ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Grundlagen der technischen Risikoanalytik

Basismethoden der Risikoanalytik

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Inhalt

- Standisierter Ansatz, screening-Methoden:
  - Checklisten
  - Master Logic Diagramm (MGL)
  - Fishbone-Diagramm
- Standardisierter Ansatz, tabellarische Methoden:
  - Hazard and Operability Study (HAZOP)
  - Failure Mode and Effects Analysis (FMEA)
  - Zurich Hazard Analysis (ZHA)
- Analytischer Ansatz, formale Methoden:
  - Ereignisbaum (ETA)
  - Fehlerbaum (FTA)

Einführung in methodische Ansätze

Intuitiver Ansatz

Expertenschätzung
Brainstorming
What-If-Methode
Delphi-Methode

Standardisierter Ansatz

Checklistenverfahren
PHA, ZHA
HAZOP, PAAG
MORT
Safety Review/Audit

Standardisierter Ansatz

Statistischer Ansatz

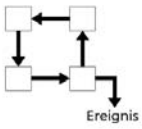
Datenauswertung
Datenanalyse

Analytischer Ansatz

Logische Bäume

Ausbreitungs-, Wirkungsmodelle

Simulationen



Checklisten

Uni Bonn
ABTEILUNG 4.2 - SICHERHEITSWESEN/UMWELTSCHUTZ

Checkliste „Laborsicherheit“

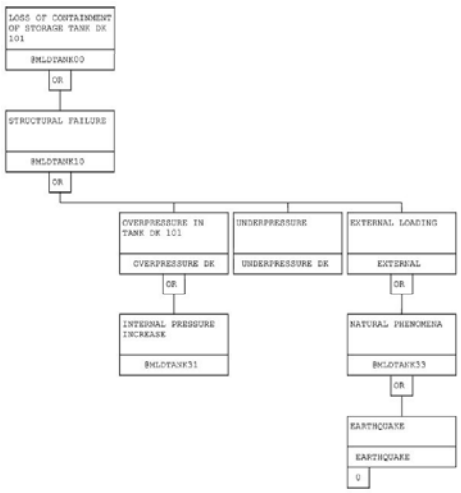
		ja	nein	
1.	Ist das Labor so möbliert, dass die Mindestverkehrsbreite bei 1 m liegt?			
	Ist zwischen gegenüberliegenden Arbeitsplätzen ein Mindestabstand von 1,45 m eingehalten?			
	Befindet sich, falls vorhanden, der Schreibarbeitsplatz im Labor an einer halbwegs geschützten Stelle?			
2.	Ist ein Notausgang oder Notausstieg vorhanden?			
	Ist der Notausgang/Notausstieg gekennzeichnet?			
	Ist der Notausgang/Notausstieg gut zugänglich?			

(Quelle: http://www.sichtech.uni-bonn.de/Wob/images/88648442.pdf)

Master Logic Diagram

- Ziel
- Finden der (Ausfall-)Ursachen eines unerwünschten Ereignisses ("top event").
- Methodik
- qualitativ
  - Definition eines unerwünschten Ereignisses,
  - Bilden von detaillierteren Sub-Ereignissen/Ereigniskategorien,
  - Abbruch bei Einzelursachen („Basisereignissen“).
- quantitativ
  - Belegen eines Basisereignisses mit einer Ereigniseintrittshäufigkeit (Ausfallwahrscheinlichkeit, -rate),
  - Aufsummierung aller Kenngrössen.
- Voraussetzung
- Die Basisereignisse sind voneinander unabhängig.

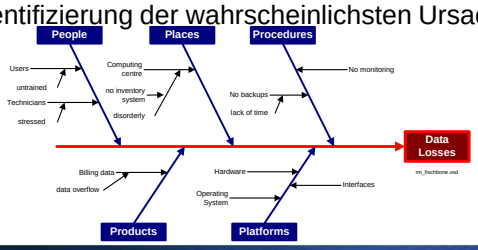
Beispiel: Master Logic Diagram



I.A. Papazoglou, O.N. Aneziris, Master Logic Diagram: in Journal of Hazardous Materials A97 (2003) 11–30

Fishbone-Diagramm (Ishikawa Diagramm)

- Methodik
- Strukturiertes Brainstorming,
- Definition des unerwünschten Effektes,
- Identifizierung der "Hauptkategorien" potentieller (Ausfall-) Ursachen des Effektes,
- schrittweises hinzufügen detaillierterer Ursachen pro Haupt- und Unterkategorien,
- Identifizierung der wahrscheinlichsten Ursachenkette.



Hazard and Operability Study (HAZOP)

- Ziel und Gründe für eine HAZOP
- Qualitative (tabellarische) Untersuchung von Prozessen durch vorgegebene Leitwörter, die Ursachen und Wirkungen einer Abweichung von einem Sollzustand erkennbar machen, d.h.
  - Erkennung von Gefahren in dem System oder hervorgerufen durch das System,
  - Erkennung der Ursachen betrieblicher Störungen und Abweichungen in der Produktion, die zu nicht spezifikationsgemässen Produkten führen können.
- Verschärfte behördliche Auflagen oder Empfehlungen, z.B. DIN IEC 56(Sec)410:1994: Analyse des Risikos technischer Systeme – Leitfaden.
- Anwendungsbereich
- (Verfahrens-)technische Systeme allgemein,
- für kontinuierlich produzierende Anlagen entworfen,
- auf diskontinuierliche Prozesse ("batch-Betrieb") übertragbar.
- Referenzdokumente
  - Gefährdungs- und Betreibbarkeitsuntersuchung (DIN IEC 56/581/CD:1998-01),
  - PAAG-Verfahren (Prognose, Auffinden, Abschätzen, Gegenmassnahmen)

Tabelle für eine HAZOP

Leitwort	Abweichung	Mögliche Ursachen	Folgen	Erforderliche Handlung

Arbeitsschritte der HAZOP

- Vorbereitung: Festlegen der Analyseschwerpunkte, Leitwörter und Prozess-variablen,
- Zusammensetzung des Teams,
- Beschaffung von Anlageninformationen,
- Dokumentation der Ergebnisse (Formular).
- zu 1. Vorbereitung
- Einfache Beschreibungen zur Erkennung von Abweichungen vom verfahrenstechnischen Sollzustand durch Verknüpfung eines Leitwortes mit einer Prozessvariablen, z. B.
- kein Massenstrom,
- mehr Systembestandteile (Korrosionsprodukte, Mehrphasenströmungen usw.),
- anderer Betriebszustand als vorgesehen, z. B. Wartung statt Normalbetrieb.

Leitwörter

- Kontinuierlicher Prozess

Leitwort	Bedeutung
kein	Verneinung der Konstruktionsvorgabe
geringer, weniger	quantitative/qualitative Abnahme
höher, mehr	quantitative/qualitative Zunahme
anders	abweichende Betriebszustände

- Diskontinuierlicher Prozess

Leitwort	Vorgang
keine	Beladung mit A
zuviel	Beladung mit A
zuwenig	Beladung mit A
andere	Beladung als mit A
umgekehrte	Beladung (Rückfluss)

zu 2. Teamzusammensetzung (Beispiel)

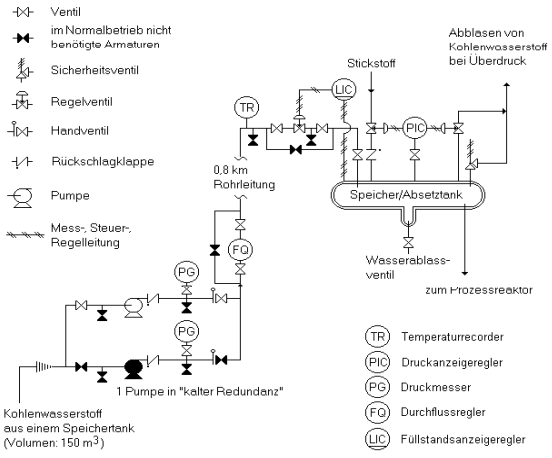
- Vorsitzender: „unabhängiger“ Experte für HAZOP,
- betriebsspezifische Experten: Betriebsleiter, Verfahrensingenieur, -techniker, Wartungs-, Instrumentierungsingenieur,
- ca. 5 bis 7 Personen, je nach Anlagengrösse, -typ und -realisierungsphase.

zu 3. Anlageninformation

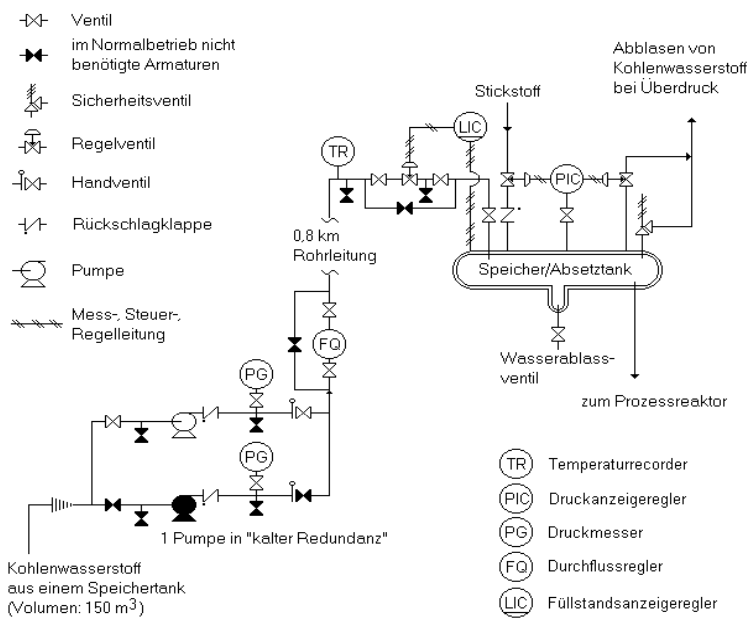
- Umfangreiche Unterlagen über:
- „Anlagen- und Systemhardware“, z.B. Konstruktionszeichnungen, Rohrleitungsschemata, Anlagenauslegungen,
- „Anlagen- und Systemsoftware“, z.B. Betriebsvorschriften, -handbücher.
- Diese Unterlagen müssen
- aktuell,
- auf dem gleichen Stand,
- in sich widerspruchsfrei sein.

- Sie sollten durch Anlagenbegehungen überprüft werden.

Beispiel: Olefin-Dimerisationsanlage



Ein Kohlenwasserstoffgemisch wird von einem Speichertank in einen N_2-gekühlten Absetztank gepumpt. Der erste und der zweite Tank sind ca. 800 Meter voneinander getrennt. Die Transferleitung führt an einem öffentlichen Verkehrsweg entlang. Der Absetz-tank erlaubt, Wasser manuell abzulassen. Überdrücke in der Ummantelung zur N_2-Kühlung werden über einen Druckanzeigeregler (PIC) erkannt. Überdrücke im Tank werden über ein Sicherheitsventil abgebaut.



Beispiel für Ergebnisse einer Analyse nach HAZOP

Leitwort	Abweichung	Mögliche Ursachen	Folgen	Erforderliche Handlung
kein	kein Fluss	1) kein KW aus dem Speicher-tank	reduzierter oder kein Output zum Prozessreaktor	a) gewährleisten guter Kommunikationsverbindungen mit Operateur an Speichertank
				b) Einbau eines Tiefstandalarms am Absetztank
		2) aktive Pumpe fällt aus	wie 1), kein Auffüllen des Absetztanks	c) entsprechend b), Überprüfung der Pumpenfilter
		3) Leitungsblockierung, Absperrventil vor oder Regelventil nach aktiver Pumpe geschlossen	wie 1), Überhitzung der aktiven Pumpe, kein Auffüllen des Absetztanks	d) entsprechend b), Überhitzungsschutz für Pumpen einbauen
		4) Leitungsbruch	kein Output zum Prozessreaktor	e) regelmässige Kontrolle der Transferleitung
höher	erhöhter Fluss	5) beide Pumpstränge in Betrieb, z.B. nach Wartungsarbeiten	Überfüllung des Absetztanks	f) Einbau eines Überfüllungsalarms an LIC
….	….	….	….	….
mehr	mehr Wasser im Medium	11) überfüllter Absetztank	falsche Prozessparameter ("run-away"-Reaktion im Prozessreaktor)	n) Absetztank häufiger entwässern und reinigen, Einbau eines LIC am Sumpf

LIC: Level Indicator and Controller (Füllstandsanzeiger und -wächter); KW: Kohlenwasserstoff.

Failure Mode and Effects Analysis (FMEA) Ausfalleffektanalyse, Fehler-Möglichkeits- und -Einfluss-Analyse (DIN 25448)

- Ziel und Gründe für eine FMEA
- Qualitative Untersuchung von Einheiten (E) hinsichtlich Ausfallarten und deren Auswirkungen auf das übergeordnete System (induktive Fragestellungen),
- Umsetzung von Unternehmenszielen (Null-Fehler-Produkte etc.) steigende Kundenanforderungen, z.B. „Just-in-Time-Service“, etc.,
- Verschärfte gesetzliche Auflagen und Hinweise, z.B.
  - innerhalb der Schweizer Störfallverordnung,
  - DIN IEC 56(Sec)410:1994: Analyse des Risikos technischer Systeme.
- Erfahrungsquellen
- 80% aller Fehler, die im Einsatz von Einheiten auftreten, beruhen auf Schwachstellen im Design (d.h. auf fehlerhafte Entwicklung und Konstruktion); viele sind Wiederholungsfehler.
- Betriebsunterlagen, -dokumente; Datensammlungen (anlagenintern, -extern)

(Quelle: Schubert, M. s.u.)

Tabelle für eine FMEA

Nr.	Einheit	Ausfallarten von (2)	Klasse: Häufigkeit von (3)	Ausfallerken-nung von (3)	vorhandene Massnahmen gegen (3)	Ausfallauswirkungen von (3) auf das System, angrenzende Einheiten	Bemerkung-en zu (7)	Klasse: Auswirkung/ Systemzustand
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)

Arbeitsschritte der FMEA

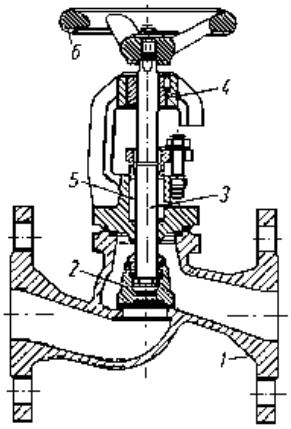
- Auflistung möglicher Ausfallarten aller Einheiten des Systems,
- Identifizierung aller Ausfallmöglichkeiten für jede aufgelistete Einheit,
- Bestimmung der Auswirkungen jeder Ausfallart auf angrenzende Einheiten und Auswertung der resultierenden Folgen auf das System oder den Systemzustand,
- Klassifizierung nach Gefahr und Auswirkung für die einzelnen Ausfallarten,
- Ermitteln möglicher Vorgehensweisen zur Reduzierung der Ausfallhäufigkeiten und Ausfallauswirkungen (Risikoverminderung),
- Ausfüllen eines Formblattes, das die Ergebnisse der Arbeitsschritte 1. bis 5. zusammenfassend darstellt.

zu 1. Auflisten möglicher Ausfallarten

Funktionselemente	Ausfallarten
schliessen	• fällt offen aus • schliesst nur teilweise
öffnen	• fällt geschlossen aus • öffnet nur teilweise
geschlossen bleiben	• öffnet vollständig • öffnet teilweise
offen bleiben	• schliesst vollständig • schliesst teilweise
Medium umschliessen	• äussere Leckage • innere Leckage

zu 2. Identifizierung der Ausfallmöglichkeiten

- Bestimmen aller Ausfallarten einer Einheit über ihre Funktionselemente.
  Einfaches Beispiel: Absperrventil, bestehend
  - Ventilgehäuse,
  - Ventilteller mit Sitzringen,
  - Spindel,
  - Mutter,
  - Stopfbuchse (Abdichtung der Spindel),
  - Antrieb (Handrad)
- Ausfallarten:
- Leckage Ventilgehäuse,
- Ventil schliesst oder öffnet gar nicht oder nur teilweise,
- etc.



zu 3. Bestimmung der Auswirkungen

- Klassifikationen für den Systemendzustand und seiner Auswirkungen,
- Beispiel: Klassifikation nach Systemendzustand.

Klasse	Systemzustand	Bezeichnung
1	sicher	„praktisch“ unverändert
2	nicht kritisch	Teilausfall
3	kritisch	Vollausfall
4	katastrophal	„überkritischer“ Ausfall

- Diese (und weitere) Klassifikationen sind vom Industrietyp abhängig.

zu 4. Klassifikation der Auswirkungen

Klasse	Auswirkung	Der Ausfall einer Einheit führt
I	sehr schwer	zum Ausfall des Systems und zu schwerwiegenden Systemschäden oder zu schwerwiegenden Schädigungen von Personen
II	schwer	zum Ausfall des betrachteten Systems, aber nicht zu schwerwiegenden Systemschäden, jedoch zur Beeinträchtigung von Personen
III	gering	zum Ausfall des betrachteten Systems, aber zu keiner Beeinträchtigung von Personen
IV	sehr gering	zu keinem Ausfall des betrachteten Systems und zu keiner Beeinträchtigung von Personen

Klassifizierung von Ereignishäufigkeiten

Klasse	Ausfallartenhäufigkeit
wahrscheinlich	> 1x Versagen in 10^4 Betriebsstunden
ziemlich wahrscheinlich	1x Versagen in 10^4 bis 10^5 Betriebsstunden
selten	1x Versagen in 10^5 bis 10^7 Betriebsstunden
sehr selten	< 1x Versagen in 10^7 Betriebsstunden

zu 6. Ausfüllen eines Formblattes (Beispiel: Olefin-Dimerisationsanlage)

System: xyz

Ausgangszustand:	Umgebungsbedingungen:	Unterlagen:
Ungestörter bestimmungs-gemässer Betrieb	Aussentemperatur 10 bis 30°C	Zeichnungen, Systemspezifikation, Datenquellen, ...

Nr.	Einheit	Ausfall-arten von (2)	Klasse: Häufigkeit von (3)	Ausfallerken-nung von (3)	vorhandene Massnahmen gegen (3)	Ausfallauswirkung-en von (3) auf das System, angren-zende Einheiten	Bemerkung-en zu (7)	Klasse: Auswir-kung/ Systemzu-stand
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
1	Absetz-tank	Geringe Leckage	Wahr-scheinlich	Sichtkontrolle, Geruch	Auffangbe-hälter, Korro-sionsschutz	Druckerniedrigung, falsche Prozess-parameter		sehr gering/ sicher
		Grosse Leckage	Sehr selten	Anzeige PIC, Sichtkontrolle, Geruch	Auffangbehält-er	Prozessunterbrech-ung	Brandgefahr	schwer/ kritisch
	etc.							

Beispiel einer FMEA nach VDA (Verband der Automobilindustrie)

Kopfdaten: .....

Produkt-/Prozess-Benennung Ersteller/Ausgabestand etc

Konstruktions-FMEA ☐ Prozess-FMEA ☒

					DERZEITIGER ZUSTAND							VERBESSERTER ZUSTAND				
Systeme/ Merkmale	**potentielle Fehler**	**pot. Folgen des Fehlers**	**D**	**pot. Fehler-ursachen**	**vorge-sehene Prüfmass-nahmen**	**A**	**B**	**E**	**R P Z**	**empfohlene Abstellmass-nahme**	**Verantwort-lichkeit**	**getroffene Massnahme**	**A**	**B**	**E**	**R P Z**
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Spule wickeln (gem. An-weisung xy)	Windungs-zahl zu hoch	Spulenwider stand zu hoch - Rel. zieht nicht an - Ausfall	-	Zähler für Windungs-zahl setzt aus	Zähler periodisch kalibrieren	6	8	8	384	Zählergetriebe säubern	W. Erwolf	neuer Zähler + Regelung Nr.	2	8	4	64

Wo könnte etwas nicht i. O. sein?

Wie könnte sich der Fehler äussern?

Was könnte im Fehlerfalle passieren?

Warum würde der Fehler/ die Folge entstehen?

Welche Massnahmen sind bez. Serienfertigung vorgesehen?

Welches Risiko (A, B. E, RPZ)?

Was sollte wer bis wann erledigen?

Welche Massnahmen wurden realisiert?

Welches Risiko (A, B. E, RPZ)?

Erläuterungen zum VDA-Formblatt

- Abschätzung einer Risikoprioritätszahl RPZ (Kennzahl) über die Parameter
  - A: Auftretenshäufigkeit,
  - B: Bedeutung,
  - E: Entdeckbarkeit des Fehlers.
- Jeder Parameter erhält dabei eine Ziffer 1 („positiv“") bis 10 („negativ“).

- Charakteristische Risikozahlen
  - 1·1·1=1 kleinstes Risiko,
  - 5·5·5=125 mittleres Risiko,
  - 10·10·10=1000 grösstes Risiko.
- In der Praxis helfen Tabellen bei der Abschätzung der Parameter.

„Zurich“ Hazard Analysis (ZHA)

- Aufgabenstellung
- Vereinfachte qualitative und semiquantitative Analyse einer Betrachtungseinheit BE (Anlage, Sub-System, Komponente, …)
- Ziel
- Ermittlung eines Risikoprofils für BE (ideal in der Entwurfsphase, jedoch meist für bestehende Anlagen).
- Arbeitsschritte
  - Definition der Systemgrenzen,
  - Sammlung benötigter Unterlagen,
  - Zusammenstellen des Expertenteams,
  - Gefahrenidentifikation,
  - Risikoabschätzung,
  - Massnahmen zur Gefahrenreduktion.

zu 1. Systemabgrenzung

- Vergleichsweise enge Definition der System- und Komponentengrenzen.
- zu 2. Sammlung benötigter Unterlagen
- Je nach vorhandenem Material, Analyseziel und verfügbarer Zeit sind Entwurfs- und Konstruktionsdaten, Komponentenbeschreibungen usw. erforderlich.
- zu 3. Expertenteam
  - Teamleiter,
  - Forschung, Entwicklung und Konstruktion,
  - Einkauf, Produktion,
  - Qualitätssicherung und -kontrolle,
  - Sicherheitstechnik,
  - Verkauf, Service, Marketing (produktionsexterne Arbeitsbereiche).

zu 4. Gefahrenidentifikation

- Auflisten aller möglichen Gefährdungen oder Schadensursachen:
  - mögliche Personen- und Sachschäden,
  - Fehlfunktionen,
  - gefährliche Umwelteinflüsse,
- Betrachtung der zeitlichen Änderung einer Betrachtungseinheit und daraus resultierenden möglichen Gefährdungen, d.h. ansatzweise Berücksichtigung dynamischer Prozesse.

zu 5. Risikoabschätzung

- Kategorisierung der Eintrittshäufigkeit

Kategorie	Häufigkeit	Bedeutung
A	häufig	oft aufgetretenes Ereignis oder häufiges Vorkommen erwartet = obere Grenze
B	öfter	öfter aufgetretenes Ereignis
C	gelegentlich	manchmal aufgetretenes Ereignis
D	selten	ein Ereignis kann vorkommen
E	unwahrscheinlich	Ereigniseintritt wird nicht erwartet
F	unmöglich	Ereigniseintritt unmöglich = untere Grenze

Anmerkung: Normalbetrieb zwischen C und D.

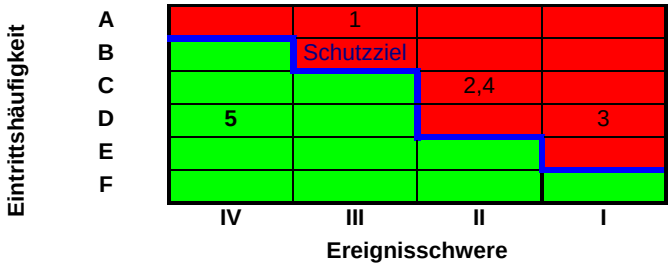
Risikoabschätzung (Forts.)

- Kategorisierung der Ereignisschwere

Kategorie	Schwere	Bedeutung
I	katastrophal	Todesfälle, Verlust des Firmenimages, grosser finanzieller Verlust/ Systemverlust
II	kritisch	schwere Personenschäden, schwerer Image- und Geldverlust, Systemteilverlust
III	begrenzt	Verletzungen, vorübergehender Imageverlust, indirekter Finanzverlust, Systemschäden
IV	vernachlässigbar	geringe Verletzungen, geringe Finanz- und Imageverluste, keine Systemschäden

Risikoabschätzung (Forts.)

- Graphische Darstellung des Risikoprofils: vereinfachtes F/C-Diagramm,
- Eintragen der ermittelten Kategorien,
- Eintragen eines Schutzzieles = Risikogrenzkurve (subjektiv, normativ - firmenintern oder behördlich),
- Eintragen der ermittelten Gefährdungen (Nummern gemäss Beispiel).



Formblatt (Beispiel: Olefin-Dimerisationsanlage)

Nr.	Gefährdung	Ursache	H	Auswirkung	S
1	geringe Mengen von KW	geringe Leckagen • Tank • Armaturen usw.	A	• Korrosion • Vergiftungen	III
2	grosse freie Mengen von KW	grosse Leckagen • Bruch Transferleitung • Bruch Tank etc.	C	• Bodenkontamination • Vergiftungen • Brände, Explosion	II
3	überhitzter Absetztank	Feuer und Versagen des Si.-Ventils und der N_2-Kühlung	D	• Zerstörung der Anlage • Tote, Verletzte	I
4	ungünstiges H_2O/KW-Verhältnis	Absetzsumpf nicht entleert	C	falsche Prozessparameter: „run away“-Reaktion im Prozessreaktor	II
5	Si.-Ventil geschlossen	Si.-Ventil defekt • Korrosion • fehlende Wartung	D	Verlust der Si.-Funktion	IV

KW: Kohlenwasserstoff, Si.-: Sicherheits-…, H: Häufigkeit, S: Schwere

zu 6. Massnahmen zur Gefahren- bzw. Risikoreduktion

- Korrekturmassnahmen: Risiken, die über die Schutzziele hinausreichen, erfordern korrektive Massnahmen; Abbau von „Katastrophenszenarien“ meist prioritär.

Tabellarische qualitative Methoden, Zusammenstellung

HAZOP	FMEA	ZHA
→ Gefahren / Betriebsstörungen	→ Mögliche Ausfallarten / Auswirkungen	→ Risikoprofil
• Kontinuierliche / diskontinuierliche Prozesse • Festlegung Leitwörter / Prozessvariablen • Eintrag in Tabelle	• Auflisten der Einheiten / Ausfallarten • Eintrag in Tabelle • Klassifizierung von Systemzustand und Auswirkungen • Klassifizierung der Ereignishäufigkeit	• Auflistung möglicher Gefährdungen • Kategorisierung der Eintrittshäufigkeit • Kategorisierung der Ereignisschwere • Grafische Darstellung / Abgleich mit Schutzziel
• Nur ein Ausfall, keine Verkettungen betrachtet		