## Risikoanalysen

# Theorie und Praxis der qualitativen und quantitativen Risikoanalyse, erläutert an Beispielen aus der Praxis

Beitrag zum sicherheitswissenschaftlichen Kolloquium
- Sommersemester 2010 der Bergischen Universität Wuppertal /
Fachgebiet Sicherheits- und Qualitätsrecht, Prof. Dr. Ralf Pieper
am 06. Juli 2010

Dipl. Phys. Dr. H. Spangenberger

Gesellschaft für Anlagen- und Betriebssicherheit mbH

67098 Bad Dürkheim

Bürgermeister-Gropp-Str. 26



#### INHALT

#### 1. Einführung

Begriffsdefinition
Ziel von systematischen Risikoanalysen
Unterschiede und Gemeinsamkeiten verschiedener Methoden
Normative Grundlagen (DIN/EN/IEC/VDI/VDE) von Risikoanalysen

## 2. Risikoanalysen als Entscheidungsgrundlage für sicherheitstechnische Anforderungen

Beispiel 1: Raumordnungs- und Planfeststellungsverfahren für den Ausbau Frankfurter Flughafen und

Einhaltung der Sicherheitsabstände zu einer Anlage, die der Störfall-Verordnung unterliegt.

Beispiel 2: Spannungseinbruch im 100kV-Netz und Ausfall der Notstromschiene,

Schlussfolgerungen aus einer quantitativen Risikoanalyse

#### 3. Möglichkeiten und Grenzen quantitativer Risikoanalysen

Probabilistische Vorgehensweise Verfügbarkeit und Zuverlässigkeit empirischer Daten zu Fehlerraten und Auswirkungsszenarien Verfügbarkeit und Akzeptanz von Risikogrenzen

## 4. Festlegung von Prüffristen und Prüfprozeduren mittels risikobasierter Analysemethoden, Wartung und Instandhaltung als Teil der Anlagensicherheit

Beispiel 3: Korrosionsschaden an einer außen befeuerten Rohbenzinleitung

#### 5. Zusammenfassung

Ausblick auf zukünftige Analysemethoden Zentrale Erfassung und Auswertung von Schadensdaten als Basis für quantitative Methoden Schlusswort



#### 1.1 <u>Begriffsdefinition</u>

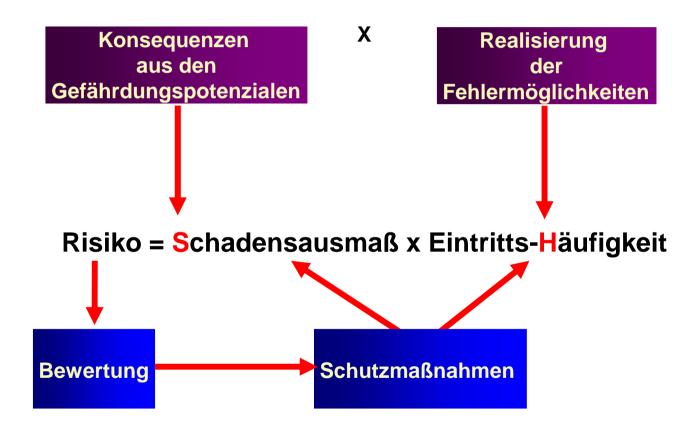
Risiko ist definiert als Produkt aus Schadensausmaß mal Eintritts-Häufigkeit:



**U**mwelt**s**chutz

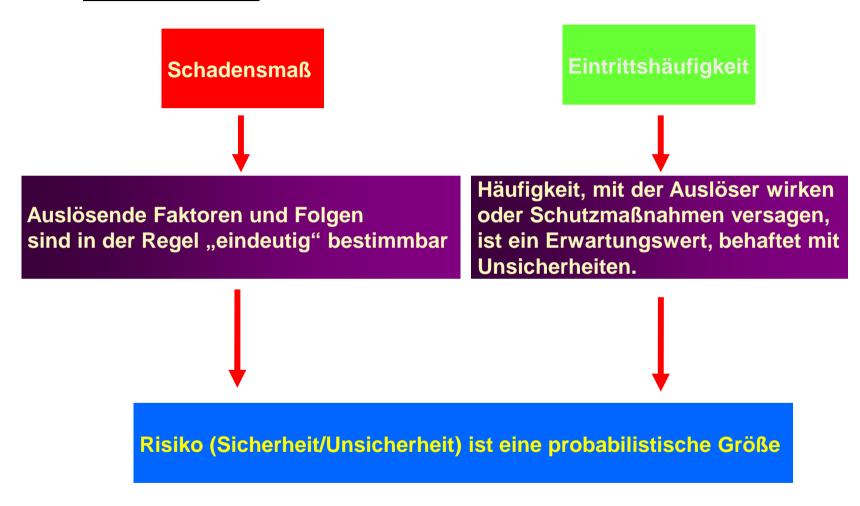
## 1.1 **Begriffsdefinition**

#### Risiko ist somit definiert als Produkt aus





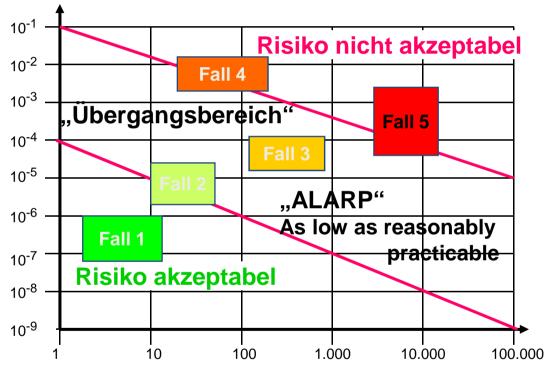
#### 1.1 **Begriffsdefinition**





#### 1.1 <u>Begriffsdefinition (Grenzrisikowerte)</u>





**Todesopfer pro Ereignis** 

#### **Niederlande:**

Akzep. individuelles Risiko 10<sup>-5</sup>/a (bestehende Anlagen) 10<sup>-6</sup>/a (neue Anlagen)

#### **Großbritannien:**

Akzep. individuelles Risiko 10<sup>-3</sup>/a (Arbeiter) 10<sup>-4</sup>/a (Öffentlichkeit)

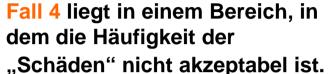
#### **Schweiz:**

F-N-Diagramm
Akzeptanzlinie bei > 10 Toten
und 10<sup>-5</sup> Ereignisse pro
Betrieb und Jahr



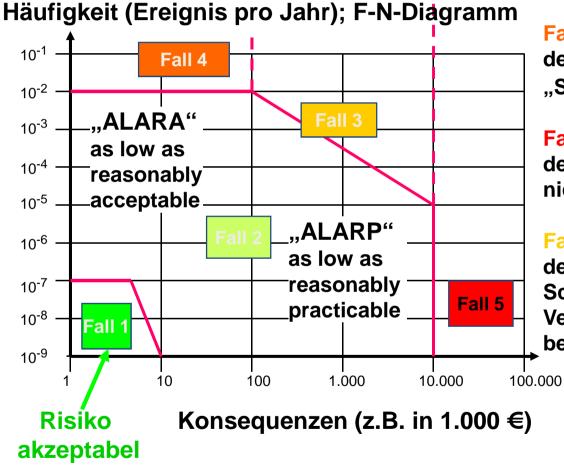
## **Begriffsdefinition (Grenzrisikowerte)**

Risiko nicht akzeptabel (versicherbar)



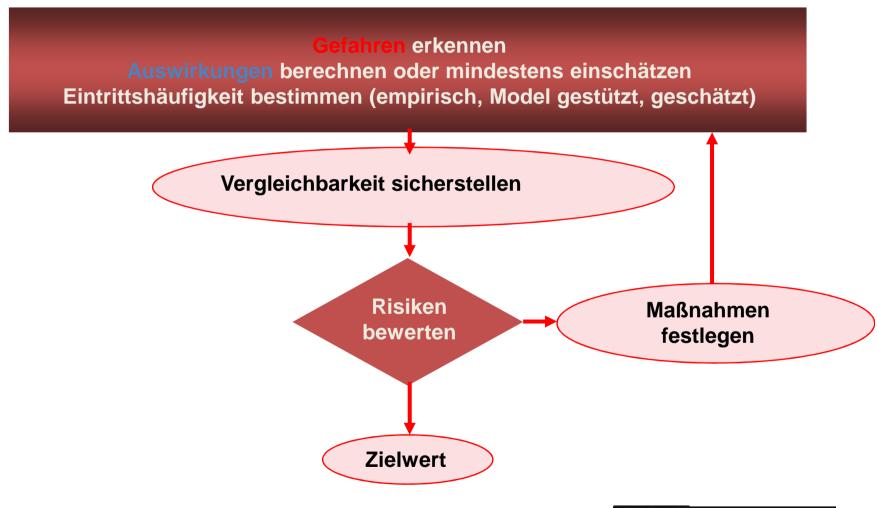
Fall 5 liegt in einem Bereich, in dem die Höhe des Schadens nicht akzeptabel ist.

Fall 3 liegt in einem Bereich, in dem Häufigkeit und Höhe des Schadens den Grad des Versicherungsschutzes bestimmen.



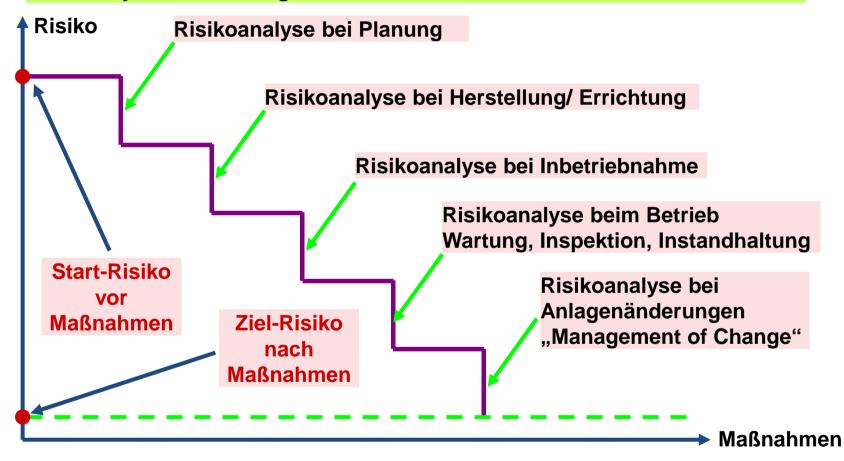
Sicherheitsmanagement Risikoanalysen **U**mwelt**s**chutz

## 1.2 Ziel von systematischen Risikoanalysen

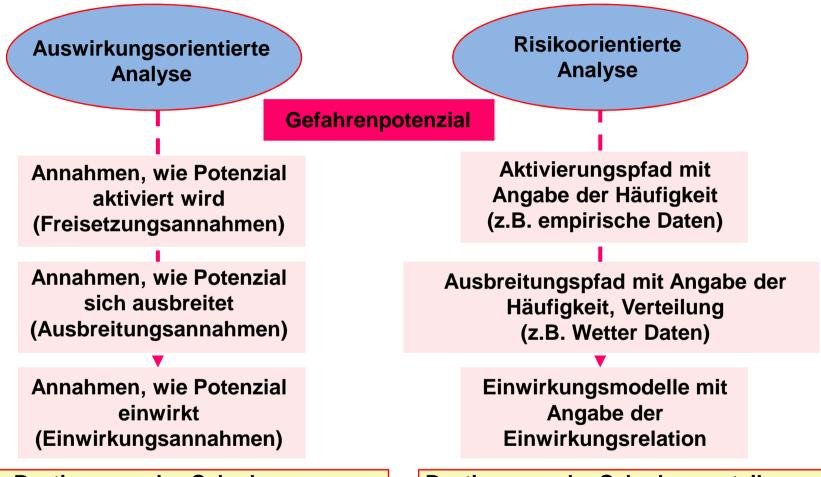


#### 1.2 Ziel von systematischen Risikoanalysen

Systematische Minimierung des Risikos durch Maßnahmen im Verlauf des "Lebenszyklus" der Anlage







Bestimmung des Schadens, keine Quantifizierung der Eintrittshäufigkeit Bestimmung der Schadensverteilung und Quantifizierung der Eintrittshäufigkeit





**Erfahrungswerte** 

Persönliches Urteil

"Bauchgefühl"

Vergleich

Nicht exakt aber akzeptabel, da "common sense" angesprochen"

## **Quantitative Betrachtung**

Analytisches Modell

Feste Anfangswerte

**Feste Endwerte** 

Vergleich der Endwerte mit "Grenzwerten"

Exakt aber "angreifbar", da "feste" Anfangswerte oft zu konservativ oder nicht zweifelsfrei bestimmt

## Probabilistische Betrachtung

Stochastische Modelle

"Unscharfe" Anfangswerte

Erwartungswerte als Ergebnis

Wahrscheinlichkeits-Verteilung

Nicht exakt aber näher an der Realität; Datenbeschaffung aufwendig, mathematisch aufwendig.



**Beispiel 1: Projektilflug** 

#### **Qualitativer Ansatz:**

Projektil kann Schutzobjekt erreichen / nicht erreichen.

#### **Deterministischer Ansatz:**

Nach den Bewegungsgleichungen kann aus dem Anfangsort und der Anfangsgeschwindigkeit die Flugbahn und damit der Trefferort bestimmt werden.

Wenn wir die Anfangsbedingungen kennen (und Reibung etc. vernachlässigen), können wir exakt berechnen, wo das Projektil auftrifft.

#### **Probabilistischer Ansatz**:

Wir kennen den Anfangszustand nicht exakt, also können wir auch nur Wahrscheinlichkeitsaussagen über den Endzustand (Trefferort) machen.



#### **Beispiel 2: Freisetzung eines Gefahrstoffes**

#### **Qualitativer Ansatz:**

Die Freisetzung ist sicherheitsrelevant/nicht sicherheitsrelevant

#### **Deterministischer Ansatz:**

Aus dem Quellterm (in kg/s (t)) bestimmt sich über ein deterministisches Ausbreitungsmodell (z.B. Gaussmodell) die Aufpunktkonzentration, Dosis.

#### **Probabilistischer Ansatz:**

Aus einem Ensemble von möglichen Quelltermen, statistischer Verteilungen der Ausbreitungsbedingungen (Wetterstatistik) ergibt sich eine Wahrscheinlichkeits-Verteilung der Konzentrationswerte an einem bestimmten Aufpunkt.



#### Beispiel 3: Abriss/ Leck an einer Leitung

#### **Qualitativer Ansatz:**

Festlegung einer maximalen Leckagefläche, die

→ "vernünftigerweise" nicht auszuschließen ist.

Ausschluss größerer Leckageflächen

→ im Sinne der "praktischen Vernunft"

#### **Deterministischer Ansatz:**

Folgt dem qualitativem Ansatz mit Eintrittswahrscheinlichkeit "1", und z. B. max. mögl. Druck;

→ Berechnung des größten anzunehmenden Massenstroms (kg/s).

#### **Probabilistischer Ansatz**:

Ermittelt Wahrscheinlichkeit für das Eintreten einer Leckfläche A in Abhängigkeit von Werkstoff, Betriebsbedingungen, Riss-, Bruchmodell,...



Deterministische Untersuchungen basieren auf deterministischen Modellen unter Verwendung von definierten (deterministischen) Anfangs- und Randbedingungen.

Die "variablen" Größen der Untersuchungen wie

- Funktion eines Bauteils,
- Eintritt einer festgelegten Leckfläche,
- Druck, Temperatur, Stoffkonzentration
- <del>Ф</del> ...

treten mit definierter Sicherheit (Wahrscheinlichkeit = "1") ein.

Den Merkmalen von kontinuierlichen Größen (Druck, Temperatur) werden in der Regel feste (konservative) Werte zugeordnet.



Probabilistische Untersuchungen basieren auf stochastischen Modellen unter Verwendung von Wahrscheinlichkeiten für die Anfangs- und Randbedingungen.

Die "variablen" Größen der Untersuchungen wie

- Funktion eines Bauteils,
- **Eintritt einer festgelegten Leckfläche,**
- Druck, Temperatur, Stoffkonzentration
- <del>0</del>

treten mit einem Erwartungswert E und einer Varianz  $\sigma$  ein. Da die günstigste Bedingung (kleinstes Risiko) ebenso im statistischen Ensemble auftritt, wie die ungünstigste, folgt als Resultat die gesamte Brandbreite des Risikos.



#### 1.4 Normative Grundlagen

Systematische Methoden z. B. PAAG oder HAZOP Ausfalleffektanalyse (DIN 25448) Fehlerbaumanalyse (DIN 25424) Ereignisablaufanalyse (DIN 25419)

P→ Prognose, A→ Auffinden, A→ Abschätzen, G→ Gegenmaßnahmen HAZ → Hazard, Op→ Operability

**Technische Normen/Richtlinien:** 

**DIN 2180** 

**DIN 19250** 

**IEC 61508** 

API 581 (Risk based inspection)



2 <u>Risikoanalysen als Entscheidungsgrundlage für</u> <u>sicherheitstechnische Anforderungen im Genehmigungsverfahren</u>

Beispiel 1: "Flugbetriebliche Auswirkungen

auf die Sicherheit von Betriebsbereichen nach StörfallV"

#### **Aufgabenstellung:**

1. Bestimmung der statistischen Häufigkeit (Wahrscheinlichkeit) für den Eintritt eines Störfalls (im Sinne der StörfallV) aufgrund eines Flugzeugabsturzes auf den Betriebsbereich oder im Einwirkungsbereich zum Betriebsbereich.

Einwirkungsbereich meint hier, ein Absturz außerhalb des Betriebsbereichs aber mit Einwirkungen (Brand, Trümmerflug) auf den Betriebsbereich in einer Art und Weise, dass auf dem Betriebsbereich ein Störfall ausgelöst wird.

 Berechnung des individuellen Risikos für Personen aufgrund der Aktivierung des Störfallpotenzials

In Großbritannien und in den Niederlande wurden Risikostudien im Zusammenhang mit dem Absturzrisiko im Nahbereich zu Großflughäfen durchgeführt.

Großbritannien (1997): Untersuchung zum individuellen Risiko von am Flugbetrieb unbeteiligten Personen ("Third Party Risk").

Niederlande (1993): Untersuchung für den Flughafen Schiphol in Amsterdam.

Ziel: Definition von Ausschlussflächen ("Public Safety Zones"), in denen "sensible" Objekte nicht mehr zulässig sein sollen.

"Grenzwert" in Großbritannien: Wert von 10<sup>-4</sup> für bestehende und 10<sup>-5</sup> für neue Objekte, d.h., wenn in einem Zeitraum von 10.000 bzw. 100.000 Jahren eine beliebige nicht mit dem Flugbetrieb in Zusammenhang stehende Person an einem beliebigen Punkt am Boden zu Tode kommt, dann ist für dieses Areal der zulässige Risikowert überschritten.

Im Zusammenhang mit dem Ausbau des Flughafens Frankfurt/Main wurden Risikostudien angefertigt. Diskussion über Risikomanagement und Grenzwerte in Deutschland, Einschalten der Störfallkommission.



#### Berücksichtigung externer Gefahrenpotenziale:

Externe Gefahrenpotenziale sind Auswirkungspotenziale, die nicht mit dem Flugbetrieb zusammenhängen, aber bei einem Treffer aktiviert werden können.

- ⇒ Auswirkungen der externen stofflichen Potenziale können weit über die Auswirkungen des primären Absturzes hinausgehen.
- ⇒ Eine größere Anzahl von Personen kann betroffen sein.
- ⇒ Das Schadensausmaß und damit das externe individuelle Risiko nimmt zu



#### Aufgabenstellung für die Durchführung einer Risikoanalyse

- Ermittlung des stofflichen Gefahrenpotenzials auf dem Betriebsbereich
- Aufstellung eines Gefahrenkatasters für den betroffenen Betriebsbereich
- Auswertung der historischen Absturzereignisse (→ Risikomodell)
  - > Ermittlung der empirischen Absturzhäufigkeiten (Absturzrate AR)
  - → Ermittlung der empirischen Absturzverteilung (AL)
  - → Ermittlung der Größe (Fläche) des primären Unfallfolgengebietes
- Berechnung der lokalen Trefferhäufigkeiten
- Dominoberechnung für den betroffenen Betriebsbereich
- Berechnung der Störfall-Eintrittshäufigkeit
- Berechnung des individuellen Einzelrisikos für Personen im Einwirkungsbereich des Absturzortes und des im Betriebsbereich aktivierten stofflichen Gefahrenpotenzials.



#### **Notwendige Informationen**

- Stoffpotenzial auf dem betroffenen Betriebsbereich innerhalb des Betrachtungszeitraums mit Detailangaben zu
  - → Stoffart
  - → Verfahrensbedingungen (Druck, Temperatur, Konzentration etc.)
  - → örtliche Lage des Stoffpotenzials
  - → Art der Lagerung, Handhabung
  - → Art der Umschließung (Rohrleitung, offener Lagerbehälter, Einhausung etc.)
  - → Art und Wirksamkeit von selbsttätig schließenden Absperreinrichtungen
  - → Angaben zu hemmenden/fördernden Maßnahmen/Einrichtungen, die auf Freisetzung, Brand, Explosion, Dominoeffekt wirken

Alle Angaben werden unter dem Blickwinkel "Einwirkungen durch einen Flugzeugabsturz" betrachtet



#### **Notwendige Informationen**

- Daten über die historischen Absturzereignisse mit Detailangaben wie
  - → Datum des Absturzes
  - → Flugphase (Start, Steigflug, Flug, Anflug, Sinkflug, Landung)
  - → Ort des Absturzes (primärer Aufschlagpunkt, endgültige Lage des –Flugzeugwracks)
  - → Art des Fluges (Passagier, Fracht, Business, Privat, Militär)
  - → Art des Flugzeugs (Hubkolben, Turboprops, Jet, 1., 2. oder 3. Generation)
  - → Herkunftsland der Airline
  - → Flughafen (Land, Größe, Ausstattung, Lage etc.)
- Flugbewegungszahlen und Flugrouten für den Betrachtungszeitraum, die über dem Untersuchungsgebiet verlaufen
- Zusammensetzung (Flugzeugmix) der Flugbewegungen auf den Flugrouten



#### **Begriffsdefinitionen:**

#### **Externes Risiko**

Risiko für eine am Flugverkehr unbeteiligte Person, am Boden außerhalb des Flughafengeländes durch einen Absturz zu Tode zu kommen.

#### Einzelrisiko

Das Einzelrisiko gibt Auskunft darüber, mit welcher Wahrscheinlichkeit pro Jahr ein Mensch, der sich fortwährend an einem bestimmten Ort im Untersuchungsraum aufhält, an den Folgen eines Flugzeugunfalls zu Tode kommt.

#### **Gruppenrisiko**, kumuliert

Das Gruppenrisiko gibt die Wahrscheinlichkeit pro Jahr an, nach der eine Gruppe von N Personen gleichzeitig aufgrund eines Flugzeugabsturzes, stirbt.

#### **Störfallhäufigkeit**

Eintrittswahrscheinlichkeit für einen Störfall, welcher durch einen Flugzeugabsturz auf oder im Einwirkungsbereich einer Anlage nach Störfall-VO ausgelöst wird.



#### **Definition:**

Risiko = Schadensausmaß x Eintrittswahrscheinlichkeit

Schadensausmaß → Messgröße: Anzahl Tode

Eintrittswahrscheinlichkeit → Messgröße: Ereignisse pro Jahr

Risiko → Messgröße Tode pro Jahr

Grenzwerte (?) → Third Party Risk (GB, NL) R ≤ 10<sup>-5</sup> Schweizer W-A-Methode

Schweizer w-A-wethode

**SFK-2003** 

**OVG-Hessen-2009** 



## Häufigkeit für ein Ereignis pro Jahr



**Todesopfer pro Ereignis** 



#### Beschreibung der Methode

Analyse der Absturzereignisse bzgl. Häufigkeit, Art, Ort etc..

⇒ Bestimmung der Absturzrate (Absturz pro Flugbewegung)

Analyse der Absturzereignisse bzgl. Absturzort in Bezug auf Flughafenbezugspunkt (bzw. Bahnschwelle).

⇒ Bestimmung der Absturzverteilung

Analyse der Absturzereignisse bzgl. der Größe des Schadensgebiets und des Schadensausmaßes.

⇒ Bestimmung der primären Schadensfläche



#### **Erkenntnisse**:

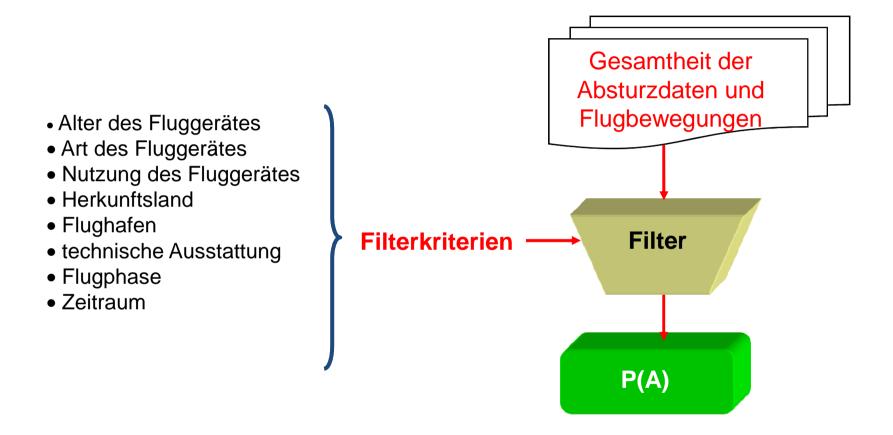
#### Die Absturzrate wird bestimmt durch

- Zeitraum der Auswertung
- Land und Ort (Flughafen) der Ereignisse
- Generation (Typ, Alter etc.) des Flugzeugs
- ...
- ⇒ Die **Absturzrate** (AR) liegt zwischen 0,96 und 0,05 Abstürze pro 1 Million Flugbewegungen (abhängig von den Auswahlkriterien)

#### Die Absturzverteilung zeigt eine Häufung der Ereignisse mit

- abnehmendem Abstand zur Bahnschwelle,
- abnehmendem Abstand zur An- Abfluggrundlinie.
  - ⇒ Trefferhäufigkeit (Risiko) nimmt mit Nähe zum Flughafen und Flugroute zu.







Das Ereignis Treffer "T" bedingt das Ereignis Absturz "A". Mathematisch ausgedrückt lautet der Zusammenhang:

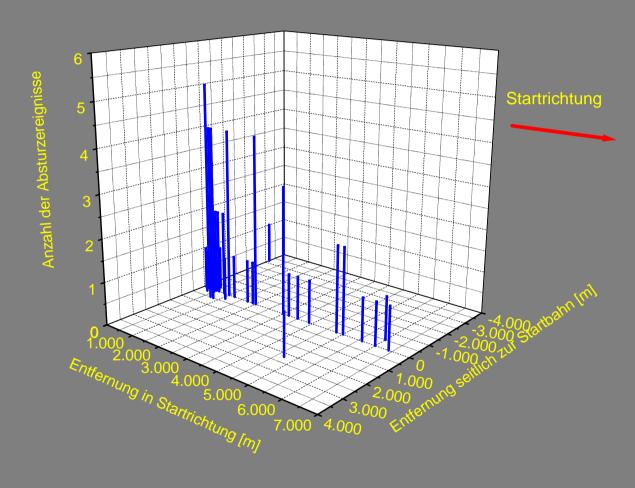
$$P(T \cap A) = P(T|A) \cdot P(A)$$

Unter der Annahme, dass es sich um zwei stochastisch unabhängige Variablen  $P(T \mid A)$  und P(A) handelt, können beide voneinander unabhängig bestimmt werden. Dieser Annahme folgend werden unterschiedliche Datensätze für die Ermittlung der **Absturzrate** (entspricht P(A)) und der **Absturzverteilung** (entspricht  $P(T \mid A)$ ) verwendet.

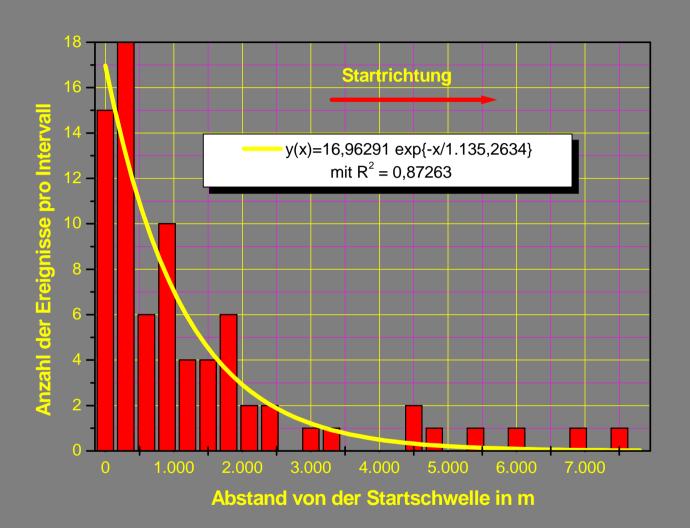
$$P(A) = AR = \frac{A \quad (Anzahl \ der \ Abstürze)}{M \quad (Anzahl \ der \ Flugbewegungen)}$$



## Verteilung der Abstürze beim Start

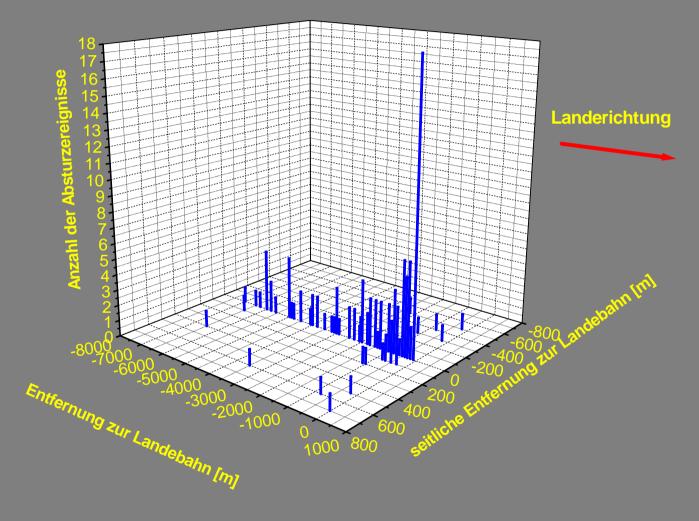




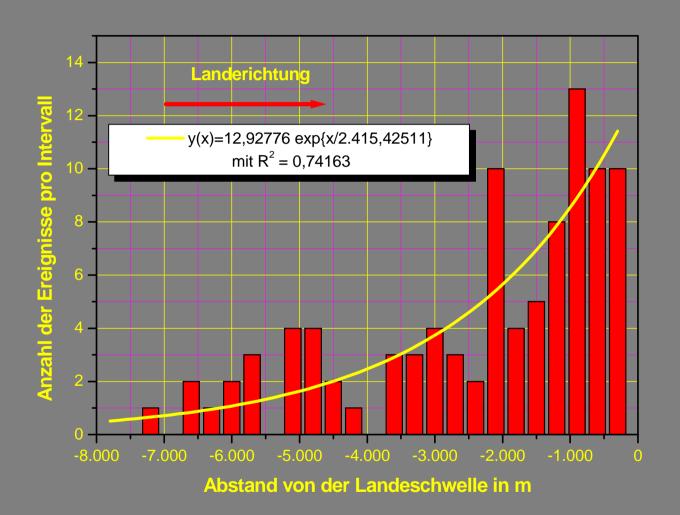




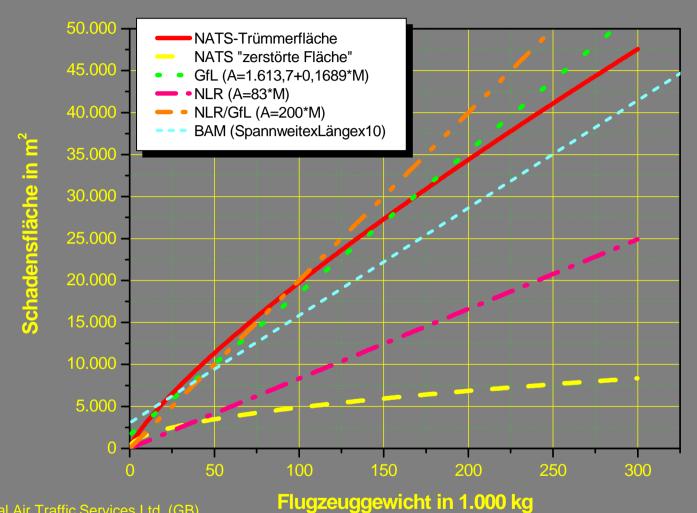
## Verteilung der Abstürze beim Landen







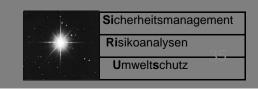




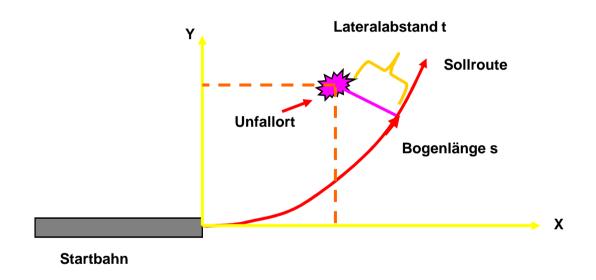
NATS: National Air Traffic Services Ltd. (GB)

NLR: Nationaal Lucht- en Ruimtevaartlaboratorium (NL)

GfL: Gesellschaft für Luftverkehrsforschung (D)
BAM: Bundesanstalt für Materialprüfung (D)



## Projektion der Unfallort-Koordinaten auf die Bahnroute





## R<sub>T</sub>: Trefferhäufigkeit für einen Punkt P(x,y) mit primärer Schadensfläche A<sub>T</sub>

$$R_T(x,y,A_T) = \sum_{i=1}^4 \sum_{j=1}^M AR_i \cdot N_{i,j} \cdot \iint_{A_T} f_{x,y}^i(s,t) \cdot ds \cdot dt$$

AR<sub>i</sub> → Absturzrate für die versch. Absturzkategorien (i)

N<sub>i,j</sub> → Anzahl der Flugbewegungen (Start, Landung, Route)

f<sup>i</sup><sub>x,y</sub>(s,t) → bedingte Wahrscheinlichkeit für einen Absturz an einem Ort P(x,y) bezogen auf die longitudinale (s) und laterale (t) Koordinate der Flugbahn.

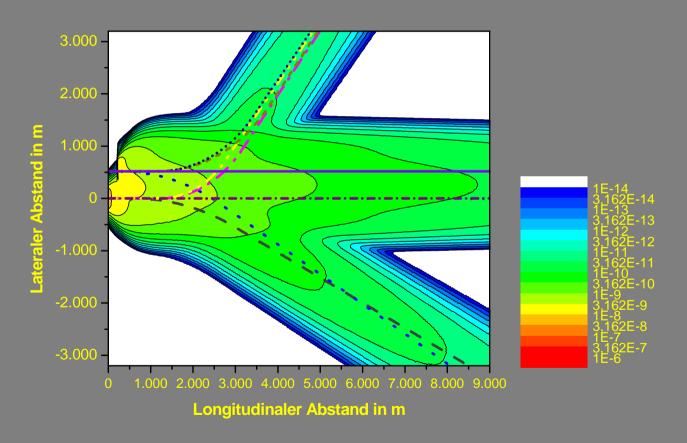
i: Absturzkategorien Start, Landung, Overrun (Start/Landung)

j: Flugrouten (i = 1 bis M)

 $A_{T}$ : Trefferfläche

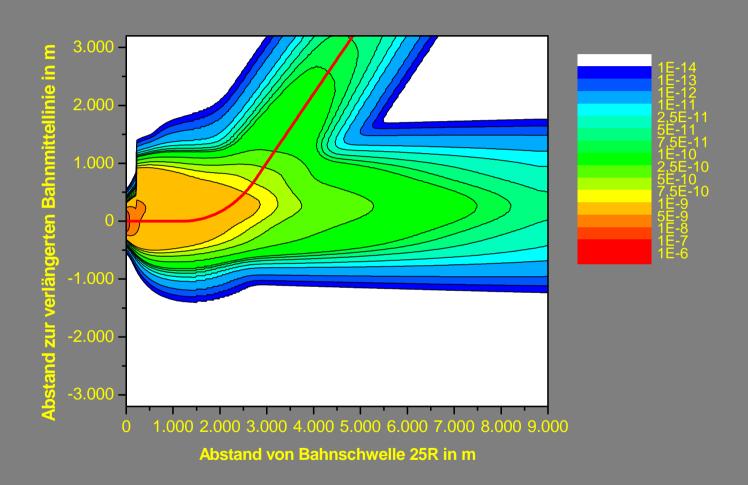


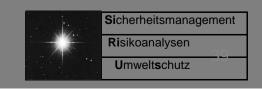
Ergebnis der Auswertung: Verteilung der Trefferhäufigkeit





Ergebnis der Auswertung: Verteilung der Trefferhäufigkeit





Wenn die Trefferhäufigkeit für das primären Ereignis "Flugzeugabsturzes" bestimmt ist, kann ausgehend vom Einwirkungsbereich des Absturzortes, ermittelt werden, welche benachbarte Anlagebereiche durch das primäre Ereignis "Absturz" geschädigt werden.

D. h. Untersuchung der durch den Absturz ausgelösten, Folgeereignisse wie Freisetzung, Brand und Explosion.

Letztere wirken so, dass es an primär nicht betroffenen Anlageteilen ebenfalls zu Freisetzungs-, Brand- und/oder Explosionsereignissen kommt.

#### → DOMINO-Effekt-Berechnung

#### Voraussetzung:

#### Kenntnis über

- die örtliche Verteilung der gefahrenrelevanten Stoffe und Verfahren
- die Stoffeigenschaften (toxisch, brennbar explosiv)
- die Stoffmengen
- Auswirkungsbegrenzende Einrichtungen (Schutzmauern, Einhausungen...)



#### **Ergebnis**:

Die differenzierte Berücksichtigung der lokalen Gefahrenpotenziale zeigt, dass ein Absturz in den Bereich von Produktionsanlagen, d.h. dort, wo sich die zusammenhängenden stofflichen Gefahrenpotenziale befinden, mit einer sehr hohen Wahrscheinlichkeit der Verlust dieser Anlagen eintritt.

## Eintrittshäufigkeit für Eintritt Störfall

1,629 10<sup>-5</sup> Erwartungswert für ein Ereignis in 61.400 Jahren.

### **Untere Schranke**

4,142 10<sup>-6</sup>, Erwartungswert für ein Ereignis in 241.400 Jahren.

## **Obere Schranke**

3,34 10<sup>-5</sup>, Erwartungswert für ein Ereignis in 29.900 Jahren.



#### Ergebnis:

ohne Berücksichtigung des stofflichen Gefahrenpotenzials

1,62 10<sup>-6</sup> (617.284 a<sup>-1</sup>)

 $3,62\ 10^{-7}\ (2.762.431\ a^{-1})$ 

mit stofflichem Gefahrenpotenzial

 $2,643\ 10^{-5}\ (37.836\ a^{-1})$  im Bereich der Produktionsanlagen  $3,62\ 10^{-7}\ (2.762.431\ a^{-1})$  in den nicht durch Domino-Effekten überdeckten

Anlagearealen.



## **Zusammenfassung:**

Im Zusammenhang mit dem externen Risiko Flugzeugabsturz sind die Wechselwirkungen mit örtlich vorhandenen Gefahrenpotenzialen zu betrachten.

Es sind dem Grad des Risikos angemessen entsprechende Vorkehrungen bei

- der Katastrophenschutzplanung,
- der Minimierung der Gefahrenpotenziale am Boden oder
- der Minimierung der Absturzhäufigkeiten

vorzusehen.



## Beispiel 2: "Netzstörung und Schwarzfall"

## **Ereignisbeschreibung:**

Durch ein Gewitter kommt es in einer 110 kV Ringleitung zu einem kurzzeitigen Spannungseinbruch.

Spannungsüberwachung erkennt Spannungseinbruch (<U) und

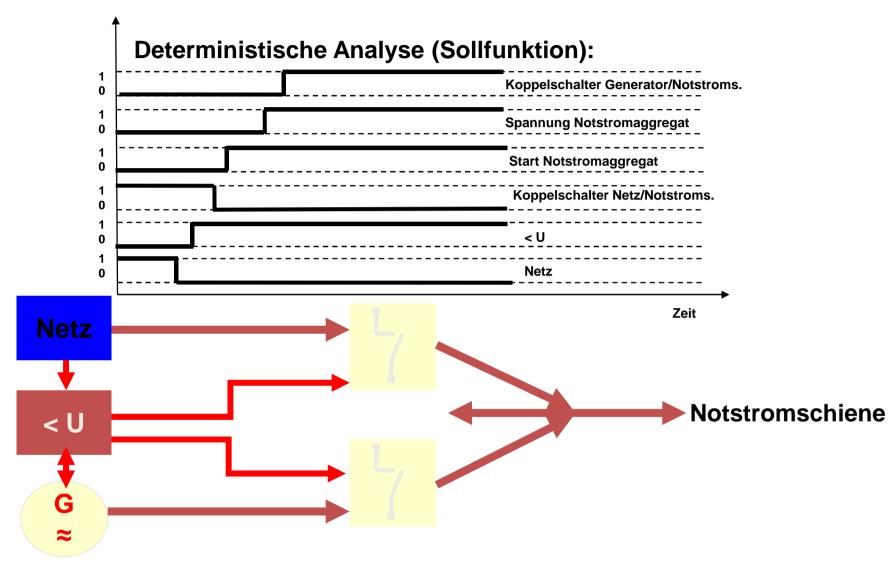
- trennt Notstromschiene von der Netzschiene,
- startet den Notstromdiesel und den Generator.

Spannungsrückkehr wird erkannt,

- Aufschaltung des Notstromgenerators auf Notstromschiene wird gesperrt,
- Rückschaltbefehl für Koppelschalter Notstrom- / Netzschiene wird nicht ausgeführt, da Koppelschalter in Blockade
- → Notstromschiene wird trotz laufendem Notstromgenerator und vorhandenem Netz nicht versorgt.



Beispiel 2: "Netzstörung und Schwarzfall"



## Beispiel 2: "Netzstörung und Schwarzfall"

## Risikoanalyse:

Ein Netzeinbruch ist ein stochastischer Prozess, d. h.:

- Der Spannungseinbruch tritt mit einer statistischen Häufigkeit auf.
- Der Zeit-Spannungsverlauf wird durch ein Ensemble von möglichen Ereignisabläufen beschrieben.
- Das Ansprechverhalten der Spannungsüberwachung besitzt eine Zeitunschärfe.
- Die Koppelschalter besitzen eine Schalthysterese.
- Die Anlaufzeit des Notstromgenerators inkl. Spannungsüberwachung bis zum Aufschalten auf die Notstromschiene ist "endlich".

Verhalten der Umschaltung bei Netzwiederkehr vor Erreichen eines stabilen Notstrombetriebs?

Koppelschalter Netz/Notstromschiene erhält Schließsignal während der das Öffnungssignal ausgeführt wird. → Koppelschalter geht in Blockade



## Beispiel 2: "Netzstörung und Schwarzfall"

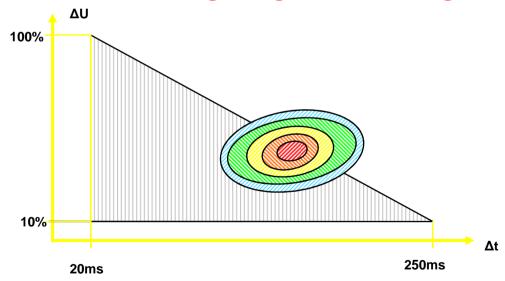
## Risikoanalyse:

Statistische Analyse der beteiligten Komponenten mittels Monte-Carlo-Simulation.

Monte-Carlo-Simulation der Netzstörung.

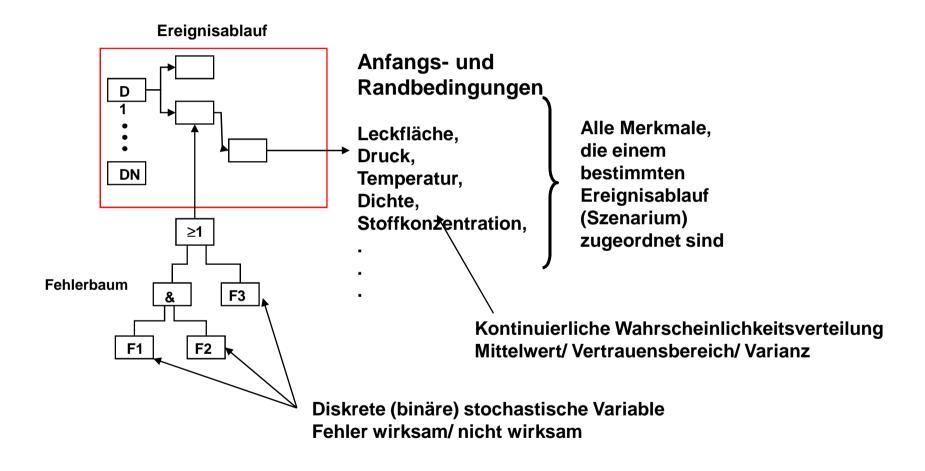
Bestimmung der Eintrittswahrscheinlichkeit für eine Blockade des Koppelschalters.

LÖSUNG: Zeitverzögerung für Auslösung des Schließsignals.





#### 3.1 Probabilistische Vorgehensweise

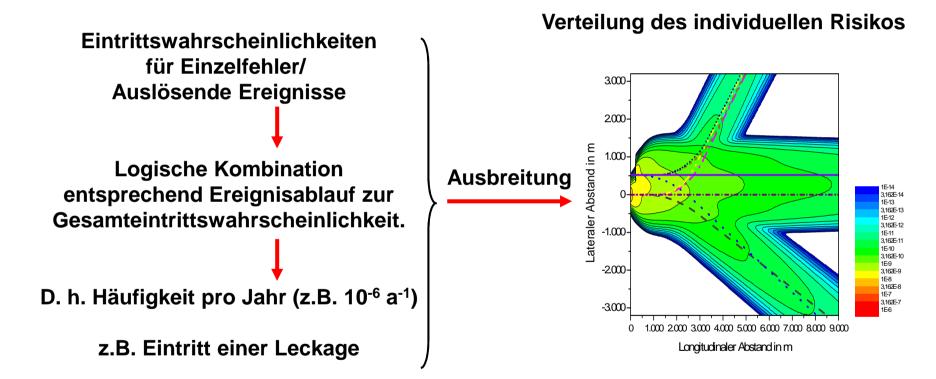




#### 3.1 Probabilistische Vorgehensweise



### 3.1 Probabilistische Vorgehensweise





- 3 <u>Möglichkeiten und Grenzen quantitativer Risikoanalysen</u>
- 3.2 Verfügbarkeit und Zuverlässigkeit empirischer Daten zu Fehlerraten und Auswirkungsszenarien

"Je exakter der Mensch plant, um so sicherer trifft ihn der Zufall"

Risiken, Gefahren sind in Grenzen erkennbar ("praktische Vernunft")

aber

der Zeitpunkt des Eintritts ist nicht planbar und das Ausmass kann nur mit Unsicherheiten vorhergesagt werden.



- 3 <u>Möglichkeiten und Grenzen quantitativer Risikoanalysen</u>
- 3.2 Verfügbarkeit und Zuverlässigkeit empirischer Daten zu Fehlerraten und Auswirkungsszenarien

Unsicherheit bestehen durch

- Statistische Unsicherheiten und Zufallsfehler (keine Messung ist exakt).
- Zeitliche Schwankungen von Modellgrößen, die nur unzureichend erfasst oder bekannt sind.
- Systematische Fehler.
- Unsichere subjektive Einschätzungen.
- Unsicherheiten in der Modellierung.

Einige der Unsicherheiten könnten durch entsprechenden Aufwand minimiert (aber nie vollständig beseitigt) werden.

Andere Unsicherheiten sind Ausdruck unseres eingeschränkten Wissens über bestimmte Zusammenhänge, Abläufe.



#### Verfügbarkeit und Akzeptanz von Risikogrenzen

Verbindliche Risikogrenzwerte gibt es für die EU derzeit nicht. In den Niederlanden, Großbritannien sowie in der Schweiz liegen "Grenzwerte" vor. Insbesondere in der Schweiz liegt mit der Richtlinie

"Beurteilungskriterien zur Störfall-Verordnung" eine verbindliche Vorgabe vor.

StFV

Artikel 6 Beurteilung des Kurzberichts, Risikoermittlung

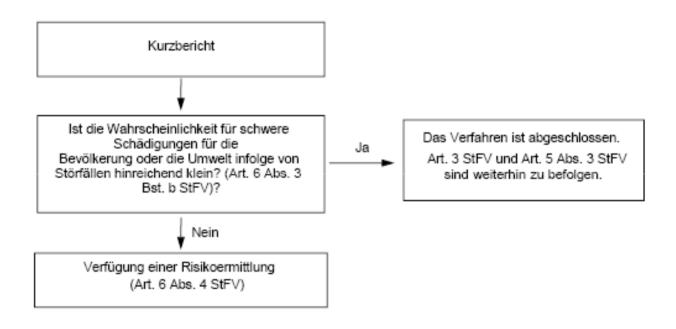
- Sie [die Vollzugsbehörde] beurteilt, nach einer allfälligen Besichtigung vor Ort. ob die Annahme zulässig ist, dass:
  - b. bei Verkehrswegen die Wahrscheinlichkeit, mit der ein Störfall mit schweren Schädigungen eintritt, hinreichend klein ist.
- Ist diese Annahme nicht zulässig, so verfügt sie, dass der Inhaber eine Risikcermittlung nach Anhang 4 erstellen muss.

Artikel 3 StFV gilt immer

Auch nach Abschluss des Verfahrens auf Stufe Kurzbericht hat der Inhaber die allgemeinen Sicherheitsmassnahmen zu befolgen (Art. 3 StFV) und den Kurzbericht bei wesentlichen Änderungen zu ergänzen (Art. 5 Abs. 3 StFV).



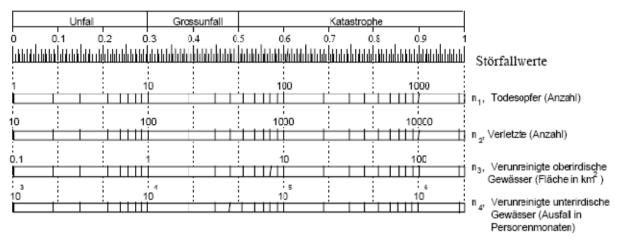
## 3.3 Verfügbarkeit und Akzeptanz von Risikogrenzen



Figur 1: Vorgehen bei der Beurteilung der hinreichend kleinen Wahrscheinlichkeit



## 3.3 Verfügbarkeit und Akzeptanz von Risikogrenzen

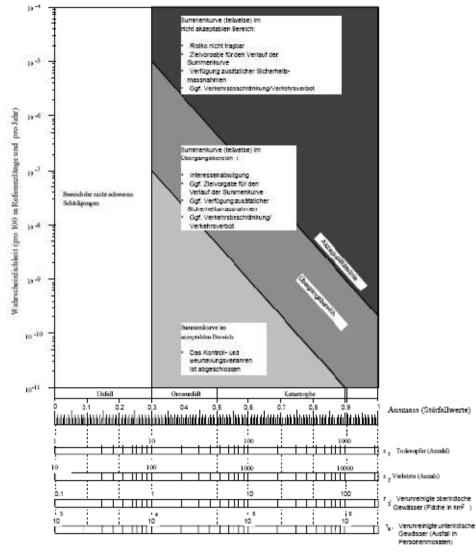


Figur 2: Zuteilung von Störfallwerten



# 3.3 Verfügbarkeit und Akzeptanz von Risikogrenzen





Figur 3: W-A-Diagramm mit Kriterien zur Beurteilung des Risikos.



### 3.3 Verfügbarkeit und Akzeptanz von Risikogrenzen

Die Bestimmung von Risikowerten und die Festlegung von Risikogrenzen müssen im gleichen Kontext stehen (→ Vergleichbarkeit).

Aus der systematischen Auswertung von schweren Unfällen und den damit verbundenen Konsequenzen (Anzahl betroffener Personen, Umweltschäden, Investmentschäden) lassen sich Risikogrenzwerte "technisch begründet" festlegen.

Die Akzeptanz ist eine gesellschaftspolitische Aufgabe:

- Persönliche Betroffenheit
- → Wirtschaftliche Belange (Wettbewerbsfähigkeit)
- Transparenz der gewählten Verfahren zur Bestimmung des Risikos und der Risikogrenzen



## 3.3 Verfügbarkeit und Akzeptanz von Risikogrenzen

Für den Ausbau des Flughafen Frankfurt/Main wurden im PFB vom sowie im Beschluss des Hessischen Oberverwaltungsgerichts die folgenden Risikowerte als gesellschaftlich akzeptiertes Risiko eingestuft

Einzelrisiko für Wohnimmobilien: 3 x 10-5

(gleich einem Ereignis in 33.000 Jahren)

Einzelrisiko für Gewerbeimmobilien: 1 x 10-4

(gleich einem Ereignis in 10.000 Jahren)

Gruppenrisiko für 1 betroffene Person: 1 x 10-1

(gleich einem Toten in 10 Jahren)

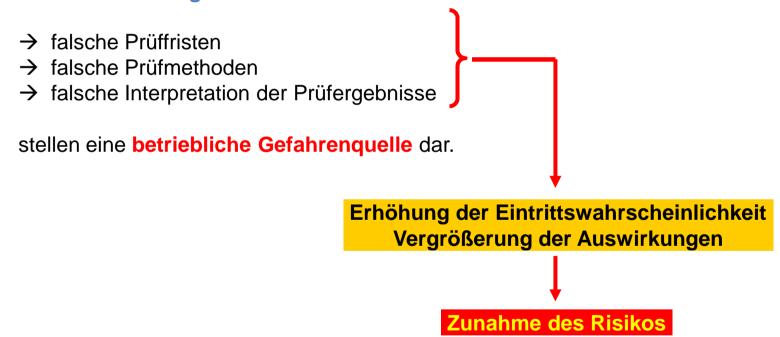
**Gruppenrisiko für 10.000 betroffene Person:** 1 x 10-5

(gleich 10.000 Toten in 100.000 Jahren)



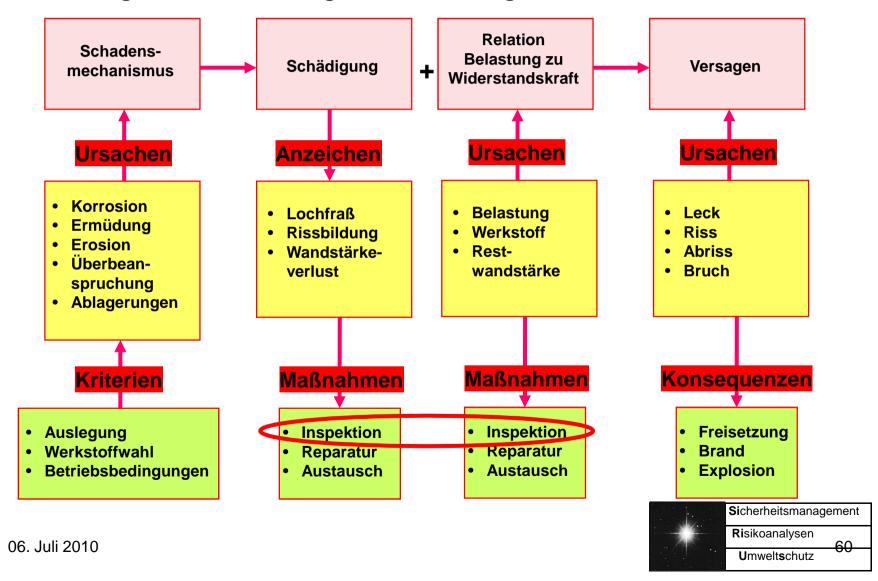
## 4.1 Wartung und Instandhaltung als Teil der Anlagensicherheit

Wartung und Instandhaltung sowie wiederkehrende Prüfungen sind Teil des Sicherheitsmanagements.

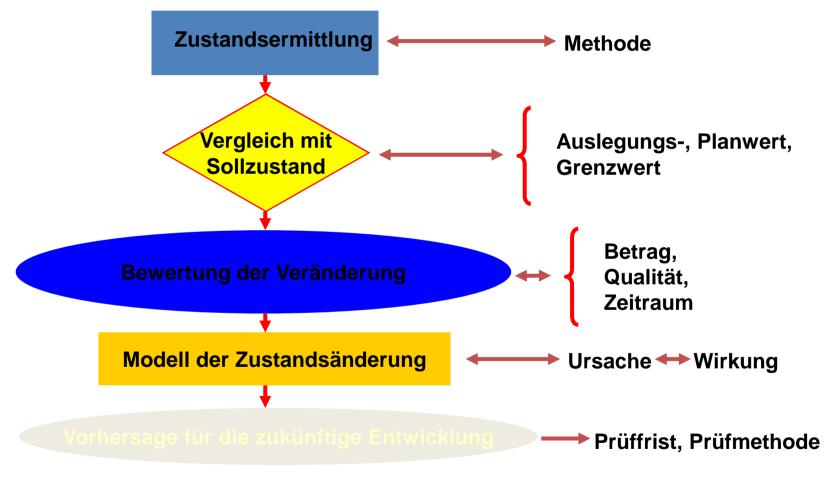




4.1 Wartung und Instandhaltung als Teil der Anlagensicherheit



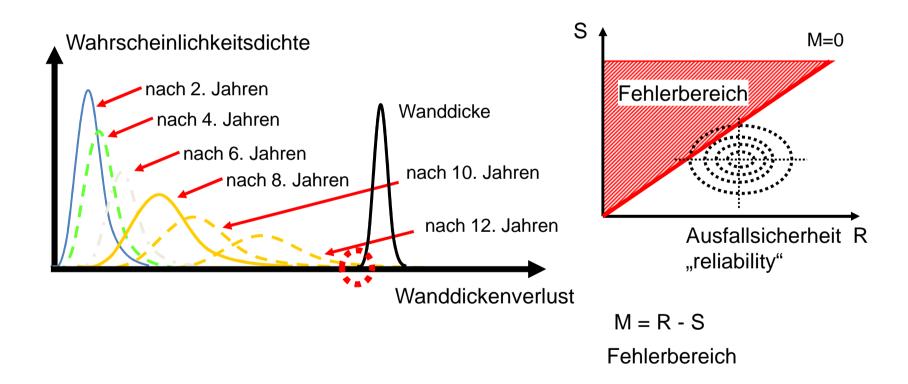
- 4 Festlegung von Prüffristen und Prüfprozeduren mittels risikobasierter Analysemethoden
- 4.1 Wartung und Instandhaltung als Teil der Anlagensicherheit





## 4.1 Wartung und Instandhaltung als Teil der Anlagensicherheit

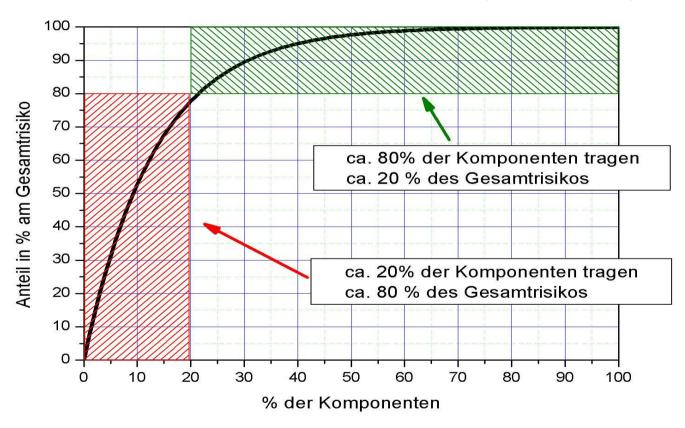
Durch empirische Daten wird ein statistisches Modell über die Fehlerrate bestimmt.





#### 4.1 Wartung und Instandhaltung als Teil der Anlagensicherheit

Risikobasierte Methoden erfordern die Identifizierung der Risiko tragenden Komponenten.





4.4 Beispiel: Korrosionsschaden an einer außen befeuerten Rohbenzinleitung

#### Ausgangszustand:

Edelstahlleitung  $\varnothing_{\text{innen}}$  168,3 Wandstärke: 8,7 bzw. 7.1 mm Werkstoff: ASTM A 335-95A P5 (W-Nr. 1.7362), ein Cr-Mo-Stahl mit 5 % Cr-Anteil

Außen-Direktbefeuert

Wanddicken-Historie durch Messung an den außen liegenden Rohrleitungen. "Übertragung" der Befunde auf die innen liegenden, nicht inspizierten Rohrleitungen.





4.4 Beispiel: Korrosionsschaden an einer außen befeuerten

Rohbenzinleitung

#### **Endzustand:**

Vollständiger Aufriss
Freisetzung von Rohbenzin
mit ca. 300℃ und max. 32bar.
Vollständige Zerstörung des
Erhitzers sowie einiger
benachbarter Anlageteilen.

Projizierter Prüfzyklus: 5 Jahre Schadenseintritt, 3 Jahre nach Inbetriebnahme (Austausch).

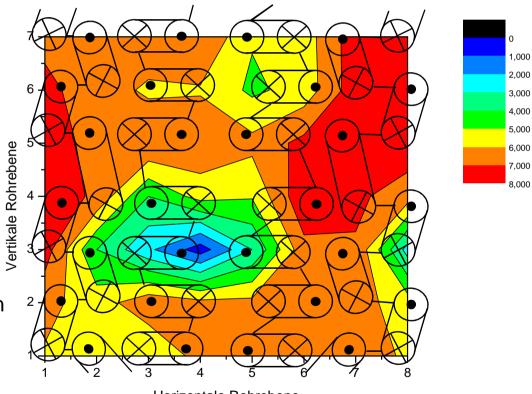




# 4.4 Beispiel: Korrosionsschaden an einer außen befeuerten Rohbenzinleitung

## Verteilung der Restwandstärken:

Im zugänglichen
Außenbereich wurden
durchgängig "sichere"
Restwandstärken
gefunden.
Im inneren, nicht
zugänglichen Bereich
lagen bereits erhebliche
Wanddickenminderungen
vor.



Horizontale Rohrebene



- 4 Festlegung von Prüffristen und Prüfprozeduren mittels risikobasierter Analysemethoden
- 4.4 Beispiel: Korrosionsschaden an einer außen befeuerten Rohbenzinleitung

## Schlussfolgerungen:

Die Festlegung der Prüffristen sollte nicht allein auf der historischen Entwicklung des Korrosionspotenzials aufbauen. Zu beachten sind:

- → Prognose der zukünftigen Entwicklung des Korrosionspotenzials.
- → Änderungen in der Betriebsweise.
- → Auswirkungen von Störungen des bestimmungsgemäßen Betriebs auf die Zeitstandsfestigkeit von Produkt führenden Apparaten und Rohrleitungen.



## 5 Zusammenfassung

#### 5.1 Ausblick auf zukünftige Analysemethoden

## Die Entwicklung geht in Richtung

- Risikobasierte Sicherheitsanalyse,
- Risikobasierte Auswahl, Spezifikation von Schutzsystemen (siehe IEC 61508)
- Risikobasierte Wartung und Inspektion (Beispiel: API 581 "Risk based inspection")

Als Analysemethoden stehen bereits heute EV-Systeme zur Verfügung

Expertsysteme werden weiterentwickelt.



- 5 Zusammenfassung
- 5.2 Zentrale Erfassung und Auswertung von Schadensdaten als Basis für quantitative Methoden

Risikobasierende Sicherheitsanalysen, quantitative Risikoanalysen erfordern Daten über

- Ausfallhäufigkeiten,
- Fehlerraten im Anforderungsfall
- Gefahrenpotenzial <-> Konsequenzrelationen

Solche Daten lassen sich nur durch eine systematische Erfassung von schweren Unfällen mit Angaben über

- Art, Menge, Zustand der beteiligten Stoffe, Verfahren etc.
- Ablauf des Ereignispfades
- Art und Umfang der Konsequenzen

ermitteln.

→ Konsequente Auswertung von "schweren Unfällen" inkl. systematische Ursachenanalyse

## 5 Zusammenfassung

#### 5.3 Schlusswort

Alle Methoden beginnen mit einer qualitativen Bewertung und "Vertrauen" auf den "gesunden Sachverstand".

Die deterministische Methode vertraut darauf, dass man die Randbedingungen und die Anfangsbedingungen realistisch beschreiben kann.

Die probabilistische Methode ergänzt die deterministische Methode durch die "naturgegebenen" Unsicherheiten.

Soweit diese ausreichend beschreibbar sind, entsteht ein Abbild der "Realität".

Kein Risikowert ist frei von Unsicherheiten, daher müssen diese mit angegeben werden.

Nur unter gleichen Randbedingungen können Risikowerte miteinander verglichen werden.

**Si**cherheitsmanagement

Risikoanalysen

Umweltschutz

- 5 Zusammenfassung
- 5.3 Schlusswort

## Ich danke für Ihre Aufmerksamkeit!

