Texte 11/01

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 -

Begoña Hermann, EcoTeam GmbH, Trier
Uwe Dülsen, Schwedt/Oder
Klaus Kämpf, Prognos GmbH, Basel
Rainer Müller, Leipzig
Kerstin Tschiedel, Schwedt/Oder

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-bestimmungsgemäßen 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 Normalbetrieb 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 Bericht 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-Aspekten 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, 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.

Üblicherweise wird der bedienende Mensch über das planmäßige Fahren einer verfahrenstechnischen Anlage im Normalbetrieb hinaus zum Beherrschen 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 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.).

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 Verhaltenen 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.

- π To develop new methods to determine the requirements to be met by operators (compared with the objective human limits).

- π To analyse existing rules and instruments aimed at taking into account the human factor and to derive recommendations for their further development.

- π To check the options to include human factor aspects in existing corporate management systems.

- π 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 be 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 rquired 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 automatisation, thus requiring more staff.

Several representation forms for the operating concept of **continuous processes** were analysed. Existing plants where 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 where 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 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.