

# Auf den Weg zur systemischen Sicherheit

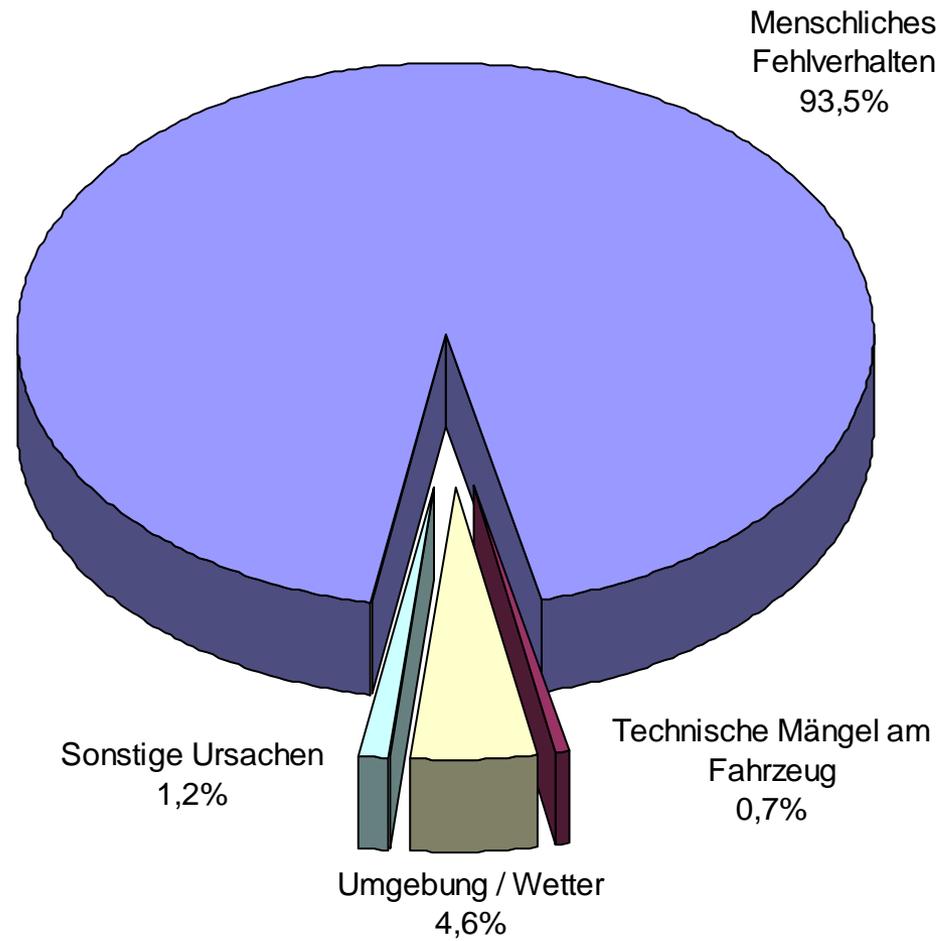
Beispiel: Assistenzsysteme im  
Fahrzeug

Prof. Dr. Dr. h.c. Alf C. Zimmer

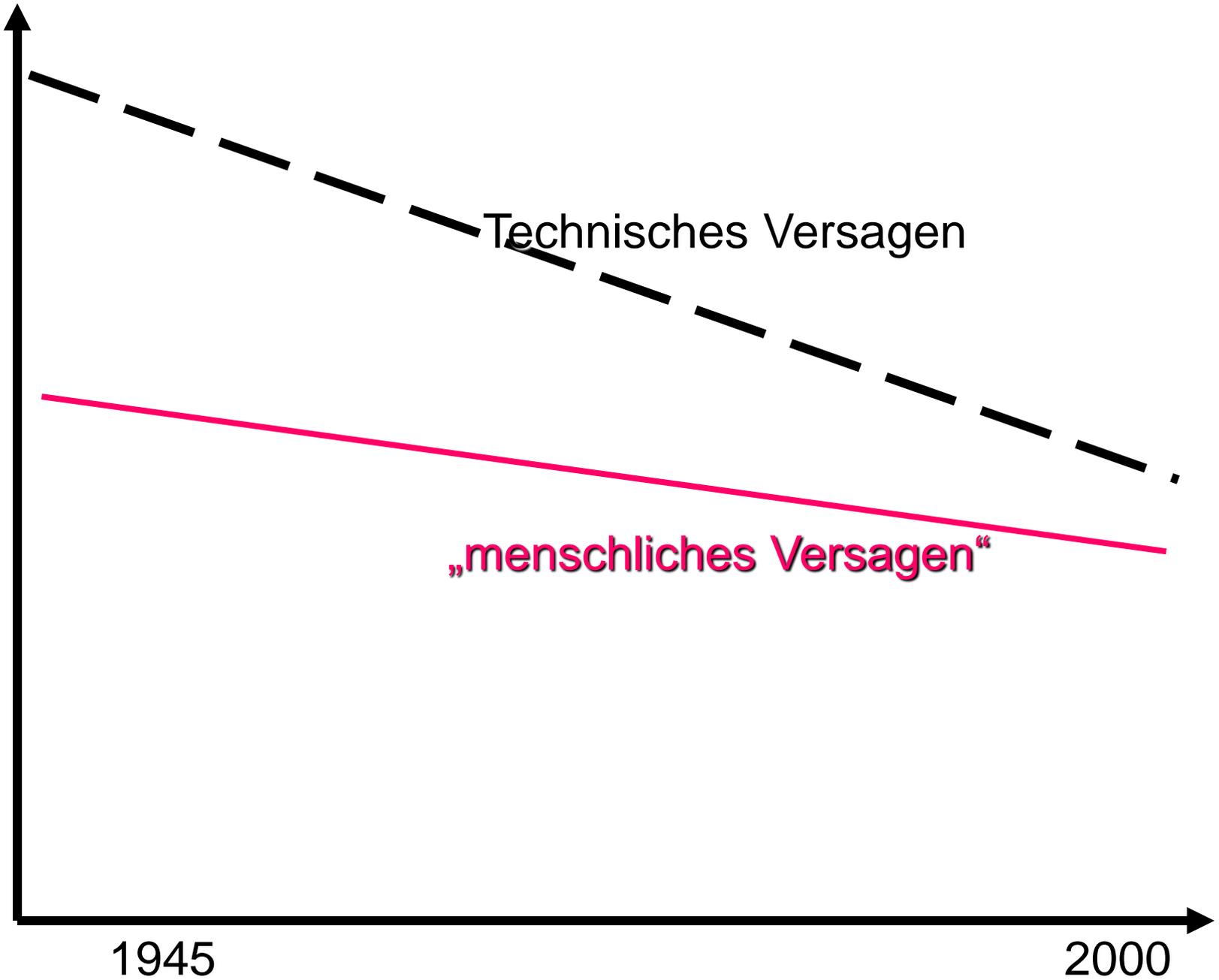
Fakultät Psychologie, Pädagogik und Sportwissenschaft

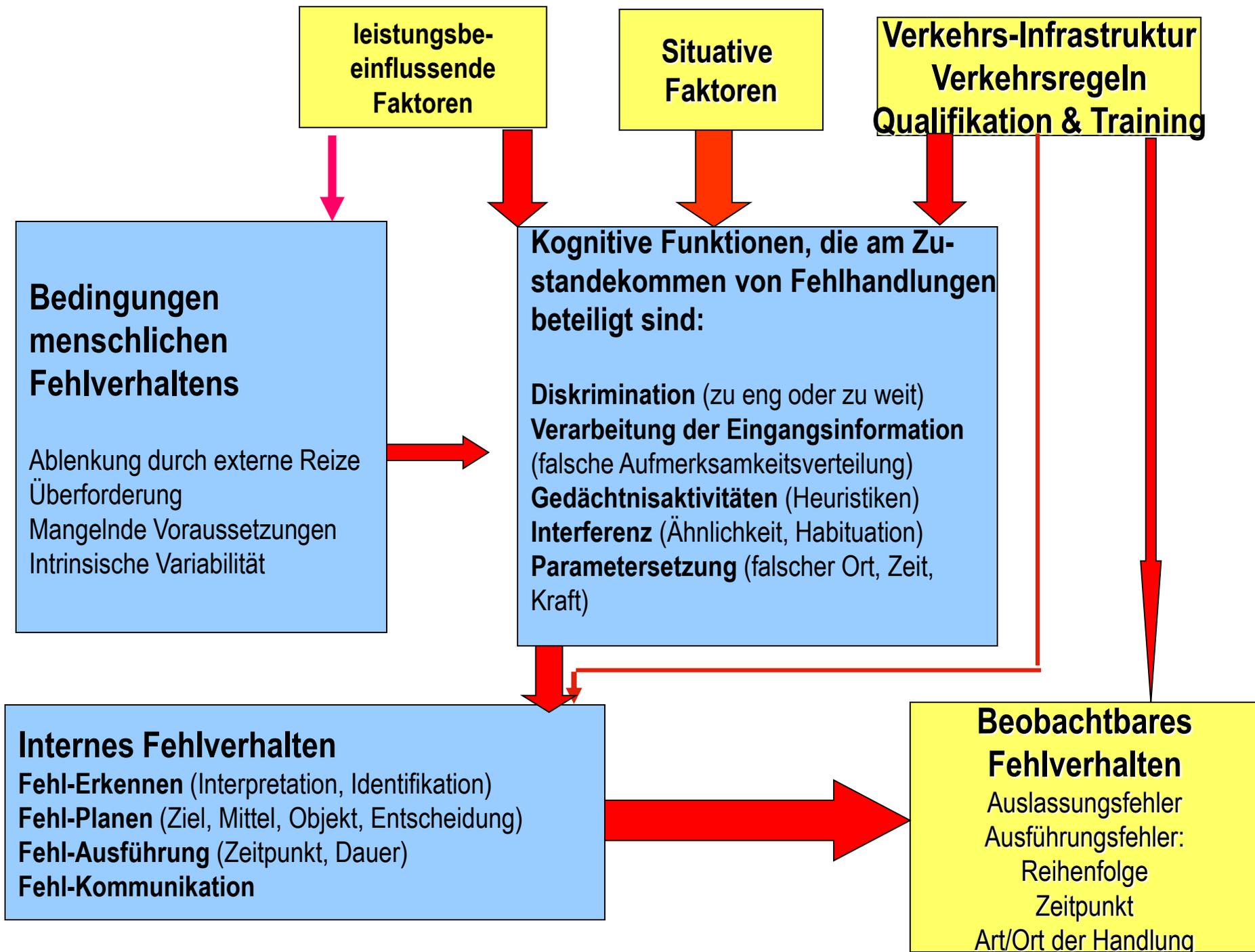


Universität Regensburg



Quelle: GIDAS-Datenbank

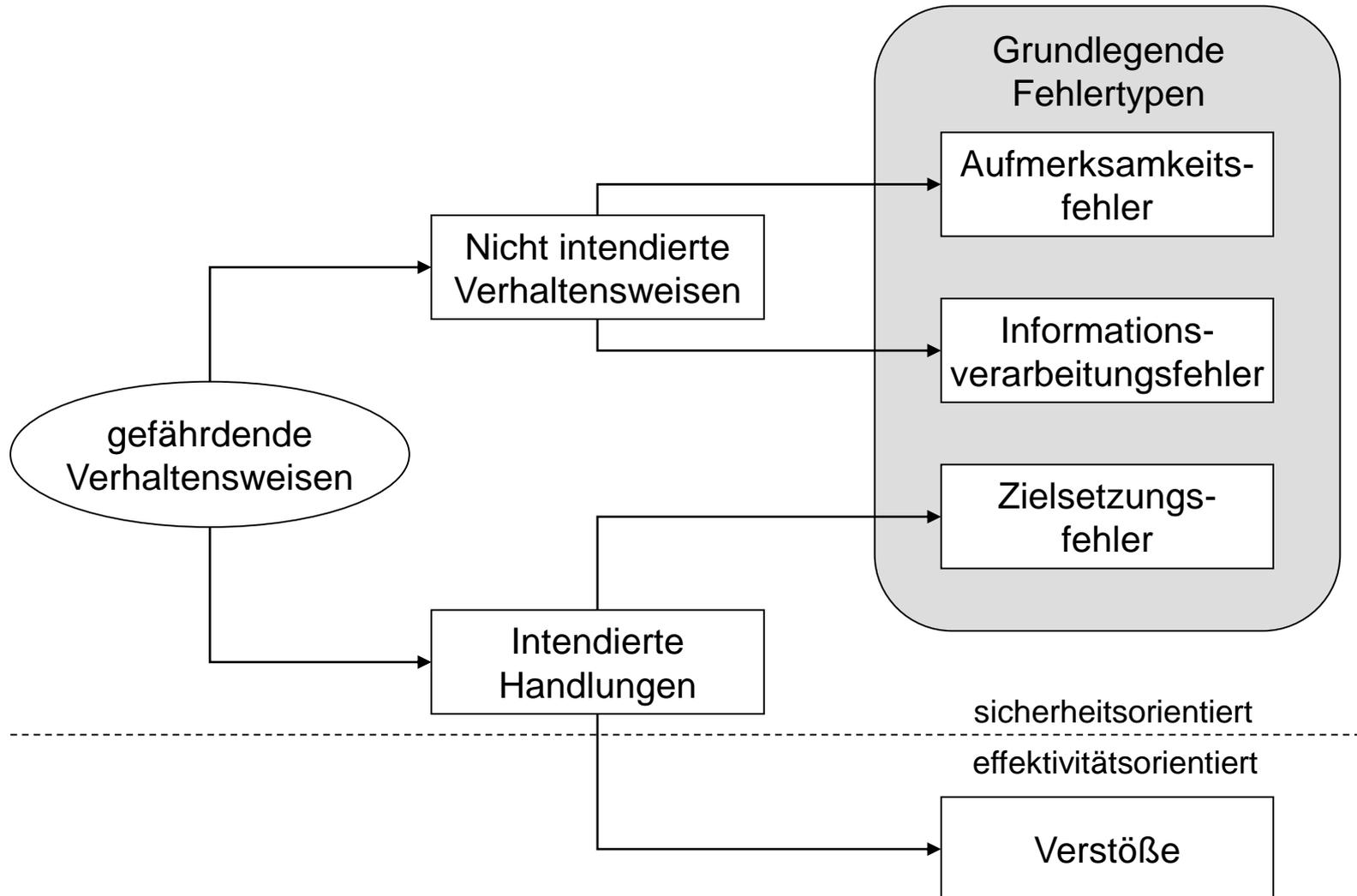




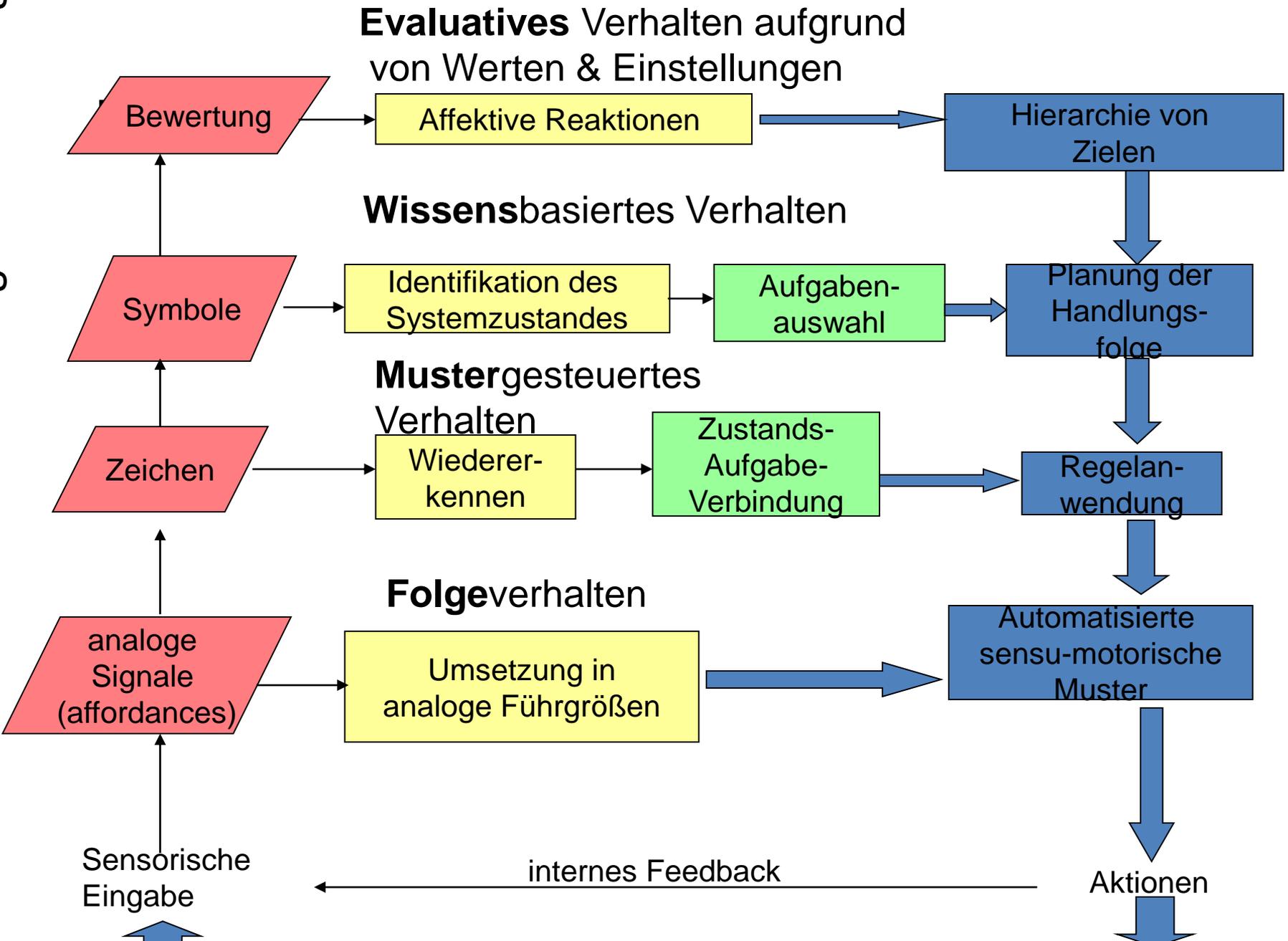
# Fehleranalyse nach Rasmussen (1982):

- Mechanischer oder struktureller Fehler
- Informationsfehler
- Diagnosefehler
- Zielsetzungsfehler
- Fehler in der Auswahl der Vorgehensweise
- Handlungsfehler
- Bedienungsfehler

# Fehleranalyse nach Reason (1990):



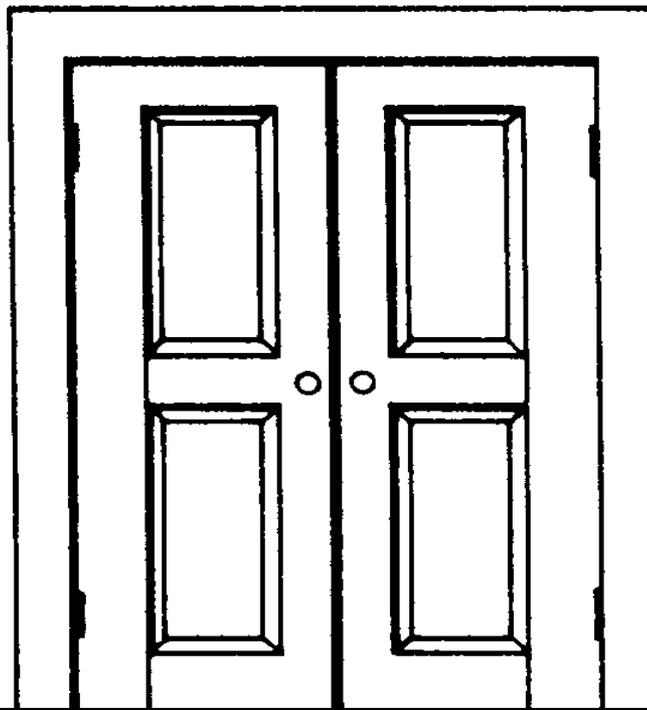
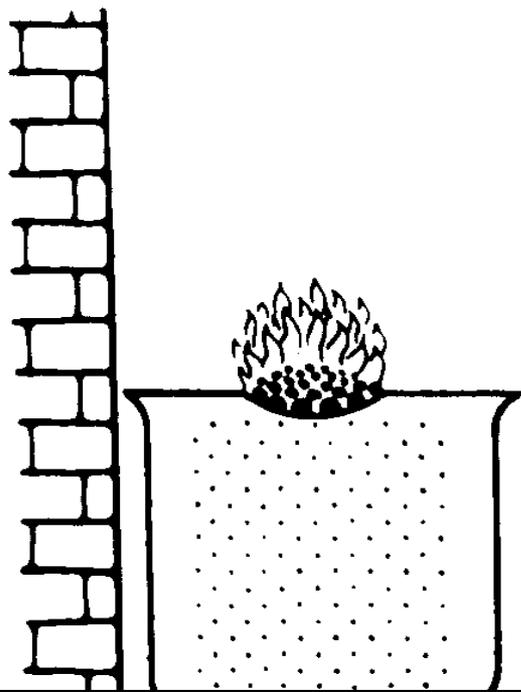
Ebenen der Verhaltenssteuerung bei Warnung



Innovationsphasen

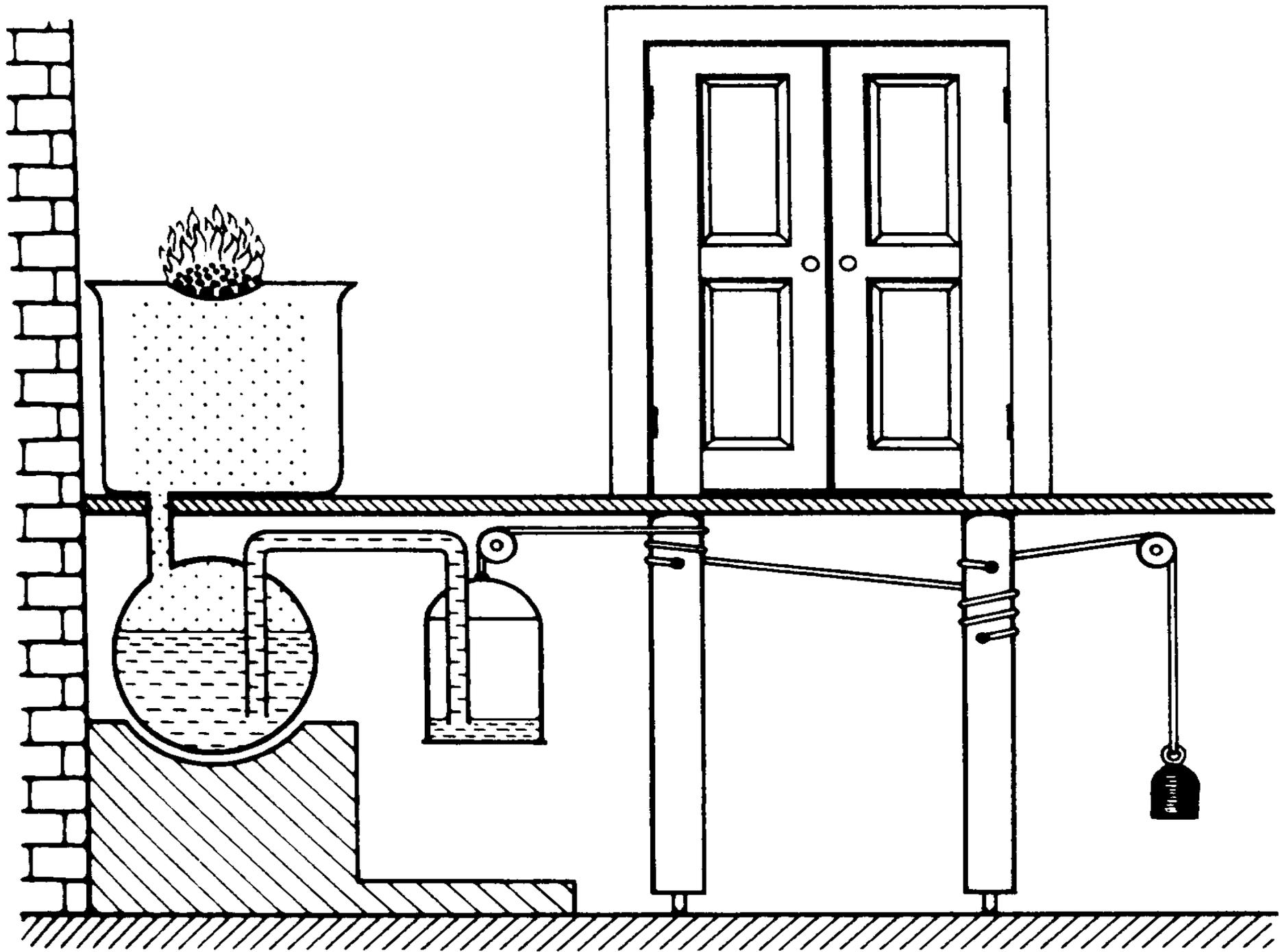
technischer Reifegrad

Orientierung am Nutzer



# Mangelnde Systemtransparenz hat zur Folge:

- Entwicklung falscher mentaler Modelle bezüglich der inhärenten Kausalität
- Anwendung nicht zutreffender Heuristiken (z.B. ‚Viel hilft viel‘ o.ä.)
- Falsche Interpretation des Systemverhaltens und darauf aufbauend:
- Nicht zielführende bzw. schädigende Eingriffe bei Bedienung und Instandhaltung/Reparatur



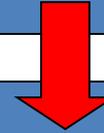
# **Sicherheitskulturen**

- **Die juristische Sicherheitskultur**
- **Die ingenieurwissenschaftliche Sicherheitskultur**
- **Die systemische Sicherheitskultur**

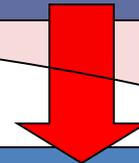
# Die juristische Sicherheitskultur

- **Hauptkennzeichen:** schuldhaftes oder fahrlässiges Fehlhandeln
- **Hauptfragen:** Wer konnte zu welchem Zeitpunkt den *nach menschlichem Ermessen* zu erwartenden Auslöser des negativen Ereignisses erkennen? Wer hatte die *zumutbare* Möglichkeit, die Auswirkungen dieses Auslösers zu verhindern?

Menschliche **Fehler** werden bei Unfällen als am wenigsten zwingend und daher als vermeidbar angesehen

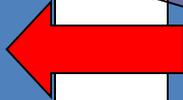


Warum? Menschen sind freie Agenten, die zwischen richtig und **falsch** wählen können

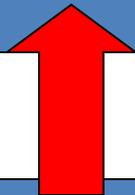


Weil **Fehler** daher als teilweise absichtlich angesehen werden, erfolgt **Schuldzuweisung**

Gegen **Fehler** (= **schuldhaftes Handeln**) werden Warnungen und Sanktionen eingesetzt



Bei Unfällen ist dies wirkungslos, daher treten die **Fehler** weiterhin auf.



**Wiederholungs-Fehler** nach Warnungen oder Bestrafungen werden als besonders schuldhaft angesehen,

# Die ingenieurwissenschaftliche Sicherheitskultur

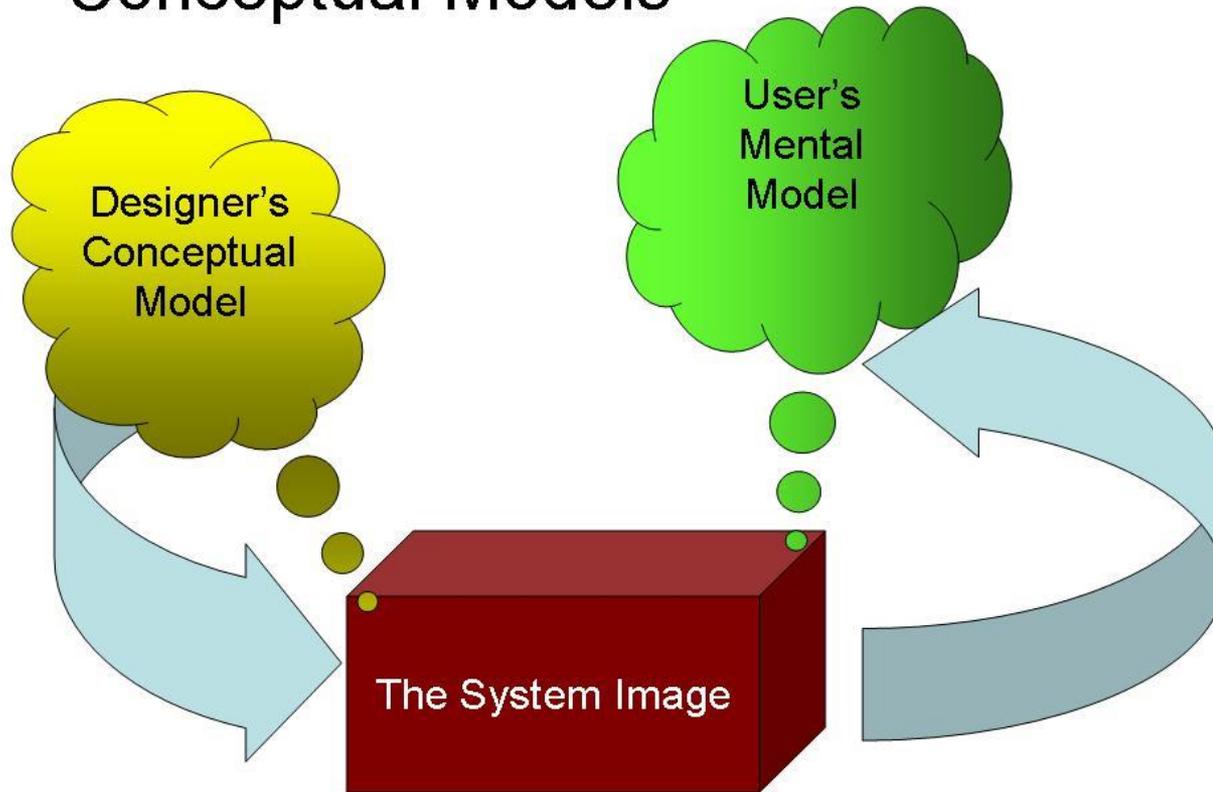
- **Hauptkennzeichen:**

Zuverlässigkeit von Systemelementen  
(technische und menschliche)

- **Hauptfragen:**

1. Welche Systemkomponenten sind besonders unzuverlässig?
2. Durch welche Maßnahmen lässt sich die Zuverlässigkeit des Gesamtsystems am *effizientesten* steigern?

# Conceptual Models



# Konsequenzen von Assistenz im Fahrzeug

als Beispiele für gute und problematische Mensch-Maschine-Passung

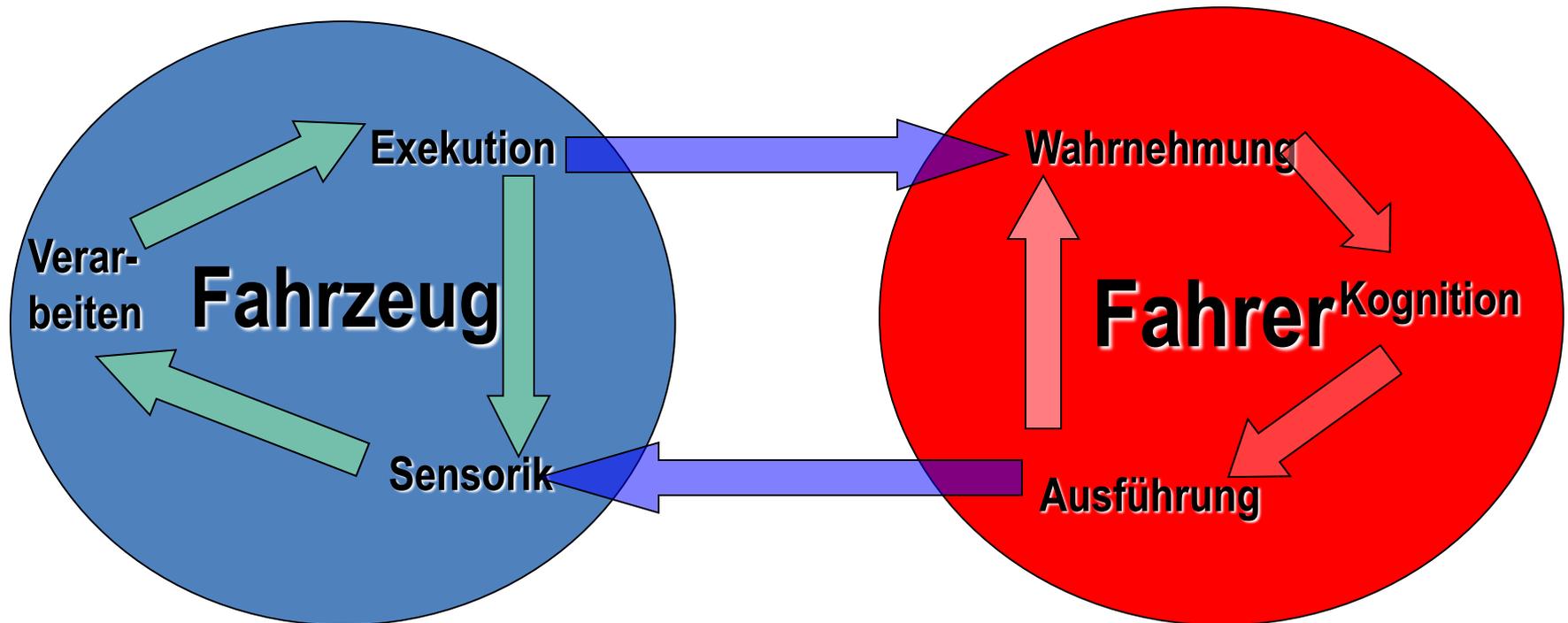
- **ENTLASTUNG** bei der Handhabung (ACC, ABS etc.)
- **ENTLASTUNG** bei der Fahrtplanung (Navigationssysteme)
- **BELASTUNG** durch Überwachung  
eventuell:
- **ÜBERFORDERUNG** bei Übernahme (ACC)
- **PROBLEM:** Kompetenzverlust
  - Mangelnde Handlungskompetenz ohne Assistenz
  - Mangelnde Differenzierung bei der Anwendung von Assistenz

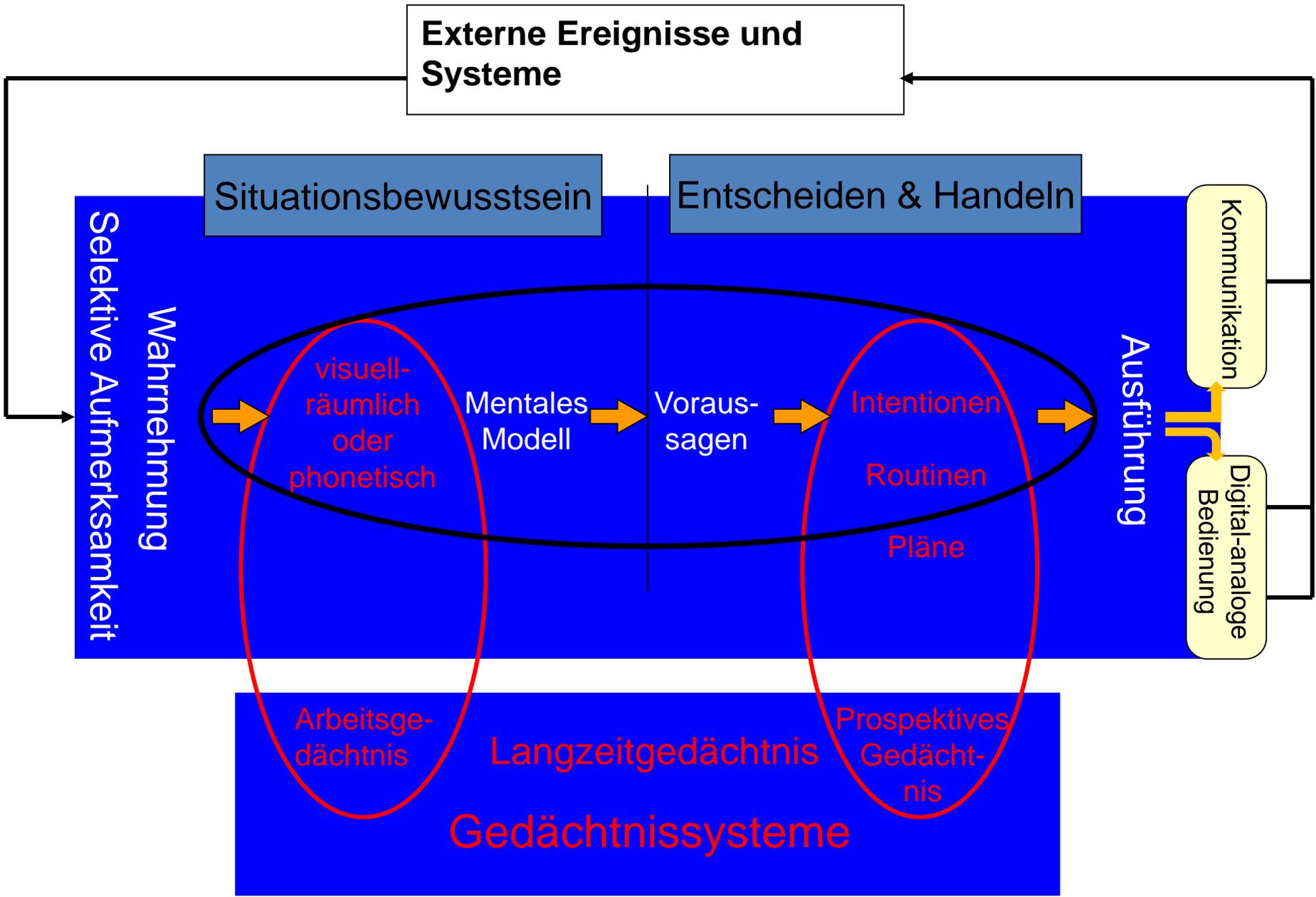
# Die systemische Sicherheitskultur

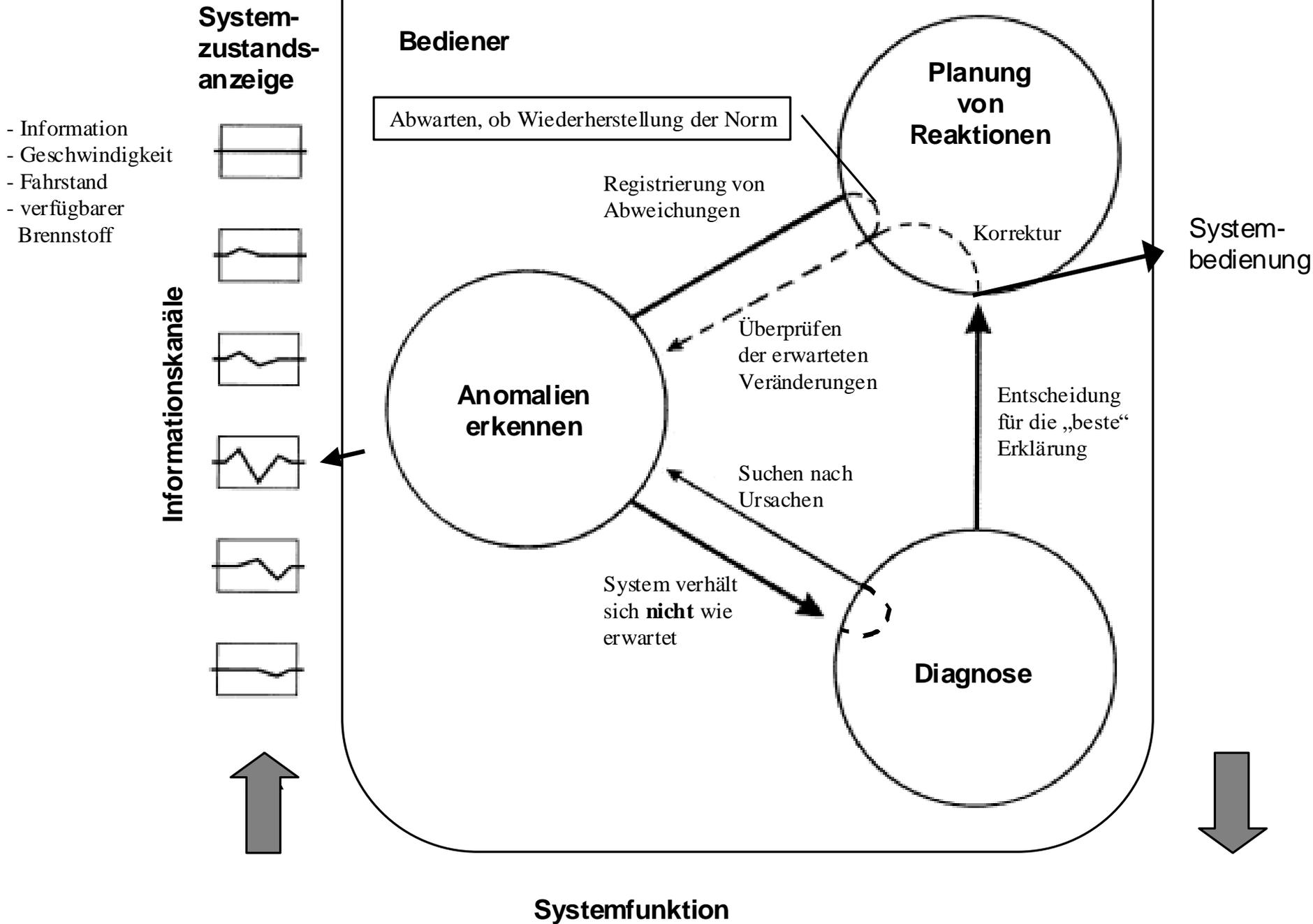
- **Hauptkennzeichen:** Sicherheit ist eine Funktion des **gesamten Mensch-Technik-Umwelt-Systems**
- **Hauptfragen:** Welche *Interaktionen* bestehen zwischen den Systemkomponenten? Welche Systemarchitektur ist besonders *fehlerverzeihend*? Welche Systemarchitektur entwickelt sich am ehesten in Richtung *Voraussagbarkeit und Stabilität*?

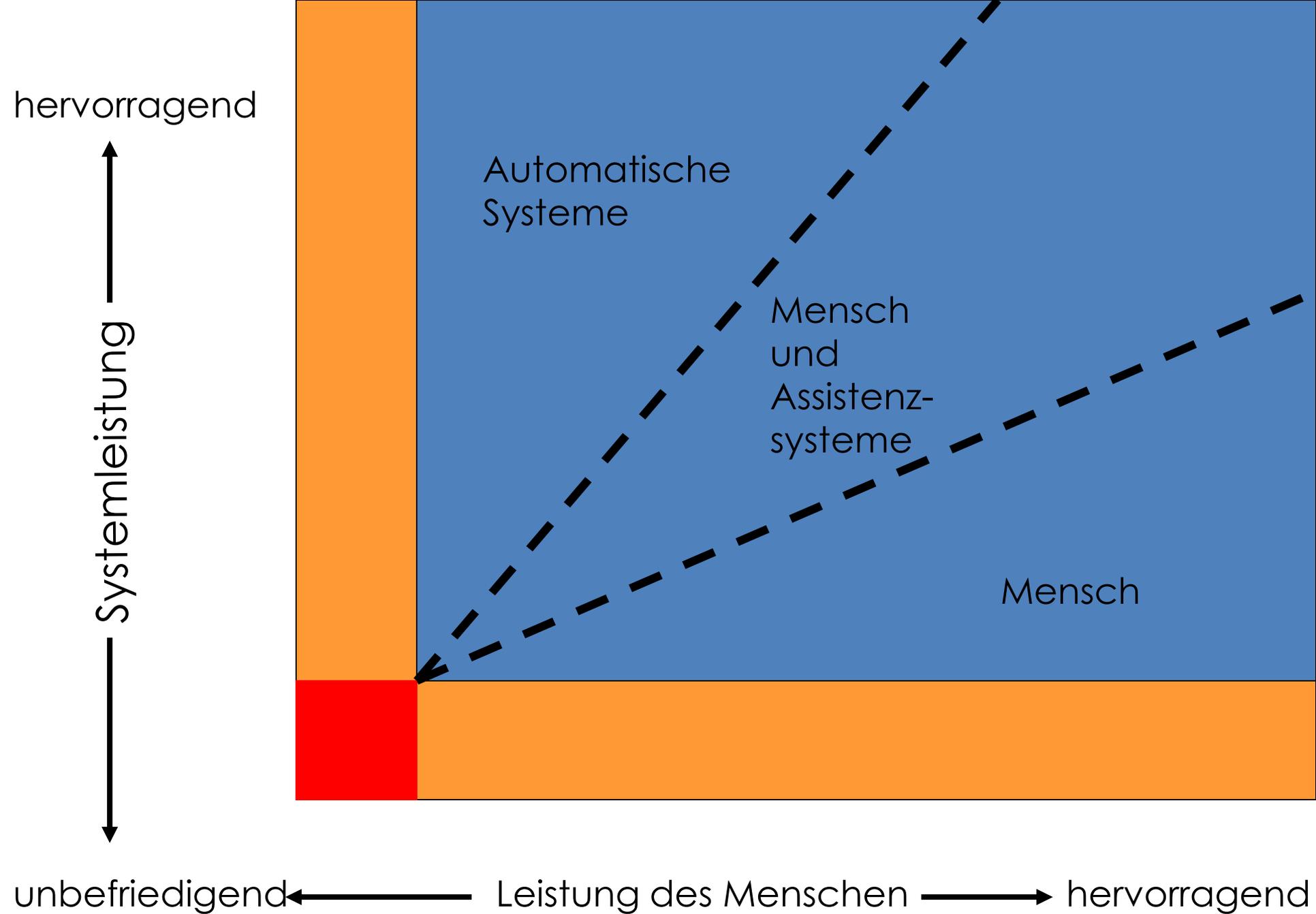
# Integration

## Hollnagel's Joint Cognitive Systems









# Geschätzte Fehlerwahrscheinlichkeiten

(Swain&Gutman, 1983; in Klammern : Zimmer et al. 1999)

- Analoganzeige falsch ablesen • **.003** (beim Fahren **.09**)
- Graphen falsch interpretiert • **.01** (falsche Interpretation von Symbolen neuer Systeme: **bis .3**)
- Signal übersehen • **.0003** (beim Fahren **zwischen .13 und .30**)  
**aber:**
- Situationsdiagnose • hochgerechnet **0.75** (beim Fahren **weniger als .01**)

**PROCESSES****GFTs**

<b>PROCESSES</b>	<b>GFTs</b>
Statement of goals	Incompatible goals
Organization	Organizational deficiencies
Management	Poor communications
Design	Design failures Poor defences
Build	Hardware failures Poor defences
Operate	Poor training Poor procedures Poor housekeeping
Maintain	Poor training Poor procedures Poor maintenance management

The diagram illustrates the relationship between various processes and their associated Goal Failure Types (GFTs). The processes are listed in the left column, and the GFTs are listed in the right column. Arrows indicate that the GFTs from the Design, Build, Operate, and Maintain processes contribute to the formation of Error-enforcing conditions, which are highlighted in a shaded box on the right side of the diagram.

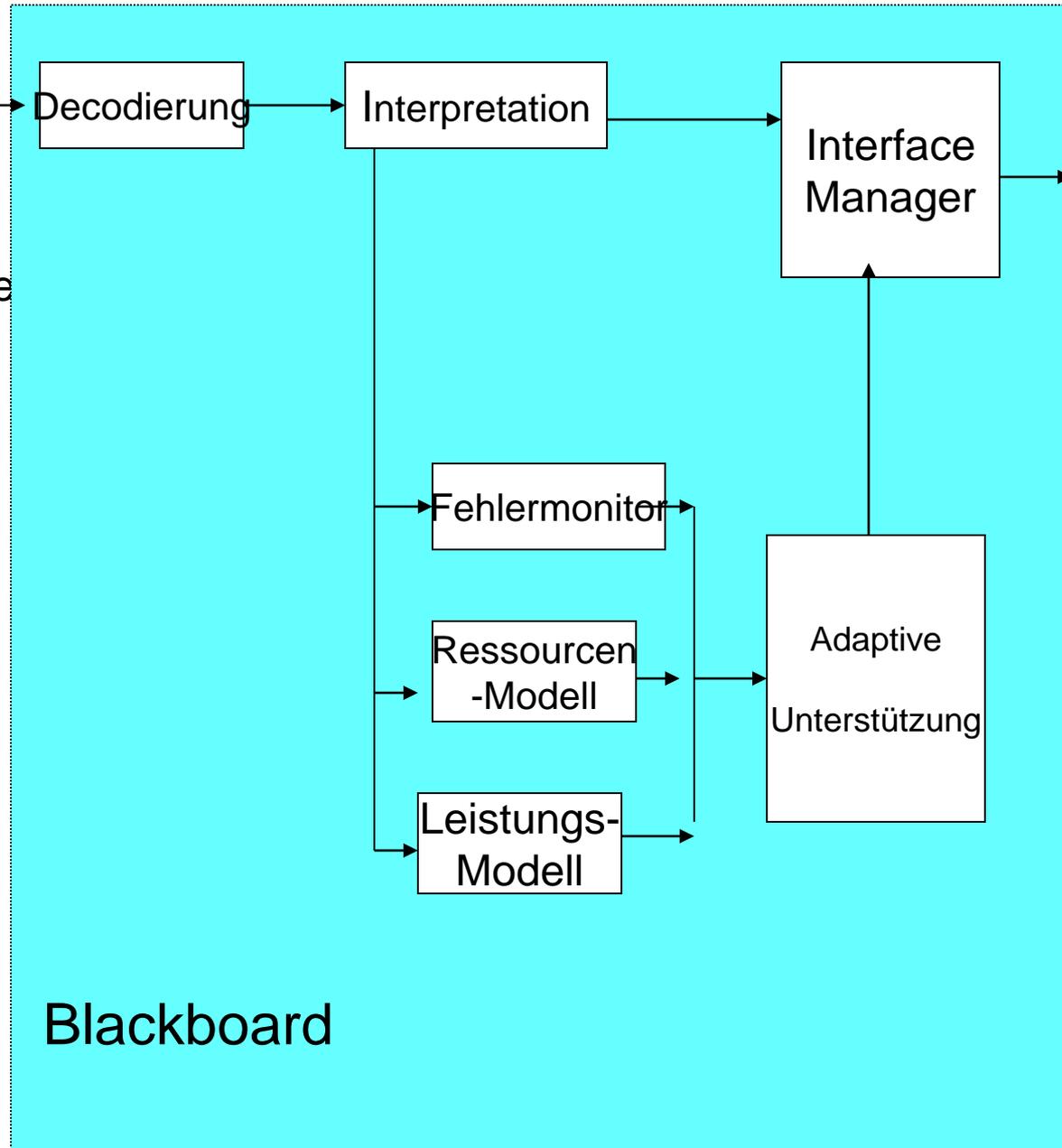
**Error-enforcing conditions**

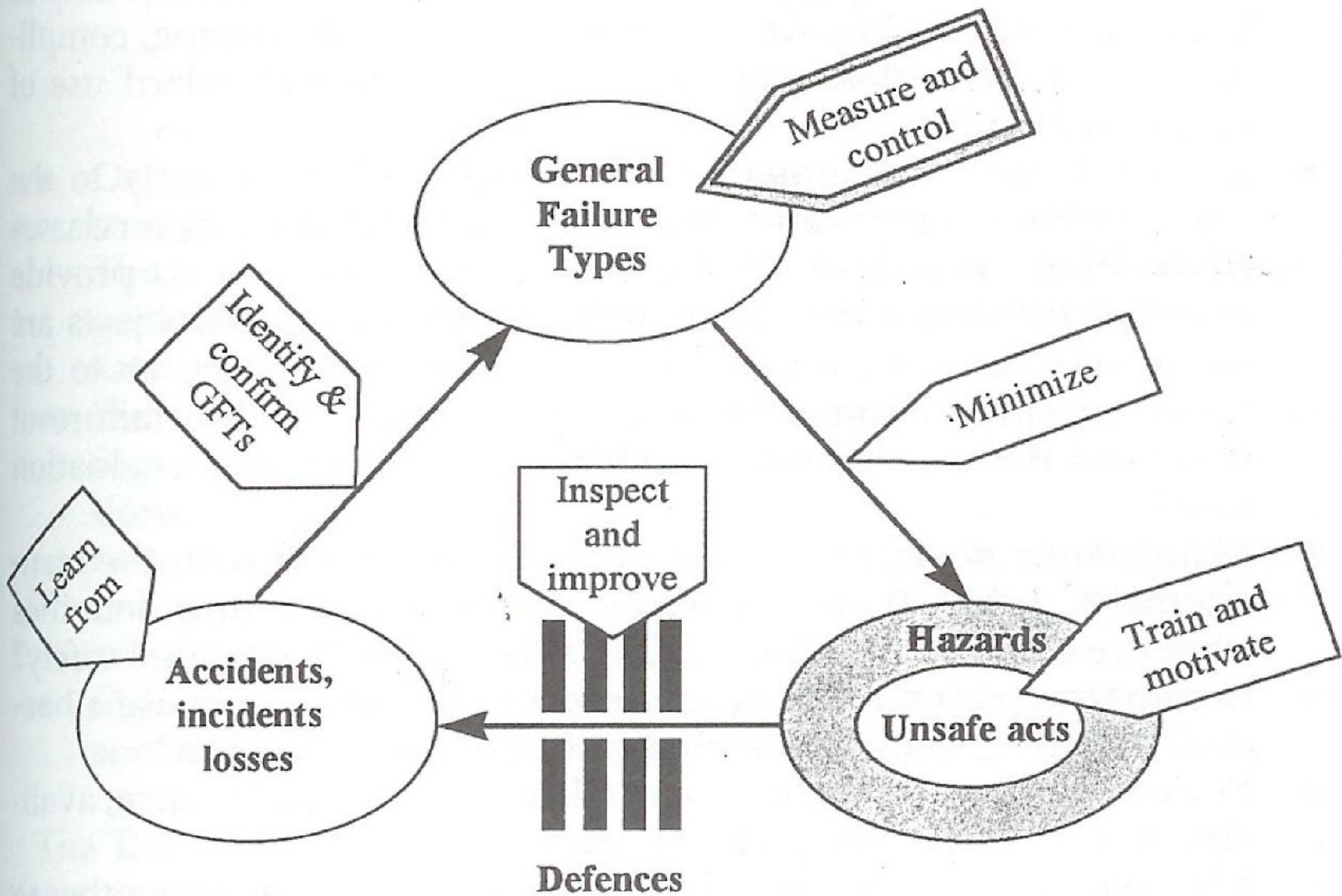
# Fehlerabwehrmaßnahmen durch Telematik und Assistenztechnologie

- Enforced compliance: ***direkter Eingriff***
- Implied compliance: ***Eingriff über Information oder Rückmeldung***
- Induced Compliance: ***Eingriff über veränderte Gestaltung der Regelung***

# Eingaben

Bedienelemente  
Menus  
Spracheingabe  
von anderen Modulen  
Sensorik





**General Failure Types**

**Measure and control**

**Identify & confirm GFTs**

**Minimize**

**Inspect and improve**

**Learn from**

**Accidents, incidents losses**

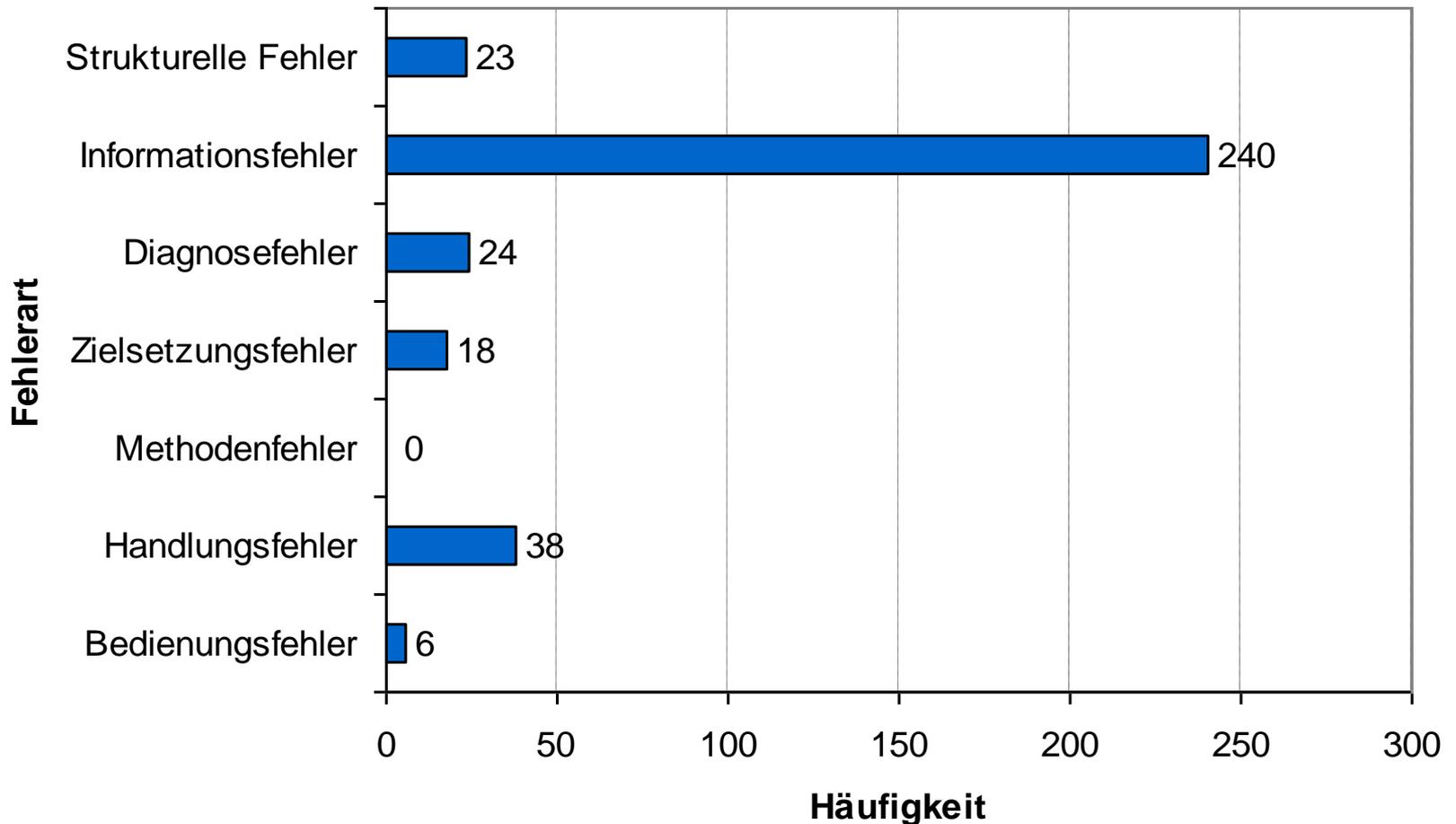
**Train and motivate**

**Hazards**

**Unsafe acts**

**Defences**

# Fehleranalyse nach Rasmussen (1982):



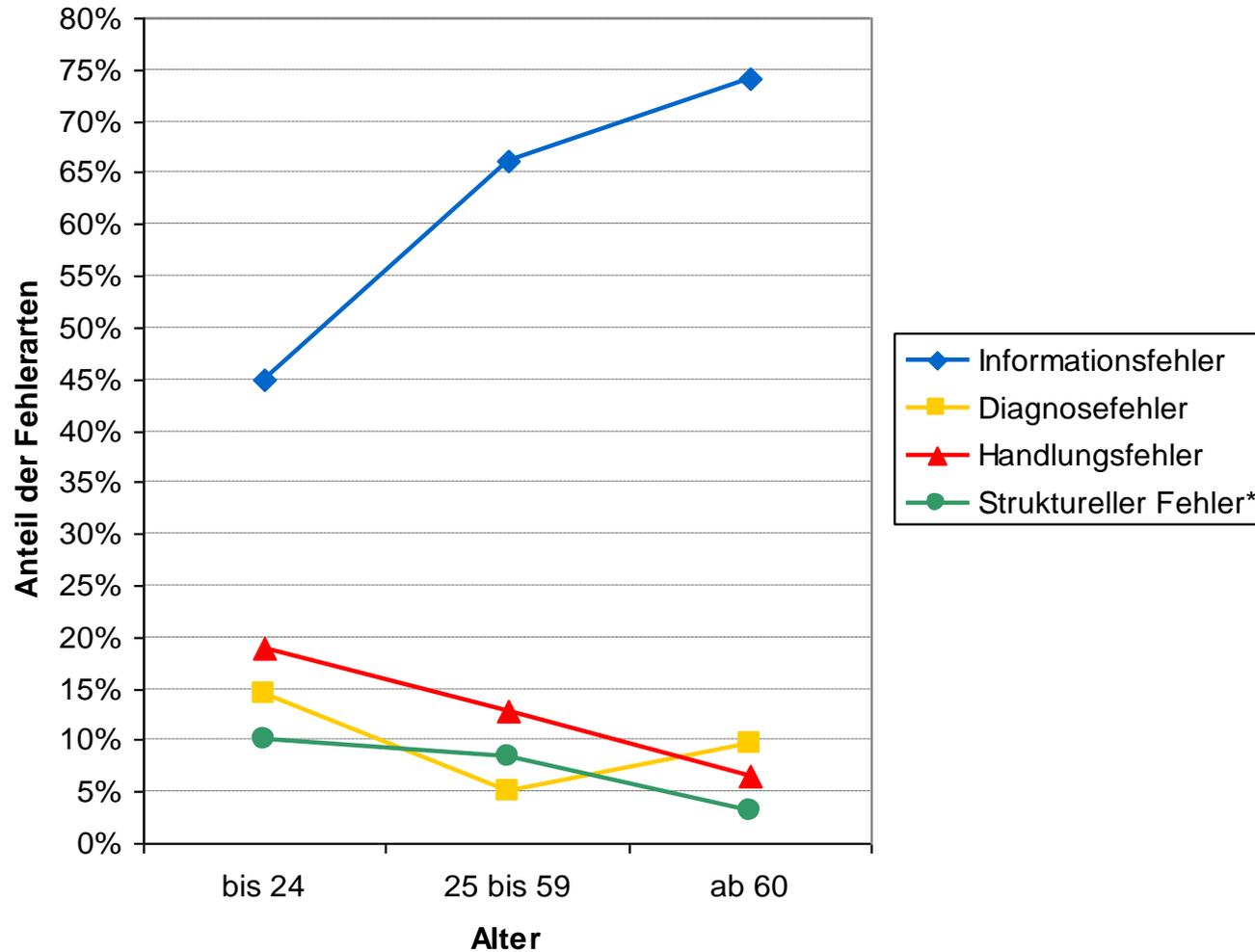
Anzahl Unfälle: N=312

# Relative Risiken der Unfallverursachung

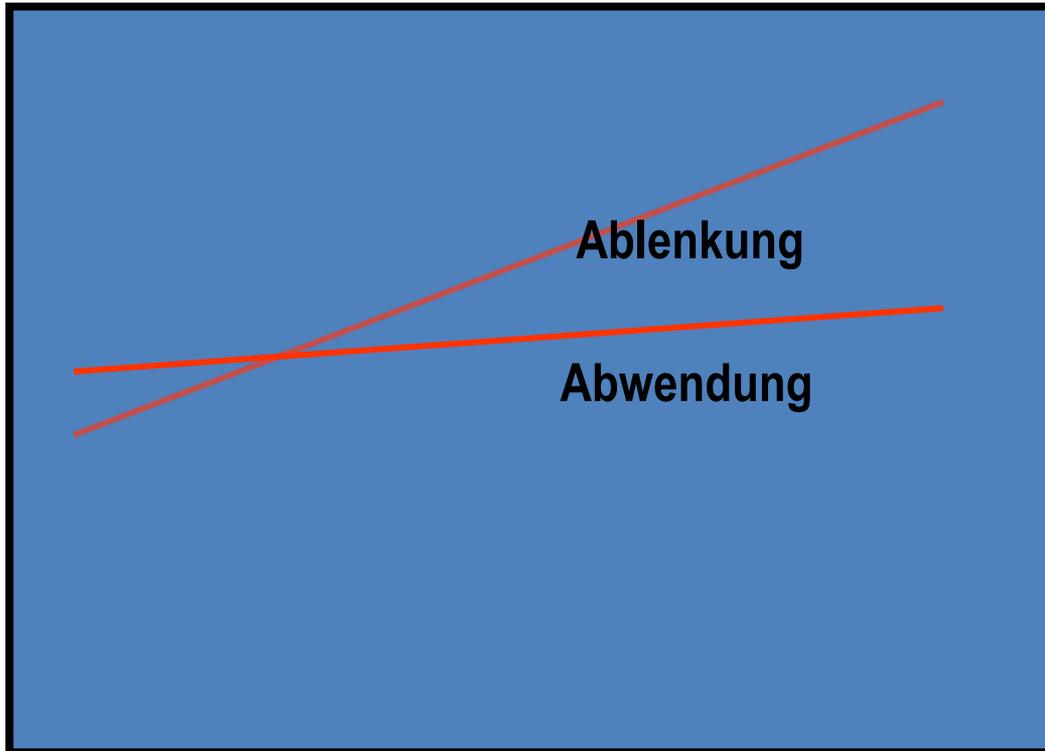
- Negative Emotion (RR=2.01)
- Müdigkeit (RR=1.94)
- Kognitive Ablenkung (RR=1.90)
- Nicht angepasste Geschwindigkeit (RR=1.85)
- Ablenkung durch Navigationsaufgabe (RR=1.65)
- Verstoß (RR=1.62)
- Mangelnde Ortskenntnis (RR=1.62)
- Alkoholisierung (RR=1.55)
- *Kein* früher absolviertes Fahrsicherheitstraining (RR=1.40)
- Mangelnder Sicherheitsabstand (RR=1.39)
- Ablenkung durch Objekte außerhalb des Fahrzeugs (RR=1.32)
- Ablenkung durch Objekte innerhalb des Fahrzeugs (RR=1.30)
- Sonnenblendung (RR nicht definiert); 12 Unfälle (4%), nur Unfallverursacher

Kein signifikanter Einfluss von Alter, jährlicher Fahrleistung, Mangelnder Vertrautheit mit Fahrzeug, Dauer des Führerscheinbesitzes

# Beispiel: Fehlerarten in Abhängigkeit vom Alter



**Reaktions-  
zeiten**



**Ablenkung**

**Abwendung**

**Junge Fahrer**

**Ältere Fahrer**

# Funktionsstärken von **Fahrern** bzw. **technischen Systemen:** **Wahrnehmung bzw. Sensorik**

- Signalaufnahme multimodal und in großen Bereichen
- Detektion schwacher Signale durch Aufmerksamkeitssteuerung & Kontrastverstärkung
- automatische Form- & Raumwahrnehmung
- effiziente Bewegungswahrnehmung
- Detektion von Signalen außerhalb des menschlichen Wahrnehmungsbereiches
- hoch präzise Registrierung und Speicherung von Mess-Daten
- Kontextunabhängigkeit

# Ablaufkontrolle:

## Fahrer

- Kontextspezifische und schemageleitete effektive Suche im Gedächtnis
- Strategienwechsel bei Misserfolg
- Flexibilität hinsichtlich Perspektivenwechsel
- schnelle Plausibilitätsüberprüfung

## technisches System

- Automatische & vollständige Suche in großen Datenmengen - schlagwortgesteuert
- Vollständige Durchführung aller spezifizierten Optionen incl. Permutationen von Reihenfolgehängig
- Parallele Abarbeitung mehrerer komplexer Funktionen

# Planung:

## Fahrer

- Voraussage und Antizipation komplexer Abläufe
- Adaptivität, schnelles Lernen durch Rückmeldung
- Induktives Schließen
- Lösung unvollständig spezifizierter oder neuer Probleme
- Komplexe Entscheidungen auch bei unvollständiger oder widersprüchlicher Information

## technisches System

- Exakte Wiederholung spezifizierter Prozesse mit großen Datenmengen (z.B. Matrizen)
- vollständige Durchführung deduktiver Schlüsse
- vollständige Suche nach Entscheidungsalternativen, die mit allen Daten kompatibel sind und Bewertung nach vorgegebener Strategie

# Orientierung in Bedienungsanleitungen:

## Fahrer

- Effiziente Suche nach bedeutungsgleichen oder ähnlichen Begriffen
- Schnelles Erfassen von Kernaussagen bei Texten (gist)
- (tiefe) Verarbeitung: Repräsentation unabhängig von der grammatikalischen Struktur

## technisches System

- Schnelle Suche nach spezifischen Suchworten und ihren logischen Verknüpfungen

# Informationsverarbeitung:

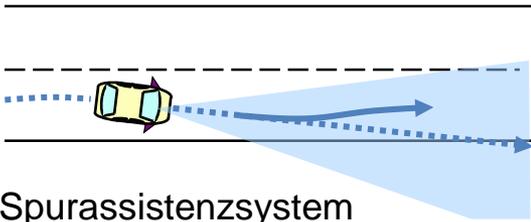
## Fahrer

- Adaptive Regelung bei wechselnden Randbedingungen
- schnelle Detektion relevanter Stellgrößen
- Stabilität durch Variabilität

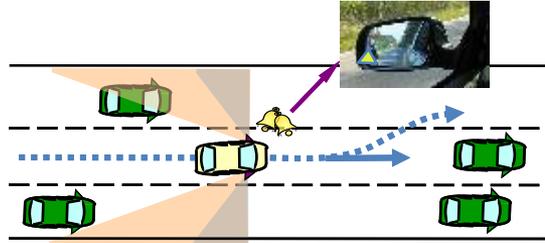
## technisches System

- Effizientes Differenzieren und Integrieren
- schnelle Reaktionen auf vorher definierte Signalmuster und Parameter
- gleichbleibende Qualität bei Produktion und Überwachung über lange Zeit

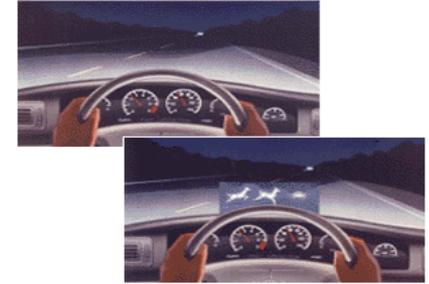
# Überblick Fahrerassistenz-Funktionen:



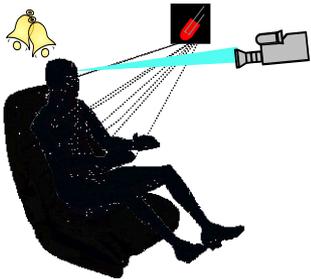
Spurassistenzsystem  
(Lane Departure Warning)



Spurwechselassistent

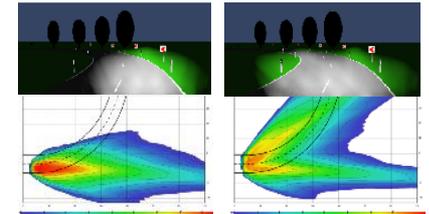


Night Vision

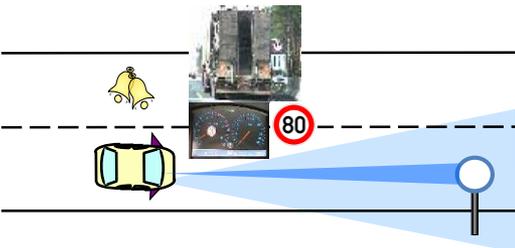


Aufmerksamkeitskontrolle

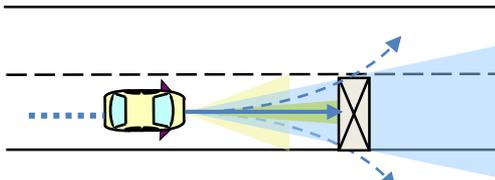
Fahrerassistenzsysteme  
auf dem Weg zum  
„Unfallvermeidenden Auto“



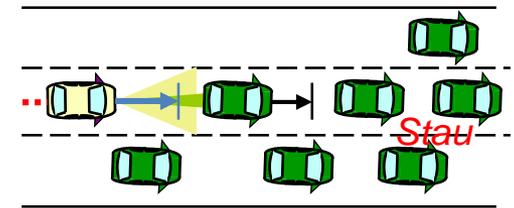
Adaptives Kurvenlicht



Verkehrszeichenerkennung

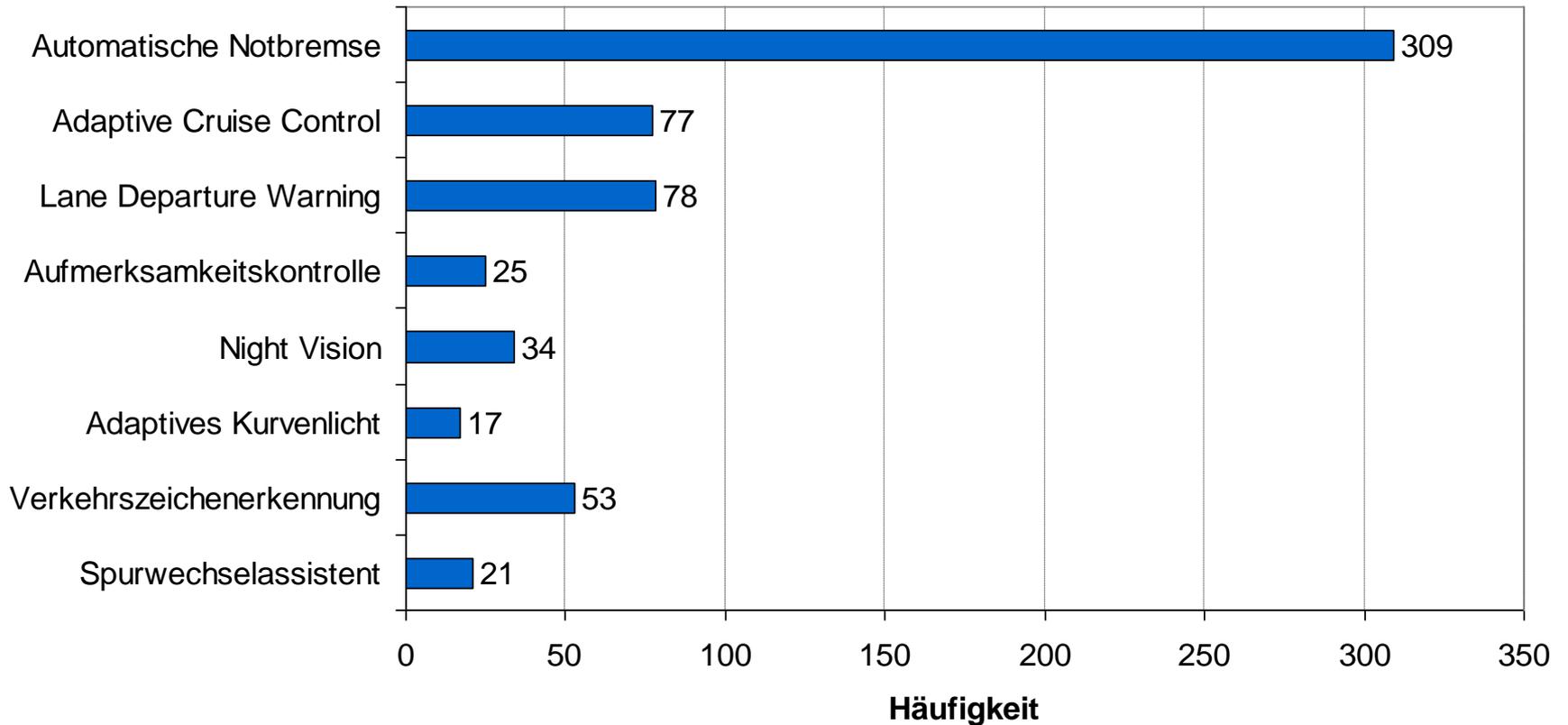


Automatische Notbremse



Abstandstempomat  
(Adaptive Cruise Control)

# Potenziale von Fahrerassistenzsystemen



Anzahl Unfälle: N=312; Anzahl Fahrer: N=528, Mehrfachnennungen möglich

**Vielen Dank für Ihre Aufmerksamkeit!**

Prof. Dr. Dr. h.c. Alf C. Zimmer

# Referenzen

- Die berichteten fahrbezogenen Daten stammen u.a.aus den Projekten MoTiV-MMI und KOMI-ZIF und SANTOS
- Finanzierung: BMBF+T, BMW AG, DaimlerChrysler AG, Bosch AG, General Motors Opel, Freistaat Bayern
- Projektmitarbeiter: K.Dahmen-Zimmer, I.Scheufler, W.Piechulla, M.Praxenthaler J.Bernhardt, I.Kaiser u.v.a.