

# Grundlagen der technischen Risikoanalytik

## Spezielle Problematiken II - Humanfaktoren



## Humanfaktoren im Cobra Führerstand



Der Cobra-Führerstand wurde in enger Zusammenarbeit zwischen der Industrie und den Verkehrsbetrieben gestaltet, um den modernsten Erkenntnissen bezüglich Ergonomie gerecht zu werden. Eine grosse Frontscheibe verschafft einen guten Ausblick und vermeidet tote Winkel.



Der Fahrshalter ist auch beim Cobra als Handrad ausgeführt. Da auf keine Kompatibilitäten mit bestehenden Fahrzeugen Rücksicht genommen werden musste, konnte nun eine echte Geschwindigkeitssteuerung mit Tempomatfunktion eingebaut werden. Der Fahrshalter kann individuell positioniert werden.



Zahlreiche Angaben über den aktuellen Zustand des Fahrzeugs können über den Bildschirm abgerufen werden. Im Normalbetrieb werden die IBIS-Funktionen (Linie, Kurs, Zeitabweichung) angezeigt, im Fall von Fehlbedienungen zeigt der Bildschirm entsprechende Meldungen sowie Abhilfemassnahmen.

## Einbezug der Humanfaktoren: (1/2)

- Beachtung der menschlichen Faktoren
- Darstellung von menschlichen Fehlern und menschlicher Zuverlässigkeitsanalyse:
  - Accident Initiation and Progression Analysis (AIPA)
  - Technique for Human Error Rate Prediction (THERP)
  - Success Likelihood Index Methodology (SLIM)
- Zusammenfassung
- Referenzen

## Einbezug der Humanfaktoren: (2/2)

### Nicht-Beachtung menschlicher Fehler resultiert in:

- Missachtung wesentlicher Faktoren,
- unrealistische Analyse-Ergebnisse als menschliche Faktoren tragen bedeutsam zu Unfällen in verschiedenen Industrien bei

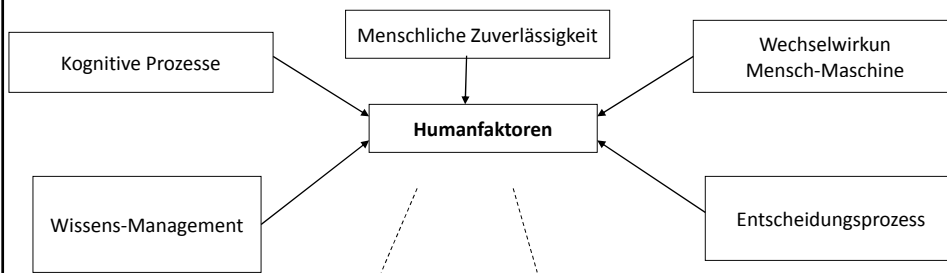
### Der menschliche Einfluss auf die Operation eines Systems schließt ein,

- regelmäßige betriebliche Handlungen
  - Wartungshandlungen, wie Besichtigung und Reparatur
  - Kontrolle oder Umgang mit kleinen Störungen
  - Beendigung laufender Störung sowie Milderung ihrer Folgen
- Menschliche Handlungen schließen **geplante** (trainierte) und **ungeplante** Handlungen ein.
- Es besteht Bedarf nach analytische Methoden welche **absichtliche**, böswillige Handlungen wie Sabotage berücksichtigen.

## Human Reliability Analysis (HRA) (Menschliche Zuverlässigkeits Analyse)

### Humanfaktoren:

- die Studie aller Aspekte, welche Menschen und ihr Verhalten beeinflussen können
- angewandt in vielen Disziplinen (engineering, biomechanics, psychology, etc... )
- Zusammengesetzt aus verschiedenen Gebieten einschließlich der Menschlichen Zuverlässigkeitsanalyse



## Repräsentation menschlicher Fehler

### Human Reliability Analysis

- Identifizierung und das Verstehen von wichtigen Faktoren, die die menschliche Leistung betreffen könnten. Insbesondere Umstände, welche das System in „unsichere“ Bedingungen führen können.
- Betrachtung menschlicher Fehler als integraler Bestandteil einer Fehler- oder Ereignisbaumanalyse; Teil der Probalistischen Sicherheits-Analyse (PSA) resp. Probalistischen Risiko-Analyse (PRA).

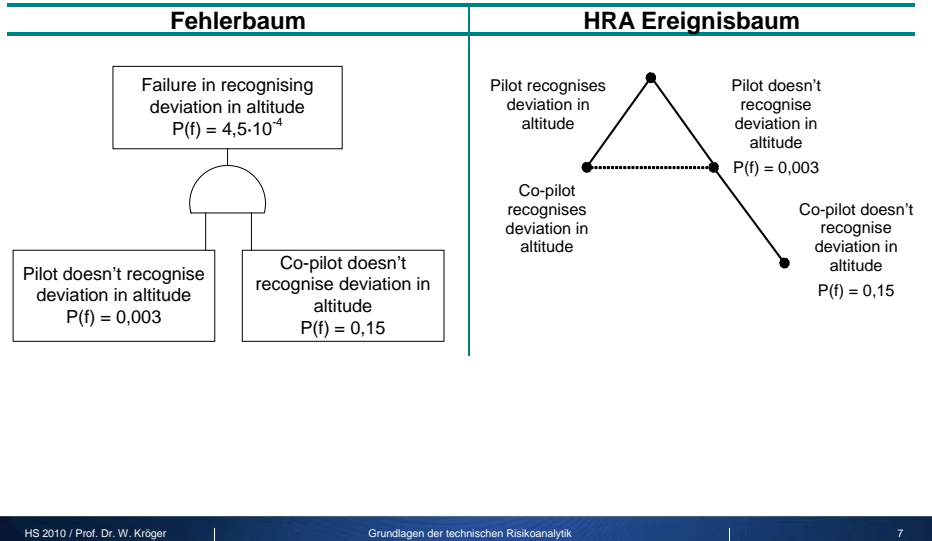
### Beispiel einer Fehlerbaumanalyse

- beinhaltet die Mensch-Maschine Wechselwirkung, explizit und implizit,
- Modelliert menschliche Fehler sowie Fehler von Komponenten,
- kann helfen, die wichtigsten Folgen von menschlichen Fehlern zu identifizieren.

### Voraussetzungen

- Ausführliche Kenntnisse des Systems und der erforderlichen Handlungen / Aufgaben (Handbücher).
- Zusätzliche Faktoren wie Handlungs- und Aufgabe-Ketten in Betracht ziehen

## Fehlerbaum und HRA Ereignisbaum



## Vorbereitung einer HRA (1/2)

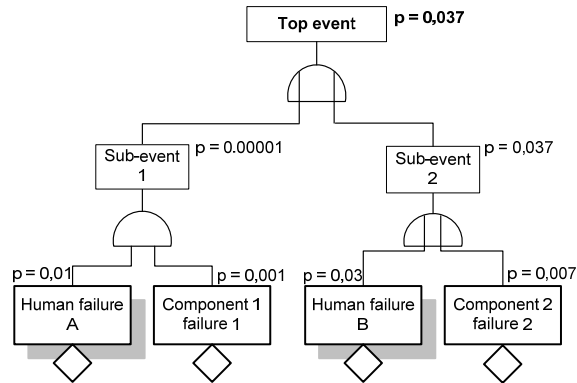
- Analyse von Handlungen und Aufgaben**
  - Einschätzung der erforderlichen Information
  - Identifizierung des Zustands vorher und nach der Aufgabe-Ausführung
  - Identifizierung der Informationsübertragung
  - Identifizierung einer entsprechenden Klassifikation
  - Identifizierung von Verbindungen unter dem Personal und Handlungen
- Analyse des Einflusses von Handlungen auf die System-Sicherheit**
  - Selektion wichtiger Handlungen
- Quantifizierung des Verhaltens**
  - praxisorientierte Methoden für die Identifizierung von Fehlerwahrscheinlichkeiten:

THERP: Aufgliederung	AIPA: Zeitabhängigkeit	SLIM: Experten basiert
Aufgliederung von Handlungen in einfache Subhandlungen bis Abschätzungen verfügbar sind (wie FTA).	Das Verhalten des verantwortlichen Maschinenbedieners wird als ein Verhältnis der erforderlichen und Verfügbarkeitszeit für die richtige Antwort modelliert.	Expertenbefragung, um Handlungen zu bewerten, welche menschliche Fehler-Wahrscheinlichkeiten beeinflussen. Die Identifizierung der Wahrscheinlichkeit beruht dann auf einer Kalibrierung der Expertengutachten und auf der Erfahrung.

## Vorbereitung einer HRA (2/2)

### 4. Darstellung des Verhaltens innerhalb eines logischen Frameworks

- Entwicklung einer quantitativen Fehler- / Ereignis-Baum mit Komponentenausfällen und menschlichen Handlungsfehlern



## Accident Initiation and Progression Analysis (AIPA)

### Ansatz

- Der Bediener (Einzelperson oder Team) reagiert auf eine geforderte Handlung auf Basis von Kontroll-Informationen nicht sofort.
- Genügend Zeit vorausgesetzt, wird der Bediener am wahrscheinlichsten Massnahmen ergreifen, welche die Situation nicht erschweren werden. Das ist besonders so, wenn die ergriffenen Massnahmen wohlbekannt und trainiert worden sind.
- Wenn der Bediener erkennt, dass die getroffenen Handlungen nicht zum gewünschten Systemzustand führen, wird er weitere Massnahmen ergreifen.

## Modell

$$Pr_{OF} = \exp\left[-\frac{t}{MTOR}\right] \text{ und } Pr_{OF} \geq 1 - Pr_S$$

wobei:

$Pr_{OF}$ : Bediener Fehlerwahrscheinlichkeit

$t$ : Verfügbare Zeit, bezogen auf die technische Charakteristik des Systems

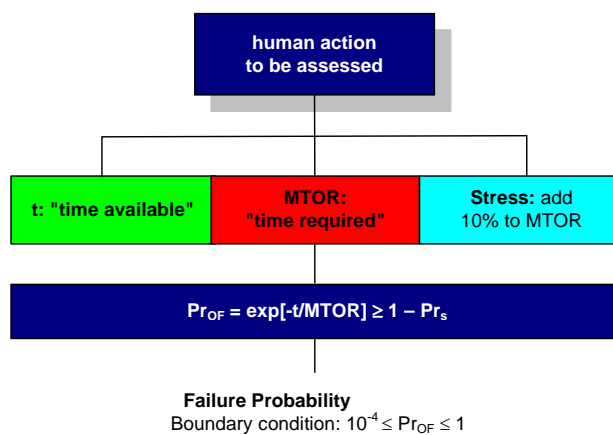
$MTOR$ : Mittelzeit zu einer richtigen Bediener-Antwort (Expertenwissen)

$Pr_S$ : Erfolgswahrscheinlichkeit (zwischen 0.99 und 0.9999; individuell definiert pro Handlung)

## Beeinflussung durch Stress

Wenn Stress das übliche Niveau überschreitet, ist  $MTOR$  um 10% zu erhöhen.

## Assessment



Das AIPA-Modell wird durch seine leichte Anwendbarkeit charakterisiert.

## Beispiel

In einem Pumpsystem wird ein Tank in 10 Minuten gefüllt und in 50 Minuten entleert. Das Überfüllen des Tanks mehr als 30 % führt zum Bruch einer Scheibe, und das Medium wird in die Umgebung freigegeben. Die Wahrscheinlichkeit eines Bedieners unpassend auf diese Situation zu antworten, wird als  $3 \cdot 10^{-4}$  als gegeben angenommen (Optimum in dieser Situation).

Gemäss der Beschreibung der Anlage hat der Bediener 3 Minuten, um die Schalter zu öffnen, die Aufgabe verlangt 30 Sekunden. Das schnelle Schließen der Schalter wird den Bediener unter zusätzlichen Stress bringen.

Aufstellung der Gleichung:  $Pr_S = 1 - 3 \cdot 10^{-4} = 0,9997$   
 $t = 3 \text{ min}; MTOR = 0,5 \text{ min}$

$$Pr_{OF} = \exp\left[-\frac{3}{0,5 \cdot (1 + 0,1)}\right] = 4,3 \cdot 10^{-3}$$

Erfüllte Grenzbedingung:  $Pr_{OF} \geq 1 - Pr_S$  und  $1 \cdot 10^{-4} Pr_{OF} \leq 1$ .

## Technique for Human Error Rate Prediction (THERP)

THERP Quantification Process [1], [2]

### Phase 1: Vertrautmachen

- Visit der Anlage
- Rezension von Informationen von System-Analysten
- Bereitstellung von Informationen an System-Analysten

### Phase 2: Qualitative Bewertung

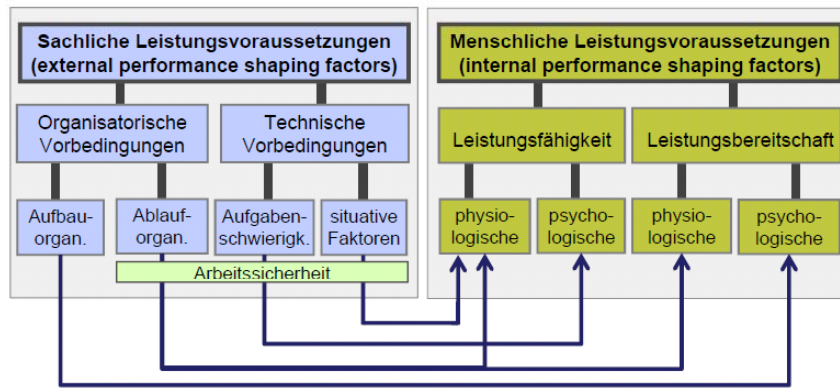
- Talk- or walk-through
- Aufgaben-Analyse menschlicher Handlungen
- Entwicklung von HRA Ereignisbäumen

### Phase 3: Quantitative Bewertung

- Zuteilung nominaler HEPs (human error probabilities)
- Schätzung relativer Effekte von PSFs (Performance Shaping Factors)
- Bewertung von Abhängigkeiten
- Bestimmung von Erfolgs- und Fehlerwahrscheinlichkeiten
- Bestimmen Sie die Wirkungen von Wiederherstellungsfaktoren

### Phase 4: Integration

- Führen Sie eine Empfindlichkeitsanalyse



### Beispiel: Diagnose eines "Anormalen" Ereignisses (Kernreaktor)

- Der Fehler der Hauptwasser-Versorgung und der Notwasser-Versorgung eines Dampfgenerators wird angenommen.
- Kontrollraum-Personal muss dieses Ereignis richtig diagnostizieren und Wiederherstellungsreaktionen innerhalb von 20 Minuten auslösen.
- Dem Personal muss bewusst sein, dass eine Korrekturhandlung rechtzeitig sein muss; sonst muss das sogenannte "feed & bleed cooling," (Notkühlung) begonnen werden. Unzulängliche Reaktionen können auf Kernschmelzen hinauslaufen.

### Bewertung von Wahrscheinlichkeiten:

- Die Bewertung von human error probabilities (HEP) benötigt Modelle und Regeln (siehe folgende Seite)
- Bewertung: Wenn Regel 2a auf die gegebene Situation angewendet wird, so ergibt sich die Wahrscheinlichkeit einer falschen Diagnose zu  $Pr(F) = 0.01$ .
- Viele zusätzliche Situationen und menschliche Abhängigkeiten werden in THERP betrachtet.



## Regeln und Modelle zur Bestimmung von HEPs

1. Use upper bound of Fig. A if:
  - a. the event is not covered in training **or**
  - b. the event is covered but not practised except in initial training of operators for becoming licensed **or**
  - c. the talk-through and interviews show that not all the operators know the pattern of stimuli associated with the event.
2. Use lower bound of Fig. A if:
  - a. the event is a well-recognised classic (e.g., Three Mile Island incident, 1979), and the operators have practised the event in the simulator qualification exercises **and**
  - b. the talk-through and interviews indicate that all the operators have a good verbal recognition of the relevant stimulus patterns and know what to do or which written procedures to follow.
3. Use nominal Human Error Probability (HEP) of Fig. A if:
  - a. the only practise of the event is in simulator re-qualification exercises and all operators have had this experience **or**
  - b. none of the rules for use of upper or lower bound apply.

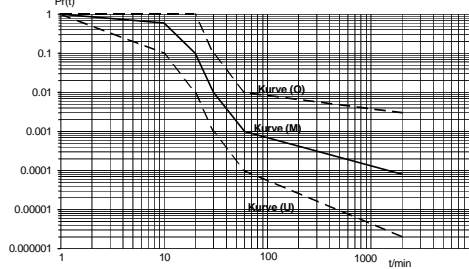


Fig. A: time t in minutes after a compelling signal of abnormal situation.

## Success Likelihood Index Methodology (SLIM)

Das Ziel der "Success Likelihood Index Methodology (SLIM)" ist die menschliche Fehlerwahrscheinlichkeit (HEP) zu quantifizieren, um "Handlungen" zu ergreifen oder Aufgaben zu erfüllen.

### Performance Shaping Factor (PSF):

Faktoren, die beträchtlich die Durchführbarkeit einer "Handlung,, betreffen, wie:

- Angemessenheit der Zeit
- Schnittstelle der menschlichen Maschine und Anzeigen von Bedingungen
- Ausbildung und Erfahrung
- Komplexität der Aufgabe
- Stress

### Vorgehen

1. Definition der "Handlungen"
2. PSF Einschätzung und Gewichtung
3. Gruppierung von "Handlungen"
4. Kalibrierung der SLI
5. Umwandlung der SLI in menschliche Fehlerwahrscheinlichkeiten

### Step 1: Definition der "Handlungen"

Das Personal charakterisiert und definiert die "Handlungen" in Zusammenarbeit mit Experten der „Human Reliability Analysis,, und Systemanalyse-Experten.

### Step 2: PSF Einschätzung und Gewichtung

- Interviews mit operativem Personal, um den PSF für bestimmte "Handlungen" abzuschätzen. Die Einschätzung zeigt, inwieweit der PSF hilft oder die Ausführung einer Handlung verhindert.
- Eine Rangliste im Intervall von 0 bis 10 muss für jeden PSF aufgestellt werden, um konsistente Ergebnisse von den verschiedenen Experten zu erhalten (siehe folgende Beispiel-Tabelle)

### Step 2: PSF Rating

**Definition:** This example of PSF represents the extent to which operating instructions enhance the ability of an operator to conduct a certain "action".

#### Scaling guidance $r_k$

Rating	Example of a fictitious process with the following rating:
0	Instructions are precisely defined. Operators are able to easily follow the instructions.
1	-
2	Instructions are precisely defined. Operators are able to easily follow the instructions but the clarity could be affected by prior changes or modifications.
3	-
4	-
5	Instructions are available. Some interpretations by the operator are necessary to take certain "actions".
6	Several steps in the procedure may require the operator to return to a previously completed step (e.g. continuous "actions" or keeping ahead skipped tasks)
7	Instructions are being used but due to an urge to act the operator is only capable to use them as check-up.
8	The "action" is a coincidental event for which the instructions can only give a vague advice.
9	Instructions are poorly composed and may lead to wrong actions
10	No instructions exist for this "actions"

## Step 2: PSF Weighting

**PSF "plant-human-machine interface and gauges system"**: scaled on the possibility of a human-machine interface to provide informations to succesfully take an "action"

Weighting $w_k$	Example of a fictitious process
0: insignificant	Other factors are so dominating that I do not care about how good or bad these indicators are because they will not change the human error probability of this specific "action"
1: low	This is an "action" based on the experience of responding to many alarms that require little or no diagnosis. I can easily prove the correctness of my "action" in various ways.
2: normal	Patterns of indicators absolutely force an "action" and check the correct response of the facility but they do not require a thorough checking or assessment.
4: high	A successful "action" is not possible without an adequate response to the facility's gauges. We have to consider specific parameters to diagnose the problem and/or checking the facility.

## Step 3: Zusammenfassung der Gewichtung

Failure Likelihood Index (FLI)

$$FLI = \sum_{k=1}^n w_k \cdot r_k$$

wobei

$k =$  PSF ( $k=1, 2, \dots, n$ )  $w_k$ : Gewichtung;  $r_k$ : Rating.

•  $w_k$  und  $r_k$  sind Durchschnittlie von Expertenbewertungen

## Step 4: Kalibrierung und Transformation

Transformation der FLI (= relative human error probabilities) in geforderte HEP:

die kalibrierte FLI-Skala ist eine quantitative Beziehung zwischen der FLI-Skala und den menschlichen Fehlerwahrscheinlichkeiten HEP:

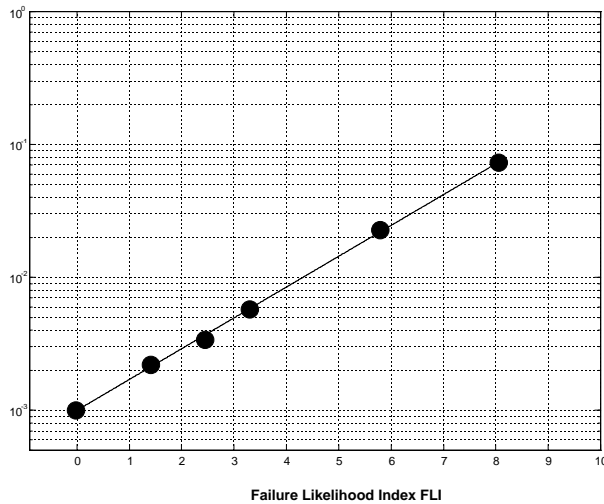
$$\log_{10}(HEP) = a \cdot FLI + b$$

wobei

$a$ : Steigung;  $b$ : Achsenkreuzung.

## Beispiel einer kalibrierten Skalierung

Human Error (HEP)Probability HEP



## First generation and second generation models

### First generation HRA:

AIPA, THERP, SLIM, SPAR HRA, etc...

- HRA ist limitiert auf die menschlichen Handlungen, welche auch in den PSA Ereignisbäumen beinhaltet sind,
- Binäre Darstellung menschlicher Handlungen
- Wenig Beachtung kognitiver Aspekte menschliche Handlungen

### Second generation

- CREAM (Cognitive Reliability and Error Analysis Method)
- ATHEANA (A Technique for Human Error ANALysis)
- Hauptcharakteristik:
  - Explizite Rolle des Kontextes in Identifikation und Wahrscheinlichkeitsabschätzung
  - Anwendbar auf verschiedene Benutzer in unterschiedlichen Zusammenhängen
  - Konsistenz, Überprüf- und Wiederholbarkeit
  - Computersimulation zur Identifikation und Quantifizierung

## Zusammenfassung

- Menschliche Fehler können die Zuverlässigkeit und Gefahr verursacht durch technische Systeme beträchtlich beeinflussen.
- HRA liefert die Methoden, menschliche Fehler zu modellieren und innerhalb einer umfassenden Analyse zu messen. Jedoch sind die Analysen mit grossen Unsicherheiten behaftet.
- Durch die Einschliessung von menschlichen Faktoren werden Analysen realistischer, aber auch komplizierter und umfassender.
- Die vorgeschlagenen "Methoden" setzen nicht verfügbare empirische Daten ein.
- HRA ist nur ein Segment im Gebiet von menschlichen Faktoren (Wissens-Management, Fehler, Einfluss der Sicherheitskultur, böswilligen Angriffe, usw.).

### References

1. Kirwan, B., *A Guide to Practical Human Reliability Assessment*. 1994, London: Taylor & Francis.
2. Swain, A.D. and H.E. Guttmann, *Handbook of Human-Reliability Analysis with Emphasis on Nuclear Power Plant Applications (Final Report)*. 1983, U.S. Nuclear Regulatory.; Washington D.C. p. 1-554.
3. Khramenkov, S.V. and O.G. Primin, *Operational Paper - Ensuring the reliability of the water piping of the Moscow water supply system*. Journal of Water Supply, 2005. **52**(2): p. 127-131.