahl gleichzeitig auszuführender Bedienhandlungen immer durch technische Mittel umgangen bzw durch die automatische Prozeßsteuerung übernommen wird.

In diesem Fall ist das Erreichen einer kritischen Zahl von Bedienhandlungen für einen Bediener, wie es aus der einfachen Kombination der Störungen nach den beschriebenen Abläufen in den Betriebsvorschriften möglich wäre, nicht zu befürchten.

Obwohl bei der Anlagenplanung keine Untersuchungen für eine Bedienbarkeit der Anlage aus der Sicht des Bedieners vorgenommen wurden, bleibt die Anlage auch bei extremen Situationen beherrschbar.

Mit dem Anlagenbetreiber einer petrochemischen Anlage wurden die Betriebsvorschriften hinsichtlich Bedienbarkeit (durch das Bedienpersonal) untersucht. Das in Kapitel 7.1 dargestellte Szenario von zwei gleichzeitigen "Dennoch-Störfällen"

- Bruch einer Rührwerkswelle (Ausfall 1. Kristallisator) und
- Ausfall Standregelventil eines Reaktors (z.B. Ausfall des Antriebes)

in einer kontinuierlich arbeitenden Anlage (kontinuierlicher Fließgutprozeß) wird durch den Betreiber als ein mögliches und betrachtenswertes Störungsgeschehen gesehen.

Ein Szenario wie das dargestellte ist nicht Gegenstand einer Betrachtung in der Planungsphase. Trotz aller Sicherheitsbetrachtungen und der Realisierung entsprechender Technik zur Abwendung des Erreichens einer gefährlichen Situation wird die Möglichkeit des Eintretens des dargestellten Falls für denkbar gehalten. Die Beherrschbarkeit dieser Situation durch das Bedienpersonal wurde jedoch keiner Prüfung unterzogen.

Aufgrund der konkreten Anlagekonfiguration ergaben sich aus der Diskussion mit dem Betreiber zu diesem Beispiel folgende Erkenntnisse:

- Erst die Kombination der Bedienhandlungen bei mindestens zwei Störungen im o. g. Sinne können Handlungsanforderungen so auflaufen lassen, daß eine kritische Zahl sieben gleichzeitig erreicht wird.
- Es wird keine Notwendigkeit für eine Bedienstellendarstellung auf den Bildschirmen gesehen.
- Es gibt "Allgemeine Planungsunterlagen Bau" (als Begriff für einen internen Vorschriftenkatalog), die dem Anlagenplaner für die Errichtungsunterlagen bis in das kleinste Detail (z.B. Form, Farbe, Schrift der Rohrleitungsbescilierung) vorschreiben, wie und unter Berücksichtigung welcher Vorschriften zu planen und zu errichten ist. Für die Planung der Betriebsabläufe sind dagegen keine Vorschriften vorhanden.
- Die Gleichzeitigkeit von sieben Bedienerhandlungen ist bei dem vorliegenden Automatisierungsgrad nicht betrachtenswert, weil automatische "Rampen" über speicherprogrammierbare Systeme (SPS) realisiert sind, die An- und Abfahrprozeduren erledigen und die auch bei Störungen der beschriebenen Art durch einen Knopfdruck des Bedieners angesprochen werden können.
- Die Anlage ist so konzipiert, daß alle Steuer- und Regelsysteme bei Störungen, die in ihren Abläufen nicht beeinflußt werden können, in die "gefährlose Lage" gehen.

Die Stellung der Regeleinrichtung wird in der Planungsphase festgelegt. (Die drei Möglichkeiten: Öffnen, Schließen oder Verharren sind in den RI-Schemata an den Armaturenzeichen dargestellt.) Da das Verharren selten angewandt wird, spricht man allgemein von "gefährloser Endlage".

- Die Anlage ist so konzipiert, daß sie selbst bei einem generellen Energie- und Hilfsstoffausfall unter der Ausnutzung des Fahrens in die "gefährlose Endlage" in einen unkritischen Anlagenzustand fährt und dort bis zum Wiederanfahren verharrt.

### Die Bedienersituation in der Anlagenmeßwarte

Bezogen auf das bisher benutzte Beispiel ergibt sich nachfolgende Konfiguration/Situation in der Anlagenmeßwarte:

Die Meßwarte ist mit einem Prozeßleitsystem TDC 3000 von Honeywell ausgerüstet. Bei Ausfall der Netzstromversorgung ist eine automatische Umschaltung auf eine Batterieversorgung installiert, die für ca. 20 Minuten eine Stromversorgung für MSR-Aufgaben übernehmen kann. Damit ist gewährleistet, daß dem Meßwartenfahrer (einer pro Schicht) die Information auch bei Stromausfall erhalten bleibt. Neben der Bildschirmanzeige ist das Laden der Betriebsvorschriften von einem zentralen Rechner in dieser Zeit noch möglich.

Des Weiteren sind die Transmitterstromein- und -ausgänge in die Meßwarte über diese Notstromversorgung befristet gewährleistet. Das muß aber nicht bedeuten, daß der Meßwartenfahrer die Anlage noch steuern kann (diese Möglichkeit hängt von den Druckverhältnissen im Steuerluftbehälter ab).

Es sind 8 Bildschirme vorhanden, die zur Erfassung von ca. 1'260 Meßstellen, die in 95 Anlagendetailbildern zusammengestellt sind. Diese Anlagendetailbilder sind einzeln abrufbar. Zusätzlich stehen Übersichtsbilder und ausgewählte Gruppenzusammenstellungen über den Zustand von bestimmten Anlagenteilen zur Verfügung.

Eingehende Alarne werden auf einem Bildschirm gebündelt. Der Alarm wird akustisch und optisch (blinkend) angezeigt. Nach dem Quittieren des Alarms verbleibt ein optisches Dauersignal. Sämtliche eingehenden Alarne werden archiviert und sind chronologisch abrufbar.

### Aktuelle Störungssituation mit extremen Bedingungen

Im 1. Quartal 2000 wurden durch einen Stromausfall für 20 Minuten alle elektrischen Antriebe (z.B. Pumpen, Rührwerke, Förderschnecken, Verdichter und Gebläse) außer Betrieb gesetzt. Der Meßwartenfahrer hatte die Möglichkeit zur Information über den Anlagenzustand durch die Umschaltung der Stromversorgung des Prozeßrechners auf Batteriebetrieb. Er konnte Bedienhandlungen nur noch soweit ausführen, wie im Vorrats- oder Stabilisierungsbehälter für Steuerluft noch ein ausreichender Druck für das Betätigen der Regelarmaturen vorhanden war. Danach kann der Meßwartenfahrer keinerlei Bedienhandlungen mehr vornehmen, da mit dem Stromausfall auch sämtliche anderen Energien und Hilfsstoffe nicht mehr zur Verfügung standen. Die Anlage ging somit in die "gefährlose Endlage" (hier ist der für die Einstellung der Regelarmaturen verwendete Begriff in seiner Bedeutung auf den Anlagengesamtzustand ausgedehnt worden, weil durch das Einfahren der Regelarmaturen in diese gefährlose Endlage sich für die Gesamtanlage ein Verharzungszustand einstellt). Sie verharrte dort über die Zeit des Stromausfalls und konnte nach Wiederverfügbarkeit des elektrischen Stroms ohne Probleme auf Produktionszustand und -bedingungen gefahren werden.

Bei lokalen Störungen im Prozeß wird der Meßwartenfahrer auf seine Anforderung durch einen Schichtleiter unterstützt, der dann in der Regel die Bedienhandlungen unter der maximal möglichen Verwendung der SPS-Rampen zur Behebung der Störung übernimmt. Dem Meßwartenfahrer obliegt dann in dieser Zeit die Beobachtung des übrigen störungsfreien Prozesses.

Das Ziel der Bedienhandlungen ist dann auf die möglichst schnelle Korrektur der Prozeßparameter für eine hohe Anlagenverfügbarkeit gerichtet, nicht so sehr auf die Abwendung einer gefährlichen Situation.

Der Stromausfall im 1. Quartal 2000 hat beispielhaft gezeigt, daß bei einer Häufung von Störungen, die letztendlich die kritischen Zahl der beherrschbaren Bedienhandlungen überschreiten können, als Endzustand sich die "Gefahrlose Endlage" einstellt. Das heißt, daß bei einem Nichthandeln des Bedieners schlimmstenfalls ein Verharrungszustand der gesamten Anlage eintreten wird.

### Störungskompensationsgraph

Auf der Grundlage der für die untersuchte Anlage im Rahmen des PAAG-Verfahrens herausgearbeiteten betrieblichen Gefahrenquellen einschließlich der getroffenen Gegenmaßnahmen wurden die möglichen Eingriffe der Bediener in Gefahrensituationen in Form eines "Störungskompensationsgraphen" bildlich dargestellt.

In Zusammenarbeit mit dem Betreiber der untersuchten Anlage wurde die anhand der PAAG-Aufzeichnungen, der Fließbilder sowie der Betriebsvorschriften erstellte Darstellung präzisiert. Die Abbildungen 7-9 und 7-10 veranschaulichen die Ergebnisse.

Die Erprobung an der realen Anlage ergibt wesentliche Weiterentwicklungen des Verfahrens

- Es ist erforderlich, den Symbolvorrat der Darstellung dahingehend zu erweitern, daß unterschieden werden kann in Informationen, zu denen die technische Ausrüstung den Vergleich mit einem Schwellwert (Grenzwert) schon vorgenommen hat und Informationen, zu denen der bedienende Mensch selbst noch eine Bewertung vornehmen muß.
- Bei hochkomplexen Anlagen sind auch Rück- bzw. Auswirkungen auf technisch vor- und nachgelagerte Anlagen zu berücksichtigen (Abbildung 7-11). Bei der Untersuchung komplexer Anlagen ist es daher erforderlich „Bilanzkreise“ zu definieren, um die Übersichtlichkeit zu erhalten.
- Übergeordnete Notabschaltsysteme sind hinsichtlich ihrer Auswirkungen auf die Anlage sowie die nachfolgenden Bedienhandlungen tiefgreifend zu analysieren.

## Bewertung der Ergebnisse

### Eigenschaften der untersuchten Anlagen

Die untersuchten Anlagen haben für alle vorausgedachten Störungen dem Bediener übergeordnete automatische Notabschaltsysteme. Es bleiben keine durchdachten Störungen übrig, bei denen die Sicherheit vom rechtzeitigen und richtigen Handeln des Bedieners abhängt. Die Hauptaufgabe des Bedieners ist das planmäßige Fahren der Anlage zur Sicherung der Produktausbeuten und -qualitäten sowie zur rechtzeitigen Erkennung von Abweichungen (als Prophylaxe).

Der bedienende Mensch ist im Hinblick auf die Anlagensicherheit fast ausschließlich dafür vorgesehen, bei sich anbahnenden Störungen die Zeit bis zum zwingenden Eingriff des Notabschaltsystems zu nutzen, durch Optimierung der nach der Störung noch möglichen Fahrweise die Produktionsstörung infolge einer Stillsetzung zu vermeiden (Umsteuern auf andere Arbeitspunkte der Anlage, Anfahren von Reserveaggregaten etc.). Daraus folgt, daß dem Bediener wesentliche sicherheitsrelevante Aufgaben im engeren Sinne planmäßig nicht mehr zugedacht sind.

Die Betrachtung vorausgedachter Störungen und Bedienhandlungen wird zur Beurteilung der Bedienbarkeit gefordert. Andererseits ist es allgemein übliche, notwendige und akzeptierte Strategie, bedienende Menschen zum Beherrschen oder Behandeln unvorhergesehener Situationen ständig im Einsatz zu haben.

Redundanz im Automatisierungssystem ist selbstverständlich geworden. Bei besonders sicherheitsrelevanten Prozeßgrößen sind für die Grenzwertgeber 2-von-3-Systeme oder diversitäre Redundanz installiert. Damit wird eine Zuverlässigkeit des Notabschaltsystems erreicht, bei der Handeingriffe zur Kompensation von Versagen der technischen Sicherungen nicht mehr im Blickfeld sind.

Zu den betrachteten Anlagen lagen geprüfte Sicherheitsanalysen auf der Basis des PAAG-Verfahrens vor.

### Bedienstellen-Schema

Die Anlage, in der die Untersuchungen zum Bedienstellen-Schema vorgenommen wurden, ist durch ein sehr hohes Niveau automatischer Notabschaltsysteme gekennzeichnet. In Folge dessen ist kein weiterer Sicherheitsgewinn durch eine Vorsorgebetrachtung mit dem Bedienstellen-Schema erreichbar.

Wegen der besonderen Konfiguration der untersuchten Anlage ist keine generelle Aussage zu der Anwendbarkeit der Methode möglich. Dieses wäre an einer Anlage mit geringerem Automatisierungsgrad (insbesondere mit weniger ausgefeiltem Notabschaltsystem) zu prüfen. Dessen ungeachtet steht auch der Betreiber hinter der Forderung, vom Anlagenpla-

ner eine Dokumentation der Bedienstrategie zum Nachweis der Bedienbarkeit zu verlangen. Dafür wird aber der Störungskompensationsgraph als geeigneter angesehen.

Für die betrachtete Anlagenkategorie ist somit das Bedienfunktionen-Schema nicht als geeignetes Hilfsmittel akzeptiert worden. Damit ist noch keine Aussage für Anlagenklassen mit geringerem Automatisierungsgrad, geringerem Funktionsumfang oder weniger ausgeprägten Notabschaltsystemen möglich. Die Beurteilung wird wesentlich davon beeinflußt, ob eine Sicherheitsanalyse nach einem tabellarischen Verfahren (z.B. PAAG) schon vorliegt.

### Balkendiagramm zur Darstellung der Gleichzeitigkeit

Das Balkendiagramm ist die einzige untersuchte Möglichkeit, Zeitabhängigkeit und Gleichzeitigkeit zu betrachten.

Im Praxistest wurden folgende Erkenntnisse gewonnen:

- In der Regel erfolgt keine Prüfung der an den Bediener gestellten Anforderungen hinsichtlich der Erfüllbarkeit (unter Berücksichtigung der menschlichen Leistungsgrenzen).
- Im Rahmen der Anlagenplanung werden mögliche technische Störungen in Hinblick auf die höchste Rate der Vermeidung von Produktionsunterbrechungen untersucht. "Dennoch-Störfälle" werden dabei zufällig und zwangsweise mit in die Minimierung der Auswirkung von Störungen einbezogen.
- Im Rahmen einer energischen Personalreduzierung bzw. -einsparung werden die technischen Möglichkeiten zur Schadensabwehrung maximal ausgeschöpft. Unter diesem Aspekt ist dem Bediener die Handlungsfolge durch Programmierung der einzelnen möglichen (erkennbaren, vorausgedachten) Störungsfolgen aus der Hand genommen.
- Trotz der nachgewiesenen Beherrschbarkeit extremer Betriebssituationen ist nicht auszuschließen, daß Ereignisse wie das Eintreten von zwei gleichzeitigen "Dennoch-Störfällen" beim Betrieb der Anlage auftreten können. Situationen, die zu einem Überschreiten der menschlichen Leistungsgrenze führen können, werden "zufällig" durch die Einbeziehung (automatisierungs-)technischer Mittel in der Planung und Ausführung der Anlage erkannt und verhindert.
- Der befragte Anlagenbetreiber hält eine Untersuchung bzw. Betrachtung der Bedienbarkeit seiner Anlage in der Planungsphase für notwendig. Zusätzliche Darstellungen für den Bediener auf der Prozeßleittechnik wird dagegen als nicht notwendig angesehen.
- Zur Durchführung der Untersuchung muß zunächst der Bedienablauf aus den Bedienanweisungen konstruiert werden und jedem Schritt eine Zeitschätzung zugeordnet werden.

- Allgemeine Planungsvorschriften, wie die im untersuchten Betrieb vorhandenen "Allgemeinen Planungsunterlagen Bau", sind grundsätzlich für alle störfallrelevanten Anlagen zu empfehlen. Werden diese internen Vorschriften, die dem Anlagenplaner bis in das kleinste Detail vorschreiben, wie und unter Berücksichtigung welcher Vorschriften zu planen und zu errichten ist, noch hinsichtlich der Analyse der Bedienabläufe erweitert, zwingen sie den Planer technischer Abläufe zur systematischen Untersuchung der Bedienbarkeit

Der Aufwand für die Untersuchung ist beträchtlich. Deshalb ist die Einführung in die Anlagenplanung problematisch. Es ist aber jedem in der Thematik Tätigen mindestens einmal zur Erarbeitung zu empfehlen, da dabei das Problembewußtsein wesentlich weiterentwickelt wird.

### **Störungskompensationsgraph**

Die Entwicklung und praktische Erprobung des Störungskompensationsgraphs erfolgt auf der Basis einer vorliegenden PAAG-Tabelle. "PAAG" steht hier als Beispiel für eine tabellarisches Verfahren aus der Gruppe der HAZOP-Verfahren nach IEC 61882 (Guide for Hazard and Operability Studies, noch nicht abgeschlossener Entwurf).

Folgende Vorteile einer solchen Darstellung sind zu benennen:

- Als Ausgangspunkt können vorhandene Untersuchungen der betrieblichen Gefahrenquellen genutzt werden (neben dem PAAG-Verfahren sind auch andere tabellarische Verfahren nutzbar),
- es erfolgt eine systematische Untersuchung der Eingriffsmöglichkeiten des Bedieners in die Anlagensteuerung unter Berücksichtigung übergeordneter Notaussysteme,
- die dem Gesamtsystem innewohnenden technischen und/oder organisatorischen Sicherheitsbarrieren zur Verhinderung eines Störfalls werden dokumentiert,
- die grafische Darstellung hilft die Einzelfehlerorientierung der Tabelle zu überwinden,
- der Zwang zur grafischen Darstellung trägt zur Vollständigkeit der betrachteten Fehlermöglichkeiten bei,
- die Grafik lässt Zustandsrückmeldungen erkennen, die für den Bediener keine Handlungsaufforderungen (also weniger wichtige Informationen) sind.

Die Gesamtübersicht über die Anlagen- und Bediensicherheit wird durch eine grafische Darstellung der Ergebnisse wesentlich verbessert. Die Beurteilung der Sicherheit wird damit effektiver und zugleich intensiver.

Die vorgeschlagene (oder eine vergleichbare) Darstellung könnte Eingang in die untergesetzlichen Regelwerke finden.

### **Wertung durch den Anlagenbetreiber**

Im Rahmen der Untersuchungen wurde bestätigt, daß die Anlagensicherheit in den beiden untersuchten kontinuierlich betriebenen Anlagen durch automatische Überwachungs- und Verriegelungssysteme gesichert wird. Diese Systeme spiegeln die Sicherheitsphilosophie des Praxispartners (Anlagenbetreibers) wider, gemäß der die Anlage im Falle einer Störung ohne Eingriff des Betriebspersonals in einen sicheren Zustand überführt wird. Ebenso werden uneindeutige Anlagenzustände (z.B. widersprüchliche Signale) erkannt und behandelt.

Aus diesen sicheren Zustand (Beharrung) kann die Anlage dann wieder gestartet werden. Für den Neustart der Anlage ist die klare, eindeutige Darstellung des Beharrungszustandes für den Bediener wichtig.

Durch diese Herangehensweise kann der Bediener selbst – auch bei bisher nicht betrachteten unabhängig voneinander und gleichzeitig auftretenden Störungen – durch ein Überangebot von Informationen nicht zum Risikofaktor werden. Dies wird dadurch erreicht, daß z.B. nicht beachtete Alarme durch die bei der Anlagenplanung vorgedachten und in den SPS- und Tripsystemen<sup>11</sup> festgelegten Abläufe zu einem sicheren Anlagenzustand führen.

Hierfür müssen die für die Sicherheit wichtigen Anlagenparameter und die notwendigen Abläufe in der Planungsphase vollständig erfaßt werden.

Die bildschirmgesteuerte Anlage setzt die durchgehende Verfügbarkeit der Prozeßleittechnik einschließlich der Visualisierung voraus. Da auch die Prozeßleittechnik gestört sein kann, ergibt sich die Notwendigkeit, daß bei gleichzeitigem Auftreten einer solchen Störung und einer technischen Störung im Anlagenfeld die Anlagensicherheit gewährleistet sein muß. Die Auswirkungen dieser gekoppelten Störungsvariante könnten mit dem Störungskompensationsgraphen erfaßt und dargestellt werden.

Bei weiteren Anlagenplanungen und -änderungen sollen daher die Erkenntnisse aus den Arbeiten zu diesem Projekt insbesondere in Hinblick auf die Ausfälle der Prozeßleittechnik bzw. der Visualisierung der Prozesse angewandt werden.

---

<sup>11</sup> Ein Tripsystem ist ein Notabfahrtsystem zum Überführen der Anlage in einen gefahrlosen Zustand.

## Kriterien für den Umfang der Untersuchungen

### Abschneidekriterien für den Umfang der Untersuchungen

Hinsichtlich der zu betrachtenden technischen Ausfälle, insbesondere bei den Informationsquellen für den Menschen werden die beiden folgenden Kriterien empfohlen:

- Ausfälle werden nicht angenommen bei 2-von-3-Systemen
- Es wird nicht angenommen, daß beide Alarmgeber oder Meßsysteme in diversitärer Redundanz ausfallen.

Als weiteres Kriterium wird empfohlen:

- Es wird nicht angenommen, daß Sicherheitsventile versagen.

### Kriterien für die Zerlegung von Anlagen in Betrachtungsabschnitte

Die Darstellbarkeit verlangt, komplexe Anlagen in zu betrachtende Abschnitte zu zerlegen. Ein einfaches Kriterium ist die Trennung in Betrachtungsabschnitte jeweils an Apparaten mit Speicherfunktionen, so wie im Abbildung 7-9 auch vorgenommen.

Die Basis dafür ist, daß durch die Speicherfunktion gewöhnlich ein zeitlicher Spielraum entsteht, ehe sich Vorgänge in dem betrachteten Abschnitt unvermeidlich auf vor- oder nachgeschaltete Anlagenteile auswirken. Es wird unterstellt, daß dieser Spielraum groß genug ist, so daß keine zusätzliche Belastung des Bedieners in einer Situation mit Kapazitätsengpaß entsteht. Durch diese Speicherfunktion wird ermöglicht, die aneinandergrenzenden Anlagenteile nacheinander zu bearbeiten.

### Betrachtung gleichzeitiger Primärausfälle

Problematisch ist die Annahme von gleichzeitigen Ausfällen technischer Apparate, Maschinen oder Armaturen (unabhängige Primärursachen, nicht Ketten zwangsläufiger Folgen). Gerade durch gleichzeitige Ausfälle kann ein Überlauf in der Leistungsfähigkeit eines Bedieners verursacht werden. Andererseits gehen alle bisherigen Verfahren zur Beurteilung der Anlagensicherheit nur von Einzelfehlern aus. Das Beispiel in Kapitel 7.1 ging davon aus, daß an der Anlage zwei primäre Ausfälle – Apparat und Armatur – gleichzeitig auftraten (nicht zu verwechseln mit Ketten von Ausfällen).

Will man die Sicherheitsbetrachtungen auf solche gleichzeitigen Primärausfälle ausdehnen, so ergibt sich durch die notwendige Kombinatorik eine explosionsartige Vergrößerung des Untersuchungsumfangs. Darüber hinaus ist zu unterscheiden, ob die Störungen in den nachfolgenden Ausrüstungen separat verlaufen, oder ob es zu Überschneidungen kommt.

Der zweite Fall bedarf tiefgreifender Analyse, da sich widersprechende Signale auftreten können.

Es bietet sich folgende Festlegung dazu an: Sofern bei den automatischen Notabschaltsystemen Vollständigkeit angestrebt wurde, werden nur einzelne Primärausfälle für die Kompensation durch Handeingriffe betrachtet.

Bei Kleinanlagen, wo auf vollständige automatische Notabschaltsysteme verzichtet wurde, ist die Betrachtung von jeweils zwei gleichzeitigen Primärausfällen anzustreben. Bei geringen Anlagenumfang dürfte das überschaubar bleiben.

## Anregungen für die Weiterentwicklung der Anlagengestaltung

### Anzeige des Handlungsspielraumes im Prozeßleitsystem

Alle Aktivitäten eines Bedieners sind nur zwischen Beginn einer Störung und zwangsläufigem Eingreifen der automatischen Notabschaltung möglich. Zur Entlastung des Bedieners ist es deshalb wünschenswert, ihm den verbleibenden Spielraum anzuzeigen.

Abhängig von der jeweiligen Prozeßgröße ist dies andeutungsweise üblich, indem ein Alarm für einen geringeren Wert als dem, der den Noteingriff aktiviert (Warn- und Schaltalarm), installiert ist. Zur Verarbeitung dieser Information muß der Bediener aber jeweils selbst als gedankliche Leistung die Verknüpfung mit der Geschwindigkeit der Prozeßgrößenänderung herstellen.

Für die Zukunft ist deshalb anzustreben, ihm die Größe des verbleibenden Fensters für seine Handlungen in den zwei Dimensionen "Prozeßgrößendifferenz" und "Zeit" anzuzeigen. Mit den Möglichkeiten moderner Prozeßleitsysteme ist die technische Realisierung problemlos, man muß sich nur darüber klar werden, welche Größen dafür heranzuziehen sind.

Zwischen einzelnen Prozeßstufen gibt es üblicherweise Apparate mit Speicherfunktion. Bei dem in Abbildung 7-9 betrachteten Anlagenabschnitt ist das der Behälter B 101 im Eingang und der Abscheider A 101 am Ausgang. In beiden Gefäßen ist eine Niveauänderung tolerierbar, ehe eine Störung sich auf vor- oder nachgeschaltete Anlagenabschnitte auswirkt. Aus dem zeitlichen Gradienten dieser beiden Niveauänderungen und der verbleibenden Niveautoleranz ist das verbleibende Handlungsfenster situationsabhängig bestimmbar. Dabei ist die automatische Auswahl des jeweils engeren Fensters technisch kein Problem.

Auf diese Weise kann der Bediener von relativ schwierigen Überlegungen, die unter dem Stress einer Störung die Handlungsfähigkeit begrenzen, wesentlich entlastet werden. Somit wird vermieden, daß der Bediener in einer Stresssituation geistige Kapazität in Wege investiert, die keine Erfolgsaussicht mehr haben.

## Auswahl der dem Bediener zu präsentierenden Informationen

Es ist seit langem Lehrmeinung, dem Bediener nur Informationen oder Informationsumfänge anzugeben, aus denen er eine Handlung ableiten kann bzw. muß (siehe z.B. Müller, R. 1979, S. 166 ff.) Damit sollte die Menge der Informationen begrenzt werden. Die Beschäftigung mit dem Störungskompensationsgraphen zeigt Stellen (in Abbildung 7-9 mit A1 und A2 markiert), an denen der Bediener über Aktivitäten des übergeordneten Notabschaltsystems rückinformiert wird, ohne daß von ihm eine Handlung erwartet wird, oder ihm überhaupt noch eine Handlung möglich ist.

Die Regel, nur Informationen zu präsentieren, aus denen Handlungen abzuleiten sind, muß auch auf solche Informationen angewandt werden. Damit werden die Rückinformationen zur Entlastung der aufzunehmenden Informationsmenge infrage gestellt.

Es wird aus folgenden Gründen nicht empfohlen, diese Informationen, die am Ende einer "Sackgasse" stehen, ganz wegzulassen:

- Es ist nicht leicht zu übersehen, ob diese Informationen in anderen Zusammenhängen noch handlungsrelevant sind.
- Erkennt der Bediener daraus, daß er einen begonnenen Therapieversuch der Anlage abbrechen muß, so ist das auch eine daraus abgeleitete Handlung.

Es folgt, daß durch Farbwahl oder ähnliches diese Informationen als weniger wichtig gekennzeichnet werden sollten.

### 7.7.2 Demonstrationsbeispiel Batch-Anlagen

#### Probleme bei der Darstellung der Bedienerbelastung

Bei der Erarbeitung und Praxiserprobung einer Darstellungsform für die Bedienerbelastung in Batch-Anlagen tauchten einige Probleme auf, die im folgenden diskutiert werden sollen:

- Berücksichtigung von Nebentätigkeiten: Neben der Haupttätigkeit des Bedieners die chemischen Prozeßabläufe zu begleiten, gehören in der Regel diverse Nebentätigkeiten zum Aufgabenspektrum des Schichtpersonals. Unter anderem sind zu nennen:
  - Stoffe für den Ansatz zusammenstellen
  - Apparate reinigen
  - Proben entnehmen
  - Inspektionen durchführen
  - Reparatur- und Wartungsarbeiten durchführen
  - Dokumentationen erstellen

- Bestellungen für den Betrieb vorbereiten
- Arbeitsplanungen durchführen
- Mitarbeiter unterweisen
- Mitarbeiter kontrollieren.

Diese Nebentätigkeiten sind im allgemeinen nicht einem genauen Zeitpunkt zuzuordnen, sondern sollen durch das Personal lediglich irgendwann innerhalb eines definierten Zeitraums erledigt werden.

Bei der Bedienerbelastung innerhalb einer Schicht bzw. einer Produktionsphase sind diese Nebentätigkeiten zwingend zu berücksichtigen. Dies kann ggf. dazu führen, daß in den Betriebsanweisungen festzuhalten ist, daß in bestimmten Produktionsabschnitten, in denen sicherheitsrelevante Bedienschritte abzuwickeln sind, keine derartigen Nebentätigkeiten parallel zu verrichten sind.

- Meßwertbeobachtungen**: Aus den betrieblichen Unterlagen sind meist nicht vollständig alle notwendigen Meßwertbeobachtungen erkennbar. Insbesondere ist in der Regel nicht direkt ableitbar, wie stark der Bediener durch Meßwertbeobachtungen in Anspruch genommen ist (ständig, alle 5 Minuten, einmal pro Stunde an den Meßstellen AB, BC, DE usw., siehe Abbildung 7-12). Die Meßwertbeobachtungen sollten zukünftig ebenso präzise in der Rezeptanweisung festgehalten werden, wie alle sonstigen Bedienhandlungen.
- Die Bedienschritte, die eine Schicht umzusetzen hat, sind nicht zwingend einem einzelnen Bediener zugeordnet; das Personal regelt unter sich, wer welche Aufgabe gerade erledigen soll. Dies ist nicht nur ein Problem für die Erfassungsmöglichkeit der Bedienerbelastung, sondern insbesondere auch ein Problem der eindeutigen Verantwortlichkeit für einzelne Bedienschritte.
- Die Darstellung der Bedienerbeanspruchung erlaubt nicht direkt eine Bewertung, ob der Bediener zu irgendeinem Zeitpunkt bereits überlastet ist. Bediener sind je nach Erfahrung, Qualifikation, Stressresistenz oder auch Teamqualität sehr unterschiedlich belastbar.
- Die Anforderungen an den Bediener in vorhersehbaren Störsituationen sind im allgemeinen nicht im Detail dokumentiert, so daß eine Bedienerbeanspruchung in Störsituationen nicht aus bestehenden Unterlagen ableitbar ist.

Diese Probleme wurden mit dem Anlagenbetreiber diskutiert. Dabei wurde immer wieder die große Sorge geäußert, daß es durch zusätzliche Dokumentations- und Protokollpflichten zu einer weiteren Informationsflut kommen könnte, die am Ende nicht in einem vernünftigen Aufwand-Nutzen-Verhältnis steht.

## Schlußfolgerungen aus dem Demonstrationsbeispiel Batch-Anlagen

Die Erarbeitung einer Darstellungsform für die Bedienerbeanspruchung zeigte auf, daß zum Teil auf bestehenden betrieblichen Unterlagen (wie Rezept-/Arbeitsanweisungen) aufgebaut werden kann, daß jedoch insgesamt die Bedienhandlungen nicht detailliert genug dokumentiert sind, um sie als Bedienerbeanspruchung darstellen zu können.

Die Darstellung der Bedienschritte innerhalb des chemischen Prozesses in einer proportionalen Zeitachse mit paralleler Darstellung zeitlich parallel erfolgender Bedienschritte ist geeignet, potentiell überfordernde Prozeßschritte optisch direkt erkennbar zu machen.

Die derzeit offensichtlich noch bestehenden Informationslücken zur Bedienerbeanspruchung sollten langfristig abgebaut werden. Kurz- bis mittelfristig sollten jedoch mindestens in folgenden Situationen genauere Analysen der Bedienerbelastung erfolgen:

- nach Ereignissen und Beinahe-Ereignissen
- nach Äußerungen der Mitarbeiter über Arbeitsüberlastung
- wenn bei der Produktionsplanung schon erkennbar wird, daß es zu Streß für die Mitarbeiter kommen kann
- wenn bei der Anlagenplanung ein hoher Bedienaufwand vorgesehen wird
- wenn es sich um eine kritische Reaktion handelt, mit ggf. schnellen Fehlentwicklungen im chemischen Prozeßablauf.

Bei Batch-Anlagen mit hohem Potential an möglichen Fehlbedienungen kann auf diese Human Factor-Aspekte auf Dauer nicht verzichtet werden.

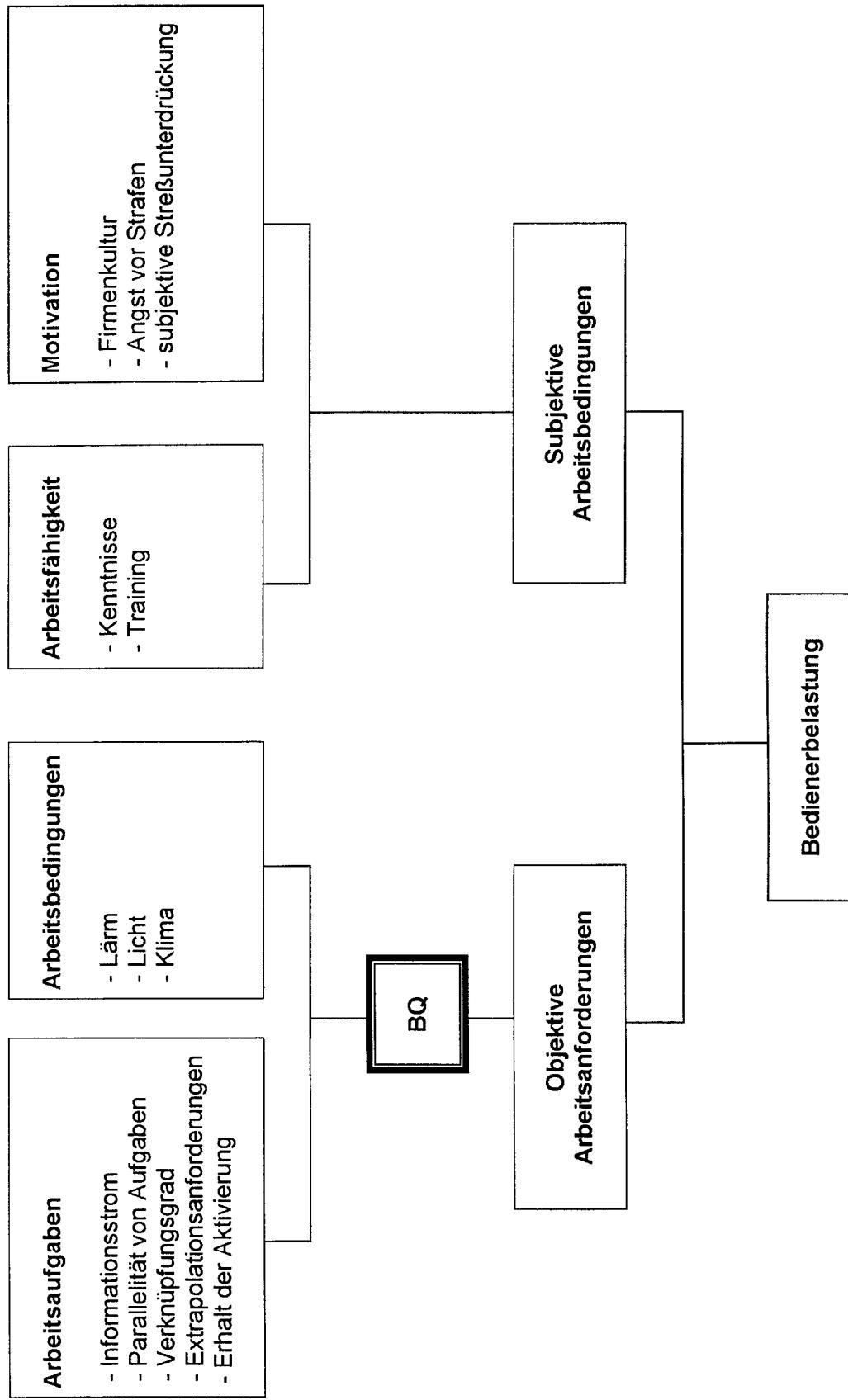
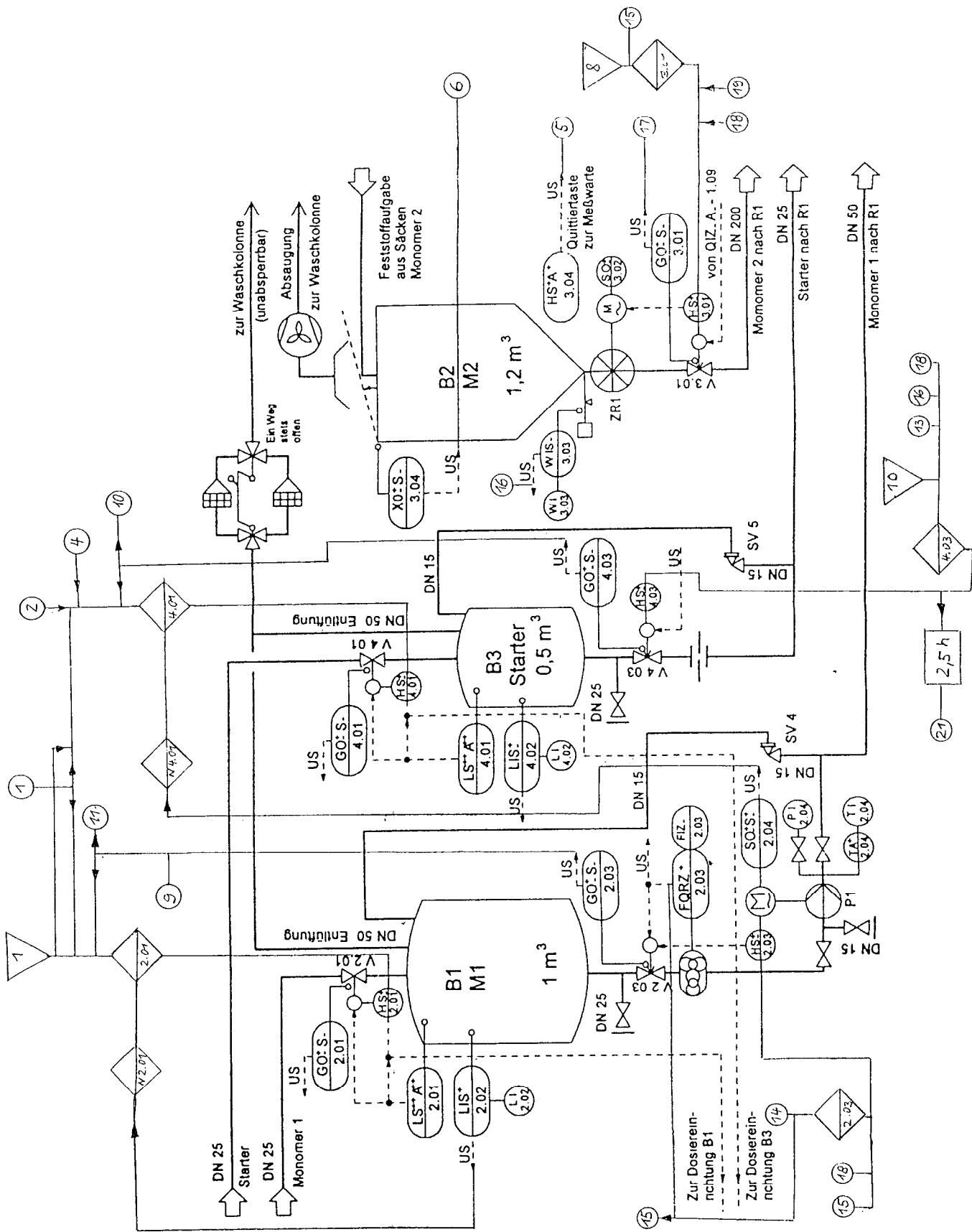


Abb. 7-1: Einflüsse auf die Leistungsfähigkeit eines Bedieners  
BQ - betrachteter Bilanzquerschnitt

**Copolymerisationsanlage**  
**Teilanlage "Rohstoffversorgung"**

**Abb. 7-2:** RI-Fließbild der Teilanlage "Rohstoffversorgung" mit eingetragenen Bedienfunktionen  
(Beispiel aus der BAuA-Schrift RW 27)



# Copolymerisationsanlage

## Teilanlage "Reaktor"

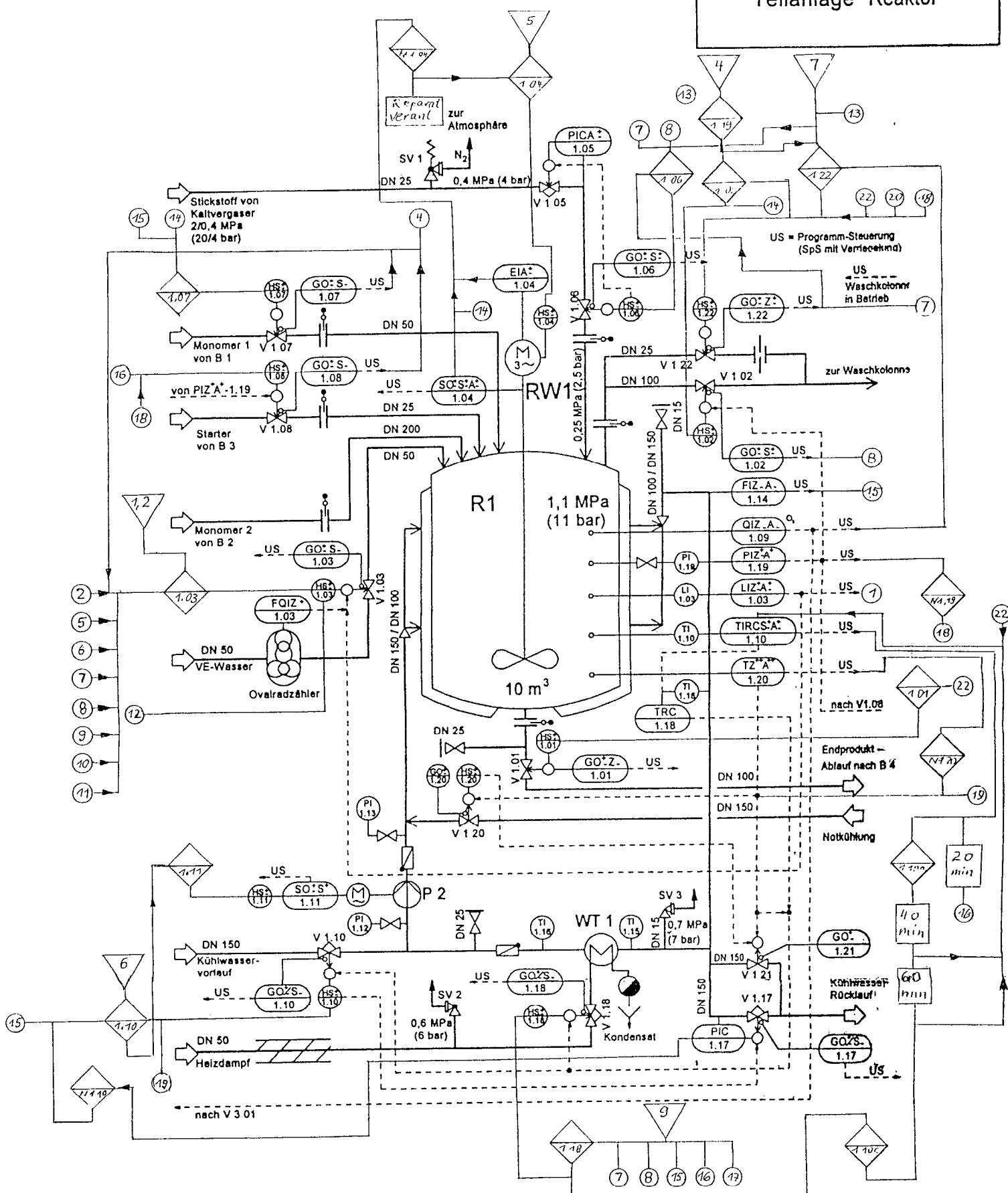


Abb. 7-3: RI-Fließbild der Teilanlage "Reaktor" mit eingetragenen Bedienfunktionen  
(Beispiel aus der BAuA-Schrift Rw 27)



Bedienfunktionen aus der Warte



Handeingriff auf Stellglied



Handeingriff auf Reglersollwert



Noteingriff



Bedienfunktion vor Ort



Schritt des Produktionsplanes

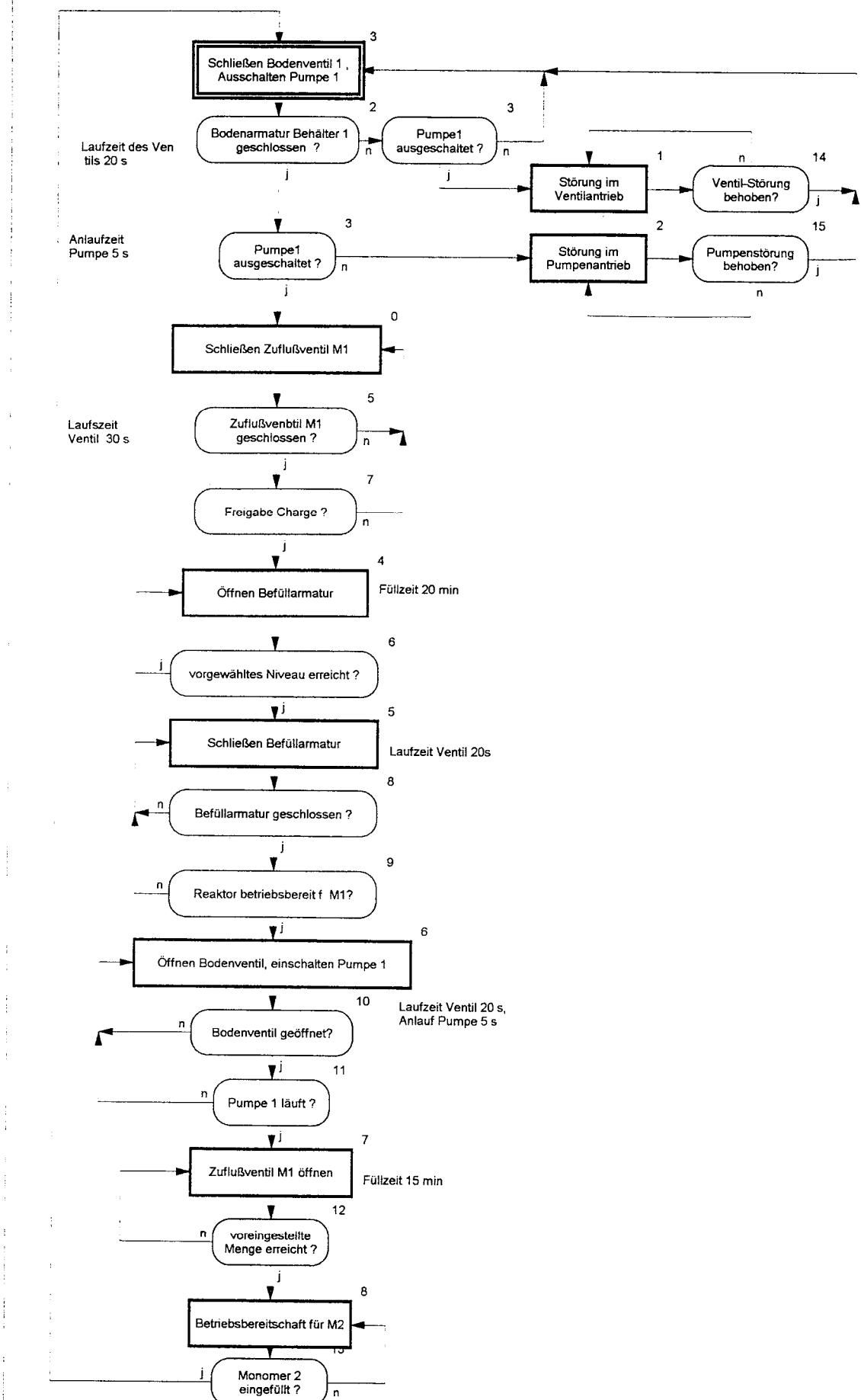


Signalkopplung an parallele redundante Aggregate



Konnektoren

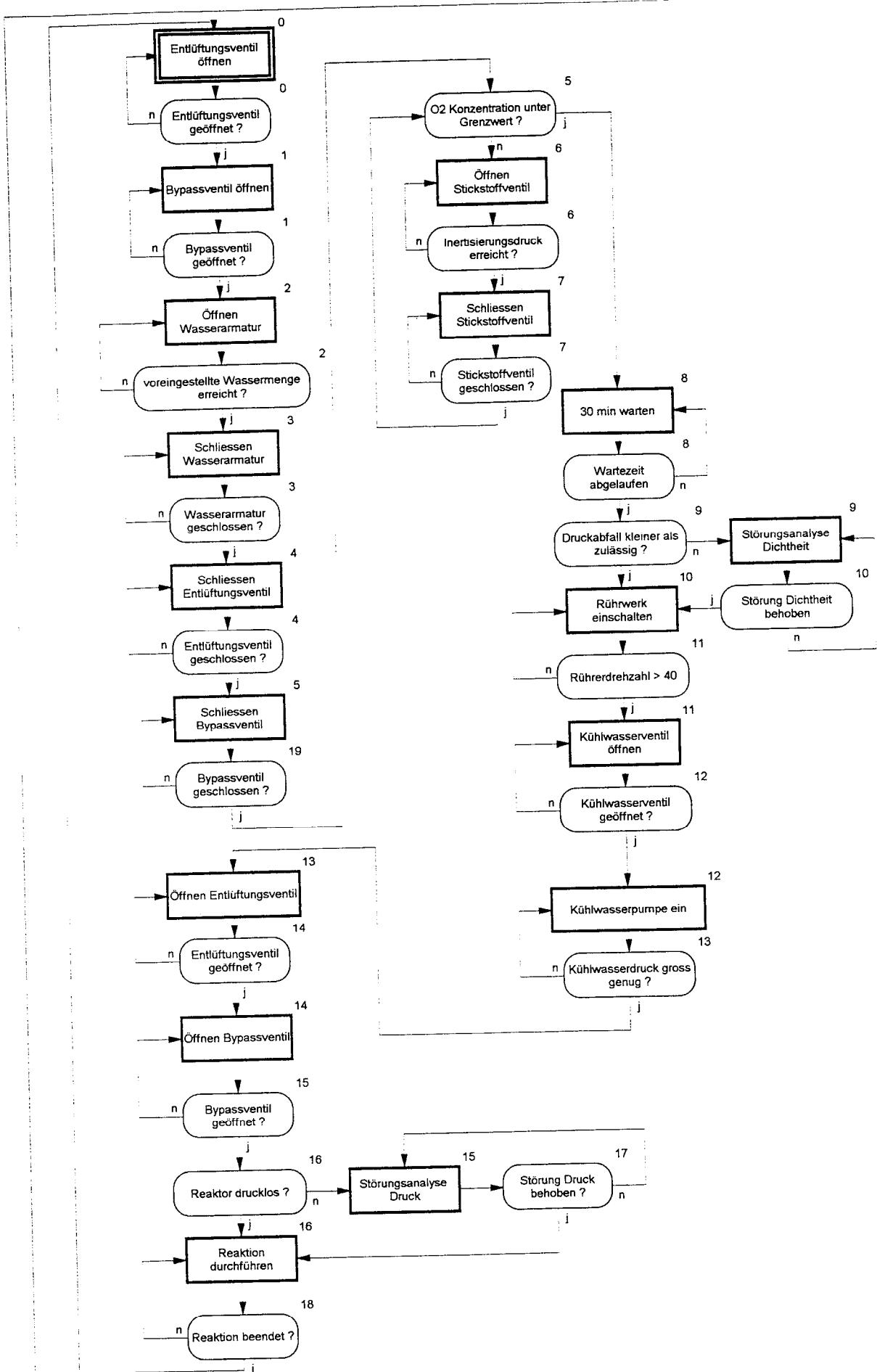
**Abb. 7-4:** Erläuterung der verwendeten Symbole



Erstellt mit TeCAD © AVI-GmbH

Zust.	Änderung	Datum	Name	Freigeg.	BfAA Rw 27	Prozeßablaufplan	Blatt
						1 von 2	

**Abb. 7-5:** Prozeßablaufplan für den Teilprozeß 1 "Monomer 1"  
(Beispiel aus der BAuA-Schrift Rw 27)



Erstellt mit TeCAD © AVI-GmbH

		Datum	22.01.99	Zeichnungs-Nr.:	
		Bearb.	R. Müller		
		Gepr.		Reaktor vorbereiten und Füllen	Blatt
Zust.	Änderung	Datum	Name	Freigeg.	Prozeßablaufplan

Abb. 7-6: Prozeßablaufplan für den Teilprozeß 2 "Reaktor vorbereiten und füllen" (Beispiel aus der BAuA-Schrift Rw 27)

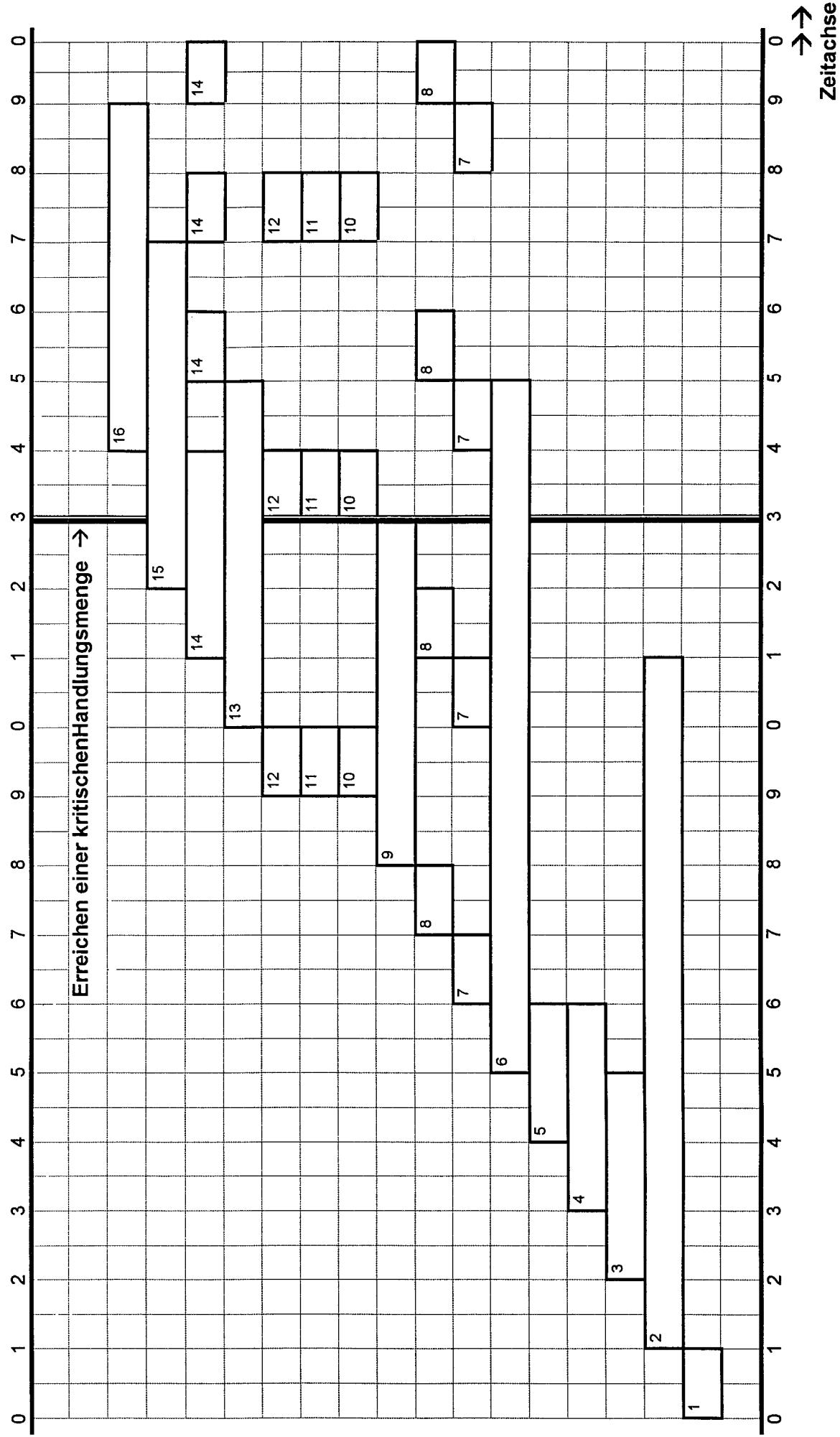


Abb. 7-7: Balkendiagramm zur Erfassung von Bedienabläufen

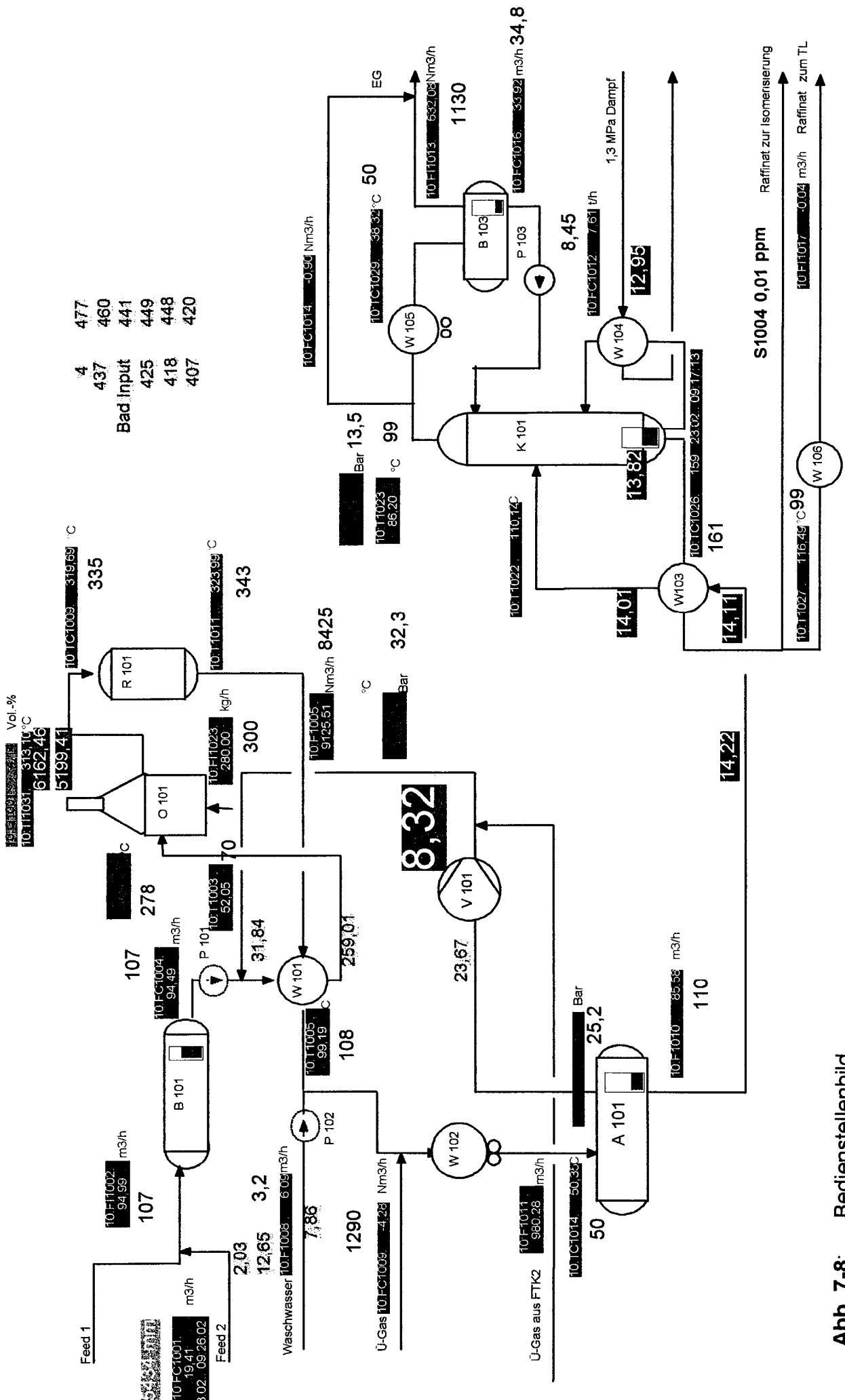


Abb. 7-8: Bedienstebild

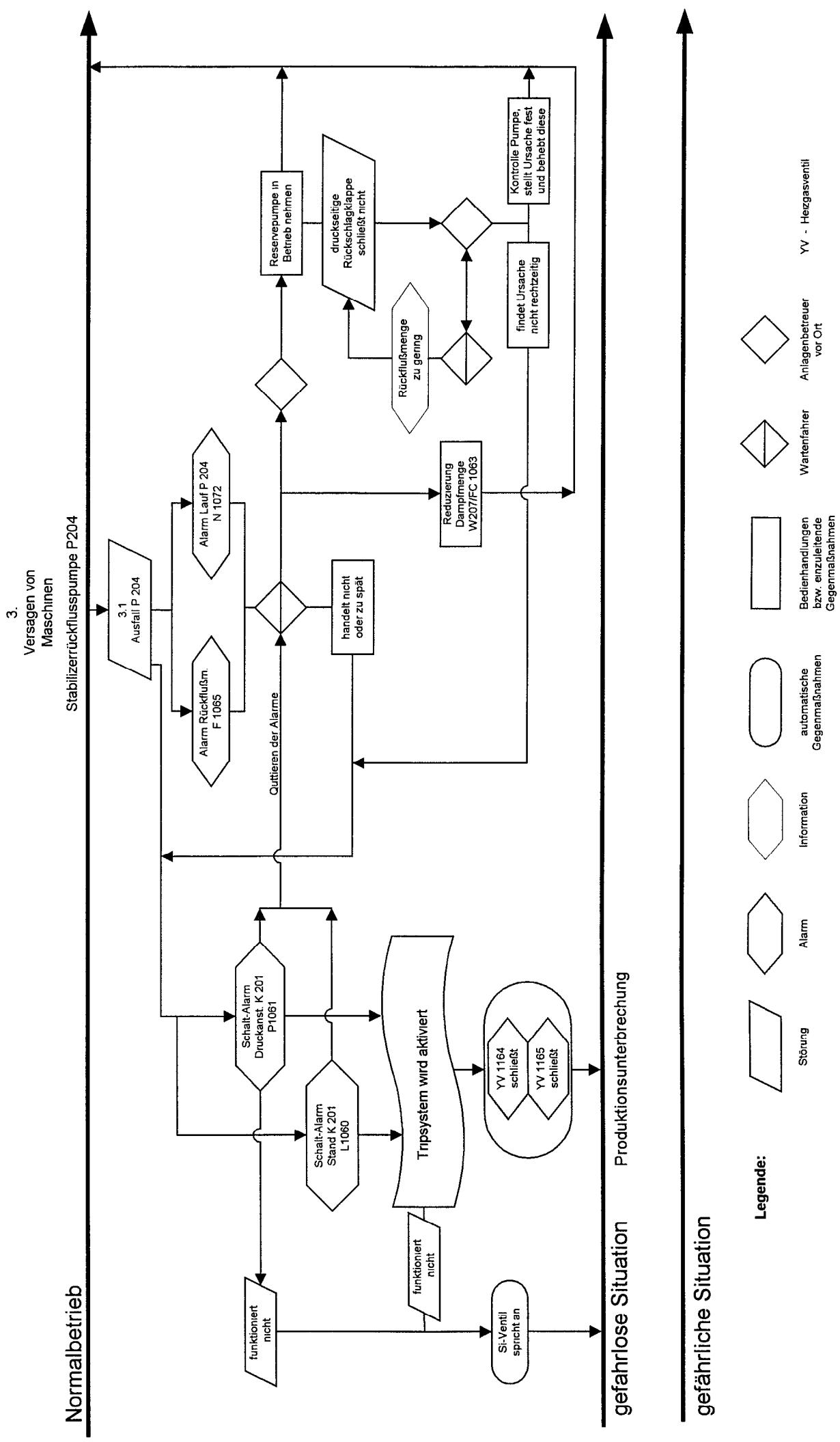


Abb. 7-9.

Störungskompressionsgraph – Ausfall Stabilizerrückflusspumpe

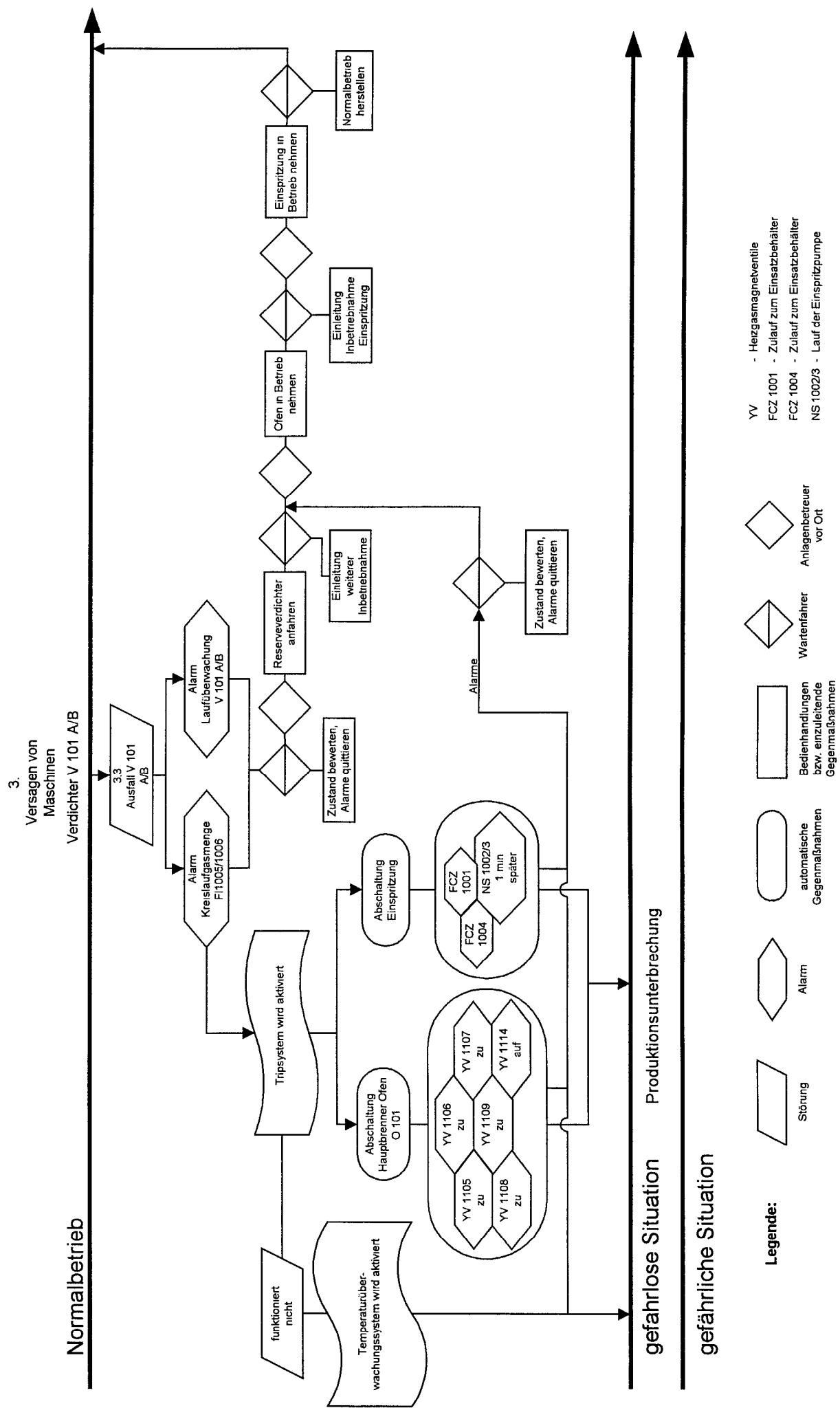


Abb. 7-10: Störungskompensationsgraph – Verdichterausfall

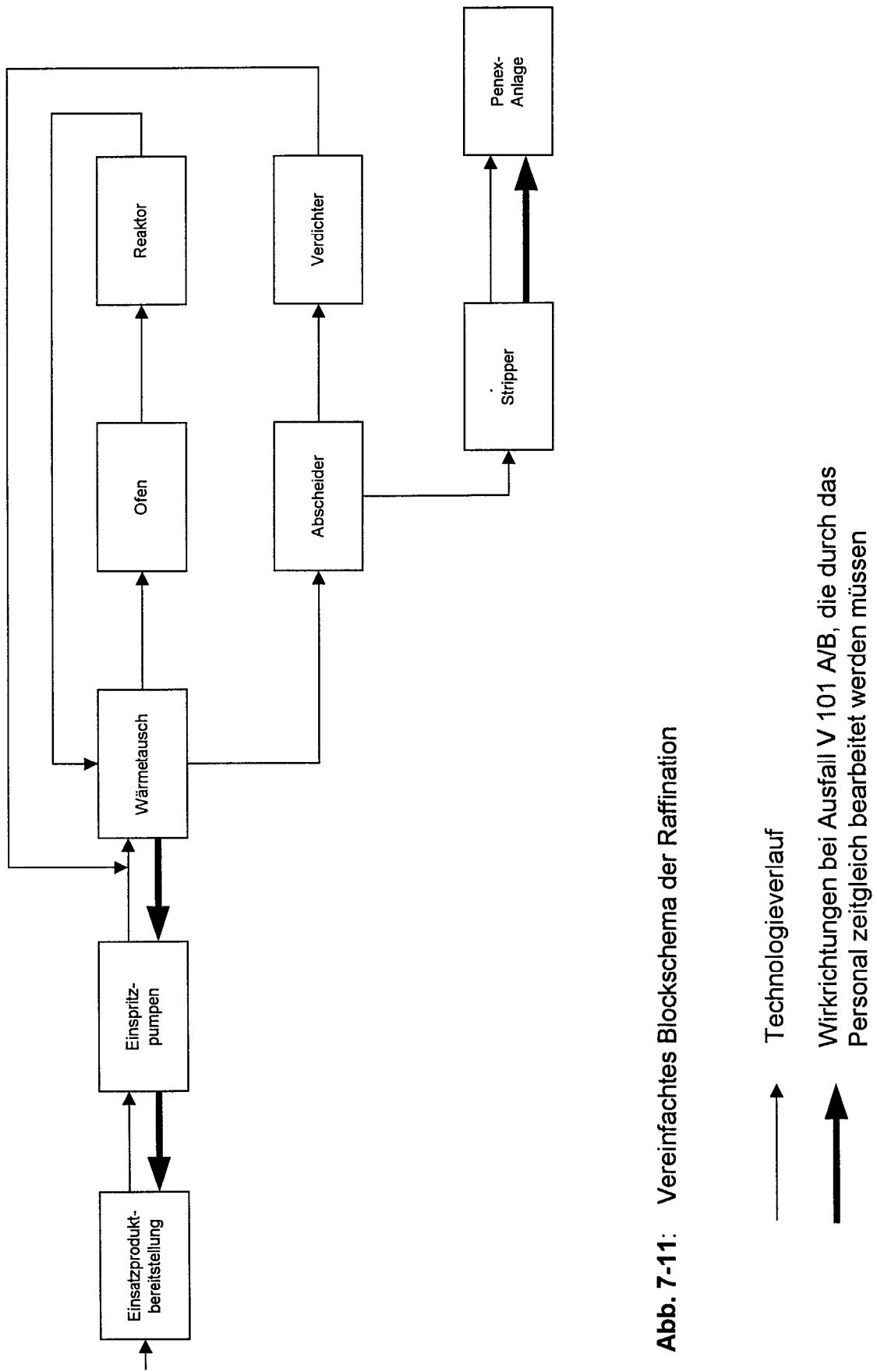


Abb. 7-11: Vereinfachtes Blockschema der Raffination

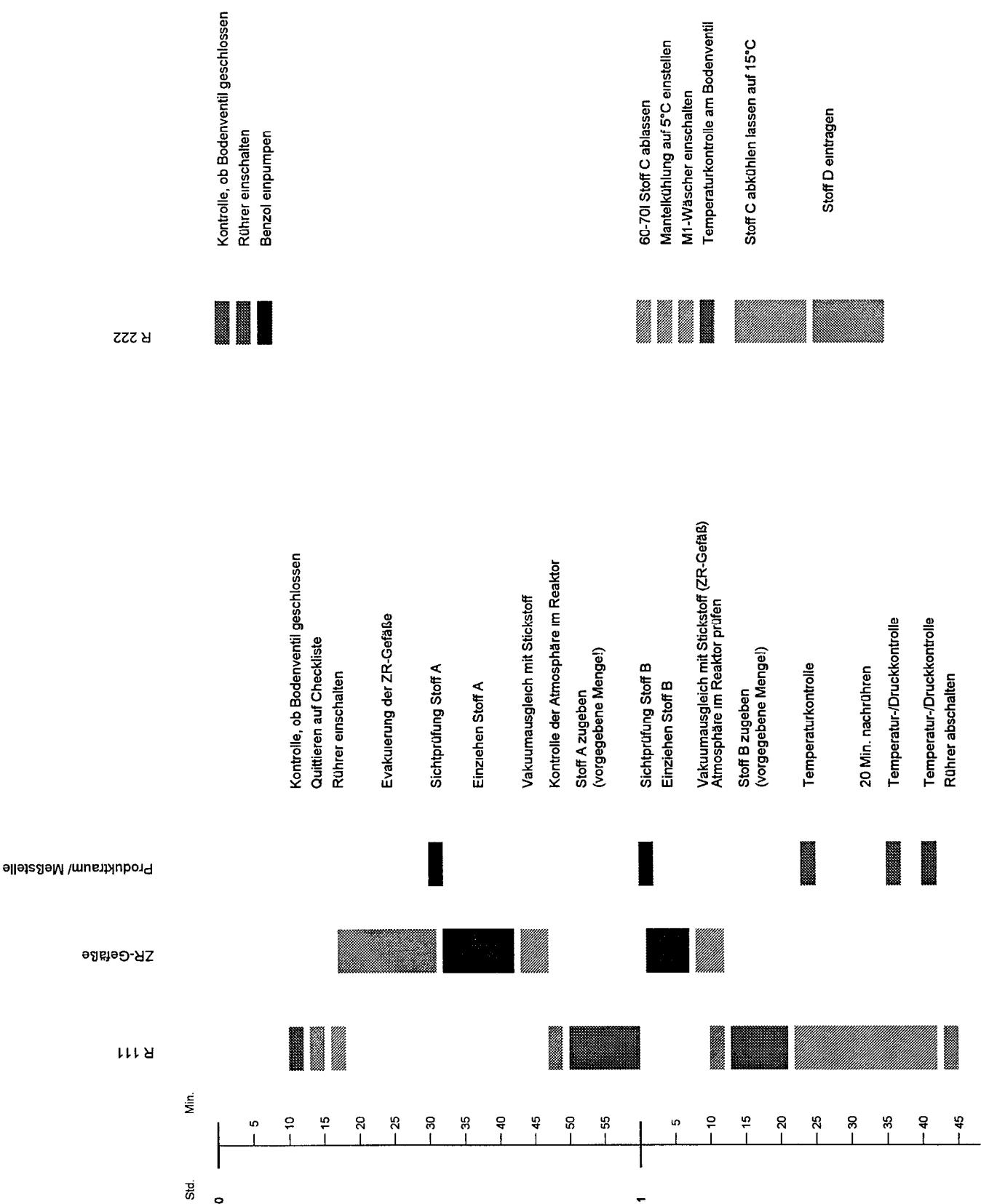
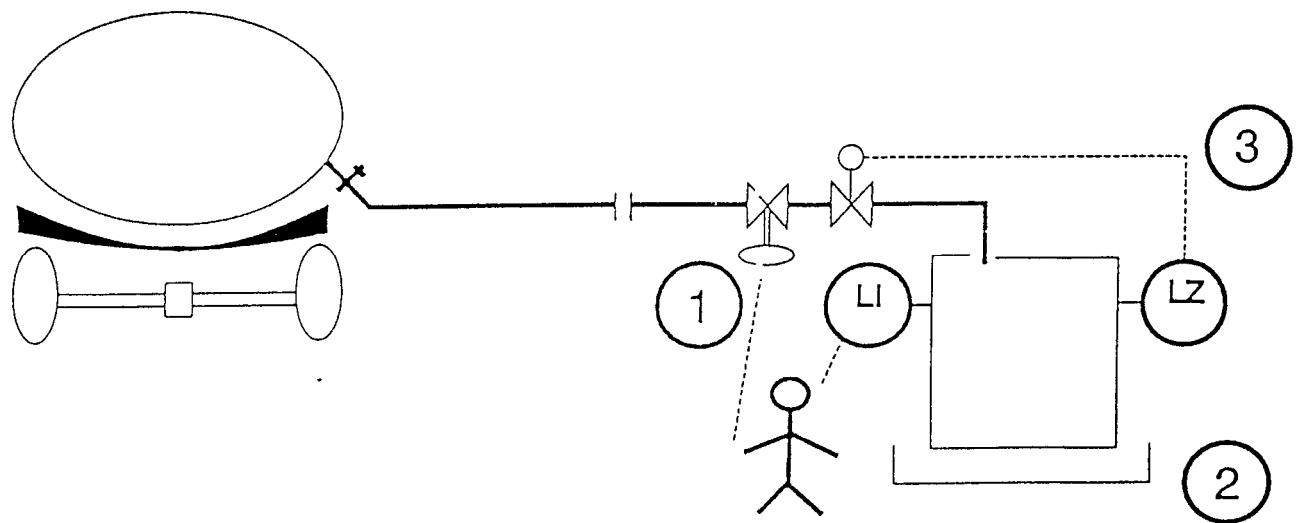


Abb. 7-12:

Ausschnitt aus der vorgeschlagenen Darstellungsform der Bedienkonzeption in Batch-Anlagen (Darstellung Normalbetrieb)

Ausschnitt aus der vorgeschlagenen Darstellungsform der Bedienkonzeption in Batch-Anlagen (Darstellung Normalbetrieb)



- ① Korrekte Bedienung
- ② Auffangtasse
- ③ Überfüllungssicherung

**Abb. 7-13:** Einfaches Beispiel für Sicherheitsbarrieren

**Tabelle 7-1: Monomer 1 - Prozeßvariablen  
(BAuA-Schrift Rw 27)**

Nr.	Aussage negative Aussage	Ausdruck
0	Handbedienung freigegeben Nicht Handbedienung freigegeben	erster Verfahrensschritt
1	Reaktor 1 leer Reaktor 1 nicht leer	LIZA 1 03
2	Bodenarmatur Behälter 1 geschlossen ? Nicht Bodenarmatur Behälter 1 geschlossen ?	GOS 2 03
3	Pumpe 1 ausgeschaltet ? Nicht Pumpe 1 ausgeschaltet	SOS 2 04
4	Rückmeldung vom Notprogramm Nicht Rückmeldung vom Notprogramm	von: Notprogramm
5	Zuflußventil M1 geschlossen ? Nicht Zuflußventil M1 geschlossen ?	GOS 1.07
6	Vorgewähltes Niveau erreicht ? Nicht vorgewähltes Niveau erreicht ?	LIS 2 02
7	Freigabe Charge ? Nicht Freigabe Charge ?	von: Reaktor vorbereiten und füllen
8	Befüllarmatur geschlossen ? Nicht Befüllarmatur geschlossen ?	GOS 2.03
9	Reaktor betriebsbereit für M1 ? Nicht Reaktor betriebsbereit für M1 ?	von: Reaktor vorbereiten und füllen
10	Bodenventil geöffnet ? Nicht Bodenventil geöffnet ?	GOS 2 03
11	Pumpe 1 läuft ? Nicht Pumpe 1 läuft ?	SOS 2 04
12	Voreingestellte Menge erreicht ? Nicht voreingestellte Menge erreicht ?	FQRZ 2 03
13	Monomer 2 eingefüllt ? Nicht Monomer 2 eingefüllt ?	HSA 3.04
14	Ventilstörung behoben ? Nicht Ventilstörung behoben ?	von: Störungsbeseitigung Ventil
15	Pumpenstörung behoben ? Nicht Pumpenstörung behoben ?	von: Störungsbeseitigung Pumpe 1

**Tabelle 7-2: Monomer 1 - Operationsvariablen  
(BAuA-Schrift Rw 27)**

Nr.	Aussage Negative Aussage	Opera- tionen*)	Ausdruck
0	Schließen Zuflußventil M 1 Nicht Schließen Zuflußventil M1		V 1 01
1	Schließen Bodenventil 1,Ausschalten Pumpe Nicht Schließen Bodenventil 1,Ausschalten Pumpe		V 2 03, HS 2.03
2	Störung im Ventilantrieb Nicht Störung im Ventilantrieb		Störung im Ventilantrieb
3	Störung im Pumpenantrieb Nicht Störung im Pumpenantrieb		Störung im Pumpenantrieb
4	Öffnen Befüllarmatur Nicht Öffnen Befüllarmatur		V 2.01
5	Schließen Befüllarmatur Nicht Schließen Befüllarmatur		V 2 02
6	Öffnen Bodenventil 1, Ausschalten Pumpe Nicht Öffnen Bodenventil 1, Ausschalten Pumpe		HS 2.03
7	Zuflußventil M1 öffnen Nicht Zuflußventil M1 öffnen		V 1.07
8	Betriebsbereitschaft für M2 Nicht Betriebsbereitschaft für M2		Übergang in Teilprozeß Monomer 2

\*) Die Spalte Operationen ist im Programm für die Weiterverarbeitung in der Steuerungstechnik enthalten Für die Betrachtung der Bedienhandlung hat sie keine Bedeutung

**Tabelle 7-3: Reaktor vorbereiten und füllen - Prozeßvariablen  
(BAuA-Schrift Rw 27)**

Nr.	Aussage Negative Aussage	Ausdruck
0	Entlüftungsventil geöffnet ? Nicht Entlüftungsventil geöffnet ?	GOS 1 02
1	Bypassventil geöffnet ? Nicht Bypassventil geöffnet ?	GOZ 1 22
2	Voreingestellte Wassermenge erreicht? Nicht voreingestellte Wassermenge erreicht?	FQIZ 1 03
3	Wasserarmatur geschlossen ? Nicht Wasserarmatur geschlossen ?	GOS 1 03
4	Entlüftungsventil geschlossen ? Nicht Entlüftungsventil geschlossen ?	GOS 1 02
5	O <sub>2</sub> -Konzentration unter Grenzwert ? Nicht O <sub>2</sub> -Konzentration unter Grenzwert ?	QIZA 1 19
6	Inertisierungsdruck erreicht ? Nicht Inertisierungsdruck erreicht ?	PICA 1.05
7	Stickstoffventil geschlossen ? Nicht Stickstoffventil geschlossen ?	GOS 1 06
8	Wartezeit abgelaufen ? Nicht Wartezeit abgelaufen ?	Zeitglied abgelaufen, T 1
9	Druckabfall kleiner als zulässig ? Nicht Druckabfall kleiner als zulässig ?	PIZA 1.19
10	Störung Dichtheit behoben ? Nicht Störung Dichtheit behoben ?	von Störungsbeseitigung Dichtheit
11	Rührerdrehzahl > 40 ? Nicht Rührerdrehzahl > 40 ?	SOSA 1 04
12	Kühlwasserventil geöffnet ? Nicht Kühlwasserventil geöffnet ?	GOS 1 10
13	Kühlwasserdruck groß genug ? Nicht Kühlwasserdruck groß genug ?	PIC 1.17
14	Entlüftungsventil geöffnet ? Nicht Entlüftungsventil geöffnet ?	GOS 1 02
15	Bypassventil geöffnet ? Nicht Bypassventil geöffnet ?	GOZ 1 22
16	Reaktor drucklos ? Nicht Reaktor drucklos ?	PIZA 1.19
17	Störung Druck behoben ? Nicht Störung Druck behoben ?	von Störungsbeseitigung Druckentlastung
18	Reaktion beendet ? Nicht Reaktion beendet ?	von Teilprozeß Reaktion durchführen
19	Bypassventil geschlossen ? Nicht Bypassventil geschlossen ?	GOZ 1 22

**Tabelle 7-4: Reaktor vorbereiten und füllen – Operationsvariablen  
(BAuA-Schrift Rw 27)**

Nr.	Aussage Negative Aussage	Opera- tionen*)	Ausdruck
0	Entlüftungsventil öffnen Nicht Entlüftungsventil öffnen		V 1 02
1	Bypassventil öffnen Nicht Bypassventil öffnen		V 1 22
2	Öffnen Wasserarmatur Nicht Öffnen Wasserarmatur		V 1 03
3	Schließen Wasserarmatur Nicht Schließen Wasserarmatur		V 1 03
4	Schließen Entlüftungsventil Nicht Schließen Entlüftungsventil		V 1.02
5	Schließen Bypassventil Nicht Schließen Bypassventil		V 1.02
6	Öffnen Stickstoffventil Nicht Öffnen Stickstoffventil		V 1 06
7	Schließen Stickstoffventil Nicht Schließen Stickstoffventil		V 1 06
8	30 min warten nicht warten 30 min		Zeitglied erzeugen, T 1, 30 min
9	Störungsanalyse Dichtheit Nicht Störungsanalyse Dichtheit		
10	Rührwerk einschalten Nicht Rührwerk einschalten		HS 1 045
11	Kühlwasserventil öffnen Nicht Kühlwasserventil öffnen		V 1 10
12	Kühlwasserpumpe ein Nicht Kühlwasserpumpe ein		HS 1 11
13	Öffnen Entlüftungsventil Nicht Öffnen Entlüftungsventil		V 1.02
14	Öffnen Bypassventil Nicht Öffnen Bypassventil		V 1.22
15	Störungsanalyse Druck Nicht Störungsanalyse Druck		
16	Reaktion durchführen Nicht Reaktion durchführen		

\*) Die Spalte Operationen ist im Programm für die Weiterverarbeitung in der Steuerungstechnik enthalten. Für die Betrachtung der Bedienhandlung hat sie keine Bedeutung.

**TABELLE 7-5:** Untersuchung der betrieblichen Gefahrenquellen

Anlagentyp Nr. aus PAAG-Liste	Ursache / Gefahrenquelle	Auswirkung	Erkennen / Gegenmaßnahmen
<b>1. Mitteldruck Erdöldestillation</b>			
	Nachfolgende Ausführungen wurden dem PAAG-Verfahren (6. Fehlbedienung) der Sicherheitsanalyse entnommen		
6.1	Anlage beim Anfahren nicht ausreichend inertisiert	Bildung zündfähiger Gemische	nicht erkennbar / geschultes Fachpersonal; Durchführung der Inertisierung nach Betriebsanweisung (O <sub>2</sub> -Gehalt < 3Vol%)
6.2	Fehlschaltungen	Einstellung nicht bestimmungsgemäßer Betriebszustände	gegebenenfalls Alarm in der Meßwarte / Überwachung aller sicherheitstechnisch relevanten Parameter; Bedienung nur durch geschultes Fachpersonal

Anlagentyp Nr. aus PAAG-Liste	Ursache / Gefahrenquelle	Auswirkung	Erkennen / Gegenmaßnahmen
<b>2. Abfallver- brennungsanlage</b>	<p>Auszug aus Punkt 2.5 "Beschreibung der Störfalleintrittsvoraussetzungen" der Sicherheitsanalyse <i>Im Anhang 8 der Sicherheitsanalyse wird für die sicherheitstechnisch bedeutsamen Anlagenteile eine Untersuchung der betrieblichen Gefahrenquellen und ihrer Ursachen durchgeführt. An dieser Stelle erfolgt auch eine Gegenüberstellung der betrieblichen Gefahrenquellen und der Vorfahrten des Anlagenbetreibers, die in Bezug auf die jeweilige Gefahrenquelle störfallbegrenzend bzw. störfallverhindern können.</i></p> <p>In der PAAG wird für sicherheitstechnisch bedeutsame Anlagenteile ein Versagen von Ausrüstungsgegenständen und menschliches Versagen mit seinen Auswirkungen diskutiert. Erkennungsmöglichkeiten und Gegenmaßnahmen sind in einer tabellarischen Gegenüberstellung aufgezeigt.</p> <p>In Ergänzung zu diesen Betrachtungen werden vernünftigerweise nicht auszuschließende Störfälle diskutiert, um z.B. bisher ausgeschlossene Doppelfehler, grob fahrlässiges Verhalten oder Systemverkettungen, die nicht immer sicher erkannt werden, ebenfalls einer Gefahrenbeurteilung unterzuhören zu können.</p>		
<b>BE 1 Zwischenlagerung/ Konditionierung</b>	<p>Verwechseln oder unsachgemäße Bedienung von Handabsperrmaturen allgemein</p> <p>6.1</p>	<p>veränderte Betriebsparameter, ggf. Entleerung von Behältern</p> <p>6.2</p>	<p>über direkte oder indirekte Auswirkungen durch Fehlbedienende selbst (z.B. Produktfreisetzungen), ggf. durch in der Meßwarte eingehende Daten / Handeln nach Betriebsvorschrift; Anwesenheit und Kontrolle bei vor-Ort-Steuerung von Ausrüstungen / Armaturen (z.B. Entleerungen); Beobachtung der Meßeinrichtungen vor Ort und Ziehen richtiger Schlüssefolgerungen für die Handlungsabläufe (geschultes Personal); ausreichende Beleuchtung;</p> <p>- / automatische Noteingriffe; in Meßwarte eingehende Alarne müssen vom Anlagenfahrer quittiert werden; Alarne werden optisch und akustisch angezeigt; Ziehen richtiger Schlüssefolgerungen (geschultes Personal); bau- und sicherheitstechnische Maßnahmen</p>

Anlagentyp Nr. aus PAAG-Liste	Ursache / Gefahrenquelle	Auswirkung	Erkennen / Gegenmaßnahmen
6.3	Falsches Stellen von Wegen zu den Eingangsbehältern		siehe Punkt 6.1 - Produktverwechslung
BE 2 Thermische Behandlung	Verwechseln oder unsachgemäße Bedienung	ggf. Austritt brennbarer Stoffe, ggf. ungewolltes Abfahren der Anlage	über direkte oder indirekte Auswirkungen durch Fehlbedienenden selbst, ggf. durch in der Meßwarte eingehende Daten Handeln nach Betriebsvorschrift; Anwesenheit und Kontrolle bei Zündvorgang der Brenner; Beobachtung der Meßeinrichtungen vor Ort und Ziehen richtiger Schlußfolgerungen für die Handlungsabläufe (geschultes Personal); ausreichende Beleuchtung
6.1	Nichterkennen von Notsituationen	ggf. großer Sach- und Personenschaden	- automatische Noteingriffe; in Meßwarte eingehende Alarne müssen vom Anlagenfahrer quittiert werden; Alarne werden optisch und akustisch angezeigt; Ziehen richtiger Schlußfolgerungen (geschultes Personal); bau- und sicherheitstechnische Maßnahmen
BE 4 Rauchgasreinigung	6.1 6.2	Verwechseln oder unsachgemäße Bedienung von Handabsperrmaturen allgemein Nichterkennen von Notsituationen	ggf. Produktaustritt mit Grundwassergefährdung ggf. großer Sach- und Personenschaden über direkte oder indirekte Auswirkungen durch Fehlbedienenden selbst, ggf. durch in der Meßwarte eingehende Daten / Handeln nach Betriebsvorschrift; geschultes Personal optische und akustische Alarneingriffe; in Meßwarte eingehende Alarne sind zu quittieren; geschultes Personal

Anlagentyp Nr. aus PAAG-Liste	Ursache / Gefahrenquelle	Auswirkung	Erkennen / Gegenmaßnahmen
3. Catalytic Cracking	<p>Auszug aus Punkt 2.4 "Beschreibung der Gefahrenquellen" 2.4.1.6. "Fehlbedienungen" der Sicherheitsanalyse</p> <p>Die Anlagen sind sicherheitstechnisch so ausgelegt, daß im normalen Betriebszustand eine Fehlbedienung nicht zu einer Gefahr für die Anlage oder für Personen führen kann.</p> <p>Das Prozeßleitsystem zeigt die Auswirkungen einer Fehlbedienung in der Meßwarte an, da fehlerhafte Aktionen des Anlagenpersonals Alarne auslösen, bevor sicherheitstechnisch gefährliche Situationen eintreten. Entstehende Gefahren werden rechtzeitig erkannt, und es können entsprechende Gegenmaßnahmen eingeleitet werden. <b>/Anmerkung der Autoren: Das setzt unrealistisch voraus, dass die grenzenlose Vierfalt menschlicher Fehlermöglichkeit im Voraus vollständig durchdacht wurde./</b></p> <p>Bei den Anlagen handelt es sich um geschlossene Anlagen. Produktflüchtende Apparate und Leitungen besitzen keine permanenten Öffnungen zur Atmosphäre. Alle zur Atmosphäre führenden Produktleitungen sind mit Blindflanschen gesichert. Nur im Ausnahmefall werden die Leitungen zum Entwässern und Entlüften geöffnet, wobei diese Arbeiten im einzelnen geplant werden und ihre Durchführung überwacht wird. Eine Freisetzung von Kohlenwasserstoffen, H<sub>2</sub>S-haltigen Gasen usw. setzt ein völlig unkoordiniertes und grob fehlerhaftes Arbeiten des Betriebspersonals voraus, was in Anbetracht des Einsatzes von besonders ausgebildetem und regelmäßig in den besonderen Gefahren der Anlage geschultem Personal nicht zu erwarten ist.</p>		
BE 1 Einsatzprodukt- Vorwärmung 6.1	<p>An der Reservepumpe ist der Druckschieber geschlossen</p> <p><b>/Anmerkung der Autoren: Was ist hierbei die Bedienhandlung?/</b></p>	<p>Bei Ausfall der Betriebspumpe läuft die Reservepumpe über das Auto-Start-System an. Es wird jedoch kein Produkt in die Anlage gefördert.</p>	<p>Sicherheitstechnisch relevante Parameter werden über Trippschaltungen überwacht. So wird insbesondere bei Ausfall der Einsatzproduktversorgung der Vorheizer über die Verriegelung automatisch außer Betrieb genommen.</p>
BE 2 Vorheizer 6.1	Offene Umfahrung der Schnellschlußventile in der Heizgas- bzw. Pilotgashauptleitung	Im Störungsfall kann ungehindert Heizgas zu den Brennern strömen, was zu Überhitzungen führen kann.	Beide Umfahrungsarmaturen werden im geschlossenen Zustand gesichert. (LC-Armaturen, d.h. im geschlossenen Zustand verriegelt)

Anlagentyp Nr. aus PAAG-Liste	Ursache / Gefahrenquelle	Auswirkung	Erkennen / Gegenmaßnahmen
<b>BE 3</b> Reaktor/Regenerator 6.1	Verstellen der hydraulischen Handeinstellung am Slide-Valve für verbrauchten Katalysator	Störung der Verbrennungsreaktionen im Regenerator und Änderung des Temperaturprofils. Gefahr der Überschreitung der Auslegungstemperatur	Kontinuierliche Überwachung des Sauerstoffgehaltes im Regeneratorabgas und des Temperaturprofils über den Regenerator. Rauchgaskühlung mit Dampf am Kopf des Regenerators.
<b>BE 4</b> Luftverdichter A /Offen 6.1	Schließen der Hochdruckdampfzufuhr zur Turbine	Ausfall des Luftverdichters  Druckanstieg im Hochdruckdampfnetz	Bei Unterschreitung einer festgelegten Luftmenge schließt die Spezialrückslagklappe des Luftverdichters. Beim Auftreten kritischer Betriebszustände wird die Anlage automatisch in einen sicheren Zustand gebracht.
<b>BE 6</b> Luftverdichter B 6.1	Fehlschaltungen vor Ort und in der Meßwarte	Es können gefährliche Betriebszustände entstehen.	Bei Ausfall der Dampfabnahme über die Turbine wird ein Signal zum Regelventil gegeben, wodurch ein Druckanstieg vermieden wird. Die Dampfmenge, die über die Turbine abgenommen wurde, wird über sofort in das Mitteleindruck-Dampfsystem entspannt.
<b>BE 7</b> Nicht belegt			Sicherheitstechnisch relevante Parameter werden über Tripschaltungen überwacht. Beim Auftreten kritischer Betriebszustände wird die Anlage automatisch in einen sicheren Zustand gebracht.

Anlagentyp Nr. aus PAAG-Liste	Ursache / Gefahrenquelle	Auswirkung	Erkennen / Gegenmaßnahmen
<b>BE 8</b> <b>Hauptkolonne</b> 6.1	Schließen der LCO-Zuführung zum Abdichtsystem der	Die Stopfbuchsenpackung wird undicht und es besteht die Gefahr des Durchschlagens von Slurry (Produktaustritt).	Die Zuführungen der Kühl- und Spülmedien LCO und HCO zur Pumpe werden während der Anlagenrundgänge durch das Anlagenpersonal kontrolliert und wenn erforderlich nachgestellt.
<b>BE 13</b> <b>Naßgasverdichter</b>		sicherheitstechnisch relevante Bedienungsfehler sind nicht möglich	
<b>BE 14</b> <b>Hochdruck-Abscheider</b> 6.1	Fehlerhafte Einstellung der Produktzuführungen zu den Hochdruck-Trimkondensatoren	Beinflussung der Kondensationsleistung und damit der Produktzusammensetzung im Behälter. Es entstehen keine Gefährdungen für die Anlage. Sicherheitstechnisch nicht relevant.	- / -
<b>BE 15</b> <b>Absorber</b> 6.1	Geöffnete Entleerung beim Anfahren der Pumpe	Austritt von Kopfbenzin mit einer Temperatur von ca. 45°C. Brandgefahr.	Vor der Inbetriebnahme von Ausrüstungen ist zu kontrollieren, daß alle Entleerungen und Entlüftungen geschlossen sind.
<b>BE 16</b> <b>Wasch-Kolonne</b>		Sicherheitstechnisch relevante Bedienungsfehler sind unwahrscheinlich.	
<b>BE 17</b> <b>Stripper</b> 6.1	Nicht vollständig geschlossene Abstreifarmatur am Behälter	Übertritt von Flüssiggasdämpfen in das Sauerwassersystem.	- Zonenfestlegung im Sauerwassersystem - Einhaltung der Ex-Schutz- Maßnahmen - Ausführung des Abstreifens mit Dopperarmatur

Anlagentyp Nr. aus PAAG-Liste	Ursache / Gefahrenquelle	Auswirkung	Erkennen / Gegenmaßnahmen
BE 18 Butan-Kolonne 6.1	Geöffnete Entlüftungsleitung der Pumpe zur Fackel	Verringerte Flüssiggasausbeute und erhöhte Fackelbelastung.	Kontrolle der Ausrüstungen bei verminderter Flüssiggasab- gabe. Die Ursache für die verminderde Flüssiggasausbeute und erhöhte Fackelbelastung wird ermittelt und beseitigt. Schließen der Armatur in der Entlüftungsleitung
BE 19 Luftverdichter/ Benzin- Merox-Reaktoren 6.1			Standüberwachung mit Hochalarm zur Messwarte
BE 20 Flüssiggas-Merox 6.1	Mangelnde Sorgfalt bei NaOH- Übernahme zum Behälter	Überlaufen von 18-%iger NaOH ins Freie.	- Drucküberwachung des Behälters - Ausreichende Dimensionierung der Sicherheitsventile
BE 21 Propankolonne 6.1	Nicht vollständig geschlossene Abstreicharmatur am Behälter	Mißstand von Flüssiggas in den NaOH-Kreislauf und Druckanstieg im Behälter.	Einbindung der Entleerungen in das Fackelsystem. Vorbereitung von Reparaturen und Wiederimbetriebnahme von Pumpen nach Betriebsvorschrift.

Anlagentyp Nr. aus PAAG-Liste	Ursache / Gefahrenquelle	Auswirkung	Erkennen / Gegenmaßnahmen
<b>4. Polyether- Herstellung</b>	Ausführungen zur Fehlbedienung im Text-Teil (PAAG nicht angewendet)	<p>Bedienfehler infolge menschlichen Versagens sind als betriebliche Gefahrenquelle grundsätzlich nicht gänzlich auszuschließen. Durch umfangreiche Voreilehrungen wurde jedoch weitgehend möglichen Bedienfehlern entgegengewirkt. So ist es z.B. nicht mehr möglich, durch Öffnen von Handarmaturen ... Produkt frei zu entnehmen, Leitungen zu entspannen oder in anderer Weise einen Produktaustritt zu veranlassen. Dazu wurde die EMR seitige Ausstattung der Ausrüstungen und Anlagenteile auf einen neuen hohen Stand gebracht. Umfangreiche Verriegelungen der Armaturen, vor allem im sicherheitsrelevanten Bereich, und komplexe Steuerung der Vorgänge über das Prozeßleitsystem sorgen dafür, daß fehlerhafte menschliche Eingriffe, die zu Produktaustritten mit unmittelbarer Gefährdung führen können, praktisch kaum noch auftreten. Weiterhin sorgen die getroffenen organisatorischen Vorsorgemaßnahmen wie regelmäßige Sicherheitsunterweisungen, Sicherheitsbegehung, detaillierte Betriebsanweisungen, schriftliche Anweisungen, Arbeitsabsprachen, "Patenschaften" für Neulinge, Fortbildung u. ä. für eine deutlich höhere Bedien Sicherheit.</p> <p>Eingesetzt werden für die Arbeiten nur ausgebildete Mitarbeiter. Unbefugten ist der Aufenthalt im Anlagenbereich untersagt, gleichemmaßen ein Eingreifen in das Anlagengeschehen.</p>	
<b>5. TDI-Anlage</b>	Ausführungen zu menschlichem Fehlverhalten im Text-Teil (PAAG nicht angewendet)	<p>Bedienfehler infolge menschlichen Versagens sind als betriebliche Gefahrenquelle grundsätzlich nicht gänzlich auszuschließen. Es werden jedoch durch die getroffenen organisatorischen Vorsorgemaßnahmen, wie regelmäßige Belehrungen, Arbeitsabsprachen, Beaufsichtigung, schriftliche Anweisungen, "Patenschaften" für Neulinge usw. die Möglichkeiten, Fehler zu begehen, die die Sicherheit in Frage stellen, auf ein Minimum reduziert.</p>	

**Tabelle 7-6:** Isomerisierungsanlage - Auszug aus der PAAG Liste

Störung	Ursache	Erkennen	Auswirkung	Gegenmaßnahmen
<b>1. Produktver- wechslung</b>	ist ausgeschlossen			
<b>2. Mechanisches Versagen</b>				
2.1	Versagen des Stabilizers durch Überdruck	Anlagenpersonal	Produktfreisetzung, Bildung - zündfähige Atmosphäre - Grundwassergefährdung	ausreichende Auslegung und Dimensionierung für max. zulässigen Betriebsdruck; ausreichend dimensioniertes Sicherheitsventil; Prüfung nach DruckbehV; Wartung; Regelmäßige Kontrolle durch Anlagenpersonal; Ausreichend dimensionierter und dichter Auffangraum
<b>3. Versagen von Maschinen</b>				
3.1	Ausfall der laufenden Stabilizer- Rückflußpumpe	Laufüberwachung; Füllstandhochalarm in der Kopfvorlage	Ausfall des Rückflusses zum Stabilizer; Temperatur- und Druckanstieg im Stabilizer-Kopf; Füllstandanstieg in Stabilizer-Kopfvorlage	druckseitige Rückschlagklappe der ausgefallenen Pumpe schließt; Reservepumpe in Betrieb nehmen
3.4	Ausfall der laufenden Frischluagepumpe	Laufüberwachung; Mengentiefalarm	Ausfall des Laugekreislaufes; Sicherheitstechnisch nicht relevant	Druckseitige Rückschlagklappe der ausgefallenen Pumpe schließt; Reservepumpe in Betrieb nehmen
3.6	Ausfall eines Lüfters am Stabilizer-Kondensat	Laufüberwachung; Druckhochalarm in der Stabilizer-Kopfvorlage	Temperatur- und Druckanstieg in der Stabilizer-Kopfvorlage	automatisches Abregeln des Druckes über Regelventil zum Heizgas; ggf. Reduzierung der Einsatzmenge

## 8. Möglichkeiten zur Integration der Ergebnisse in betriebliche Managementsysteme

### 8.1 Schnittstelle Mensch-Organisation

Die Vermeidung von Fehlbedienung in verfahrenstechnischen Anlagen ist nur erreichbar über eine Verbesserung der Schnittstellen zwischen den drei Basiselementen

Technik – Organisation – Person.

Der im Rahmen dieses Projekts erarbeitete "Leitfaden zur Bediensicherheit" (Materialband zu diesem Endbericht) behandelt die Schnittstelle Mensch - Technik. In diesem Kapitel wird die Schnittstelle Mensch - Organisation genauer betrachtet und nach Verbesserungspotentialen hinsichtlich Berücksichtigung des Faktor Mensch überprüft werden. Die in der Wirtschaft sich seit vielen Jahren entwickelnden Managementsysteme bieten hierzu den Ansatzpunkt.

#### Definition „Management“

Management ist die sachorientierte Leitung von Betrieben und die mitarbeiterorientierte Führung zur Verwirklichung geplanter Maßnahmen und Ziele.

#### Definition „Managementsystem“

Ein Managementsystem ist ein formal verankertes Regelwerk zur Gestaltung, Lenkung und Entwicklung komplexer Organisationen. Es regelt Planung, Umsetzung und Kontrolle von Prozessen.

Zu den mittlerweile in der produzierenden Wirtschaft durchgängig etablierten Qualitätsmanagementsystemen sind zwischenzeitlich Umweltmanagementsysteme, Arbeitsschutzmanagementsysteme und - als Folge der europäischen Seveso II-Richtlinie - Sicherheitsmanagementsysteme hinzugekommen. Haben sich diese zunächst nebeneinander entwickelt, so tendieren die Betriebe zwischenzeitlich dazu, sie zu integrieren und als

- Total quality management (TQM)
- bzw. total environmental management (TEM)
- bzw. integriertes Managementsystem (IMS)

zu gestalten.

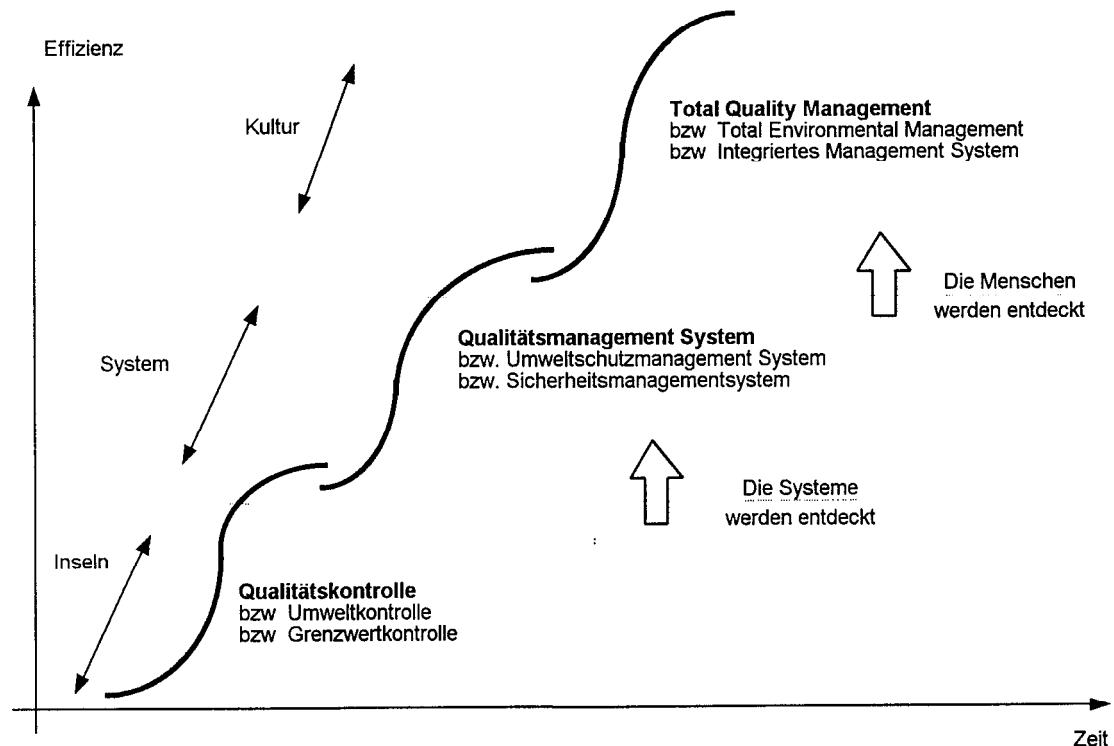


Abbildung 8-1: Technologie-Entwicklung Effizienzsteigerung (aus: Adams, 1995)

## 8.2 Integrierte Managementsysteme (IMS)

Die Entwicklung hin zu integrierten Managementsystemen ist nicht mehr aufzuhalten, da sie klare Vorteile bieten:

- IMS/TQM verbessert die Effizienz (→ geringere Anzahl an Regelungen, geringerer Aufwand für Audits)
- IMS/TQM verringert die Gefahr von Widersprüchen
- IMS/TQM erhöht für die Mitarbeiter die Transparenz und damit die Akzeptanz
- IMS/TQM erleichtert die Aufweitung des Systems um neue Anforderungen.

Alle Managementsysteme beinhalten gleiche Aufbauelemente, die Ausgangspunkt für die verschiedenen Themenstellungen bieten (vgl. Abbildung 8-3).

Allen gemeinsam ist auch die Bedeutung der Dokumentation einschließlich der schriftlich festzulegenden Regeln und Verfahrensweisen in einem Managementhandbuch.

Die Dokumentation des Integrierten Managementsystems zu Sicherheit und Umweltschutz beinhaltet alle Einzeldokumentationen, wie Qualitätsmanagementsystem (QMS), Arbeitsschutz-

managementsystem (AMS), Umweltmanagementsystem (UMS), Sicherheitsmanagementsystem (SMS), die jedoch nicht ein Nebeneinander von Insellösungen darstellen sollen, sondern sich zu einem Gesamtsystem ergänzen sollen.

Vor diesem Hintergrund wird allgemein ein einheitlicher Aufbau empfohlen (vgl. Abbildung 8-2).

1. Zweck
2. Geltungsbereich
  - räumlich
  - zeitlich
  - personell
3. Erläuterungen, Begriffe, Abkürzungen
4. Zuständigkeiten (Aufbauorganisation)
5. Vorgehensweise (Ablauforganisation)
6. Dokumentation (Formulare)
7. Mitgeltende Regelungen
8. Anlagen

Abbildung 8-2: Standardgliederung der Einzel-Regelungen (aus: Adams, 1995)

ELEMENTE	THEMENSTELLUNGEN
<b>Politik, Leitlinien</b>	<ul style="list-style-type: none"> <li>— zur Sicherung der Produktqualität (QMS) → DIN 9001</li> <li>— zum Schutz der Umwelt → DIN ISO 14001/EMAS (UMS)</li> <li>— zum Schutz der Arbeitnehmer (AMS) → OHRIS, ASCA</li> <li>— zum Schutz gegen Störfälle (SMS) → Seveso II-RL</li> </ul>
<b>Aufbauorganisation</b>	<ul style="list-style-type: none"> <li>— Verantwortlichkeits-/ Zuständigkeitsregelung für die Produktqualität</li> <li>— Verantwortlichkeits-/ Zuständigkeitsregelung für den Umweltschutz</li> <li>— Verantwortlichkeits-/ Zuständigkeitsregelung für den Arbeitsschutz</li> <li>— Verantwortlichkeits-/ Zuständigkeitsregelung für die Anlagensicherheit</li> </ul>
<b>Lenkung der Dokumente</b>	<ul style="list-style-type: none"> <li>— Checklisten, Prüfnachweise, Protokolle usw. zur Qualitäts sicherung</li> <li>— Checklisten, Prüfnachweise, Protokolle, Verbrauchszahlen usw. zum Umweltschutz</li> <li>— Checklisten, Prüfnachweise, Protokolle, Berichte zum Arbeitsschutz</li> <li>— Checklisten, Prüfnachweise, Protokolle, Auditberichte, Kontrollberichte zur Anlagensicherheit</li> </ul>
<b>Ablauforganisation</b>	<ul style="list-style-type: none"> <li>— Regelung der Verfahrensweisen zur Qualitätssicherung</li> <li>— Regelung der Verfahrensweisen zum Umweltschutz</li> <li>— Regelung der Verfahrensweisen zum Arbeitsschutz</li> <li>— Regelung der Verfahrensweisen zur Sicherung der Anlage gegen Störfälle</li> </ul>
<b>Kontrolle und Korrektur</b>	<ul style="list-style-type: none"> <li>— werden die Verfahrensweisen zur Qualitätssicherung eingehalten (→ Statistik, Prüfungen)?</li> <li>— werden die Verfahrensweisen zum Umweltschutz eingehalten (→ Berichte, Prüfprotokolle)?</li> <li>— werden die Verfahrensweisen zum Arbeitsschutz eingehalten (Überwachung, Messung)?</li> <li>— werden die Verfahrensweisen zur Sicherung der Anlage gegen Störfälle eingehalten?</li> </ul>
<b>Leistungsbeurteilung und Review</b>	<ul style="list-style-type: none"> <li>— wird mit den Verfahrensweisen und Zuständigkeits regelungen das definierte Qualitätsziel erreicht?</li> <li>— werden mit den Verfahrensweisen die definierten Umwelt schutzziele erreicht?</li> <li>— werden mit den Verfahrensweisen die definierten Arbeits schutzziele (z.B. Anzahl an Unfallfehltagen) erreicht?</li> <li>— werden mit den Verfahrensweisen die definierten Sicher heitsziele erreicht?</li> </ul>

**Abbildung 8-3:** Managementsysteme – gleiche Elemente für unterschiedliche Themenstellungen

Die zu behandelnden Regelungsbereiche orientieren sich dann am Zielthema:

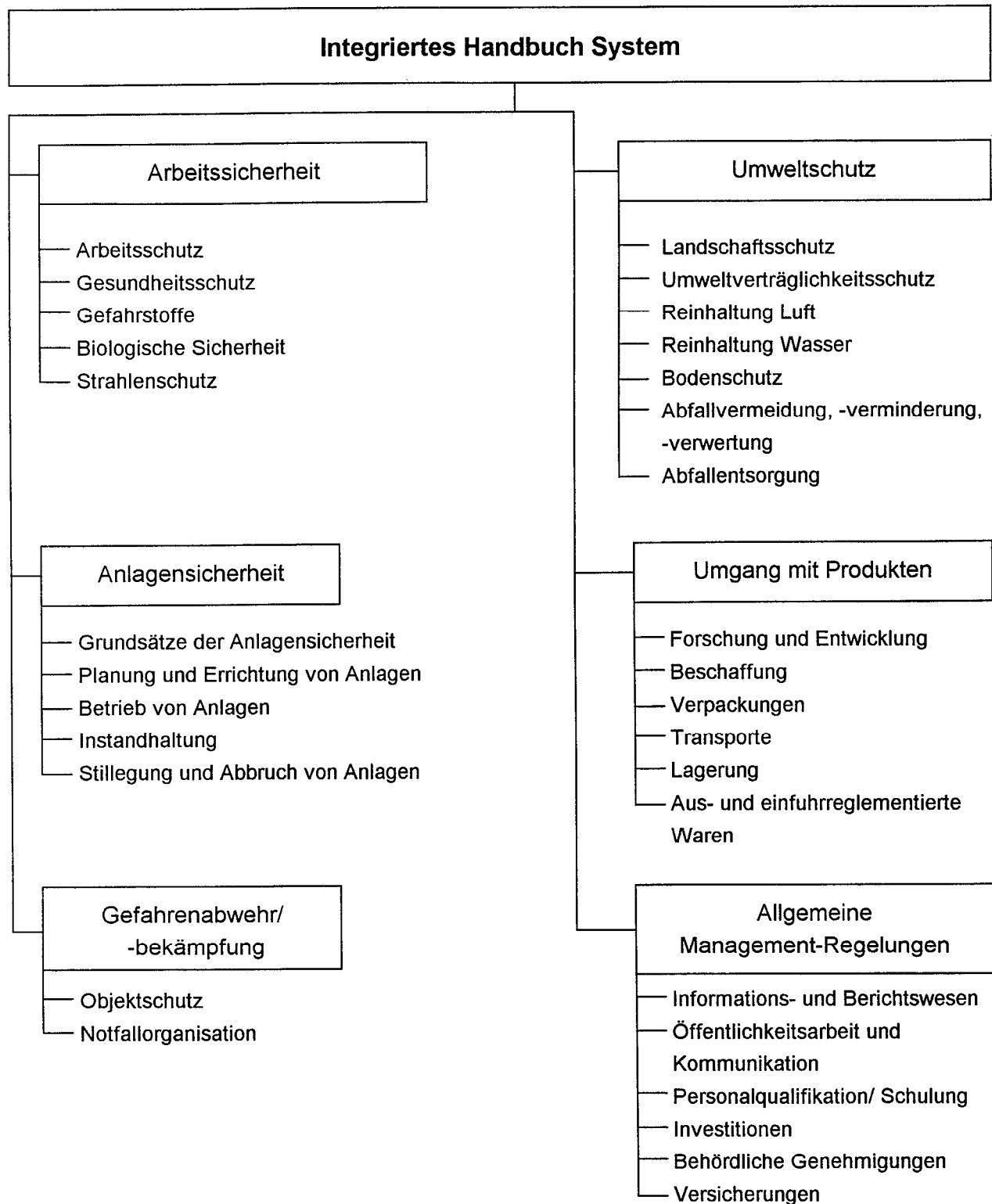


Abbildung 8-4: Integriertes Managementsystem (aus: Adams, 1995)

### 8.3 Managementhandbücher – Tote Papieransammlung oder aktives Steuerungsinstrument?

Managementhandbücher sind die Dokumentation der Organisation. Die Organisation soll systematisch sein, d.h. vollständig (= alle notwendigen Bereiche abdecken), logisch aufgebaut (= das, was man sucht, kann schnell gefunden werden) und entsprechend der Erkenntnisse moderner Unternehmensführung (= mitarbeiterorientiert). Das Managementhandbuch beinhaltet nicht nur die unternehmerischen Vorgaben, sondern dient sodann der Validierung der gewählten Organisation und ihrer Optimierung.

Vor Einführung eines Managementsystems existieren in den Unternehmen häufig lediglich historisch gewachsene Anweisungssysteme, die einzelfallbezogen nach Bedarf geändert oder ergänzt werden. Sie werden nach und nach unüberschaubar, entstehen isoliert und können sich damit auch widersprechen. Bei neuen Mitarbeitern kann damit schon allein die Unkenntnis oder die Unüberschaubarkeit zur Nichtbeachtung von Vorgaben führen. Oft weiß niemand mehr im Betrieb, welche Anweisungen noch gültig sind und welche nicht mehr. Nach und nach entwickelt sich so eine ineffiziente Organisation, mit der die Mitarbeiter irgendwie leben, ohne klare Vorgaben zu haben.

Die Ankündigung der Einführung eines Managementsystems und der Erstellung eines Managementhandbuchs ruft bei Führungspersonal und Mitarbeitern statt Erleichterung oft eher Abwehr hervor:

- "Wir wollen Produkte produzieren, kein Papier"
- "Das ist bei uns alles ganz anders"
- "Das haben wir schon immer so gemacht und es hat doch funktioniert"

Schon die erste genauere Analyse der bestehenden Anweisungen zeigt dann aber, daß diese

- nicht transparent
- sich überschneidend
- unvollständig
- lückenhaft
- widersprüchlich
- nicht mehr aktuell

sind.

Solche Organisationsmängel stellen ein Risiko für die Sicherheit des Betriebes dar. Viele Betreiber berichten im Nachhinein, daß die Erstellung des Handbuchs und der Dokumente dazu geführt hat, daß man jede Regelung auf Sinnhaftigkeit geprüft hat, die Regelungslücken festgestellt hat und damit Ineffizienz vielfach erst sichtbar wurde.

Nun ist das Aufstellen der Regeln nur der erste Schritt zu einem Managementsystem. Das Managementsystem beinhaltet auch die festgelegten Verfahrensweisen zur Umsetzung der Regeln, die Überprüfung der Einhaltung der Regeln und die regelmäßige Revision der Regeln.

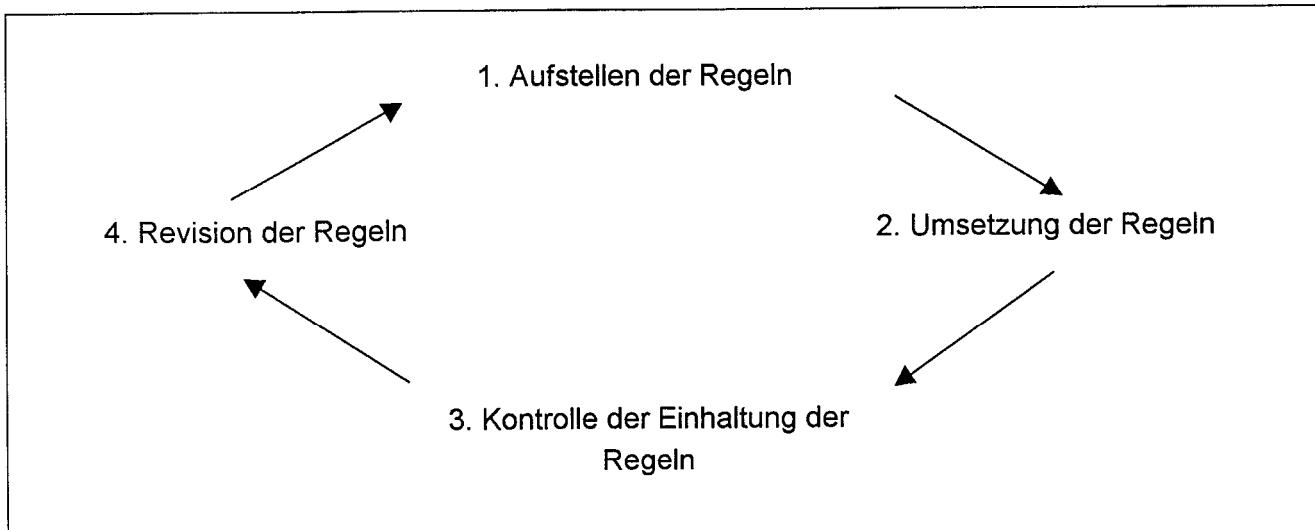


Abbildung 8-5: Stufen im Managementsystem

Wenn ein Managementsystem das Zusammenwirken komplexer Organisationen regeln soll, dann heißt dies grundsätzlich „Regelung des Zusammenwirkens einer größeren Anzahl von Menschen, mit verschiedenen Aufgaben, verschiedenen Funktionen, auf verschiedenen Hierarchieebenen, mit verschiedenen Ausbildungen.“ Dies wird schon dadurch erkennbar, daß die in Abbildung 8-5 dargestellten Stufen des Managementsystems direkt die Lernwege des Menschen widerspiegeln:

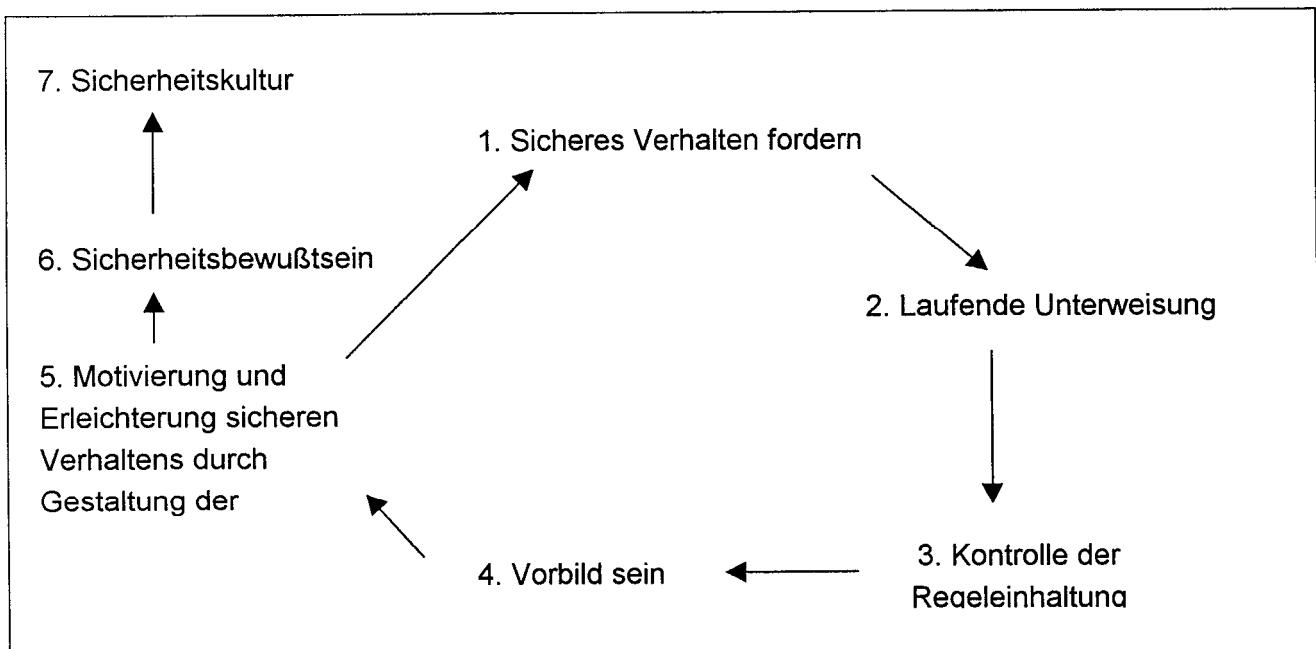


Abbildung 8-6: Sicherheitslernen

**Merksatz**

Je niedriger die Hierarchiestufe des Aufgabenträgers und je gefährdungsrelevanter die übertragenen Pflichten, desto eingehender muß die Belehrung erfolgen und desto ernster muß die Kontrollpflicht genommen werden.

Dieser Merksatz muß – so richtig er ist – ergänzt werden durch den Hinweis, daß daraus nicht der Umkehrschluß zu ziehen ist, höhere Hierarchiestufen brauchten gar nicht kontrolliert zu werden. Adams stellte schon 1995 in seiner Organisationsstudie zum Hoechst Störfall (vom Februar 1993) fest, daß gerade die dem Betriebsleiter übergeordnete Hierarchiestufe, die die erforderlichen Ressourcen zur Verfügung stellen und entsprechende Kontrollen wahrnehmen soll, ihren Aufgaben nicht detailliert genug nachkommt (teilweise liegt dies wohl auch daran, daß ihre Aufgaben nicht genügend detailliert beschrieben sind).

Ein Managementhandbuch wird nach den Abbildungen 8-5 und 8-6 dann keine „tote Papieransammlung“ sein, wenn die Regelung der Organisation mit dem Menschen, der sie ausfüllen soll, eng verknüpft ist.

Was soll das heißen? Es soll heißen, daß eine stetige Verbesserung des (Sicherheits-)Managements/der Organisation nur dann erreicht wird, wenn die psychologischen Erkenntnisse über menschliches Lernen und Handeln konsequent berücksichtigt werden.

Allein das Aufstellen von Regeln wird deshalb keineswegs zum Ziel führen, denn:

**Merksatz**

- gesagt ist noch nicht gehört
- gehört ist noch nicht verstanden
- verstanden ist noch nicht einverstanden
- einverstanden ist noch nicht ausgeführt
- ausgeführt ist noch nicht beibehalten.

Dieser Merksatz ist grundlegend für die Personalführung und damit auch für die Grundlinie eines Managementsystems.

### **Regeln – das Herz des Managementsystems**

Der Titel dieses Abschnittes scheint ein Widerspruch zu sein: Das Herz ist Sinnbild für etwas Lebendiges; Regeln sind eher ein Sinnbild für etwas Formales, Trockenes, vom Leben Abgehobenes.

Die Integration des Human Factor in Managementsysteme bedeutet jedoch gerade die Auflösung dieses Widerspruches, nämlich formale Regeln zu dem lebendigen Handeln der betroffenen Mitarbeiter zu transferieren. „Beim Aufbau eines Managementsystems sind Mitarbeiter zu Beteiligten zu machen“, so steht es in allen Merkblättern, Handlungshilfen und Handbüchern zum Aufbau von Managementsystemen.

Doch was heißt das?

Als Grundsätze sind zu beachten:

- Es sind alle Mitarbeiter einzubinden. Betroffene sind zu Beteiligten zu machen. Eine Regel, an deren Formulierung man selbst beteiligt war, wird sehr viel eher eingehalten als eine, die „von oben“, womöglich sogar „anonym“ vorgegeben wird.
- Hochmotivierte Mitarbeiter sollten nicht blockiert werden. Auch wenn Hochmotivierte gelegentlich über das Ziel hinausschießen, so sollten sie nicht blockiert, sondern ihr Engagement (sanft) in die gewünschten Bahnen umgelenkt werden, denn gerade aus den Hochmotivierten können die Multiplikatoren für das gewünschte Verhalten gemacht werden.
- Gewünschtes Verhalten muß vorgelebt werden.
- Eine offene Informationspolitik erhöht die Akzeptanz (warum wurde die Regel aufgestellt, wer hat sie aufgestellt, wozu dient sie, welche Folgen hat eine Nichteinhaltung).
- Alle Vorschläge sind ernst zu nehmen, d.h. nicht zwangsläufig, daß jeder Vorschlag zu übernehmen ist, es heißt aber, daß niemand bloßgestellt oder ohne weiteren Kommentar übergangen wird, wenn er einmal einen – auf den ersten Blick – nicht sinnvollen Vorschlag gemacht hat.
- Die direkt Betroffenen sind frühzeitig einzubinden.
- Es ist das Prozeßverständnis zu fördern, d.h. manche Regeln müssen erst einmal testweise eingeführt werden, um zu sehen, ob sie einhaltbar sind bzw. zum Ziel beitragen. Stellt sich heraus, daß sie nicht geeignet sind, so sind sie umgehend zu revidieren. Ein solches Vorgehen kann fälschlicherweise als mangelnde Planung ausgelegt werden. Es muß deshalb regelrecht dafür geworben werden, daß das Regelwerk eines Managementsystems nichts Statisches ist, sondern eine ständige Anstrengung zu stetiger Verbesserung.
- Es ist ein Bewußtsein für Verantwortung zu schaffen.
- Die Einhaltung der Regeln ist zu kontrollieren.
- Nicht einhaltbare Regeln sind zu eliminieren.

Die Abbildung 8-7 zeigt noch einmal auf, daß der Umgang mit Regeln im Managementsystem sehr viel komplexer ist als vielfach angenommen. Das Aufstellen der Regeln ist nur einer von vielen notwendigen Schritten.

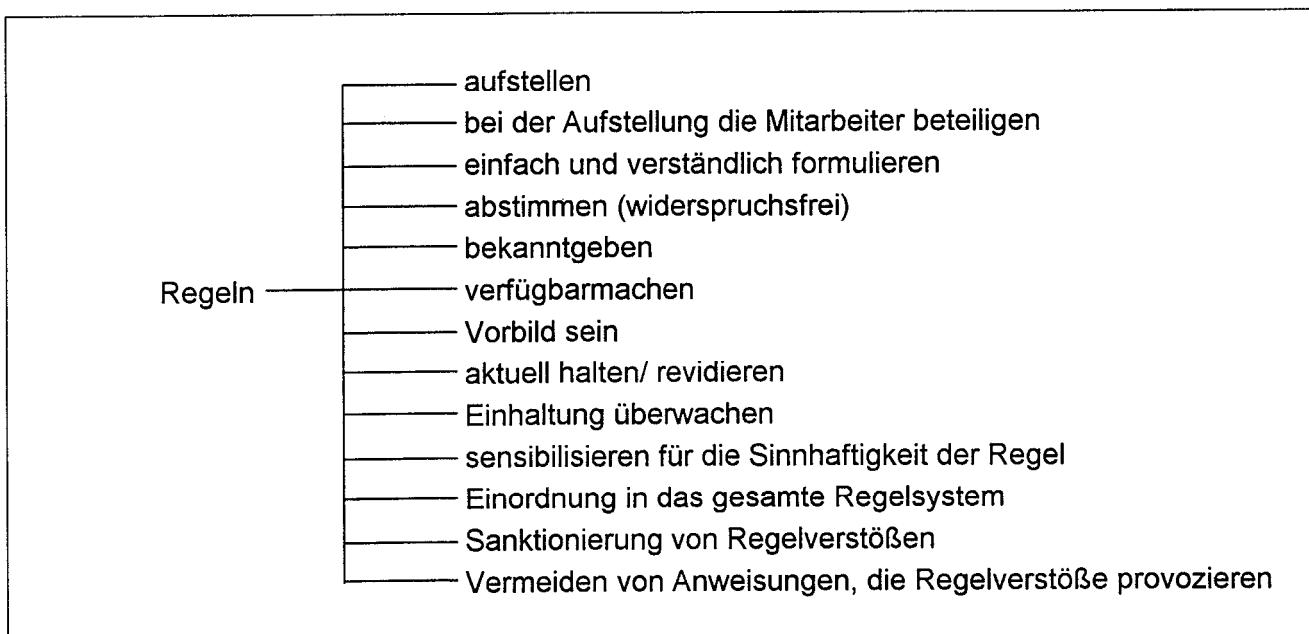


Abbildung 8-7: Umgang mit Regeln

In einem gelebten Managementsystem werden Regeln als etwas Positives vermittelt, da sie den Mitarbeitern Verhaltenssicherheit geben und von ständigem Entscheidungswang entlasten.

### Wie können Managementsysteme zur Vermeidung von Fehlbedienung beitragen?

Ein Managementsystem beschreibt die Regeln, wie mit der Schnittstelle Mensch-Organisation und der Schnittstelle Mensch-Technik umzugehen ist, damit das Ganze möglichst reibungslos funktioniert. Die Dokumentation der Regeln ist Grundvoraussetzung einer einheitlichen Vorgehensweise und einem einheitlichen Verständnis für das von allen geforderte betriebliche Vorgehen. Geregelte, allgemeingültige Vorgehensweisen sind ebenso Grundbedingung für sicheres Verhalten im Betrieb und dienen damit direkt der Vermeidung von Fehlverhalten. So war es nur folgerichtig, daß die EU durch die Seveso II-Richtlinie – und in der Folge die deutsche Umsetzung in die neue Störfall-Verordnung - zur Verbesserung/Gewährleistung der Anlagensicherheit zukünftig auch ein Sicherheitsmanagement fordert.

Ein integriertes Managementsystem (IMS)/ein ganzheitliches Qualitätssicherungssystem (TQM) sichert übergreifend:

- Einen einheitlichen und damit für das Personal durchschaubaren Aufbau.
- Widerspruchsfreiheit und damit Anwendbarkeit der Regeln.
- Vollständigkeit und damit eine verlässliche Arbeitsgrundlage für das Personal.
- Verantwortlichkeit, weil die Zuordnung von Verantwortung abdeckend und klar geregelt ist.

Wenn die Regeln bekannt sind, sind dem Personal damit auch im Bedarfsfall die erwarteten Reaktionen bekannt; es muß nicht lange nachdenken und kommt nicht in Versuchung, eine falsche Reaktion zu zeigen.

## 8.4 Berücksichtigung des Human Factor im Sicherheitsmanagementsystem (SMS)

Der menschliche Faktor (Human Factor) bezieht sich in dem hier zu betrachtenden Sinne auf den Bereich der Anlagensicherheit. Es ist deshalb nur folgerichtig, wenn die Human Factor-relevanten Aspekte an das Sicherheitsmanagementsystem (SMS), wie es nach neuer Störfall-Verordnung (vom 26. April 2000) für Störfallbetriebsbereiche/-anlagen gefordert wird, angeknüpft werden.

Das Sicherheitsmanagementsystem bezieht sich nach Anhang III der neuen StörfallV auf die sieben Prüfgebiete:

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

In der Tabelle 8-1<sup>1</sup> sind den Prüfgebieten (Spalte 1) Stichworte zugeordnet (Spalte 2), wie sie sich aus dem Leitfaden SFK-GS-24 der Störfallkommission (Stand: 12.10.99) in Verbindung mit den Guidelines zum SMS der TWG 4 der EU-Kommission ergeben. In Spalte 3 sind die zu berücksichtigenden Human Factor-Aspekte stichwortartig genannt. Spalte 4 sind z.T. erläuternde Hinweise zu entnehmen.

<sup>1</sup> Die Tabelle 8-1 wurde im Rahmen dieses Forschungsvorhabens entwickelt und in der Arbeitsgruppe "Aktuelle Themen" des Arbeitskreises "Human Factor" der Störfallkommission ergänzt und abgestimmt.

**Tabelle 8-1: Zu berücksichtigende Human Factor-Aspekte im Sicherheitsmanagementsystem**

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
a) Organisation und Personal	<ul style="list-style-type: none"> <li>• Rollen/Funktionen</li> </ul>	<ul style="list-style-type: none"> <li>- Ausreichende fachliche, menschliche und organisationale Kompetenzen → geeignete Personalauswahl und Personalentwicklung</li> <li>- Qualifikation und Schulung der Vorgesetzten hinsichtlich Menschensführung</li> </ul>	<ul style="list-style-type: none"> <li>- Kennt der Vorgesetzte seine Mitarbeiter wirklich?</li> <li>* Momentane Konstitution der Mitarbeiter</li> <li>* Private Probleme erkennen – darauf reagieren</li> <li>* Gezielter Einsatz der Mitarbeiter entsprechend ihrer individuellen Fähigkeiten und Neigungen</li> </ul>

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
	<ul style="list-style-type: none"> <li>• Erkennen, Durchführen und Kontrollieren von korrigierenden oder optimierenden Tätigkeiten</li> </ul>	<ul style="list-style-type: none"> <li>– Befragungen bei den Bedienern sowohl zum technischen als auch organisatorischen Ablauf durchführen</li> <li>– Betriebsanweisungen regelmäßig auf Aktualität und Verständlichkeit durch die Benutzer sichten; ggf. aktualisieren/ergänzen</li> <li>– Auswertung von Schichtprotokollen; aufgetretene Probleme mit den Bedienern durchsprechen</li> <li>– Verfahrensfestlegung zur Personalauswahl</li> <li>– Schichtzusammensetzung: Gewährleistung einer ausgewogenen Altersstruktur sowie Spezialisierung innerhalb eines Schichtteams, um z.B. Vorhandensein und Weitergabe von „traditionellen“ Erfahrungen (Fertigkeiten) zu gewährleisten</li> <li>– Team-Rotationssystem in Anlagen mit mehreren Warten (führt zu einer Verbesserung der Arbeitsmotivation, der Kompetenzen des Einzelnen, zur Verbesserung der Bedien- sicherheit und zu verbesserten Personaleinsatzmöglichkeiten)</li> <li>– Detaillierte Beschreibung der Verantwortung</li> <li>– Detaillierte Aufgabenbeschreibung</li> <li>– Umgang mit Krankmeldungen (z.B. kurzfristiger qualifizierter Einsatz)</li> <li>• Kontrolle abweichender Situationen einschließlich Notfälle</li> </ul>	<ul style="list-style-type: none"> <li>– Zunehmend wird auch der positive Effekt auf Arbeitsklima und -disziplin durch den Einsatz von Frauen in den Leitwarten diskutiert.</li> <li>– (hierzu scheinen aus der früheren DDR konkrete Untersuchungs-ergebnisse vorzuliegen)</li> <li>– Auswertung von Schichtprotokollen</li> <li>– Regelmäßige Befragung des Betriebsleiters zu Ereignissen und insbesondere zu den Ursachen und Konsequenzen der Ereignisse</li> <li>– Unverzügliche Meldung von Störungen oder erkannten Gefahren im Verantwortungsbereich an den jeweiligen Vorgesetzten bzw. eine andere zuständige Person</li> </ul>

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
	<ul style="list-style-type: none"> <li>• Identifizierung von Schulungsbedarf, Durchführung der Schulung, Auswertung ihrer Wirksamkeit</li> </ul>	<ul style="list-style-type: none"> <li>- Schulung soll sich an den Arbeitsaufgaben der Teilnehmer orientieren</li> <li>- Auch Vorgesetzte müssen sich weiterbilden</li> <li>- Durchsprechen von kritischen Situationen: (wie z.B. Beinaheunfällen), Handlungshilfen</li> <li>- Durchführung in Form von Workshops, nicht nur eine Aneinanderreihung von Vorträgen</li> <li>- Mitarbeiter muß wissen, wann es ganz besonders darauf ankommt, dass er richtig handelt</li> </ul>	<ul style="list-style-type: none"> <li>- Bei besonders sicherheitsrelevanten Tätigkeiten</li> <li>- Bei besonders gefährlichen Tätigkeiten</li> <li>- Wann es gilt (Personal-)Ressourcen gezielt einzusetzen</li> <li>- Ein Mensch kann nicht immer aufmerksam sein</li> <li>- Gute Mitarbeiter – motivierte Mitarbeiter (→ Mitarbeiterpflege)</li> <li>- Jeder Mitarbeiter muß wissen, er hat einen Vertreter, einen Helfer; Improvisationen sind nicht geeignet</li> <li>- Anforderungen an die Trainer: Praxisnähe; Uni-Ausbildung allein reicht nicht</li> <li>- Prüfplan, ob die Schulungsinhalte eingehalten werden</li> </ul>

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
<ul style="list-style-type: none"> <li>• Innovation</li> <li>• Koordinierung der Implementation des Systems und Berichterstattung an die Unternehmensleitung</li> </ul>	<ul style="list-style-type: none"> <li>- Verbesserungsvorschläge hinsichtlich SGU (Sicherheit, Gesundheit, Umwelt) positiv bewerten und für eine schnelle Umsetzung Sorge tragen<sup>2</sup>, eine diesbezügliche Betriebsvereinbarung erleichtert derartige Vorgehensweisen</li> <li>- Das SMS muß als Grundlage der gelebten Sicherheitskultur des Unternehmens verstanden werden</li> <li>- Die Unternehmensleitung muss ein echtes und nicht nur formales Interesse an einem gelebten und sich ständig verbessrenden SMS haben und äußern.</li> </ul>		

<sup>2</sup> Beispielsweise wird bei Infraserv in Gendorf als neue Methode die Bewertung einer Verbesserungsidee direkt und sofort vor Ort eingesetzt. Der Betriebsleiter kann ohne größeren Zeitverzug eine Verbesserungsidee mit bis zu DM 800 belohnen.

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
b) Ermittlung und Bewertung der Gefahren von Störfällen	<ul style="list-style-type: none"> <li>• Verfahren zur systematischen Ermittlung der Risiken von Störfällen</li> </ul>	<ul style="list-style-type: none"> <li>- Einbeziehung des Bedienpersonals in das Planungsverfahren</li> </ul>	Derzeit in der Praxis noch nicht als sinnvoll erachtet; eventuell bei bestehenden Anlagen einführbar. Das Bedienpersonal könnte gerade zu den ergonomischen Aspekten besonders viel beitragen.

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
	<ul style="list-style-type: none"> <li>• Gefahren nach Betriebsabschluß</li> </ul>	<ul style="list-style-type: none"> <li>- Erfassung der Anzahl an Meßinstrumenten/Meßwertangaben, die durch den Bediener zu beobachten sind (nach Prozeßschritten) (→ Unterscheidung nach bestimmungsgemäßem und nicht-bestimmungsgemäßem Betrieb)</li> <li>- Know-how-Erhalt der Mitarbeiter</li> </ul>	Zur Meldephilosophie ist die VDI 3699, Blatt 5 „Prozeßführung mit Bildschirmmeldungen“ heranzuziehen.

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
c) Überwachung des Betriebes	<ul style="list-style-type: none"> <li>• schriftliche Arbeits- und Betriebsanweisungen (auch für Leiharbeiter, Fremd- und Subunternehmen)</li> <li>* für die Versorgung mir Einsatzstoffe</li> <li>* für das An- und Abfahren</li> <li>* für den bestimmungsgemäßen Betrieb</li> <li>* für Prüfvorgänge</li> <li>* für Wartung und Instandhaltung</li> <li>* für das Erkennen von und Reagieren auf Störungen</li> <li>* für zeitbegrenzte oder spezielle Betriebszustände</li> <li>* für den Betrieb bei Instandhaltungs- und Reinigungsarbeiten</li> <li>* Maßnahmen bei Anlagenstillständen</li> <li>* Notfalloperationen</li> </ul>	<ul style="list-style-type: none"> <li>- Betriebsanleitungen zum richtigen und gezielten Verhalten bei Betriebsstörungen</li> <li>- Vorgaben zum systematischen Arbeitsvorgehen bei betrieblichen Störungen (ohne dass ein komplizierter Ablauf das Handeln unnötig verzögert)</li> <li>- Einüben der erwarteten Reaktion auf nicht-bestimmungsgemäße Betriebszustände</li> </ul> <ol style="list-style-type: none"> <li>1. Erkennen des nicht-bestimmungsgemäßen Betriebszustandes</li> <li>2. (Ggf. notwendige Sofortreaktion einleiten)</li> <li>3. Situationsanalyse (in welcher Phase der Reaktion steckt man gerade?)</li> <li>4. Prüfen der Ursachen des nicht-best.gem. Betriebszustandes</li> <li>5. Überdenken der Handlungsalternativen</li> <li>6. Auswahl</li> <li>7. Ausführung der ausgewählten Handlungsalternative</li> </ol>	Hier geht es um den Menschen als letzten Sicherheitsfaktor

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
	<ul style="list-style-type: none"> <li>• regelmäßige Information und Unterweisung hinsichtlich der sicherheitsrelevanten Vorgänge</li> <li>• praktische Einübung sicherheitsrelevanter Vorgänge</li> <li>• Kontrolle, ob Arbeits- oder Betriebsanweisungen sinnvoll und einhaltbar sind</li> <li>• Kontrolle, ob Arbeits- oder Betriebsanweisungen eingehalten werden</li> </ul>	<ul style="list-style-type: none"> <li>- Nicht nur Information geben, sondern auch um Feedback bei den Beschäftigten bitten, ob die Anweisungen klar und verständlich, sowie sinnvoll und einhaltbar sind</li> <li>- Regelmäßige Sicherheitsgespräche mit dem Personal</li> <li>- Festlegen des Verhaltens und der Vorgehensweisen für alle denkbaren Betriebsstörungen</li> <li>- Prüfung, ob zwischen Störungsmeldung und erwarteter Reaktion genügend Zeit bleibt; ggf. Melde-/Alarmierungswert anpassen</li> <li>- Erfassung aller Neben-/Sekundärtätigkeiten im Betrieb (Rohstoffe besorgen, Betriebsrundgänge, Probenahmen, Kleinreparaturen u.ä.)</li> <li>- Festlegung notwendiger Informationsinhalte bei Schichtwechsel; hierfür ist eine ausreichende Zeit zur Schichtübergabe vorzusehen</li> <li>- Von Zeit zu Zeit prüfen, ob die Mitarbeiter Standort und Inhalt der Betriebsanweisungen und sonstigen relevanten Dokumentationen kennen</li> <li>- Prüfung, ob es durch Nebentätigkeiten wie Instandhaltungs- und Reinigungsarbeiten zu starker Beanspruchung des Anlagenfahrers kommen kann</li> </ul>	

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
d) Sichere Durchführung von Änderungen	<p><b>1. Festlegung, was eine Änderung ist</b></p> <ul style="list-style-type: none"> <li>• Festlegung, welche Änderungen sicherheitsrelevant sind</li> <li>• Sicherstellung, daß geklärt wird, ob geplante Änderungen genehmigungswichtig relevant sind</li> </ul> <p><b>2. Festlegung der Verantwortlichkeit/Zuständigkeit für die sichere Durchführung von Anlagen- oder sonstigen betrieblichen Änderungen</b></p> <p><b>3. Dokumentation der Änderungen in allen betroffenen betrieblichen Unterlagen</b></p> <ul style="list-style-type: none"> <li>• Verfolgung von Regelwerksneuerungen (Zuständigkeit/Verantwortlichkeit, Vorgehensweise)</li> </ul>	<ul style="list-style-type: none"> <li>- Bekanntgabe der Kriterien<sup>3</sup></li> <li>- Einführung eines Informationsverfahrens, das sicherstellt, dass alle derartigen Änderungen an die Zuständigen/Verantwortlichen weitergegeben werden.</li> <li>- Einbeziehung der Mitarbeiter in den Definitionsprozess</li> <li>- Stärkung der Verantwortlichkeiten der Beteiligten zur Informationsweitergabe über Änderungen</li> </ul> <ul style="list-style-type: none"> <li>- Einbeziehung des Bedienpersonals bei der Planung (einschließlich Bewertung des Gefahrenpotentials) von Anlagenänderungen</li> <li>- Transparenz von Entscheidungsabläufen</li> </ul> <ul style="list-style-type: none"> <li>- Beachtung der Verständlichkeit der Änderungsdokumentation für alle am Änderungsverfahren Beteiligten</li> </ul> <ul style="list-style-type: none"> <li>- Prüfung, ob durch die Anlagenänderung Bedienanforderungen geändert werden, ggf. Änderung von Arbeitsanweisungen und von Unterweisungen der Anlagenfahrer</li> </ul>	<p>Jeder sollte in der Lage sein, seinen Anteil und seine Bedeutung daran wiederzuerkennen; es soll die Notwendigkeit des Einbezugs anderer Beteiligter erkennbar sein.</p>

<sup>3</sup> Als Kriterien kommen alle Änderungen in Frage, die in der Lage sind, die Maßnahmen zur Verhinderung von Störfällen zu beeinflussen. Dies betrifft Änderungen bei: Personal, Anlage, Prozesse und Prozeßvariablen, Einsatz- und Werkstoffe, Ausstattung, Verfahren, Software, Konstruktion (Ausführung) oder äußeren Umständen.

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
	<p><b>4. Analyse und Beschreibung jedes Sicherheitsaspektes der beabsichtigten Änderung</b></p> <ul style="list-style-type: none"> <li>• Betrachtung von Sekundär- und Tertiärwirkungen von Änderungen</li> <li>• Einbeziehung von Erkenntnissen aus Beinaheunfällen</li> </ul> <p><b>5. Festlegung der Vorgehensweise für die sichere Durchführung von Anlagen- oder sonstigen betrieblichen Änderungen</b></p> <ul style="list-style-type: none"> <li>• Information und Schulung des Betriebspersonals und ggf. Fremdpersonal und Personal aus benachbarten Anlagen</li> </ul>	<ul style="list-style-type: none"> <li>- Einbeziehung Dritter, nicht direkt betriebsangehöriger Mitarbeiter bei der Beurteilung der Sicherheitsrelevanz von Anlagenänderungen (=Vermeidung der Effekte gewisser „Betriebsblindheit“)</li> </ul> <ul style="list-style-type: none"> <li>- Transparenz der Verfahrensweise zur sicherer Anlagenänderung</li> </ul>	Information sollte auch an nicht direkt betroffenes Betriebspersonal weitergegeben werden.
	<p><b>6. Überwachen eventueller Auswirkungen der Änderungen, ggf. Einleitung von Korrekturmaßnahmen</b></p> <ul style="list-style-type: none"> <li>• Sicherstellung, daß Planung und Ausführung übereinstimmen</li> </ul>	<ul style="list-style-type: none"> <li>- Einbeziehung der Beteiligten durch Übernahme bestimmter Teilaufgaben</li> </ul>	

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
e) Planung für Notfälle	<ul style="list-style-type: none"> <li>• Verfahren zur Ermittlung vorhersehbarer Notfälle (= Ergänzung der systematischen Gefahrenanalyse durch die Beobachtung des Ausfalls von vorgesehenen Schutzmaßnahmen)</li> <li>• Festlegung des Personenkreises, der diese Analyse vornehmen soll</li> </ul>	<ul style="list-style-type: none"> <li>- Einbeziehung des Betriebspersonals in die Ermittlung vorhersehbarer Notfälle</li> <li>- Einbeziehung nicht betriebsangehöriger Dritter in die Analyse (→ Vermeiden von „Betriebsblindheit“)</li> <li>- Beteiligung des Bedienpersonals in allen Phasen der Erstellung und Implementierung des internen (und auch externen) Notfallplans</li> </ul> <ul style="list-style-type: none"> <li>• Verfahren zur Erstellung der Notfallpläne</li> <li>• Verfahren zur Erprobung der Notfallpläne</li> <li>• Verfahren zur Überprüfung der Notfallpläne</li> </ul>	

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
f) Qualitäts- sicherung/ Überwachung der Leistungs- fähigkeit (Wirksamkeit) des SMS	<b>I. Aktive Überwachung</b> <ul style="list-style-type: none"> <li>• Feststellung, ob Schulungsinhalte auch umgesetzt werden</li> <li>• Feststellen, ob Arbeitsanweisungen umgesetzt werden</li> <li>• Feststellen, ob die vor- gesehenen Anlagen- wartungen durchgeführt werden</li> <li>• Feststellen, ob sichere Arbeitspraktiken um- gesetzt werden</li> <li>• Feststellen, ob die erforderlichen Vor-kehrungen zur Ver- meidung von Fehl- bedienung getroffen sind</li> </ul>	<p>Anmerkung: Dieses Prüfgebiet ist wesentlich von HF-Elementen geprägt. Es geht hier vor allem um die Kontrolle, dass das Verhalten gezeigt wird, das auch vorgeschrieben ist. Insofern decken sich die Stichworte der 2. Spalte mit den zu nennenden HF-Aspekten</p> <ul style="list-style-type: none"> <li>- Bei der Inspektion der Einhaltung sicherheitserheblicher Vorgehens- und Verhaltensweisen sollte auch darauf geachtet werden, dass die <u>Ursachen</u> für die Nicht-Einhaltung genauer erfasst werden. U.a. kommen als Ursachen in Frage: <ul style="list-style-type: none"> <li>* Unklare Formulierungen</li> <li>* Vorgehensweise nicht ausreichend detailliert vorgegeben (lässt zuviel Interpretationsspielraum)</li> <li>* Vorgeschriebene Vorgehensweise ist unpraktikabel, insbesondere weil sie nicht leistungsgerecht gegenüber Beschäftigten ist, z.B. weil sie die Leistungsfähigkeit der Beschäftigten übersteigt</li> <li>* Der Zeibedarf für die Vorgehensweise (einschließlich Dokumentation) wurde nicht im Betriebsablauf berücksichtigt</li> <li>* Die Vorgehensweise wird innerbetrieblich nicht kontrolliert</li> <li>* Die Vorgehensweise war zuvor nicht mit dem Betriebspersonal besprochen worden</li> <li>* Arbeitsplatzbedingungen verhindern bzw. erschweren eine ordnungsgemäße Vorgehensweise</li> <li>* Es sind keine ausreichenden Dokumentationshilfen vorhanden</li> </ul> </li> </ul>	

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
	<ul style="list-style-type: none"> <li>• Festlegen, ob alle Sondermaßnahmen wie Prüfungen, Überwachungen, Wartungen und Reparaturen dokumentiert werden</li> <li>• Benennung der Zuständigkeit für die regelmäßige Überwachung der Einhaltung von Vorschriften</li> <li>• Bei der Überwachung festgestellte Mängel der Wirksamkeit beseitigen</li> <li>• Kontrolle, daß Mängel der Wirksamkeit abgestellt wurden</li> </ul>		

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
<b>II. Reaktive Überwachung</b>	<ul style="list-style-type: none"> <li>• Wirksames Berichtssystem über Ereignisse, Unfälle und Beinaheunfälle</li> <li>• Zuständigkeit für die Aufarbeitung von Ereignissen</li> <li>• Verbreitung der Lehren aus Ereignissen</li> <li>• Sinnvolle Sortierung der Lehren aus Ereignissen und gezielte Verbreitung bei potentiell Betroffenen</li> </ul>	<ul style="list-style-type: none"> <li>- Bei der Aufarbeitung von Beinaheunfällen ist darauf zu achten, daß nicht nur die vordergründige Störsache (z.B. Fehlverhalten des Mitarbeiters) dargestellt wird, sondern auch die dahinterstehenden latenten Fehler (z. B. ergonomisch schlecht gestaltete Arbeitsumgebung, Doppelschicht des Mitarbeiters wegen Krankmeldung eines Kollegen, fehlende Kontrolle der Verfügbarkeit geeigneten Werkzeuges, Ignorieren von Mitarbeiterbeschwerden über Arbeitsbedingungen u.ä.)</li> <li>- Die Weitergabe der Informationen über die Untersuchungsergebnisse in geeigneter Form an die Beteiligten muß gewährleistet sein</li> <li>- Ein Untersuchungsbericht (z. B. zu einem Ereignis) sollte u.a. Aufschluß geben über: <ul style="list-style-type: none"> <li>* Ausbildungs- und Wissensstand der Beteiligten</li> <li>* Ob die Aufgabenteilung klar war und eingehalten wurde</li> <li>* Ob Mängel an der Arbeitsstätte oder Umgebungseinflüsse Einfluß auf das Geschehen hatten und</li> <li>* Ob Erkenntnisse aus der Untersuchung in die Alarm- und Gefahrenabwehrplanung miteinflussen sollten</li> </ul> </li> </ul>	

Prüfgebiet	Stichworte	HF-Bezug	Bemerkungen/Hinweise
9) Systematische Überprüfung und Bewertung (Audits und Reviews)	<ul style="list-style-type: none"> <li>• Regelmäßige Überprüfung des Sicherheitskonzeptes und des SMS</li> <li>• Bewertung des Prüfergebnisses</li> <li>• Optimierung des Konzeptes/ des SMS aufgrund der Audit-/Reviewergebnisse</li> <li>• Erstellung eines Auditplans (zu auditierende Bereiche und Aktivitäten, Häufigkeit des Audits für jeden betreffenden Bereich, Verantwortlichkeit für jedes Audit, Ressourcen- und Personalfestlegung für jedes Audit, Form von Auditprotokollen, Verfahren zum Berichten über Auditbefunde, Verfahren zur Weiterverfolgung, Zuständigkeit für die Pflege des Auditsystems)</li> <li>• Der Auditor muß seine Aufgabe unabhängig und unparteiisch wahrnehmen können</li> </ul>	<ul style="list-style-type: none"> <li>- Interesse der Unternehmensleitung an Sicherheitsaspekten</li> <li>- Interesse der Unternehmensleitung an einem wirksamen Sicherheitsmanagement</li> <li>- Ausreichende Ressourcenbereitstellung für das SMS durch die Unternehmenseleitung</li> <li>- Innerbetriebliche Verbreitung der Audit-/Reviewergebnisse</li> <li>- Für die Mitarbeiter erkennbare Reaktion auf Audit-/Reviewergebnisse</li> <li>- Es sind Gespräche mit Mitarbeitern auf allen Ebenen zu führen</li> </ul>	

## 8.5 Weiterführende Literatur zu Kapitel 8

Autor	Titel
A.D. Little	Überprüfung der Organisation des Sicherheitsmanagements der Hoechst AG, Gutachten im Auftrag der Staatl. Ämter für Immissions- und Strahlenschutz, Frankfurt am Main und Wiesbaden, 30.08.93
Adams, H.W.	Integriertes Management-System für Sicherheit und Umweltschutz: Generic-Management-System. München; Wien: Hanser, 1995
Adams, H.W.	Integrierte Management-Systeme in der chemischen Industrie. Chemie Technik, 25. Jahrgang (1995) Nr. 4
Adams, H.-W.; Helm, A.	Prüfen Sie den Handlungsbedarf, Notfallmanagement muß sein. Hüthig Dok.-Nr. 2146
Adams, H.W.; Jochum, C.	Organisation tut Not, Sicherheitsmanagement für Störfallanlagen, Hüthig Dok.-Nr. 2831
Bayerisches Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit	Schriftenreihe Managementsysteme für Arbeitsschutz und Anlagensicherheit, München 1998
Clausen, J.; Fichter, K.; Arndt, H.-K.	Materialien zum betrieblichen Umweltmanagement und Umweltcontrolling, UBA-TEXT 12/95
Dumpert, H.-D.; Knaak, J.-D.; Barduna, K.; Stuhrmann, H.-B.	Verbesserungsmöglichkeiten für die Effektivität des Sicherheitsmanagements, Forschungsbericht RW TÜV, März 1994
Hessische Landesanstalt für Umwelt (HLfU)	Leitfaden Integrierte Managementsysteme, HLfU-Schriftenreihe Umweltplanung Arbeits- und Umweltschutz, Heft 240, Fachverlag Moderne Wirtschaft, Wiesbaden 1997
Hessisches Ministerium für Frauen, Arbeit und Sozialordnung	Leitfaden Arbeitsschutzmanagement Teil I „Anleitung zur Implementierung eines Arbeitsschutzmanagementsystems“, Teil II „Inhalt und Struktur eines Arbeitsschutz-Management-Handbuchs“, Teil III „Beispielsammlung“, 1997
Keßl, G.M.	Motivation per Geldbeutel, Chemie Technik, 29. Jahrgang (2000), Nr. 1
Kirsch, B.	Zeit ist kostbar – die Mitarbeiterbesprechung, Chemie Technik, 29. Jahrgang (2000), Nr. 1
Miller, R. et al.	Analyse von sicherheitsrelevanten Ereignissen in verfahrenstechnischen Anlagen, UBA-TEXT 98/79
Moch, E.; Pietsch, K.-J.	Sicherheitsmanagement bei kleinen und mittleren Unternehmen, UBA-TEXT 67/98
Richter, B.; Kuntschner, M.	Rechnergestützte Überprüfung von Sicherheitsmanagementsystemen, Technische Überwachung Nr. 6 (1999)
Seeberger, R.; Kamm, R.	Evaluation von TQM-Sicherheitszirkeln bei KSB-AG, Psychologie der Arbeitssicherheit 8. Workshop 1995, S. 370-384

Staatliches Amt für Immissions- und Strahlenschutz, Frankfurt (SAIS)	Gutachten zur Organisation der Sicherheit der Hoechst AG, Duisburg 31.08.93
Uth, H.-J.	Störfallmanagement am Beispiel der Chemischen Industrie, UBA-TEXT 2/95
Wolf, H.	Betriebshandbücher - Instrumente zur Integration des Arbeits-, Gesundheits- und Umweltschutzes in die Unternehmensstrategie, Psychologie der Arbeitssicherheit 8. Workshop 1995, S. 584-590
Zimolong, B.	Sicherheitsmanagement: Der Zusammenhang zwischen Sicherheitsorganisation, Schulung und Sicherheitsstandard; aus: Zimolong, Trimpop 1991
Zimolong, B.; Trimpop, R. (Hrsg.)	Psychologie der Arbeitssicherheit, 6. Workshop 1991, Heidelberg

## 9. Möglichkeiten zur Umsetzung der Human Factor-Aspekte

Im Rahmen dieses Projekts konnte festgestellt werden, daß

- a. bereits umfangreiche Kenntnisse zum Human Factor existieren, aber nicht durchgängig angewendet werden (z.B. ergonomische Grundsätze in Leitwarten und der Anlage selbst)

und

- b. daß in konkreten verfahrenstechnischen Anlagen im allgemeinen noch erhebliche Lücken im Hinblick auf die Dokumentation, Prüfbarkeit und Bewertbarkeit der HF-Aspekte bestehen.

Zur Umsetzung gehört deshalb einerseits die konsequente Berücksichtigung vorhandener Erkenntnisse und andererseits die Entwicklung von Dokumentations- und Prüfmethoden zur Bedienkonzeption.

### Umsetzung durch Ordnungsrecht und Regelwerke<sup>4</sup>

Während der Bearbeitung des hier dokumentierten Projekts wurde die Störfall-Verordnung vom 20. September 1991 in Anpassung an die Seveso II-Richtlinie der EU (Richtlinie 96/82/EG) vom 9. Dezember 1996 novelliert (BGBl. 2000 Teil I, Nr. 19, S. 603-626 vom 26. April 2000).

§6 Abs. 1 Nr. 3 und 4, die das Thema Fehlbedienung betreffen, wurden dabei nur in geringem Maße gegenüber der bisherigen Fassung verändert (nach Nr. 4 soll Fehlverhalten nicht nur – wie bisher – durch Schulung, sondern auch durch „geeignete Bedienungs- und Sicherheitsanweisungen“ vorgebeugt werden). Der Vorschlag der Autoren dieses Berichts<sup>5</sup>, den Anlagenfahrer auch als letzten Sicherheitsfaktor bei Ausfall technischer Systeme zu berücksichtigen, wurde nicht aufgegriffen.

Auch in dem nach Anhang III der neuen Störfallverordnung notwendigen Sicherheitsbericht sind zur Verhinderung von Störfällen (siehe Nr. IV, Anhang III) lediglich die „technischen Parameter sowie Ausrüstung zur Sicherung der Anlagen“ verlangt, nicht aber Maßnahmen, die den Menschen/das Personal zur Verhinderung von Störfällen qualifizieren. Dies hat beim gegenwärtigen Stand durchaus nachvollziehbare Gründe:

Im Rahmen dieses Projekts wurde hervorgehoben, daß zwar bereits umfangreiche und wesentliche Erkenntnisse dazu vorliegen, wie die Schnittstelle Mensch-Technik zu verbessern ist und

<sup>4</sup> Auf mögliche Straftatbestände (z.B. resultierend aus einer Vernachlässigung technischer Kontrollen) wird an dieser Stelle nicht eingegangen.

<sup>5</sup> Siehe 1. Zwischenbericht zu diesem Projekt vom Mai 1999.

wie die Merkmale des Menschen bei der Anlagensicherheit besser zu berücksichtigen sind. Es wurde aber auch aufgezeigt, daß hinsichtlich des Human Factor noch deutliche Methodenlücken bestehen im Bezug auf Erfassung der Bedienkonzeption und – damit zusammenhängend – im Bezug auf die Prüfbarkeit der Bedienkonzeption. Insofern verwundert es nicht, daß das Thema "Fehlbedienung" auch in der neuen Störfall-Verordnung noch keinen größeren Stellenwert erhalten hat.

Die festzustellende mangelnde Umsetzung wichtiger ergonomischer Grundsätze bei Anlagen- und Leitwertengestaltung (siehe die in Kapitel 5 aufgeführten DIN/ISO-, VDI-, und NAMUR-Normen) muß jedoch Anlaß geben, ihre Berücksichtigung in geeigneter Weise verbindlicher zu gestalten.

Für das Zusammenspiel zwischen Anlagenplaner, Betreiber und Aufsichtsbehörde ist eine verbindliche Regelung wünschenswert. Dabei ist weniger wichtig, ob diese in Form einer Verwaltungsvorschrift, einer Technischen Anleitung oder einer Technischen Regel abgefaßt wird. Wesentlich ist, daß eine höhere Verbindlichkeit als bei einem Leitfaden oder einer Empfehlung erreicht wird.

Folgende Aussagen sollten in eine solche Regelung eingehen:

1. Es wird gefordert, daß nach einem der dargestellten oder einem alternativen Verfahren in den Sicherheitsbetrachtungen eine Auseinandersetzung mit der Bedienkonzeption erfolgt.
2. Es ist zu fordern, bei der Bedienkonzeption das Einzelfehlerprinzip zu verlassen und Handlungsketten zu betrachten.
3. Bei hochautomatisierten Anlagen sind auch Ausfälle der Prozeßleittechnik bzw. der Visualisierungssysteme zu untersuchen.
4. Es ist anzustreben, die Handlungs- bzw. Ereignisketten grafisch darzustellen, da damit eine größere Sicherheit der Vollständigkeit erreicht wird.
5. Abschneidekriterien, wie in Kapitel 7 dargelegt, sollten Bestandteil der Regelung sein.
6. Zerlegungskriterien, wie als Beispiel in Kapitel 7 dargelegt, sollten Bestandteil der Regelung sein.

Derzeit ist noch nicht absehbar, ob, wann und in welcher Form die drei bestehenden Verwaltungsvorschriften zur (alten) Störfall-Verordnung an die neue Störfall-Verordnung angepaßt werden.

Es kann aber schon jetzt dringend empfohlen werden, die Ergonomie betreffenden Normen, die (auch) der Vermeidung von Fehlbedienung dienen, in den Leitfäden/ Merkblättern/Verwaltungsvorschriften zur neuen Störfall-Verordnung explizit zu nennen.

Gerade durch Anlagenänderungen (die bei verfahrenstechnischen Anlagen fortlaufend stattfinden) sind zunehmend ergonomische Verschlechterungen feststellbar.

Es sollte weiterhin in den systematischen Gefahrenanalysen der Bediener bzw. die Anforderungen an den Bediener zur Störfallverhinderung oder zur Auswirkungsbegrenzung konkreter formuliert werden.

Da durch die neue Störfall-Verordnung auch der Organisation zukünftig mehr Bedeutung zugeordnet wird, sollten zukünftige Gefahrenquellenanalysen die störfallverhindernden Maßnahmen nach

- technischen
- organisatorischen und
- personellen Maßnahmen

unterscheiden.

Die derzeit verfügbaren betrieblichen Unterlagen erlauben in der Regel keine Einschätzung der Bedienerbelastung in den einzelnen Prozeßphasen und bei nicht bestimmungsgemäßen Betriebszuständen, obwohl bekannt ist, daß Überlastung einschließlich Informationsüberflutung zu menschlicher Fehlleistung führt.

Es sollte zukünftig von den Betreibern störfallrelevanter Anlagen eine Dokumentation der Bedienerbelastung erstellt werden.

Die Form der Dokumentation kann derzeit noch offen bleiben, da je nach Anlagen- und Prozeßart unterschiedliche Dokumentationsformen sinnvoll sein können (vgl. Kapitel 7).

Der Betreiber sollte jedoch nachweisen, daß mindestens für sicherheitsrelevante Bedienschritte und für vorhersehbare betriebliche Störungen Bedienerüberlastung und/oder Informationsüberlauf ausgeschlossen sind.

In Kapitel 5 wurde detailliert aufgearbeitet, in welchem Umfang technische Normen und Richtlinien das Thema "Bedienen" aufgreifen. Es wird festgestellt, daß u.a. menschliche Leistungsgrenzen bei der Informationsverarbeitung nahezu keine Berücksichtigung finden. Es wird weiterhin festgestellt, daß arbeitspsychologische Normen (wie die IEC 56 (Sec) 423 "Anwendungsleitfaden zur menschlichen Zuverlässigkeit" und die DIN/ISO 10075-2 "Ergonomische Grundlagen bezüglich psychischer Arbeitsbelastung") zu wenig den technisch denkenden Ingenieur als Zielgruppe der Norm berücksichtigen, so daß diese Normen kaum in Ansätzen seine Aufmerksamkeit finden.

Es wird deshalb notwendig sein, daß in den Normengremien stets Arbeitspsychologen und Ingenieure mit entsprechendem Gewicht und Engagement vertreten sind, damit im echten Sinne die Schnittstelle Mensch-Technik aufgearbeitet wird und nicht der Mensch durch die eine Norm und die Technik durch eine andere Norm ohne größere Bezugnahme zueinander.

## Umsetzung durch Information und Kommunikation

In zahlreichen Gesprächen während der Durchführung des Forschungsvorhabens konnte festgestellt werden, daß der aktive Umgang mit dem Faktor Mensch in technischen Fachkreisen noch weitgehend fremd ist. Technische Absicherung gegen menschliche Fehlbedienung sind in der Regel die einzige Form des Umgangs mit dem Human Factor. Es wird deshalb in den kommenden Jahren erforderlich sein, die Kenntnisse von Technikern, Ingenieuren und Chemikern zum Verhalten von Menschen sowie seinen physiologischen und psychologischen Leistungsmöglichkeiten und -grenzen zu vertiefen. Zu diesem Zweck wurde im Rahmen dieses Projekts der "Leitfaden zur Berücksichtigung der HF-Aspekte in verfahrenstechnischen Anlagen" entwickelt, der einen Einstieg in das Thema ermöglichen bzw. erleichtern soll.

Die Verbreitung der im Rahmen dieses Projekts erarbeiteten Kenntnisse/Erkenntnisse über den Menschen in verfahrenstechnischen Anlagen sollte nun über alle verfügbaren Wege und Kanäle weiterverfolgt werden:

- Verbreitung und Verfügbarmachung der Ergebnisse bzw. der Produkte des UBA-Forschungsvorhabens "Strategien zur Vermeidung von Fehlbedienung in verfahrenstechnischen Anlagen" durch
  - Veröffentlichung des vorliegenden Berichts als UBA-Text
  - ggf. Veröffentlichung des o.g. Leitfadens als eigenständige, in sich geschlossene Publikation
  - Bereitstellung im Internet (mit der Möglichkeit der freien Nutzung der Inhalte)
  - Auszugsweise Darstellung in Fachzeitschriften
  - Vorträge auf Fachveranstaltungen
  - Beteiligung an der Fortbildung von Störfallbeauftragten
  - Gezielte Verbreitung bei den betroffenen Akteuren (z.B. durch Präsentation in Behörden und Verbänden)
- Schulung und Training
  - des Führungspersonals: Lernmechanismen des Menschen, Streßreaktionen, Motivation, Gestaltung der Arbeitsatmosphäre, Bedeutung ergonomischer Gestaltung der Arbeitsumgebung, menschliche Informationsverarbeitung, Einbeziehung des Bedienpersonals in die Anlagengestaltung, Durchführung von Mitarbeitergesprächen, Gruppendynamik
  - des Bedienpersonals: Umsetzung von Wissen in Handlung, Einüben von Notfallreaktionen, umfassende Kenntnis von Prozeßabläufen, Umgang mit "unsicher" arbeitenden Kollegen, Erkennen und Äußern von Verbesserungsvorschlägen

- Begleitete Einführung des aktiven Umgangs mit dem Human Factor in Modellbetrieben: Erkennen des Hintergrundes von Widerständen, Abbau von Abwehrverhalten, Verbesserung der Kommunikation, Verdeutlichung von HF-Aspekten in der täglichen Produktion
- Ausbildung von Mediatoren: Beteiligung betrieblicher HF-Experten an Anlagenplanungen, Sicherheitsgesprächen oder bei der Aufarbeitung von Ereignissen

### **Umsetzung durch Schulung und Ausbildung**

Es wird heute zunehmend bemängelt, daß der Chemiefacharbeiter gerade bei PLT-gesteuerten Produktionen die dahinterstehenden Prozeßabläufe nicht mehr überblicken und nicht mehr durchschauen kann. Schon deshalb wird er im Fall abweichender Betriebszustände nicht auf ein Verhaltensrepertoire zurückgreifen können, das es ihm ermöglicht, die Anlage wieder in einen sicheren Zustand zu bringen.

Auch wird bei Schulung und Ausbildung noch immer der einkanalige Lernweg "Sehen – Hören – Wissensvermittlung" gewählt, obwohl längst allgemein bekannt ist, daß die Umsetzung von Wissen in Handlung einen eigenen Lernweg, nämlich das Üben und Trainieren verlangt, ganz abgesehen davon, daß die Behaltensleistung von Wissen, das man ausgeführt hat, bei rund 90% liegt (gegenüber nur Gehörtem und Gesehenem bei 50% und nur Gehörtem gar bei nur 20%). Die augenblicklich sich stark entwickelnden Simulationsprogramme (über die spielerisch am PC Notfallreaktionen eingeübt werden können) und Trainingssimulationen (bei denen Notfallreaktionen an echten verfahrenstechnischen Kleineinheiten eingeübt werden können) weisen hier den richtigen Weg auf, der jedoch in der betrieblichen Praxis noch viel zu wenig tatsächlich beschritten wird.

Hier wäre es sicher hilfreich, wenn die Behörden spätestens bei gehäuften Beinahe-ereignissen in Anlagen öfter nach diesen Schulungs- und Ausbildungsformen fragen würden.

### **Umsetzung durch Haftungs- und Versicherungsrecht**

Die weichen HF-Faktoren finden im Haftungs- und Versicherungsrecht derzeit noch wenig Berücksichtigung. Technische Verbesserungen/Absicherungen können sich direkt auf die Versicherungsprämie auswirken, wogegen Verbesserungen beim Bedienpersonal nicht als prämienrelevanter Beitrag diskutiert werden können. Auch geht die Haftung bei den meisten Versicherungen nicht soweit, daß bedienerunfreundliche Anlagenplanung eine Rolle spielen würde. Nun soll dies auch an dieser Stelle - noch - nicht diskutiert werden.

Es ist jedoch zu erwarten, daß mit zunehmender Abrundung des HF-Ansatzes auch das Versicherungs- und Haftungsrecht dem Faktor Mensch mehr Beachtung schenken wird, indem an

die versicherungsnehmenden Anlagenbetreiber neben technischen Anforderungen auch ergonomische und personelle Anforderungen gestellt werden.

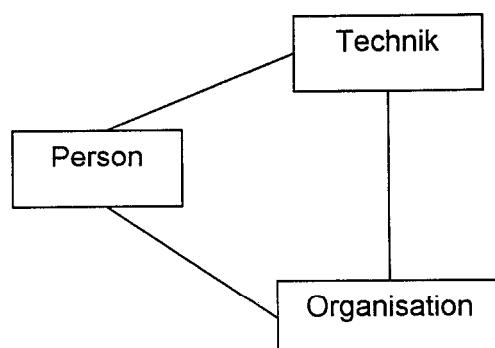
### Empfehlung zur weiteren Vorgehensweise

Es ist im Rahmen des Forschungsvorhabens deutlich geworden, daß "Strategien zur Vermeidung von Fehlbedienung" einen wichtigen Beitrag zur Störfallvorsorge leisten können. Bisher wird jedoch gleichzeitig in technischen Fachkreisen noch weitgehend geleugnet, daß konkrete Anforderungen an den Bereich Human Factor gestellt werden könnten. Vor diesem Hintergrund wird empfohlen, von rechtsverbindlichen Regelungen (die über die oben genannten Empfehlungen hinausgehen) vorerst noch abzusehen, sondern wie folgt vorzugehen:

**Schritt 1:** Schaffung eines Problembewußtseins für den Human factor<sup>6</sup>

**Schritt 2:** Entwicklung von Darstellungs-, Prüf- und Evaluierungsmethoden zur Bedienkonzeption<sup>7</sup>

Erst wenn diese beiden Schritte hinreichend abgeschlossen sind, kann von einem abgerundeten HF-Konzept ausgegangen werden, das einen integrierten Zugang zum System



ermöglicht.

Erst dann sollte Schritt 3 verfolgt werden:

**Schritt 3:** Verbindliche HF-Anforderungen für störfallrelevante Anlagen.

<sup>6</sup> Dieser Bericht soll dazu einen wesentlichen Beitrag leisten. Darüber hinaus wird der Arbeitskreis "Human Factor" der Störfallkommission das Thema weiter vertiefen.

<sup>7</sup> Diesem Bericht sind Vorschläge zur Darstellungsform der Bedienerbelastung zu entnehmen. Außerdem werden eine Reihe von existierenden Prüf-/Evaluierungsgsinstrumenten zitiert, die jedoch den entscheidenden Nachteil haben, daß sie zu umfangreich und komplex sind, um in der Praxis Anwendung zu finden.

## 10. Zusammenfassung und Schlußfolgerungen

Die Vermeidung von Fehlbedienung – also die Berücksichtigung des Human Factors – hat in der Kerntechnik und in der Flugverkehrstechnik bereits eine längere Tradition. Das Thema gewinnt in den letzten Jahren auch im Zusammenhang mit verfahrenstechnischen Anlagen zunehmend an Bedeutung. Mit rund einem Drittel aller Störfallursachen ist Fehlbedienung heute eine der wesentlichen noch verbliebenen Ansatzpunkte zur Verbesserung der Anlagensicherheit.<sup>8</sup>

Obwohl Bediensicherheit zunehmend in das Bewußtsein der Unternehmen der chemischen Industrie gelangt, erfolgt die Umsetzung der zahlreichen vorliegenden Erkenntnisse noch zögerlich. Offenbar mangelt es an einer geeigneten Kommunikation zwischen den mit Human Factor-Aspekten beschäftigten Ergonomen und Arbeitspsychologen einerseits und den technisch ausgebildeten Anlagenplanern und Betriebsleitern andererseits. Zahlreiche Gesichtspunkte des Human Factors tauchen implizit zwar in den Sicherheitsphilosophien und Werksrichtlinien der Unternehmen auf, werden jedoch bislang kaum systematisch unter der Zielsetzung "Bediensicherheit" verfolgt.

Die in Umsetzung der Seveso-II-Richtlinie im April 2000 novellierte Störfall-Verordnung fordert – ebenso wie die alte Störfall-Verordnung – Vorkehrungen zur Vermeidung von Fehlbedienungen, präzisiert diese Vorkehrungen jedoch nicht näher. Es ist derzeit noch nicht absehbar, wann und in welcher Form die Inhalte der (alten) Verwaltungsvorschriften wieder aufgegriffen werden. In jedem Fall sollte bei einer Anpassung der Verwaltungsvorschriften konkreter als bisher auf Fragen der Bediensicherheit eingegangen werden.

Auch in den einschlägigen Normen und Richtlinien sowie den üblichen Prüfungsabläufen bei Planung, Errichtung und Betrieb von Anlagen haben Human Factor-Aspekte – abgesehen von der ergonomischen Gestaltung der Bedienoberflächen, die hinreichend abgedeckt ist – noch kaum Einzug gehalten. Angesichts der üblichen Entstehungsdauer von Richtlinien und Normen erstaunt dies nicht.

Ein Blick über die Grenzen zeigt, daß es die Regelungen in Großbritannien und den USA vergleichsweise präzise Vorgaben zur Berücksichtigung von Human Factor-Aspekten enthalten, während der Human Factor in anderen Ländern (betrachtet wurden Schweiz, Frankreich, Niederlande und Korea) in Gesetzen und untergesetzlichen Regelwerken kaum berücksichtigt wird. Dies bedeutet jedoch nicht, daß Fragen der Bediensicherheit dort vernachlässigt würden. Vielmehr wird zugunsten von einzelfall-spezifischen Anforderungen auf detaillierte allgemeine Regelungen verzichtet.

<sup>8</sup> Allerdings ist die bisherige Praxis der Störfallanalyse hinsichtlich der Differenzierung von Bedienungsfehlern noch verbessungsfähig.

Üblicherweise wird der bedienende Mensch über das planmäßige Fahren einer verfahrenstechnischen Anlage im Normalbetrieb hinaus zum Beherrschenden unvorhergesehener Situationen eingesetzt. In der Regel erfolgt im Rahmen der Anlagenplanung keine Prüfung der an den Bediener gestellten Anforderungen hinsichtlich ihrer Erfüllbarkeit im Hinblick auf die physiologischen und psychologischen Leistungsgrenzen des Menschen. Dies gilt in der Regel für den Normalbetrieb ebenso wie für den nicht-bestimmungsgemäßen Betrieb.

*Die Bilanzierung der Ausführbarkeit von Bedienanforderungen scheint das zentrale Problem der Erhöhung der Bediensicherheit zu sein.*

Dies ist insofern nicht verwunderlich, als es bislang an einer Dokumentationsmethodik, die eine solche Prüfung überhaupt erst ermöglicht, fehlt.

Eine handhabbare Dokumentation der Bediensicherheit ist auch zur Verbesserung der Rechtsicherheit des Anlagenbetreibers wichtig. Gegenwärtig sieht sich der Betreiber mit der Forderung der Störfall-Verordnung nach Vorsorge gegen Fehlbedienung konfrontiert – es fehlt jedoch an konkreten Hinweisen, was unter "Sicherung gegen Fehlbedienung" zu verstehen ist und wie man dazu vorgeht.

Ein wesentliches Ziel dieses Vorhabens war die Entwicklung von Methoden zur Erfassung und Bewertung der an den Bediener gestellten Anforderungen als Hilfsmittel für Anlagenplaner und -betreiber, sowie ggf. als Prüfunterlage für den Vollzug.

Entscheidend hierfür ist, daß die Anzahl der maximal gleichzeitig durchführbaren Bedienhandlungen (auf etwa sieben) begrenzt ist. Dies definiert eine im Zusammenhang mit Fehlbedienung wichtige Leistungsgrenze des Menschen. Sie ist in dem Sinne objektiv, daß sie durch Qualifikation, Training und Motivation nicht beliebig nach oben verschoben werden kann.

Es geht hier nicht darum, Fehlbedienung als Produkt von Nachlässigkeit, Unzulänglichkeit oder Inkompetenz des Bedieners zu begreifen. Im Zentrum steht vielmehr die Frage, *warum* die Leistungsgrenzen des Bedieners überschritten werden und *wie* in der Bedienkonzeption einer Anlage vorbeugend diesen Leistungsgrenzen entsprochen werden kann.

Ausgehend von der Beobachtung, daß es zahlreiche theoretische Erkenntnisse zur besseren Berücksichtigung des Human Factor gibt, die jedoch in der Praxis erst teilweise Einzug gefunden haben, gilt es zunächst, das Problembewußtsein bei den entscheidenden Akteuren zu wecken. Ferner sind entsprechende Hilfsmittel für die betriebliche Praxis bereitzustellen.

Hierzu wurde im Rahmen des Projekts ein "Leitfaden zur Berücksichtigung der Human Factor-Aspekte in verfahrenstechnischen Anlagen" als in sich geschlossene Unterlage – vorgelegt als Materialband zu diesem Abschlußbericht – entwickelt.

Der Leitfaden besteht aus zwei Teilen:

1. Einer Darstellung der Leistungen und Leistungsgrenzen des Menschen. Hierbei steht die praxisgerechte Aufarbeitung vorhandenen Wissens im Vordergrund.
2. Elf Checklisten zur Prüfung der Human Factor-Aspekte als Hilfsmittel für die betriebliche Praxis. Die Checklisten decken die wesentlichen betrieblichen Planungsbereiche ab (Anlagendesign, Leitwartengestaltung, Personalauswahl etc.).

Die menschlichen Leistungsgrenzen des Bedieners beziehen sich dabei im wesentlichen auf die drei Schritte

Informationsaufnahme – Informationsverarbeitung – Informationsumsetzung.

Neben den Anforderungen an Anlage und Betrieb zur Berücksichtigung der menschlichen Leistungsmöglichkeiten wird auf die Veränderung dieser Leistungsfähigkeit in Störsituationen eingegangen:

In Notfallsituationen reduziert sich geplantes, systematisches Vorgehen. Mit steigender Fehlerzahl wächst die Anwendung von Stereotypen – derselbe (falsche) Gedankengang wird wieder und wieder verfolgt. Die Risikobereitschaft steigt, eine Gefahrensituation soll um jedem Preis gemeistert werden. Da ein Durchdenken der Situation im Notfall nicht mehr geleistet werden kann, muß der Bediener in solchen Situationen auf ein programmiertes Reaktionsinventar zurückgreifen können. Daraus folgt, daß Notfallsituationen (z.B. im Simulator) trainiert werden sollten – Schulungen, die ausschließlich auf die kognitive Bewältigung zielen, genügen nicht.

Aus diesen Erkenntnissen sind Handlungsansätze im Hinblick auf Bedienerqualifizierung, Anlagengestaltung und Betriebsführung ableitbar.

Kontinuierliche und diskontinuierliche (Batch-)Prozesse erfordern unterschiedliche Ansätze zur Erfassung der Bedienkonzeption. Dies liegt insbesondere daran, daß kontinuierliche Fließgutprozesse mit vergleichsweise wenig Personal, aber viel Prozeßleittechnik betrieben werden. Batch-Prozesse hingegen werden häufig bedienungsintensiv in Vielzweckanlagen mit geringem Automatisierungsgrad betrieben.

### **Kontinuierliche Prozesse**

Für kontinuierliche Prozesse wurden folgende Notierungsformen der Bedienkonzeption auf ihre Anwendbarkeit untersucht:

1. Eintragung von Bedienfunktionsstellen in das Rohrleitung- und Instrumenten-Schema (RI-Schema).

2. Notierung der Handlungsabläufe als Prozeßablaufplan.
3. Erfassung gleichzeitiger Bedienhandlungen in einem Balkendiagramm.
4. Darstellung der Bedienhandlungen anknüpfend an die Schwachstellenanalyse des PAAG-Verfahrens ("Störungskompensationsgraph").

Diese Notierungsformen wurden – mit Ausnahme des Prozeßablaufplans – anhand bestehender Anlagen getestet. Als wichtigste Ergebnisse können festgehalten werden:

- Die Eintragung der Informationsverarbeitungsknoten und ihrer Verbindungen zu Meßgebern und Stellgliedern in die RI-Schemata (vergleichbar der Darstellung von MSR- und PLT-Funktionen) ist nahezu wirkungslos, da die erforderliche Übersicht und nicht erreichbar ist und gleichzeitige Bedienanforderungen nicht erkennbar sind.
- Die Notierung der Bedienanforderungen als Prozeßablaufplan kann dem Betreiber als Erkenntnisquelle für die erforderlichen Handlungsabläufe dienen. Er erscheint jedoch nicht geeignet, als Mittel zur angemessenen Sicherung gegen Fehlbedienung behördlich vorgeschrieben zu werden. Aufgrund dieser Bewertung wurde der Prozeßablaufplans nicht in Praxiserprobung mit dem Anlagenbetreiber einbezogen. Es wurde dem Anlagenbetreiber jedoch empfohlen, das Werkzeug als Erkenntnisquelle für betriebliche Planungen zu nutzen.
- Ziel der Erfassung der Bedienhandlungen in einem Balkendiagramm war die Klärung, ob die betrachtete Anlage so mit technischen Mitteln ausgerüstet ist, daß eine Überlastung des Bedieners (Meßwartenfahrers) aufgrund einer Vielzahl gleichzeitig auszuführender Bedienhandlungen durch die automatische Prozeßsteuerung übernommen wird.

Es zeigte sich, daß durch das Auftreten von mindestens zwei (unabhängigen) Störungen Handlungsanforderungen an den Bediener so auflaufen können, daß die kritische Zahl von sieben gleichzeitigen Anforderungen überschritten wird. Aufgrund des hohen Automatisierungsgrades der betrachteten petrochemischen Anlage ist dies jedoch im Hinblick auf die Störfallvorsorge irrelevant, da die Anlage stets auf Knopfdruck des Bedieners abgefahren werden kann.

- Auf der Grundlage der im Rahmen des PAAG-Verfahrens für die als Praxisbeispiel betrachtete Raffinationsanlage herausgearbeiteten betrieblichen Gefahrenquellen (einschließlich der getroffenen Gegenmaßnahmen) wurden die möglichen Eingriffe der Bedienere in Gefahrensituationen in Form eines "Störungskompensationsgraphen" bildlich dargestellt. Durch die graphische Darstellung kann die Gesamtübersicht über die Sicherheitssituation wesentlich verbessert werden.

Es ist notwendig, die Bedienereingriffe, die Möglichkeit des Unterlassens eines Eingriffes durch den Bediener und die Wirkung des Notabfahrtsystems in einer gemeinsamen Darstellung zusammenzuführen. Dazu ist es zweckmäßig, die Gliederung nicht – wie bisher

üblich – nach Fehlerklassen, sondern nach Apparaten und/oder Prozeßgrößen vorzunehmen.

Mit einer solchen Darstellung wird übersichtlich und vollständig deutlich, unter welchen Bedingungen bzw. infolge welcher Bedienfehler noch "Dennoch-Störfälle" möglich sind.

Eine solche (oder vergleichbare) Darstellung könnte Eingang in die untergesetzlichen Regelwerke finden.

Insgesamt wurde deutlich, daß ein erheblicher Arbeitsaufwand notwendig ist, Bedienabläufe vorauszudenken (zu konstruieren). Die Betrachtung der gängigen Praxis der Anlagenplanung zeigt, daß alle Abläufe, die bei der Planung detailliert vorausgedacht werden, bei hochgradig automatisierten Anlagen in technische Lösungen zur Anlagensicherung eingehen (Notabschaltung, automatische Umschaltung auf Reserve u.ä.). Das bedeutet, es bleiben praktisch keine vorausgedachten Abläufe zur ausschließlichen Ausführung durch einen Bediener übrig.

### Batch-Prozesse

Für Batch-Anlagen wurde eine eigene Notierungsform entwickelt, um die Anforderungen an den Bediener darzustellen. Als Bedienvorgänge sind nicht nur manuelle Handlungen (z.B. Stoffzufuhr betätigen, Regler einstellen) zu verstehen, sondern auch Beobachtungsaufgaben (Temperatur, Druck etc.), da sie den Bediener ebenso wie manuelle Handlungen binden und damit zum Belastungsniveau beitragen. Bei Batch-Prozessen geht es demnach um Handlungs- *und* um Informationsüberlauf (während bei kontinuierlichen Prozessen Handlungsüberlauf eher von nachrangiger Bedeutung ist).

Sinn der Darstellung der Bedienkonzeption bei Batch-Anlagen ist

- die Ermittlung besonders beanspruchender Zeitabschnitte innerhalb der Schicht,
- die Feststellung der Notwendigkeit zusätzlicher technischer Absicherungen bei zu erwartender Überbelastung des Bedieners,
- die Feststellung des Personalbedarfs in den einzelnen Produktionsabschnitten,
- die Identifikation von Schulungs- und Trainingsschwerpunkten für die Bediener.

In Batch-Anlagen kann schon der Normalbetrieb zu Bedienerüberlastung führen. Deshalb beginnt die Darstellung der Bedienkonzeption in jedem Fall zunächst mit dem Normalbetrieb (mit dem Ziel „Vermeidung von Fehlbedienungen durch Bedienerüberlastung“). Durch eine graphische Darstellung mit vertikaler Zeitachse und horizontal aufgetragenen räumlichen Abständen der Bedienorte können die raum-zeitlichen Abläufe für den Normalbetrieb einer Batchanlage (die mehrere parallel betriebene Reaktoren oder sonstige Apparate umfassen kann) visualisiert werden. Es können auf diese Weise Beginn, Dauer und Ort der Bedienhandlung dargestellt und Konflikte

durch gleichzeitige Anforderungen identifiziert werden. Diese Darstellung erlaubt dem Betreiber eine bedienerorientierte Produktionsplanung und die Identifikation ggf. zur Entlastung des Bedieners erforderlicher Teilautomatisierungen oder sonstiger (technischer oder organisatorischer) Unterstützung.

Die praktische Erprobung dieser Notierungsform der Bedienerbelastung bei Batch-Anlagen führte zu folgenden Ergebnissen:

- Die Darstellung eignet sich zum Erkennen der Bedienerbelastung im Normalbetrieb. Allerdings genügen die Rezeptanweisungen gewöhnlich nicht als Grundlage, da sie nicht alle erforderlichen Informationen enthalten. Beispielsweise sind häufig nicht alle zu beobachtenden Meßwerte zu entnehmen.
- Für den nicht-bestimmungsgemäßen Betrieb fehlen die erforderlichen Informationen zur Darstellung der Anforderungen an den Bediener erst recht. Damit eine derartige Darstellung möglich wird, sind die Gefahrenanalysen durch entsprechende Informationen über das erwartete Verhalten des Bedieners in Störsituationen zu ergänzen.
- Aktivitäten, die auf nicht bestimmungsgemäße Betriebszustände folgen sollen (Anlage wieder in den sicheren Zustand überführen), sind zunächst als Handlungssequenz festzuhalten, können jedoch i.d.R. nicht einem bestimmten Zeitpunkt im Produktionsverlauf zugeordnet werden. Solche Bedientätigkeiten werden deshalb bei der Prüfung der Bedienkonzeption auf Durchführbarkeit nur in sich zu prüfen sein. Eventuell parallel weiterlaufende Bedienanforderungen (im Batch-Betrieb hat der Bediener durchaus auch mehrere Produktionen gleichzeitig zu überwachen und zu bedienen) werden nicht berücksichtigt.

Die Beurteilung der Bedienbarkeit erfordert weit mehr Informationen als bisher mit den Sicherheitsanalysen üblicherweise vorzulegen. Für den Fall, daß im Zuge der Anlagengenehmigung eine nachprüfbare Darstellung der Bedienkonzeption gefordert wird, ist daher der Grundsatz der Verhältnismäßigkeit zu beachten.

Im Rahmen dieses Projekts wurden die Möglichkeiten zur Umsetzung der Ergebnisse in betrieblichen Managementsystemen (z.B. Total Quality Management) geprüft und Grundsätze abgeleitet, wie Human Factor-Aspekte beim Aufbau von Managementsystemen Eingang finden können. Dies ist insbesondere angesichts der Forderung der neuen Störfall-Verordnung nach Verbesserung bzw. Gewährleistung der Anlagensicherheit durch ein Sicherheitsmanagement bedeutsam. Hierzu wurde eine Zuordnung der zu berücksichtigenden Human Factor-Aspekte zu den in Anhang III der Störfall-Verordnung genannten Prüfgebieten erarbeitet.

Langfristig sind für das Zusammenspiel zwischen Anlagenplaner, Betreiber und Aufsichtsbehörde verbindliche Regelungen zur besseren Vorsorge gegen Fehlbedienung wünschenswert.

Bei der Entwicklung von Regelungen ist insbesondere zu beachten:

- Es sollte gefordert werden, daß in den Sicherheitsbetrachtungen eine Auseinandersetzung mit der Bedienkonzeption (nach einem der in diesem Bericht dargestellten oder einem alternativen Verfahren) erfolgt.
- Es sollten über die Einzelfehlerbetrachtung hinaus auch Handlungsketten betrachtet werden.
- Die Handlungs- bzw. Ereignisketten sind zur besseren Erkennbarkeit potentieller menschlicher Fehlerquellen grafisch darzustellen.

Die Autoren hoffen, mit diesem Bericht zur verstärkten Diskussion zu Human Factor – vor allem auch in technischen Fachkreisen – beizutragen.

## **Begriffsdefinitionen**

### **Anlagenbetreuer vor Ort**

Mit Bedienung, Wartung und Instandhaltung vor Ort in der Anlage betrauter Beschäftigter.

### **Bediener**

Oberbegriff zu Anlagenbetreuer und Wartenfahrer.

### **Bedieneingriffe**

Steuernde oder transportierende Tätigkeiten eines Menschen an einer technischen Anlage.

### **Bedienerstelle (früher: Bedienerfunktion)**

Funktionelle Einheit der Bedienaufgaben, vergleichbar einer MSR- oder PLT-Stelle. Die Bedienerstelle hat als mögliche Eingänge optische und akustische Signale, als mögliche Ausgänge manuelle Eingriffe oder akustische Weitergabe.

### **Bedienkonzeption**

Die Bedienkonzeption behandelt die bestimmungsgemäße Fahrweise und die Kompensation technischer Störungen durch Bedieneingriffe. Sie stellt die Struktur und den Ablauf von Bedienhandlungen zum Betrieb einer Anlage einschließlich deren Zuordnung zu Arbeitsplätzen dar.

### **Bediensicherheit**

Im Sinne dieser Untersuchungen wird Bediensicherheit definiert als

- fehlerfreies "Fahren" einer Anlage
- Kompensation beginnender Störungen durch Handeingriff
- wenn durch den Bediener nicht beeinflußbare Störungen auftreten (z.B. plötzliches Materialversagen), dann Überführen der Anlage in einen sicheren Zustand.

### **Funktionsplan**

Notierung einer Steuerungsaufgabenstellung nach DIN 40719.

### **Meßwartenfahrer**

Bediener in der Meßwarte

**MSR- oder PLT-Stelle**

Funktionelle (realisierungsunabhängige) Darstellung der Automatisierungsfunktionen an einer Meßgröße (MSR = Meß-, Steuer-, Regelungstechnik; PLT = Prozeßleittechnik).

**PAAG (Prognose – Auffinden der Ursachen – Abschätzen der Auswirkungen – Gegenmaßnahmen, vgl. IVSS 2000)**

Verfahren zur systematischen Gefahrenanalyse durch Anwendung von Leitworten:

- |                   |   |
|-------------------|---|
| - nein/nicht      | Sollfunktion wird nicht ausgeführt                |
| - mehr            | quantitativer Zuwachs (Stoff, Wärme, Druck, Zeit) |
| - weniger         | quantitative Abnahme (Stoff, Wärme, Druck, Zeit)  |
| - sowohl als auch | qualitativer Zuwachs                              |
| - teilweise       | qualitative Abnahme                               |
| - Umkehrung       | logische Umkehrung der Sollfunktion               |
| - anders als      | andere Betriebszustände                           |

**Prozeßablaufplan (PRAP)**

Funktionelle (realisierungunabhängige) und prüfbare (auf Vollständigkeit und Widerspruchsfreiheit) Darstellung einer Steuerungsaufgabenstellung

**Schichtführer**

Vorgesetzter zu Wartenfahrer und örtlichem Anlagenbetreuer

**Störungskompensationsgraph**

Graphische Darstellung der Wechselwirkung von Schutzsystem und Bedienereingriffen zur Abwendung der Wirkungen von Störungen. In der Regel ankoppelnd an ein tabellarisches Verfahren zur Störungsanalyse, z.B. PAAG-Verfahren, und unter Berücksichtigung von voneinander unabhängigen Ereignisketten.

## Literatur

Autor	Titel
A.D. Little	Überprüfung der Organisation des Sicherheitsmanagements der Hoechst AG, Gutachten im Auftrag der Staatl. Ämter für Immissions- und Strahlenschutz, Frankfurt am Main und Wiesbaden, 30.08.93
Adams, H.W.	Integriertes Management-System für Sicherheit und Umweltschutz: Generic-Management-System. München/Wien 1995
Adams, H.W.	Integrierte Management-Systeme in der chemischen Industrie. Chemie Technik, 25. Jahrgang (1995) Nr. 4
Adams, H.W.; Helm, A.	Prüfen Sie den Handlungsbedarf, Notfallmanagement muß sein. Hüthig Dok.-Nr. 2146
Adams, H.W.; Jochum, C.	Organisation tut Not - Sicherheitsmanagement für Störfallanlagen, Fa. Hüthig Dokument-Nr. 2831, 1998
Ahrens, W.	Sicherheitsanalysen systematisiert erstellen, TU Bd. 34, Nr. 1, 1993
American Institute of Chemical Engineers (AIChE) (Hrsg.)	Guidelines for Hazard Evaluation Procedures. New York 1985
Arbeitskreis Bediensicherheit	Abschlußbericht des Arbeitskreises Bediensicherheit der Störfallkommission (SFK), Köln 1999
Arnold, U.; Dittrich, G.	Evaluation des ganzheitlichen Sicherheitskonzepts: Gefährdungsindikatoren, Psychologie der Arbeitssicherheit 8. Workshop, S. 632-642, 1995
Balzer, D.; May, V.; Müller, R.; Schulze, K.-P.	Wissensbasierte Systeme in der Automatisierungstechnik, S. 55-65. München
Bandholz, D.	Organisatorische Anforderungen der Schnittstelle Mensch/Organisation beim Betrieb von Kernkraftwerken, 3. Expertengespräch zum BMU/BfS-Konzept, S. 59-68, Salzgitter, 1994
Bauer, D.	Visuelle Optimierung von monochromen Rasterbildschirmen, Zusammenfassung, Wirtschaftsverlag NW, Verlag für neue Wissenschaft GmbH, Bremerhaven
Bayerisches Staatsministerium für Arbeit und Sozialordnung, Familie, Frauen und Gesundheit	Schriftenreihe Managementsysteme für Arbeitsschutz und Anlagensicherheit, München 1998
Bergmann J.	Einfluß der anforderungsgerechten Gestaltung von Automatisierungsanlagen und Ausführungsbedingungen in Prozeßwarten auf die Projektierung von Automatisierungsanlagen. Dissertation B (Habilitationsschrift), Leipzig 1984.

Bierwagen, T.; Eyferth, K.; Niessen, C.	Modellierung von Fluglotsenleistungen in der Streckenflug- kontrolle, Bericht über die Arbeit des DFG-Projektes, Berlin 1996
Bildungsverbund Chemie und Technik e.V. (BVCT, Hrsg.)	Beispiele für Bedienkonzeptionen in modernen Anlagen, Halle/Saale 1999
Brenk Softwaresysteme	COMPAS - Die Echtzeit-Entscheidungshilfe für das Störfall- Management. Aachen 1998
Bundesamt für Strahlens- schutz (Hrsg.)	Mensch-Maschine-Wechselwirkung in Kernkraftwerken, 3. Expertengespräch zum BMU/BfS-Konzept. Salzgitter 1994
Bundesamt für Umwelt, Wald und Landschaft (BUWAL)	Verordnung vom 27. Februar 1991 über den Schutz vor Störfällen. (Störfallverordnung). SR 814.012. AS 1991 748. Stand: 2. Februar 2000.
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (Hrsg.)	Psychische Belastung und Beanspruchung unter dem Aspekt des Arbeits- und Gesundheitsschutzes, Tagungsbericht. o.J.
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (Hrsg.)	Sprachkommunikation-Störung, Beeinträchtigung und Ein- schränkung. Schriftenreihe. Bremerhaven 1995
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (Hrsg.)	Organisation und Codierung von Bildschirminformationen für Überwachungsstätten, S. 1-50. o.J.
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (Hrsg.)	Amtliche Mitteilungen, Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, 3/98. Bremerhaven 1998
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (Hrsg.)	Überprüfung der Umsetzbarkeit der Empfehlungen der ISO 10075-2 in ein Beurteilungsverfahren zur Erfassung der psychischen Belastung, Schriftenreihe. Bremerhaven
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (Hrsg.)	Beispiele für systematische Sicherheitsbetrachtungen nach TRGS 300 „Sicherheitstechnik“. Dortmund/Berlin 1998
Cenit	Die Lösung in der CAD-Modellverwaltung, Broschüre. Stuttgart 1998
Chemical Manufacturers Association (Ed.)	A Manager's Guide to Reducing Human Errors – Improving Human Performance in the Chemical Industry, Washington, DC 1990
Chmiel, N.; Wall, T.	Fault prevention, job design and the adaptive control of advanced manufacturing technology, Applied psychology: an international review, p. 455-473. 1994
Christiandl, H.	Schwerpunkte, Aktivitäten und Ziele des BMU/BfS-Konzeptes zum Themenbereich "Human Factors (HF)", 2. Experten- gespräch zum BMU/BfS-Konzept Mensch-Maschine- Wechselwirkungen in Kernkraftwerken, Salzgitter, 1992
Clariant International Corporate ESHA (Hrsg.)	Learning Lessons No. 1, der Clariant Konzernabteilung für Umweltschutz, Sicherheit und Gesundheitsschutz, Muttenz/Schweiz 12/97

Clausen, J.; Fichter, K.; Arndt, H.-K.	Materialien zum betrieblichen Umweltmanagement und Umweltcontrolling, UBA-TEXT 12/95. Berlin
Colas, A.	Human Factors and Safety-Performance-Quality in Operations at Electricite de France's Nuclear Power Plants, p. 91-117, Nuclear Power Plant Operations
Comelli, G.	Arbeitssicherheit als Führungsaufgabe: Psychologische Aspekte der Führung - bezogen auf die Sicherheitsarbeit, Psychologie der Arbeitssicherheit 6. Workshop, 1991, S. 15-41. Heidelberg, 1992
Council on Environmental Quality	Clean Air Act. 42 U.S.C. s/s 7401 et seq. (1970). Clean Air Act Amendments November 15, 1990
Damke, S.; Pfister, H.-R.; Jungermann, H.	WinGHOST - Ein interaktives Computerprogramm zur Strukturierung von Zielen und Bewertung von Alternativen, Verlässlichkeit Mensch-Maschine-Systeme 1. Berliner Werkstatt, TU Berlin. 1995
DECHEMA	Vereinfachte Risikobeurteilung verfahrenstechnischer Anlagen, Tagungsinhalt, Frankfurt am Main 1998
Deutsche Forschungsanstalt für Luft- und Raumfahrt e.V (Hrsg.)	Schlußbericht zum Projekt "Aufbau eines Betriebsdatensystems als Metadatenbank zur Betriebsführung und Beherrschung von Störfällen"
Dörner, D.	On the difficulties people have in dealing with complexity, Simulation & Games Vol. 11 No. 1, S.87-106. 1980
Dörner, D.	Die Logik des Mißlingens – Strategisches Denken in komplexen Situationen. Reinbeck 1989
Dörner, D. et al.	Lohhausen-Vom Umgang mit Unbestimmtheit und Komplexität. Bern/Stuttgart/Wien 1983
Dörner, D.; Schaub, H.	Errors in Planning and Decision-making and the Nature of Human Information Processing, Applied Psychology: An international Review , S.433-453, 1994
Dritte StörfallVwV	Dritte Allgemeine Verwaltungsvorschrift zur Störfall-Verordnung vom 23.12.1995 (GMBI. 1995 Nr. 38, S. 782)
Dülsen, U.; Tschiedel, K.; Hermann, B.; Kämpf, K.; Müller, R.	Bediensicherheit störfallrelevanter Anlagen, Technische Überwachung 41 (2000) Nr. 5 – Mai, S 57-63
Dumpert, H.-D.; Knaak, J.-D.; Barduna, K.; Stuhrmann, H.-B.	Verbesserungsmöglichkeiten für die Effektivität des Sicherheitsmanagements, Forschungsbericht RW TÜV, März 1994
Eckhardt, D.; Otto, J.; Steidinger, M.	Grundzüge für eine Mustersicherheitsbetrachtung zum Delaborieren von Lagermunition, Schriftenreihe. 1993
Eisgruber, H.	3. VGB-Konzept zur Optimierung der Mensch-Maschine-Schnittstelle (Human-Factors-System) der Deutschen Kernkraftwerkbetreiber, Expertengespräch zum BMU/BfS-Konzept, S. 127-135. 1994
Eisgruber, H.	The VGB Human Factors System, Human Factors-Maßnahmen der Kernkraftwerks Betreiber zur Optimierung der Mensch-Maschine-Schnittstelle, In: Workshop on Human Performance in Chemical Process Safety, OECD. 1997

Elke, G.; Stapp, M.; Zimmermann, D.	Evaluation des ganzheitlichen Sicherheitskonzeptes in einem Tagebau, Psychologie der Arbeitssicherheit 8. Workshop, S. 622-631. 1995
Environment Agency	COMAH Guideline: Statutory Instruments 1999 No. 743. Health and Safety: The Control of Major Accident Hazards Regulations 1999. March 11th. 1999
Environmental Protection Agency (EPA)	Accidental Release Prevention Requirements: Risk Management Planning. 40 CFR Part 68 issued on June 20, 1996
Erste StörfallVwV	Erste Allgemeine Verwaltungsvorschrift zur Störfall-Verordnung vom 20.9.1993 (GMBI. 1993 S. 582)
Eyferth, K; Bierwagen, T.; Helbing, H.	Mentale Informationsverarbeitung von Fluglotsen, Verlässlichkeit von Mensch-Maschine-Systeme 1. Berliner Werkstatt, TU Berlin. 1995
Faßmann, W.	Nutzbarmachung neuer Informationstechnologien zur Verbesserung der Mensch-Maschine-Schnittstelle insbesondere in Kernkraftwerkswarten, 3. Expertengespräch zum BMU/BfS-Konzept, S. 72-87, Salzgitter 1994
Feldhaus, G.	Umweltnormung und Deregulierung. In:DIN-Mitteilung 76, 1997, Nr. 10, S. 680-686
Frank, M.; Wilpert, B.	Weiterentwicklung der Erfassung und Auswertung von meldepflichtigen Vorkommnissen und sonstigen registrierten Ereignissen beim Betrieb v. Kernkraftwerken hinsichtlich mensch. Fehlverhaltens, 3. Expertengespräch zum BMU/BfS-Konzept, S. 25-43, Salzgitter 1994
Freitag M.; Miller, R.; Fahlbruch, B.; Wilpert, B.	Ereignisanalyse im Kontext organisationellen Lernens, Psychologie der Arbeitssicherheit 8. Workshop, S. 120-132 , 1995
Frese, M.	Errors, error detection and error recovery, Applied psychology: an international review
Gaßner, K.	Ein Hypertextsystem zur Entscheidungshilfe bei der Diagnose von Störungen am Revolverkopf einer CNC-Drehmaschine, Verlässlichkeit von Mensch-Maschine-Systeme 1. Berliner Werkstatt, TU Berlin. 1995
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH	Ergebnisprotokoll über die 15. Sitzung des Arbeitskreises Bediensicherheit der SFK, Köln 2/1999
Gewerbeaufsicht NRW	Gesundheitsschutz am Arbeitsplatz. Jahresbericht 1993
Giesa, H.-G.; Timpe, K.-P.	Prospektive Analysenmethoden im Rahmen systematischer Sicherheitsbeurteilung, Psychologie der Arbeitssicherheit 8. Workshop, S. 94-106, 1995
Grauf, E.	Erfahrungen und Erkenntnisse aus Sicht der Betreiber: Schulung für den Notfallschutz, 2. Expertengespräch zum BMU/BfS-Konzept, S. 97-109, Salzgitter 1992
Graul, H.-P.; Krauße, H.-G.	Erfahrungen beim Einsatz rechentechnischer Hilfsmittel zur Projektierung von Binärsteuerungen. msr (1987) 6, S. 265-267
Hacker, W.	Was sind Human Factors und was leisten sie?

Hänsgen, C.; Hermann, E.; Merboth, H.	Arbeitsanforderungen, psychische Gesundheit und sicheres Verhalten, Psychologie der Arbeitssicherheit 8. Workshop, S. 308-322, 1995
Hauptmanns, U.; Rodríguez, J.	Untersuchungen zum Arbeitsschutz bei An- und Abfahrvorgängen von Chemieanlagen. Bremerhaven 1994
Hering, N.	Mensch & High Tech, Teil 1: Denkstrukturen des Menschen, Hüthig Dokument Nr. 1961, 1996
Hering, N.	Mensch & High Tech, Teil 2: Fehlerquelle Mensch im Mensch/ Maschinen-system, Fa. Hüthig: Dokument-Nr. 2089, Stand 1996
Hering, N.	Mensch & High Tech, Teil 3: Fehlerquelle Systematik, Fa. Hüthig: Dokument-Nr. 2089, Stand 1996
Hering, N.	Mensch & High Tech, Teil 4: Kommunikationsprobleme im Interaktionsbereich Mensch und Anlage, Fa. Hüthig: Dokument-Nr. 2089, Stand 1997
Hessische Landesanstalt für Umwelt (HLfU)	Leitfaden Integrierte Managementsysteme, HLfU-Schriftenreihe Umweltplanung Arbeits- und Umweltschutz, Heft 240. Wiesbaden 1997
Hessisches Ministerium für Frauen, Arbeit und Sozialordnung	Leitfaden Arbeitsschutzmanagement Teil I „Anleitung zur Implementierung eines Arbeitsschutzmanagementsystems“, Teil II „Inhalt und Struktur eines Arbeitsschutz-Management-Handbuchs“, Teil III „Beispielsammlung“, 1997
Hinz, W.	Bediensicherheit in der internationalen Normung, In: Workshop on Human Performance in Chemical Process Safety, OECD 1997
Hoechst Marion Roussel Deutschland GmbH (Hrsg.)	Sicherheitsmaßnahmen bei der Änderung in und an Anlagen, Arbeitsweisen und Verfahrensabläufen sowie bei der Durchführung von Instandhaltungsarbeiten, SGU Richtlinie IV.2, Höchst, 1/1999
Hoffmann, B.	Gefährdungsanalyse - Das berufsgenossenschaftliche Konzept im europäischen Kontext, Psychologie der Arbeitssicherheit 8. Workshop, S. 450-457, 1995
Hoheisel, D.	Bestimmung der Qualität von Verfahren zur Sicherheitsanalyse, Psychologie der Arbeitssicherheit 8. Workshop, S. 429-439, 1995
Hyland, M.A.	Projekte unter der Lupe - Fehlervermeidung bei der Anlagenplanung durch Project Challenging, Chemie Technik 27. Jhg., Nr. 8, 1998
IVSS (Hrsg.)	Das PAAG-Verfahren. Methodik, Anwendung, Beispiele. Heidelberg 2000
Kästner, C.	EG-Recht und Qualitätssicherungssysteme, Psychologie der Arbeitssicherheit 8. Workshop, S. 418-428, 1995
Keßl, G.M.	Motivation per Geldbeutel, Chemie Technik, 29. Jahrgang (2000), Nr. 1
Kirsch, B.	Zeit ist kostbar – die Mitarbeiterbesprechung, Chemie Technik, 29. Jahrgang (2000), Nr. 1

Kirschstein, G.; Weller, E.	Psychologie der Arbeitssicherheit 6. Workshop, 1991, S. 117/118. Heidelberg 1992
Konradt, U.	Betriebliches Umweltmanagement in der metallverarbeitenden Industrie, Psychologie der Arbeitssicherheit 8. Workshop, S. 567-583, 1995
Korea Office for Safety and Health (OSH)	Korea OSH Act Industrial Safety and Health Act. Act No. 4220, Jan. 13, 1990. Last amended by Act No. 6104, Jan. 7; 2000.
Kostka, S.	Studie zur aktuellen Einschätzung von Umweltmanagementsystemen, Studie im Rahmen einer Dissertation an der TU Berlin. 1994
Kraiss, K.-F.	Entscheidungshilfen in hochautomatisierter Systemingenieurpsychologie, Band 2 der Enzyklopädie der Psychologie, S. 455-475, Verlag für Psychologie, Göttingen
Künzler, K.; Grote, G.	SAM-ein Leitfaden zur Bewertung von Sicherheitskultur in Unternehmen, Psychologie der Arbeitssicherheit 8. Workshop, S. 78-93, 1995
Landesanstalt für Arbeitsschutz NRW	Sicherheit und menschengerechte Gestaltung von Leitwarten. Minden 1996
Littinski, R.	Das Sicherheitskonzept der Deutschen Shell AG, Zeitschrift für Arbeits- und Organisationspsychologie, S. 84-86, 1991 (35)
Ludborzs, B.; Nold, H.; Rüttinger, B. (Hg.)	Psychologie der Arbeitssicherheit 8. Workshop. Voraussetzungen für betriebliche Gestaltungs-, Kommunikations- und Qualifizierungskonzepte in der hochautomatisierten prozeßverarbeitenden Industrie. 1995.
Machauer-Bundschuh, S.	Dimensionen der Auswirkungen partizipativer Sicherheitsarbeit, Psychologie der Arbeitssicherheit 6. Workshop, 1991, S. 388-395. Heidelberg, 1992
Merck KGaA (Hrsg.)	Sicherheit mit Merck (Broschüre), Darmstadt 5/97
Miller, R. et al.	Analyse von sicherheitsrelevanten Ereignissen in verfahrenstechnischen Anlagen, UBA-TEXT 98/79. Berlin 1998
Miller, R. et al.	Unterstützung der Betriebssicherheit durch neue Informationstechnologie in Zusammenhang mit modernen Managementstrukturen, In: Workshop on Human Performance in Chemical Process Safety, OECD 1997
Miller, R. et al.	Analyse von sicherheitsrelevanten Ereignissen in verfahrenstechnischen Anlagen, UBA Texte 98/79. Berlin 1998
Ministère de l'Aménagement du Territoire et de l'Environnement	Arrêté du 10 mai 2000 relatif à la prévention des accidents majeurs impliquant des substances ou des préparations dangereuses présentes dans certaines catégories d'installations classées pour la protection de l'environnement soumises à autorisation
Ministerie van Volksbouwvesting, Ruimtelijke Ordening en Milieubeheer	Besluit van 27 mei 1999 tot vaststelling van het Besluit risico's zware ongevallen (BRZO) 1999. Staatsblad 1999 234.

Moch, E.; Pietsch, K.-J.	Sicherheitsmanagement bei kleinen und mittleren Unternehmen, UBA-TEXT 67/98. Berlin 1998
Mohr, G.; Figgen, M.	Staatliche Gesundheitsüberwachung in arbeitspsycho-logischen Problembereichen, Psychologie der Arbeitssicherheit 8. Workshop, S. 338-350. 1995
Monteau, M.	Arbeitssicherheit und Psychologie in Frankreich, in Psycho-logie der Arbeitssicherheit 8. Workshop, S 44-66. 1995
Müller, F.	CEA-Tool zur Unterstützung der Bilanzierung von Bedienerbelastungen in der Entwurfsphase automatisie-rungstechnischer Systeme, Dissertationsschrift, TH Leipzig 1993
Müller, R.	Computer Aided Problem Formulation of Control Problems, IFAC-Symposium on Design Methods of Control Systems, Zürich 1991
Müller, R.	New Problems and Tools for Planning of Control and Super-visory Systems, In: Wissen und Wissenschaft - Kongreß-Programm der Interkama 1992
Müller, R.	Defizite und Lösungsansätze für die Bediensicherheit störfall-relevanter Anlagen, Psychologie der Arbeitssicherheit 8. Workshop, S. 145-156, 1995
Müller, R.	Probleme und Gedanken zum Erzielen zuverlässiger Bedienkonzepte, In: Workshop on Human Performance in Chemical Process Safety, OECD 1997
Müller, R.	Beiträge zur Störfallvorsorge im Land Brandenburg, Leipzig 1998
Müller, R.	Projektierung von Automatisierungsanlagen. Berlin 1979
Müller, R.	Vorschläge zur Weiterführung der Arbeiten in der OECD zur Thematik Bediensicherheit und Bericht über die Arbeiten in Deutschland, unveröffentlichtes Dokument. 1998
Müller, R.	Vorstellungen zur Weiterentwicklung der Prozeßleittechnik für die Erhöhung der Bediensicherheit. 1998
Müller, R.	Auswertung des OECD-Workshops zur Bediensicherheit, Schlußfolgerungen und Umsetzungsmaßnahmen. 1998
Müller, R.	Forderungen an eine Leitlinie zur Nutzung von Trainingsanlagen zur Erhöhung der Bediensicherheit. Brandenburg 1998
Müller, R.; Engmann, U.; Wolf, H.	Aufbereitung und Prüfung der Aufgabenstellung – eine Voraussetzung für die Effektivität von CAD-Lösungen zur Projektierung automatischer Anlagen. msr 30 (1987) 6, S. 242-246
Müller-Demary, P.; Przygoda, M.	Sicherheitszirkel: Betroffene zu Beteiligten machen, Psycho-logie der Arbeitssicherheit 6. Workshop, 1991. Heidelberg 1992
Müller-Gethmann, H.; Musahl, H.-P.	Lernparadigmen oder Sicherheitsmotive, Psychologie der Arbeitssicherheit 8. Workshop, S. 757-771, 1995

Musahl, H.-P.	Lernpsychologische Ansätze zur Erklärung des Verhaltens in "gefährlichen" Situationen, Psychologie der Arbeitssicherheit 8. Workshop, S. 742-756, 1995
Musahl, H.-P. et al.	Arbeitssicherheit durch Gefahrenkenntnis: Evaluation und Transfer eines Programmes, Psychologie der Arbeitssicherheit 8. Workshop S. 772-789, 1995
N.N.	Analytische Behandlung des menschlichen Fehlverhaltens, Untersuchungen zum Arbeitsschutz bei An- und Abfahrvorgängen von Chemieanlagen (S. 125-131)
N.N.	Augen zu und durch? Systematisierung des Instandhaltungsmanagements, Chemie Technik 27. Jhg. 1998 (3)
Nachreiner, F.	Psychische Belastung und Beanspruchung als Gegenstand der ISO-Normungsarbeit, Carl-von-Ossietzky-Universität, Oldenburg
Nachreiner, F.; Meyer, I.; Schomann, C.; Hillebrand, M.	Überprüfung der Umsetzbarkeit der Empfehlungen der ISO 10075-2 in ein Beurteilungsverfahren zur Erfassung der psychischen Belastung. Dortmund 1998
NAMUR (Hrsg.)	Anforderungen an Systeme zur Rezeptfahrweise, NAMUR Empfehlung NE 33, Leverkusen, Stand 1993
NAMUR (Hrsg.)	Anlagensicherheit mit Mitteln der Prozeßleittechnik, NAMUR-Empfehlung NE 31, Leverkusen, Stand 1993
NAMUR (Hrsg.)	PLT-Räume; Prozeßleitwarten, Leitstände, Nebenräume, Planungshilfe für die konstruktive Gestaltung, NAMUR Arbeitsblatt NE 26, Leverkusen, Stand 1991
NAMUR (Hrsg.)	Management von Trainingssimulatorprojekten. NAMUR Arbeitsblatt NE 60, Leverkusen, Stand 1995
NAMUR (Hrsg.)	Management von Trainingssimulatorprojekten. NAMUR Arbeitsblatt NE 60, Leverkusen, Stand 1995
NAMUR (Hrsg.)	Anwendung der Bildschirmarbeitsplatz-Verordnung in Prozeßleitwarten. Leverkusen, Stand 1998
NAMUR (Hrsg.)	NAMUR-Checkliste für Meßwarten und Leitstände. NAMUR Arbeitsblatt NE 76, Leverkusen, Stand 1997 (dt. und engl.: NAMUR-Checklist for Control Rooms)
NAMUR (Hrsg.)	Besonderheiten von Bildschirmarbeitsplätzen in Meßwarten. NAMUR Arbeitsblatt NE 75, Leverkusen, Stand 1997 (dt. und engl.: Specialties of Screen Work Places in Control Rooms.)
NAMUR (Hrsg.)	Übersicht über NAMUR-Empfehlungen und -Arbeitsblätter, NAMUR Interessengemeinschaft Prozeßleittechnik der chemischen und pharmazeutischen Industrie, Leverkusen, Stand 1998
Oberhagemann, D.	Beschreibung von Safetynet, Firmeninformation. Hamm 1998
Obermeier, O.-P.	Die Kunst der Risikokommunikation. München 1999
Occupational Safety and Health Administration (OSHA)	OSHA Directives: CPL 2-2.45A (REVISED) - Process Safety Management of Highly Hazardous Chemicals Standard – 29 CFR 1910.119 issued on February 24, 1992.

OECD (Hrsg.)	Report of the OECD Workshop on Human Performance in Chemical Process Safety: Operating Safety in the Context of Chemical Accident Prevention, Preparedness and Response. Paris 24.-27.6.1997 (=UBA Texte 61/97, Berlin, 1997)
Packebusch, L.; Wachsmuth, R.	Sicherheitsgespräche – Seminar-Konzept für Sicherheitsbeauftragte, Psychologie der Arbeitssicherheit 6. Workshop, 1991, S. 606-661, Roland Arsanger Verlag, Heidelberg 1992
Rat der EWG	Richtlinie 89/391/EWG des Rates vom 12. Juni 1989 über die Durchführung von Maßnahmen zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Arbeitnehmer bei der Arbeit, Amtsblatt der Europäischen Gemeinschaft Nr. L 183 vom 29/06/1989, S. 1-8
Rat der EWG	Richtlinie 96/82/EG des Rates vom 9. Dezember 1996 zur Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen, Amtsblatt der Europäischen Gemeinschaften Nr. L 10/13 vom 14.1.1997
Reason, J.	Human Error, Performance levels and error types, Department of Psychology, University of Manchester, Cambridge University Press. 1990
Reason, J.	The Chernobyl Errors, Bulletin of The British Psychological Society, S. 201-206, Great Britain, 1987
Reason, J.	Managing the risks of organizational accidents, Ashgate Publishing Ltd. 1997
Reuter H.	Sicherheit im Spannungsfeld von Norm und Individualität, Psychologie der Arbeitssicherheit 8. Workshop, S. 669-673, 1995
Richei, A.	Entwicklung eines Verfahrens zur qualitativen und quantitativen Bewertung von Personalhandlungen in der probabilistischen Sicherheitsanalyse für Kernkraftwerke. Abschlußbericht zum Vorhaben SR 2231: Teil B, Technische Dokumentation. Bochum 1998
Richter, B.	Beurteilung von Sicherheitsmanagementsystemen gefahrenträchtiger Anlagen mit dem Programm SMVP; Essen 1999
Richter, B.; Kuntschner, M.	Rechnergestützte Überprüfung von Sicherheitsmanagementsystemen, Technische Überwachung Nr. 6 (1999)
Richter, G.	Psychische Belastung und Beanspruchung unter dem Aspekt des Arbeits- und Gesundheitsschutzes. Dortmund/Berlin 1998
Ritter, A.; Langhoff T.	Arbeitsschutzmanagementsysteme. Vergleich ausgewählter Standards. Dortmund/Berlin 1998
Rüegsegger, R.	RISIVE: Einbezug von Wissen über menschliches Verhalten in die Arbeitssicherheit, Psychologie der Arbeitssicherheit 8. Workshop, S. 244-255, 1995
Schäffler, L.	Die Bedeutung menschlicher Faktoren aus der Sicht von Behörden und Gutachtern, 3. Expertengespräch zum BMU/BfS-Konzept, S. 188-204, Salzgitter 1994

Schaub, H.; Strohschneider, S.	Die Auswirkungen unterschiedlicher Problemlöseerfahrung auf den Umgang mit einem unbekannten komplexen Problem, Zeitschrift für Arbeits- und Organisationspsychologie, S. 117-126, 1992 (36)
Schmid, S.	Entwicklung einer entscheidungsunterstützenden Methode für das Risikomanagement, Verlässlichkeit von Mensch-Maschine-Systeme 1. Berliner Werkstatt, TU Berlin, 1995
Schmidt, F.	On-Line Trainingssystem für Bedienerschulungen in kleinen und mittleren Unternehmen der Prozeßindustrie, In: Workshop on Human Performance in Chemical Process Safety, OECD 1997
Schmidtke, H.	Handbuch der Ergonomie. München 1989
Schmidtke, H.; Rühmann, H.-P.	Ergonomische Gestaltung von Steuerständen, Forschungsbericht Nr. 191
Schüpphaus, M.; Hagedorn, H.	Relevanzfaktoren im Management von Unternehmen für die Ausprägung des 'Human Factor' im Hinblick auf die Bediensicherheit von Risikoanlagen. Osnabrück, März 2000
Schüz, M.	Werte – Risiko – Verantwortung. Dimensionen des Value Managements. München 1999
Seeberger, R.; Kamm, R.	Evaluation von TQM-Sicherheitszirkeln bei KSB-AG, Psychologie der Arbeitssicherheit 8. Workshop, S. 370-384, 1995
Simon, D.	Lernen im Arbeitsprozeß – Der Beitrag Hackers Arbeitspsychologie und Piagets Entwicklungstheorie, Campus-Verlag, Frankfurt a. Main, New York 1980
Staatliches Amt für Immissions- und Strahlenschutz, Frankfurt (SAIS)	Gutachten zur Organisation der Sicherheit der Hoechst AG, Duisburg 31.08.93
Stadler, P.; Beer, B.	Förderung sicheren Arbeitshandelns bei der Anlagenplanung. Leitfaden für Planer und Arbeitsschutz-Experten. Diagnose & Transfer, Institut für Angewandte Psychologie. München 1999
Steinbach J.	Mündliche Mitteilung, Juli 1999
Steinbach, J.; Antelmann, O.; Lambert, M.	Methoden zur Bewertung des Gefahrenpotentials von verfahrenstechnischen Anlagen und Verfahren. Dortmund/Berlin 1998
Steiner, K.	Eine eindeutige und praxisgerechte Organisation – das Bindeglied zwischen Mensch und Anforderungen des Kernkraftwerkbetriebes, 3. Expertengespräch zum BMU/BfS-Konzept, S. 136-151, Salzgitter, 1994
Störfallkommission	Abschlußbericht der Störfallkommission nach § 51a Abs. 2 BlmSchG, 1997
Störfallkommission	Zur Erhöhung der Bediensicherheit störfallrelevanter Anlagen notwendige Entwicklungen, 1998

Störfall-Verordnung	Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfall-Verordnung – 12. BlmSchV) in der Fassung gemäß Verordnung zur Umsetzung EG-rechtlicher Vorschriften betreffend die Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen. 26. April 2000. Bundesgesetzblatt I Nr. 19
Stuhrmann, H.B.	VISUA für WINDOWS – ein hyperMedia Tool für den sicheren, umweltverträglichen, optimalen wirtschaftlichen Anlagenbetrieb, In: Workshop on Human Performance in Chemical Process Safety, OECD 1997
TAA (Arbeitskreis Anlagenüberwachung)	Richtlinie für die Durchführung des Meinungs- und Erfahrungsaustausches für Sachverständige nach § 29a BlmSchG, Dok-Nr. TAA/97/2, Fassung 1997
TAA (Arbeitskreis Anlagenüberwachung)	Ganzheitliche Anlagenüberwachung, Abschlußbericht, Januar 1996
Umweltbundesamt (Hrsg.)	"Lernen aus Erfahrung-Systematische Analyse von sicherheitsbedeutsamen Ereignissen in der verfahrenstechnischen Industrie", UBA-Fachgespräch, Berlin 1998
Uth, H.-J.	Störfallmanagement am Beispiel der Chemischen Industrie, UBA-TEXT 2/95. Berlin 1995
VdS Schadenverhütung GmbH (Hrsg.)	Sicherheitsorganisation-Merkblatt zur Risikobewertung, VdS 2555. Köln 1997
Wieland-Eckelmann, R.	Methoden der Belastungs- und Beanspruchungsermittlung und ihre betriebliche Umsetzung. Wuppertal o.J.
Willumeit, H.P.; Kolrep, H. (Hrsg.)	Verlässlichkeit von Mensch-Maschine-Systemen, 1. Berliner Werkstatt Mensch-Maschine-Systeme, ZMMS-Spektrum, Bd. 1. Berlin 1995
Wilpert, B.	Psychologische Aspekte der Systemsicherheit, Psychologie der Arbeitssicherheit 8. Workshop, S. 70-77, 1995
Wilpert, B.; Becker, G.	Anforderungen an neue Reaktorkonzepte aus organisationspsychologischer und ergonomischer Sicht, Mensch-Maschine-Wechselwirkung in Kernkraftwerken, 3. Expertengespräch zum BMU/Bfs- Konzept, S. 205-210, Salzgitter, 1994
Wilpert, B.; Klumb, P.	Störfall in Biblis A, Zeitschrift für Arbeitswissenschaft 45 (17), TU Berlin, 1991/1
Wilpert, B.; Miller, R.; Fahlbruch, B.	SOL: Sicherheit durch Organisationales Lernen, Technische Überwachung 38 (4), S. 40 43. Düsseldorf 1997
Wilpert, B.; Miller, R.; Fahlbruch, B.	Umsetzung und Erprobung von Vorschlägen zur Einbeziehung von Human Factors (HF) bei Meldungen und Ursachenanalyse in Kernkraftwerken, Verlässlichkeit Mensch-Maschine-Systeme 1. Berliner Werkstatt, TU Berlin 1995
Windel, A.; Zimolong, B.	Den Arbeitsplatz Leitwarte unter die Lupe genommen. 1993
Wolf, H.	Betriebshandbücher - Instrumente zur Integration des Arbeits-, Gesundheits- und Umweltschutzes in die Unternehmensstrategie, Psychologie der Arbeitssicherheit 8. Workshop, S. 584-590, 1995

Zapf, D.; Reason, J.	Human Errors and Error Handling, Applied Psychology: An international Review, p. 427 432, 1994
Zimolong, B.	Sicherheitsmanagement: Der Zusammenhang zwischen Sicherheitsorganisation, Schulung und Sicherheitsstandard; aus: Zimolong, Trimpop 1991
Zimolong, B.; Giesel, R.	Einführung eines ganzheitlichen Sicherheitskonzeptes in einem Braunkohlebergwerk, Psychologie der Arbeitssicherheit 8. Workshop, S. 612-621, 1995
Zimolong, B.; Trimpop, R. (Hrsg.)	Psychologie der Arbeitssicherheit, 6. Workshop 1991, Heidelberg
Zimolong, B.; Stolte-Fürst, B.	Können Fachleute die Wahrscheinlichkeit von Arbeitsfehlern einschätzen?, Zeitschrift für Arbeits- und Organisationspsychologie, S. 151-157, 1991 (35)
Zülich, G.; Stowasser, S.; Fischer, A.E.	Ergonomische Aspekte der Software-Gestaltung. Teil 9: Internet und World Wide Web - zukünftige Aufgaben der Kommunikationsergonomie. In: ErgoMed 2/1999.
Zülich, G.; Stowasser, S.; Fischer, A.E.	Ergonomische Aspekte der Software-Gestaltung. Teil 8: Entwicklung einer Software unter Berücksichtigung ergonomischer Gesichtspunkte. In: ErgoMed 1/1999.
Zülich, G.; Stowasser, S.; Fischer A.E.	Ergonomische Aspekte der Software-Gestaltung. Teil 7: Vorgehensweise bei der Evaluation von Software am Beispiel einer rechnerunterstützten Normkonformitätsprüfung. In: ErgoMed 6/1998.
Zülich, G.; Stowasser, S.; Fischer, A.E.	Ergonomische Aspekte der Software-Gestaltung. Teil 1: Einführung in die Software-Ergonomie. In: ErgoMed 6/1997.
Zülich, G.; Stowasser, S.; Fischer, A.E.	Ergonomische Aspekte der Software-Gestaltung. Teil 2: Ansätze aus der Psychologie der visuellen Wahrnehmung. In: ErgoMed 6/1997.
Zülich, G.; Stowasser, S.; Fischer, A.E.	Ergonomische Aspekte der Software-Gestaltung. Teil 3: Codierung von Informationen. In: ErgoMed 1/1998.
Zülich, G.; Stowasser, S.; Fischer, A.E.	Ergonomische Aspekte der Software-Gestaltung. Teil 4: Anordnung von Informationen. In: ErgoMed 2/1998.
Zülich, G.; Stowasser, S.; Fischer, A.E.	Ergonomische Aspekte der Software-Gestaltung. Teil 5: Gestaltung des Dialogs zwischen Benutzer und Rechner. In: ErgoMed 3/1998.
Zülich, G.; Stowasser, S.; Fischer, A.E.	Ergonomische Aspekte der Software-Gestaltung. Teil 6: Evaluation von Software. In: ErgoMed 4/1998.
Zweite StörfallVwV	Zweite Allgemeine Verwaltungsvorschrift zur Störfall-Verordnung vom 27. April 1982 (GMBI. 1982 S. 205, geändert durch Nr. 6 1. StörfallVwV vom 20.9.1993)

**Anhang: Einschlägige Normen**

DIN/ISO 10075	Ergonomische Grundlagen bezüglich psychischer Arbeitsbelastungen Juni 2000 Teil 2 Gestaltungsgrundsätze
DIN 19 226	Teil 1 Leittechnik, Regelungs- und Steuerungstechnik, allgemeine Grundbegriffe Febr. 1994 <i>Funktionelle Schemen</i>
	Teil 2 Begriffe zum Verhalten dynamischer Systeme Febr. 1994 <i>Regelungstheorie</i>
	Teil 3 Begriff zum Verhalten von Schaltsystemen Febr. 1994 <i>Theorie zu Schaltfunktionen</i>
	Teil 4 Begriffe für Regelungs- und Steuerungssysteme Febr. 1994
	Teil 5 Funktionelle Begriffe Febr. 1994 <i>Funktionelle regelungstechnische Beschreibung</i>
	Teil 6 Begriffe zu Funktions- und Baueinheiten Sept. 1997 <i>Funktionsorientierte Bezeichnungen von Komponenten</i>
DIN 19 227	Leittechnik, Grafische Symbole und Kennbuchstaben für die Prozeßleittechnik
	Teil 1 Darstellung von Aufgaben Okt. 1993
	Teil 2 Darstellung von Einzelheiten Febr. 1991 <i>Bauteilpläne für einzelne Regelkreise und Steuerketten</i>
DIN 19 232	Leittechnik, Prozeßautomatisierung Entwurf Juli 1998 <i>Automatisierung mit Prozeßrechnersystemen, hauptsächlich Begriffe</i> <i>Für die Bediensicherheit sind u. a. interessant:</i> <ul style="list-style-type: none"><li>• <i>Unterbrechungsreaktionszeit</i></li><li>• <i>Eingaberate</i></li><li>• <i>Ausgaberate</i></li></ul>

DIN 19 235	Messen, Steuern, Regeln, Meldung von Betriebszuständen, März 1985 <i>Begriffe, Graphische Kodierung zu Kontrolleuchten, u. a. schwarz-weiß-zeichnerische Darstellung verschiedener Leuchtenfarben</i>
DIN V 19 250	Leittechnik, grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen Vornorm Mai 1994 <i>Diagramm zur Risikoreduzierung, Risikograph- und Anforderungsklassen, d.h. siebenstufige Klassifizierung der Sicherheitsansprüche an eine Steuerung abhängig von den Auswirkungen und der Zahl der Betroffenen</i>
DIN V 19 251	Leittechnik, MSR-Schutzeinrichtungen, Anforderungen und Maßnahmen zur gesicherten Funktion Vornorm Febr. 1995 <i>Darstellung aktiver und passiver Fehler, Maßnahmen zur Fehlervermeidung</i>
DIN V 19 256	Leittechnik, Einrichtungen der Prozeßleittechnik (PLT) für industrielle Anlagen, Leitfaden für Planung, Erstellung und Betrieb <i>Begriffe, allgemeine Hinweise zur Sicherung der Funktion, u. a. speziell zur Fehlerliste, nur Betrachtung von Einzelfehlern mit dem Ziel der späteren Festlegung von Maßnahmen zur Beherrschung nicht akzeptierbarer Fehler</i>
DIN 28 004	Fließbilder verfahrenstechnischer Anlagen
Teil 1	Begriffe, Fließbildarten, Informationsinhalt Mai 1988 <i>Verfahrensfließbilder, RI-Fließbild</i>
Teil 2	Zeichnerische Ausführung Mai 1988 <i>Darstellung der Wirkungslinien</i>
Teil 3	Graphische Symbole für Apparate Mai 1988 <i>Details, der Symbole, u. a. auch für Automatisierungsfunktionen, in diesem Fall sind die in DIN 19 227 geregelten Details heranzuziehen</i>
Teil 4	Kurzzeichen Mai 1977 <i>Abkürzungen zur Kennzeichnung der maschinentechnischen Ausrüstungsteile</i>
Teil 10	Begriffe Aug. 1976
Teil 30	Graphische Symbole, Ergänzung Entwurf April 1983

DIN 33 414	Ergonomische Gestaltung von Warten
Teil 1	Sitzarbeitsplätze April 1995 <i>Geometrie-Abmessungen</i>
Teil 2	Kognitive Faktoren Entwurf Sept. 1995 <i>wesentliche Überlegungen und Definitionen zur Informationsverarbeitung im bedienenden Menschen und einer darauf ausgerichteten zweckmäßigen Darstellung</i>
Teil 3	Gestaltungskonzept Entwurf Juni 1995 <i>u. a. Anforderungsdefinitionen, Einführung des Begriffes "Dimensionalität" für die notwendige Auswahl des Bedieners zwischen verschiedenen Eingriffsmöglichkeiten oder -wegen, d. h. es wird nicht die Gleichzeitigkeit von Aufgaben, sondern die Mehrdeutigkeit der Eingriffsmöglichkeit zur Lösung einer Aufgabe betrachtet Festlegung der Entwurfsüberprüfung durch erfahrene Operatoren</i>
Teil 4	Gliederungsschema, Anordnungsprinzipien Okt. 1990 <i>Auswahl, Anordnung, Zuordnung der . Arbeitsplätze . Wartenkomponenten Anordnung der Arbeitsmittel (Instrumente, Schalter) auf den Wartenkomponenten</i>
DIN 66 233	Bildschirmarbeitsplätze
Teil 1	Begriffe Apr. 1993
Teil 2	Übersicht von Begriffen aus anderen Normen Dez. 1984
DIN 66 234	Bildschirmarbeitsplätze
Teil 3	Gruppierung und Formatierung von Daten März 1981 Beiblatt: Hinweise und Beispiele Entwurf März 1983
DIN EN 894-2	Sicherheit von Maschinen, Ergonomische Anforderungen für die Gestaltung von Anzeigen und Stellteilen <i>Erkennbarkeit, Anforderungen an Identifizierung und Interpretation, taktil unterscheidbare Griffe, Gruppierung von Anzeigen</i>
DIN 66 230	Informationsverarbeitung, Programmdokumentation Jan. 1981

DIN 66 231	Informationsverarbeitung, Programmentwicklungsdocumentation Okt. 1982
DIN 66 232	Informationsverarbeitung, Datendokumentation Aug. 1985
DIN 31 000	Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse März 1979 <i>Schutz der Beschäftigten vor Bewegung und Energie, Verriegelung von Stellteilen, gefahrlose Lage von Betätigungslementen</i>
Teil 2	Begriffe Dez. 1987 <i>Risiko, Definition als Produkt aus Eintrittswahrscheinlichkeit und Schadensausmaß</i>
Teil 10	Anforderungen an die im Bereich der Elektrotechnik tätigen Personen Apr. 1993
DIN 31 001	Sicherheitstechnische Gestaltung technischer Erzeugnisse, Schutzeinrichtungen, Werkstoffe, Anforderungen, Anwendungen <i>Schutz vor Bewegung und Energie</i>
DIN 33 409	Handzeichen zum Einweisen Apr. 1983
DIN 33 410	Sprachverständigung in Arbeitsstätten unter Einwirkung von Störgeräuschen Dez. 1981 <i>Wechselbeziehung zwischen Störgeräusch, Stimm aufwand und Abstand</i>
DIN IEC (Sec)423	Anwendungsleitfaden zur menschlichen Zuverlässigkeit Teil 1: Hauptabschnitte 1 bis 4 <i>Handbuch- bzw. Lehrbuchartige Zusammenstellung der überwiegend qualitativen Erkenntnisse.</i> <i>Ausführliche und umfangreiche Liste von Begriffsdefinitionen.</i> <i>u.a. Darstellungen zu Irrtumsmechanismen, zum Erreichen der Betreiberqualifikation (Lernen, Ausbildung, Training, Ausbildungssimulatoren)</i> <i>Klassifizierung des menschlichen Fehlverhaltens in: Versehen, Mißgriffe, Fehler, Vergehen</i> <i>Darstellung der menschlichen Leistungsgrenzen bei sequentieller Bedienung (qualitativ) und bei simultaner Bedienung (max. 7 +2 „psychologische Einheiten“)</i>

VDI/VDE 2180	Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der MSR-Technik  <i>Bereitstellung von Informationen über den Prozeß für die Überwachung, u. a. durch einen Bediener. Keine Aussagen zur Bediensicherheit im hier behandelten Sinne.</i>
VDI/VDE 3541	Steuerungseinrichtungen mit vereinbarter gesicherter Funktion  <i>Sicherung der Gerätezuverlässigkeit ohne Eingehen auf Bedienung</i>
VDI/VDE 3542	Sicherheitstechnische Begriffe ohne „Bediensicherheit“
VDI/VDE 3546	Blätter 3 und 5: Konstruktive Gestaltung von Prozessleitwarten <i>ergonomische Gestaltung der Informationsaus- und eingabe an und vom Menschen ohne Eingehen auf die Verarbeitbarkeit im Menschen</i>
VDI 4003	Allgemeine Forderungen an ein Sicherungsprogramm, Klasse A – Ergonomische Aspekte  <i>Schutz des Menschen in der Störfallsituation, Gestaltung der Umgebung zur Minimierung der Beanspruchung, anthropometrische Gestaltung, Forderungen an die Qualifikation.</i>