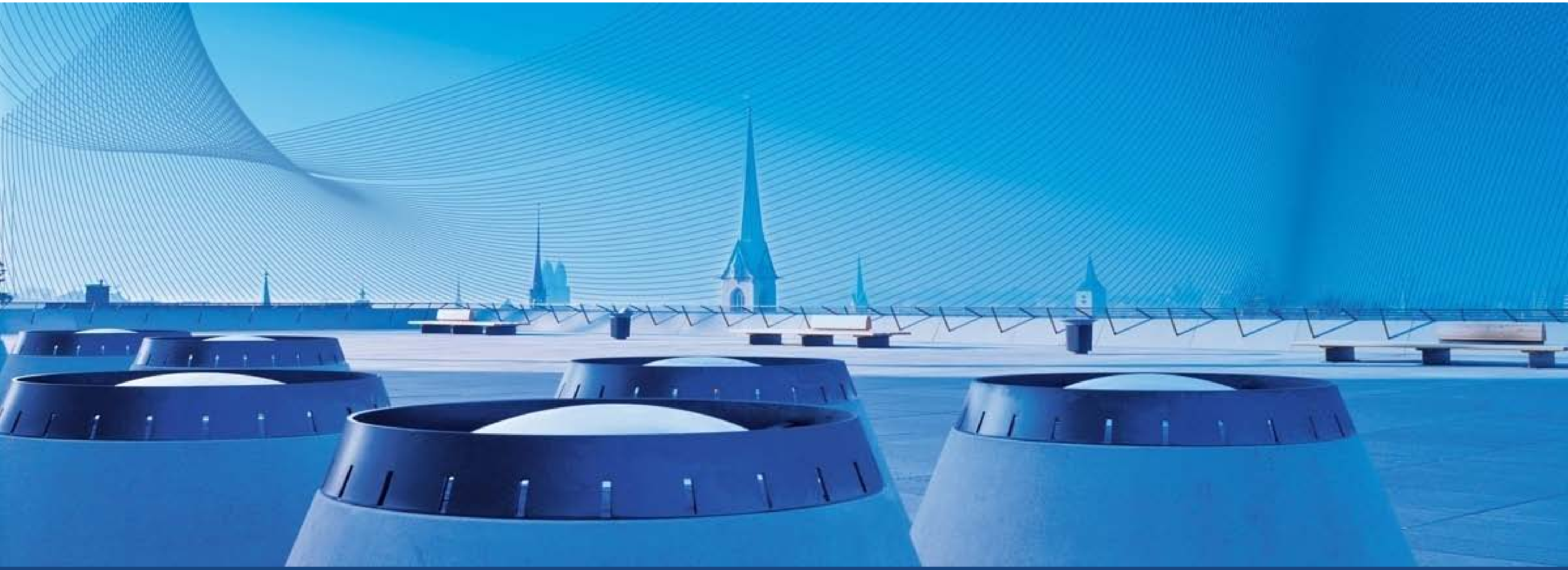
Methods of Technical Risk Assessment in a Regional Context

- Wolfgang Kröger, Professor and Head of former Laboratory for Safety Analysis (www.lsa.ethz.ch)
- Founding Rector of International Risk Governance Council Geneva (www.irgc.org)
- Executive Director, ETH Risk Center (www.riskcenter.ethz.ch)



Methods for Hazards Identification

The methods are focussed on single plants following the approach of reductionism

Contents:

- Master Logic Diagram.
- **Haz**ard and **Op**erability Study (HAZOP).
- **F**ailure **M**ode and **E**ffects **A**nalysis (FMEA).

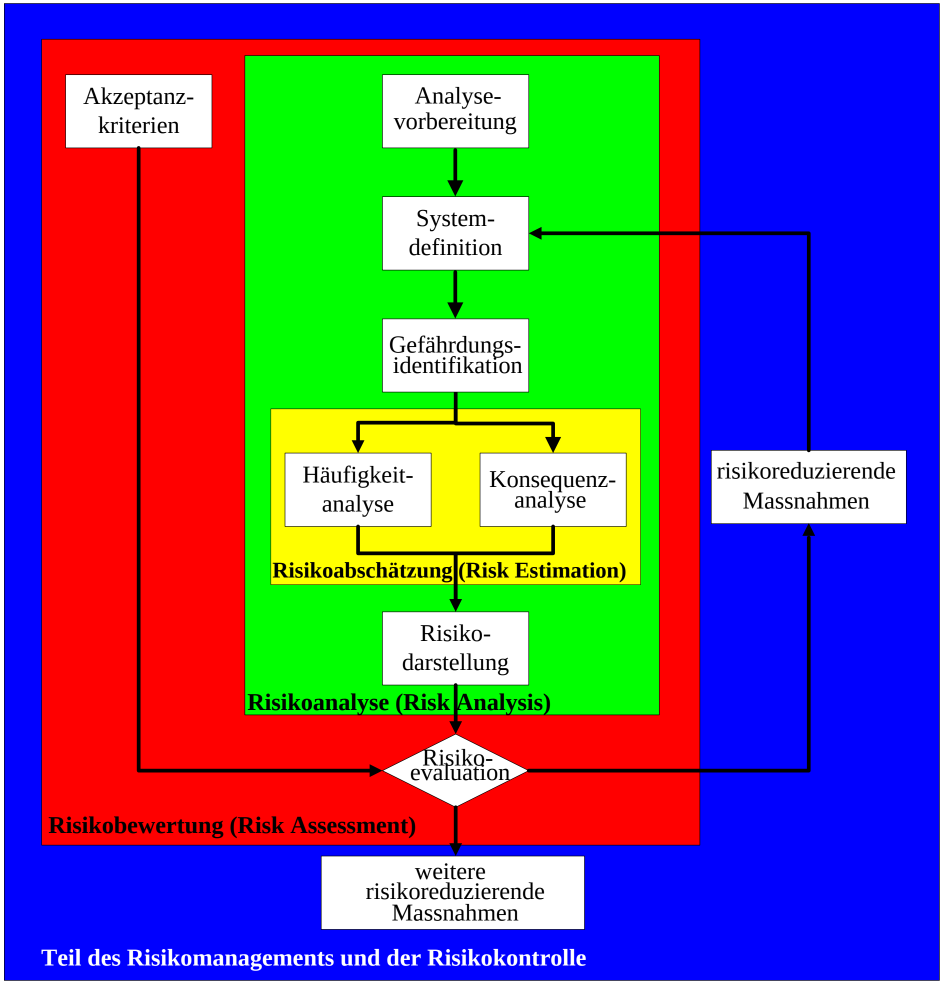
} Qualitative, tabular

- **F**ault **T**ree **A**nalysis (FTA).
- **E**vent **T**ree **A**nalysis (ETA). On next lecture: 13/10/2009.

} Quantitative, formal

- References.

Ablauf einer Risikoanalyse



- Je nach Zielsetzung und Ressourcen finden unterschiedliche Methoden Verwendung (Methodenvielfalt)
- Zur Unterstützung dienen "Hilfsdisziplinen", wie die Zuverlässigkeitsanalyse

Literatur:

- DIN IEC 56 (Sec) 410: Analyse des Risikos technischer Systeme
- DIN EN 1050: Sicherheit von Maschinen - Leitsätze zur Risikobeurteilung
- E DIN EN 292-1 bzw. 2: Sicherheit von Maschinen - Grundbegriffe, allgemeine Gestaltungsleitsätze; Teil 1: Grundsätzliche Terminologie, Methodologie, Teil 2: Technische Leitsätze
- ISO/IEC Guide 73: Risk Management - Vocabulary - Guidelines for Use in Standards

Master Logic Diagram [1]

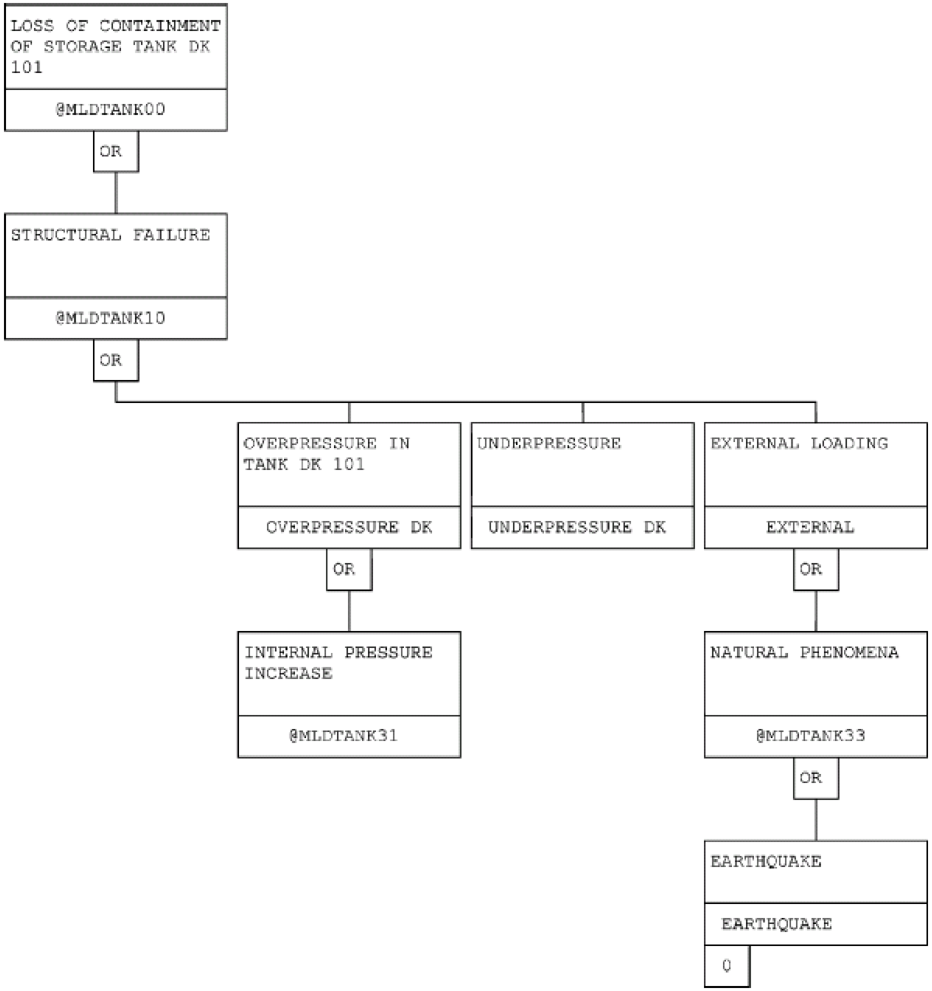
Purpose

- Identification of causes (of failures) of an undesired event („top event“).

Methodology

- Definition of an adverse top event.
- Build up detailed sub-events / categories.
- Cut-off at basic events.
- Assign event frequency (failure probability or rate) to basic event.
- Summation of all parameters (if independent from each other).

Example: Master Logic Diagram



Hazard and Operability Study (HAZOP)

Goals and purposes of a HAZOP [2, 3]

- Qualitative analysis of processes in a chemical engineering system (continuous or “batch” operation) based on given guide words, which highlight causes and consequence of deviations from desired physical parameters, i.e.
  - Identification of hazards within the system and caused by the system.
  - Identification of causes of operational disturbances and deviations in the production, which can lead to defective products.
- Fulfilment of regulatory requirements and recommendations.

Working steps of a HAZOP

1. Preparation: Definition of the focus of the analysis, guide words, process variables, etc.
2. Selection of the team members.
3. Collection of plant data and information.
4. Completing the HAZOP-form which summarizes the results.

1. Preparation:

Identification of deviations from the target state by linking **guide words** with **process variables**, e.g.

- No/less/more mass flow.
- More/less system constituents (corrosion products, multi phase flow, etc.).
- Other operational states than foreseen, e.g. maintenance instead of normal operation.

2. Selection of the team members (example):

- Independent chairman, expert in HAZOP.
- Company experts: design engineer, process engineer, commissioning manager, instrument design engineer.
- About 5 to 7 persons depending on facility size, type and/or state of design realisation.

3. Plant data and information:

Comprehensive data of:

- “Plant- and system hardware”, like piping and instrument drawings, plant models, procedures, safety analysis reports.
- “Plant- and system software”, like operation instruction, operation manuals.

The data and information must be:

- Up to date.
- Sufficiently detailed and must going into the same depth.
- Without contradictions/conflicts.

HAZOP - form

4. Completing the HAZOP form:

Guide word	Deviation	Possible cause	Consequences	Action required

Example: Skating rink

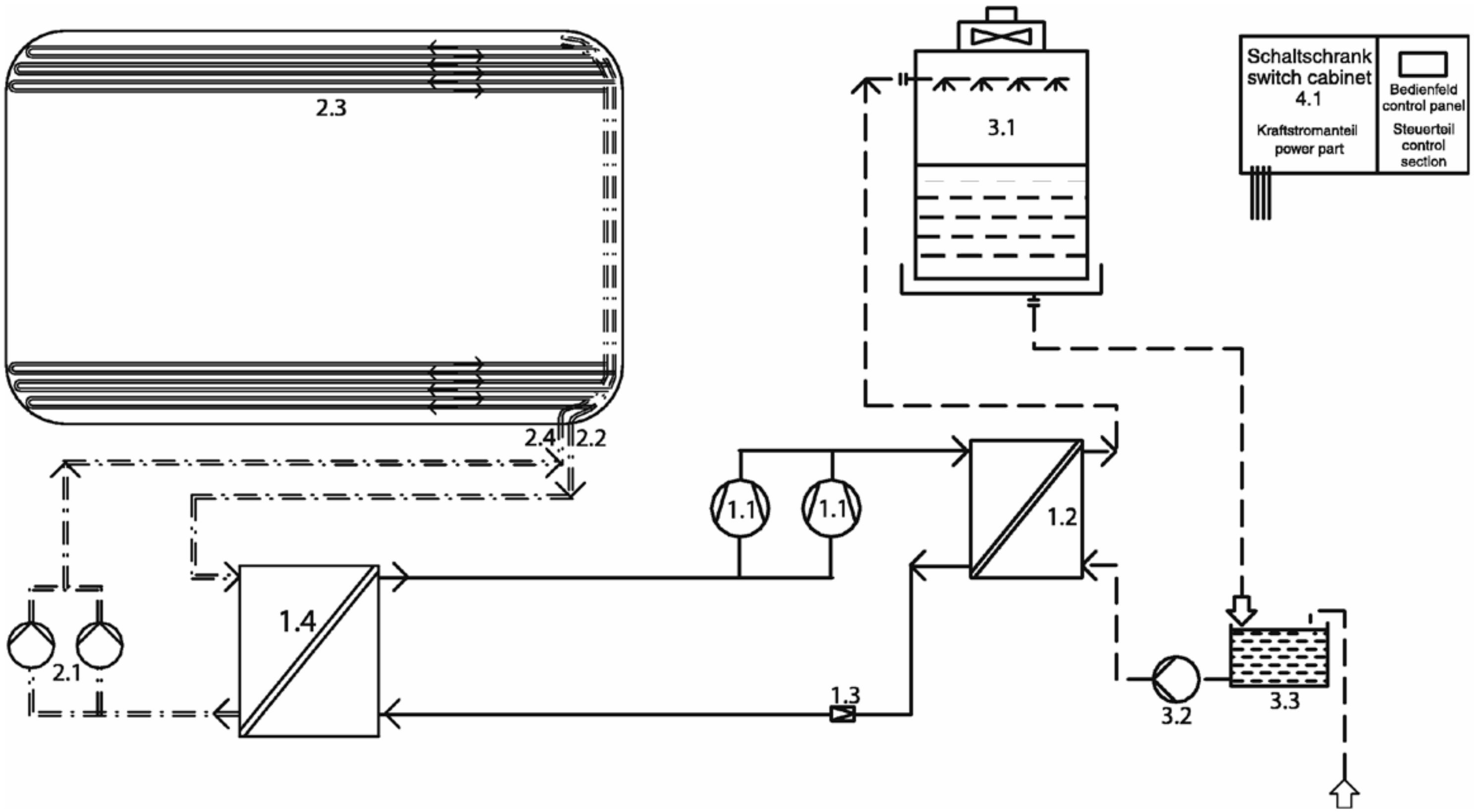
- An (older) outdoor skating rink is located in a residential area.
- About 10 tons of ammonia (NH_3) are used as cooling liquid.
- The facility is subject to the Swiss Ordinance of Protection Against Major Accidents established in 1991.

The **question** is, whether the risk due to the operation of the skating rink is acceptable or a complete revision is necessary.

General conditions

- The skating rink is only operated in winter.
- System boundaries are proposed to be the technical facilities including the skating rink.
- Cooling facility with direct cooling liquid evaporation Störfallverordnung (StFV).

System Layout



Flow diagram for a refrigeration plant with secondary refrigeration – cooling carrier: brine
refrigerant: ammonia (NH_3)

1.0 refrigerant circuit ———	1.4 evaporator	2.3 piping system	3.2 cooling water pumps
1.1 compressor with motor drive	2.0 cooling carrier circuit –·–·–	2.4 return main	3.3 cooling water sump
1.2 condenser	2.1 cooling carrier pumps	3.0 cooling water circulation - - - -	4.0 electrical installations
1.3 expansion valve	2.2 supply main	3.1 cooling tower	4.1 switch cabinet

Advantages of a HAZOP

- Guided systematic approach.
- Interdisciplinary analysis of a facility.
- Intensive use of facility specific data/information and expert judgment.
- Internationally established method, applicable within the StFV.

Disadvantages

- Dangerous combinations of events may remain undetected.
- No thorough examination of external events (mostly).
- Less suitable for analysis of small facility modifications.
- No systematic analysis and collection of component failures.
- Strong dependence on expert knowledge and experience.
- Labour intensive and time consuming (may range up to months).

Failure Mode and Effects Analysis (FMEA)

Goals and purposes for applying a FMEA [6]

- Qualitative analysis of units in respect to various failure modes and the impacts to superordinated systems (inductive questioning).
- Realisation of company goals (high quality products, etc.), customers increasing demands (conditions of use, service, etc.).
- Fulfilment of regulations and standards (e.g. [5]).

Working steps of a FMEA

1. Listing of failure modes of all units.

2. Identification of all potential failures for each listed unit and of the criticality of the facility caused by the specified failure modes.

3. Classification of each failure according to hazard and consequence.

4. Determination of procedures to reduce failure frequency and consequence (risk).

5. Completing the FMEA-form which summarizes the results of steps 1 to 4.

1. Listing of failure modes of all units

Functions	Types of Failure
Closing	Fails open Only partly closed
Opening	Fails closed Only partly opened
Remain closed	Opens completely Partly opens
Remain opened	Closes completely Partly closes
Enclose a medium	External leakage Internal leakage

3. Classification of consequences

Class	Consequence	The failure of a unit leads to …
I	Catastrophic	… a total failure of the system and may cause deaths
II	Critical	… major system damage and may cause severe injuries
III	Marginal	… minor system damage and may cause minor injuries
IV	Minor	… no serious system damage or injuries

Classification of the event frequencies

Class	Failure frequency
Frequent	1x failure in less than 10^4 hours of operation
Reasonably probable	1x failure between 10^4 and 10^5 hours of operation
Rare	1x failure between 10^5 and 10^7 hours of operation
Extremely unlikely	1x failure in more than 10^7 hours of operation

$1 year \mathrel{\hat{=}} 8760h \approx 10^4$

5. Completing the FMEA-form (example: skating rink)

System: Skating rink		
Initial state: Normal daily routine	Environmental conditions: Temperature 8°	Documentation: Plans, system specifications, …

Nr.	**Unit**	**Failure mode of *(b)***	**Class: Frequency of *(c)***	**Failure recognition of *(c)***	**Countermeasures against *(c)***	**Failure effect of *(c)* on the adjoined units**	**Comments *(g)***	**Class: Effect / facility state**
(a)	***(b)***	***(c)***	*(d)*	*(e)*	*(f)*	***(g)***	*(h)*	*(i)*
1								
2								
3								

Advantages of a FMEA

- Systematic approach.
- Interdisciplinary assessment of a facility.
- Intensive use of facility documentation and expert judgment.
- Applicable for an analysis within the StFV.
- Internationally accepted method.

Disadvantages of FMEA

- Dangerous “event chains” may remain undetected.
- No thorough examination of external events (mostly).
- Strong dependence on expert knowledge and experience.
- Labour intensive and time consuming (“paper mill”).

Summary

HAZOP	FMEA
→ Hazards / operational disturbances.	→ Possible failure modes of single units and related effects.
• Definition of guide words / process variables. • Continuous / discontinuous processes.	• Listing of units / failure types. • Classification of system states and effects. • Classification of event frequencies.
• Entries in tables, only discrete failures are considered, no event chains.	

Fault Tree Analysis (FTA)

Problem description:

It is not possible to analyse complicated, highly-reliable or novel systems as “black box”, i.e. there is a lack of knowledge at system level but predictions of failure probability, reliability and risk at system level are needed.

Approach: System decomposition.

The behaviour of the overall system is determined by known behaviour as well as known logical and functional linking of system units.

Method of FTA [7, 8, 9]

Starting point of FTA is a **predefined** system state (failed state as "top event"). The subsequent task is to find event combinations leading to the "top event". The branches are tracked top-down (top event -> intermediate events -> basic events) - the reasoning is **deductive**.

What is Fault Tree Analysis:

- Fault tree analysis (FTA) is a top-down approach to failure analysis, starting with a potential undesirable event (accident) called a TOP Event, and then determining all the ways it can happen.
- The analysis proceeds by determining how the TOP Event can be caused by individual or combined lower level failures or events. The causes of the TOP Event are "connected" through logic gates.
- FTA is the most commonly used technique for causal analysis.

Working steps of a FTA:

1. Definition of the "TOP Event".

2. Identification of all basic event combinations which result in the "TOP Event".

If quantitative:

3. Assignment of failure probabilities to basic events.

4. Boolean modelling and calculations of probabilities.

5. Analysis of dominating failure combination and impacts (importance analysis), proposals for system improvement/optimisation.

1. Definition of the "top event":

- **In general:** system failure.
- **In particular:** loss of specific functions and services meaning the failure of the overall system, (e.g. rupture of a gas storage tank).

2. Identification of basic event combinations:

The formal combination of events constitutes the logical structure of the system considered or the derived Boolean model (fault tree). The model consists of:

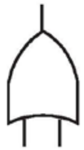
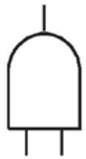
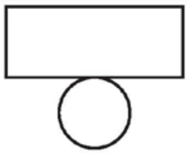
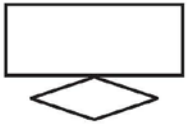
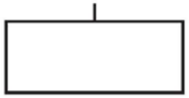
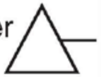
- Input events: Lower event ("input" to the gate).
- Gates (logic operation): Show the relationship of lower events needed to result in a higher event (logic AND, OR).
- Output events: Higher event ("output" of the gate).

The behaviour of the gates is determined by the **Rules of Boolean Algebra**.

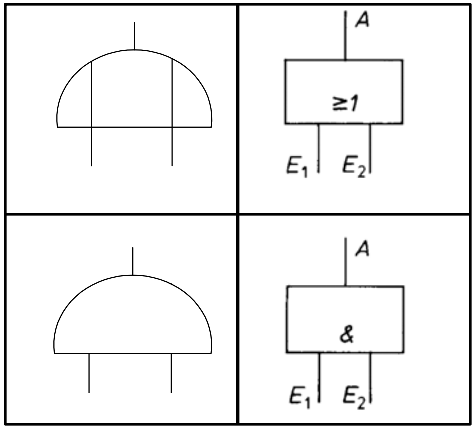
Required information for a FTA

- **Component level:**
  - Different relevant failure modes of individual units (to fix most relevant one).
  - Relevant external "influences", e.g. maintenance, environmental impacts.
  - For quantitative analyses: Failure probabilities.
- **System level:**
  - Precise definition of the operation mode in question.
  - The system boundaries (which parts of the system are included in the analysis, what type of external stresses should be included in the analysis – war, sabotage, earthquake, lightning, etc.).
  - The level of resolution (how detailed should the analysis be?).

Fault Tree Symbols

Logic gates	 OR-gate	The OR-gate indicates that the output event occurs if any of the input events occur
	 AND-gate	The AND-gate indicates that the output event occurs only if all the input events occur at the same time
Input events (states)		The basic event represents a basic equipment failure that requires no further development of failure causes
		The undeveloped event represents an event that is not examined further because information is unavailable or because its consequences are insignificant
Description of state		The comment rectangle is for supplementary information
Transfer symbols	Transfer out  Transfer in 	The transfer-out symbol indicates that the fault tree is developed further at the occurrence of the corresponding transfer-in symbol

Alternative Symbols



3. Assignment of failure probabilities:

Problems

- Lack of data (e.g. reliability figures of highly reliable tailor-made components in nuclear power plants, components designed to work under changing operating conditions in the chemical industry, etc.).
- Development of the database usually causes an extensive amount of work.

4. Boolean modelling and calculation of probabilities:

Summary of the assumptions/preconditions

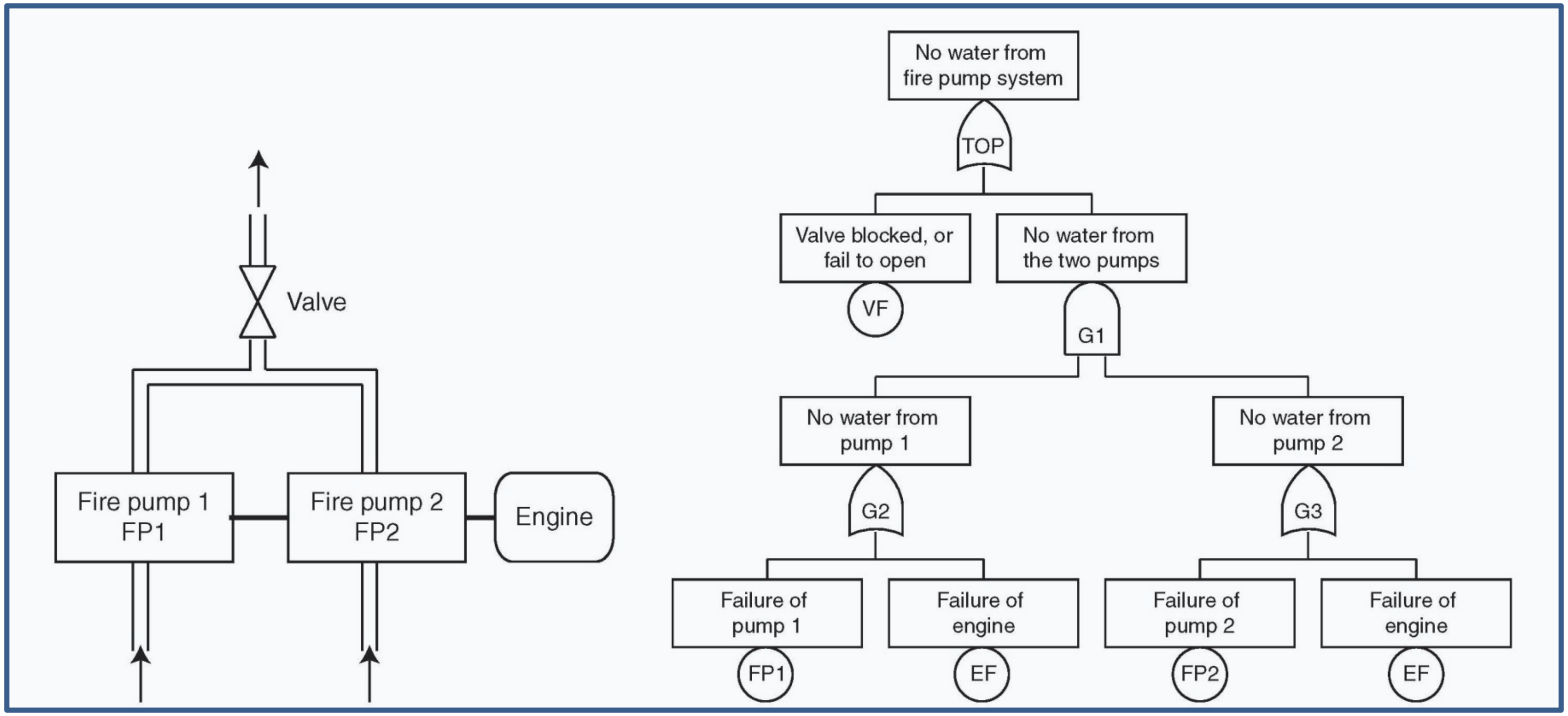
- A technical system consists of units (components).
- The units are both technically and logically connected.
- The state of each unit follows a binary logic (TRUE/FALSE, on/off, intact/defect).
- Available logic operators are:
  - conjunction: AND ($\cap$).
  - disjunction: OR ($\cup$).

Labelling of the probabilities:

p_i: probability of survival of the *i*-th unit.

q_i: probability of failure of the *i*-th unit.

Example: Redundant Fire Pump



TOP Event: No water from fire water system.

CAUSES for TOP Event:

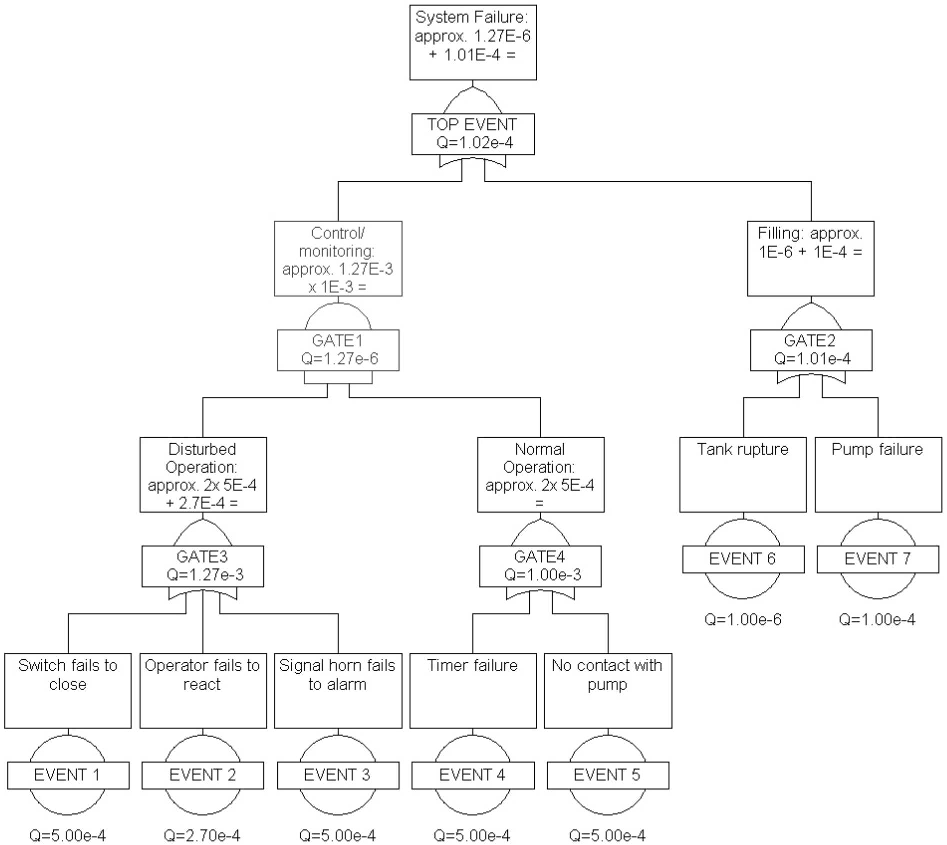
- VF = Valve Failure
- G1 = No output from any of the fire pumps
- G2 = No water from FP1
- G3 = No water from FP2
- FP1 = Failure of FP1
- FP2 = Failure of FP2
- EF = Failure of Engine

Examples of probabilities used in quantitative FTAs

Unit or functional components	**Survival Probability p_i**	**Failure Probability q_i**
Electromechanical parts: switches, timer, horn, contacts	0.9995	$5 \cdot 10^{-4}$
Passive element: storage tank	0.999999	10^{-6}
Active element: pump	0.9999	10^{-4}
„Functional element human being": operator	0.99973	$2.7 \cdot 10^{-4}$

- $q_{operator}$: Probability of a wrong operator response on a perceived signal
- q_{pump}: Probability of pump operation despite of being switched off

Example from industry: Pumping-storage system



Boolean Function Failure:

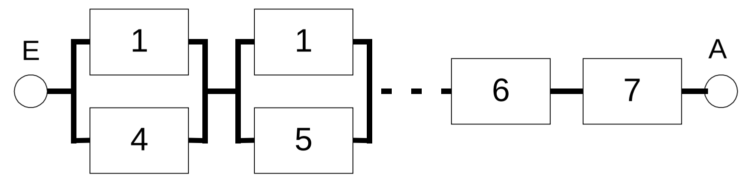
$$y = \left[\left(\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_3 \right) \wedge \left(\bar{x}_4 \vee \bar{x}_5 \right) \right] \vee \left(\bar{x}_6 \vee \bar{x}_7 \right)$$

multiply

$$y = \bar{x}_1\bar{x}_4 \vee \bar{x}_1\bar{x}_5 \vee \bar{x}_2\bar{x}_4 \vee \bar{x}_2\bar{x}_5 \vee \bar{x}_3\bar{x}_4 \vee \bar{x}_3\bar{x}_5 \vee \bar{x}_6 \vee \bar{x}_7$$

This is a serial-parallel and serial system:

Reliability Block Diagram



Computation:

$$F_{SP} = 1 - \prod_{i=1}^{6} \left(1 - q_{1i} q_{2i} \right) = 1 - \left[\left(1 - q_1 q_4 \right) \left(1 - q_1 q_5 \right) \ldots\text{etc} \right]$$

$$F_s = 1 - \left[\left(1 - q_6 \right) \left(1 - q_7 \right) \right]$$

$$F = F_{SP} + F_s = \ldots = 1.0227 \cdot 10^{-4}$$

Use the following simplifications for simple systems only (i.e. each basic event appears only once in the fault tree):

$\Pr(A \cap B) = P(A) \cdot P(B)$
$\Pr(A \cup B) = \Pr(A) + \Pr(B) - \Pr(A \cap B)$
Approximation with small probabilities: $\Pr(A \cup B) \approx \Pr(A) + \Pr(B)$

Note

For any number of random events A_i (i = 1, 2, ..., n), the inclusion – exclusion principle is applied:

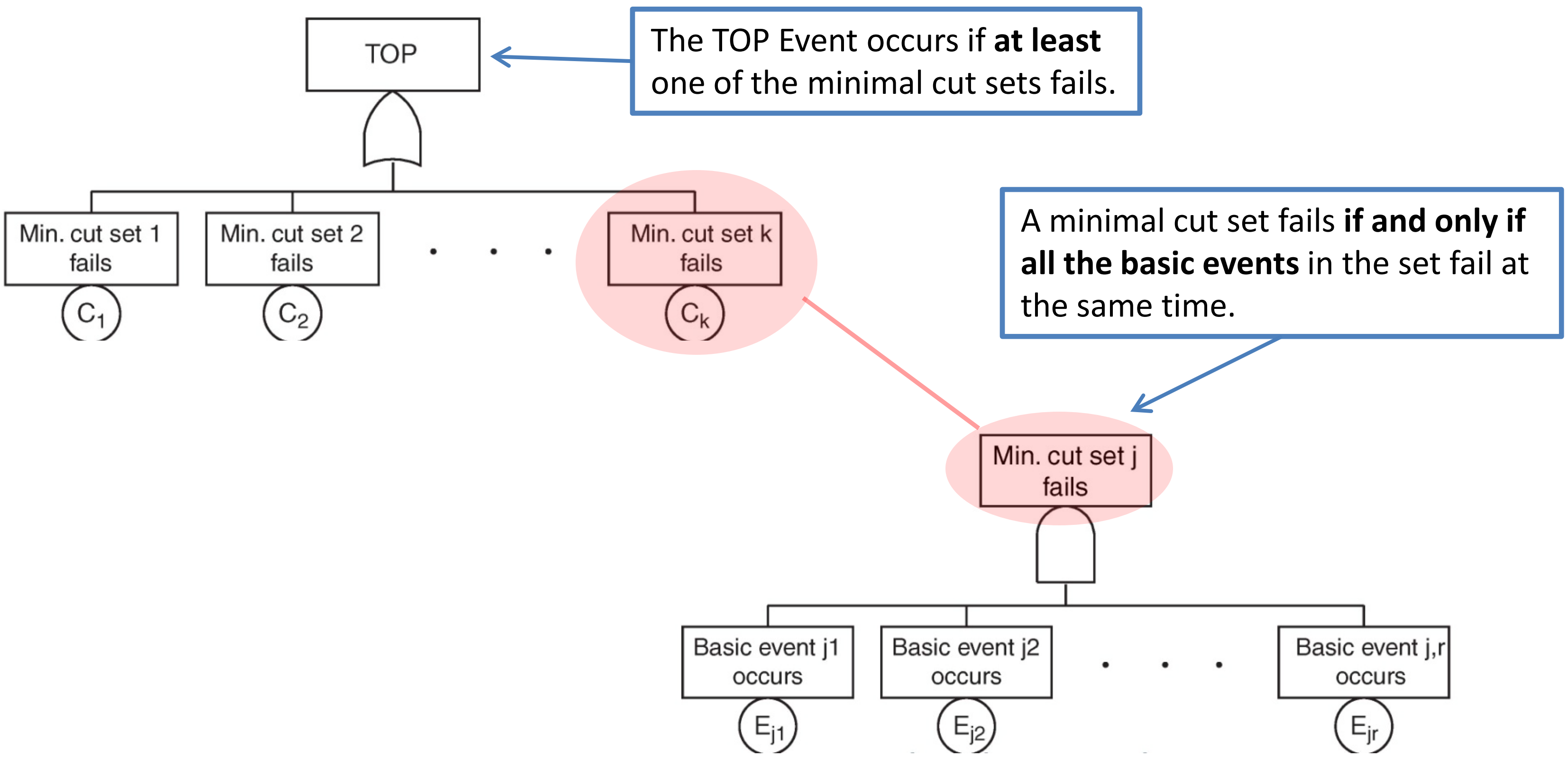
$$\Pr\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=}^{n} \Pr(A_i) - \sum_{\substack{i_1 i_2 = 1 \\ i_1 < i_2}}^{n} \Pr(A_{i1} \cap A_{i2}) + \sum_{\substack{i_1 i_2, i_3 = 1 \\ i_1 < i_2 < i_3}}^{n} \Pr(A_{i1} \cap A_{i2} \cap A_{i3}) + \ldots + (-1)^{n-1} \Pr(A_1 \cap A_2 \cap \ldots \cap A_n)$$

Rare event approximation for small $Pr(A_i)$:

$$\sum_{i=}^{n} \Pr(A_i) - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \Pr(A_i \cap A_j) \leq \Pr\left(\bigcup_{i=1}^{n} A_i\right) \leq \sum_{i=}^{n} \Pr(A_i)$$

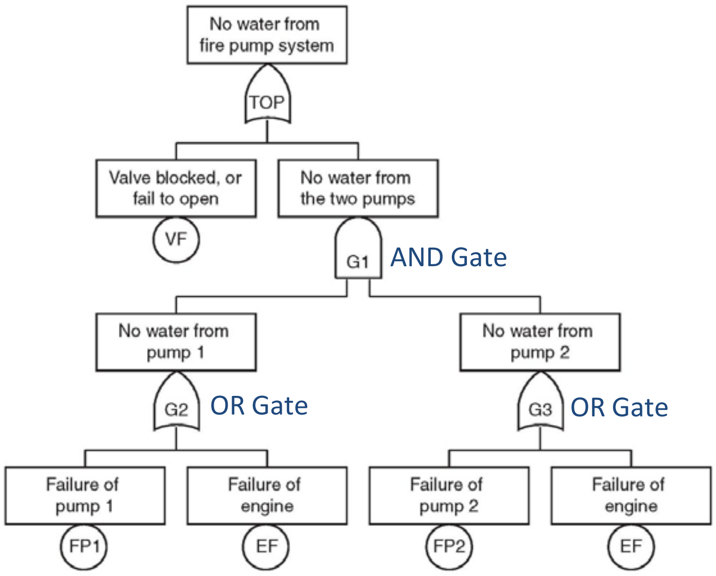
Cut Sets

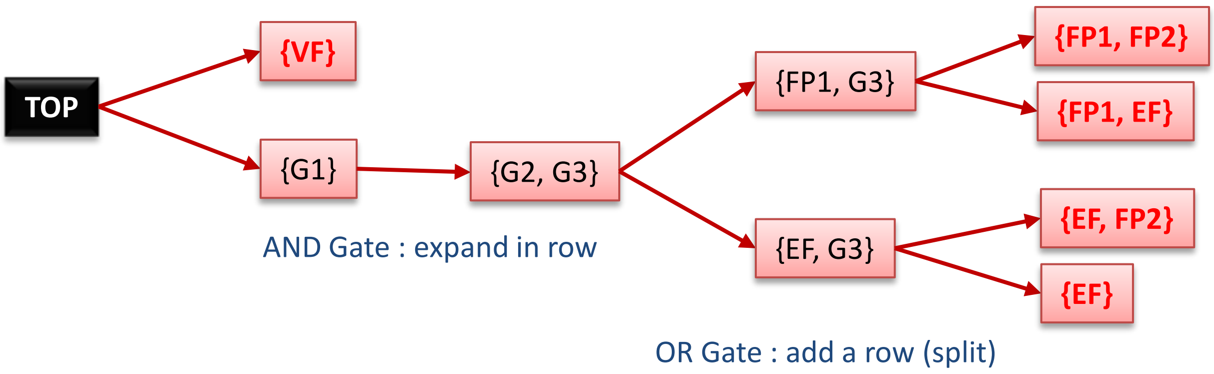
- A cut set in a Fault Tree is a set of basic events whose (simultaneous) occurrence ensures that the TOP Event occurs.
- A cut set is said to be **minimal** if the set cannot be reduced without loosing its status as a cut set.



Minimal Cut Sets Generation

- Minimal cut sets can be used to understand the structural vulnerability of a system.
- The longer a minimal cut set is, the less vulnerable the system (or TOP event in Fault Trees) is to that combination of events.
- Numerous cut sets indicate higher vulnerability.
- Cut sets can also be used to discover single point failures (one independent element of a system which causes an immediate hazard to occur and/or causes the whole system to fail.)





Denote by d_j the occurrence of all basic events in minimal cut j. Top event T becomes a union event of cut set events d_j s where m is the total number of minimal cut sets:

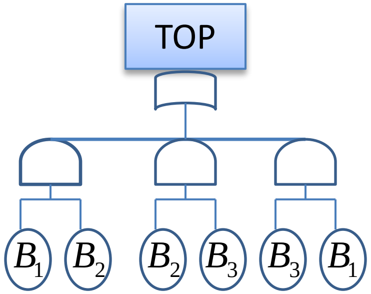
$$T = \bigcup_{j=1}^{m} d_j$$

System unavailability is the probability of the union event:

$$Q_S = \Pr\left\{ \bigcup_{j=1}^{m} d_j \right\}$$

Example : Consider a 2/3 system, that is a system with 3 Basic (independent) Events B_1, B_2, B_3 and the 3 following minimal cut sets events:

$$d_1 = B_1 \cap B_2 \quad , \quad d_2 = B_2 \cap B_3 \quad , \quad d_3 = B_3 \cap B_1$$



2/3 System

The expansion based on the inclusion – exclusion formula yields:

$$Q_S = A - B + C$$
$$A \equiv \Pr\{d_1\} + \Pr\{d_2\} + \Pr\{d_3\} = Q^2 + Q^2 + Q^2 = 3Q^2$$
$$B \equiv \Pr\{d_1 \cap d_2\} + \Pr\{d_2 \cap d_3\} + \Pr\{d_3 \cap d_1\} = Q^3 + Q^3 + Q^3 = 3Q^3$$
$$because \;\; \Pr\{d_1 \cap d_2\} = \Pr\{d_2\} \cdot \Pr\{d_1 | d_2\} = \Pr\{d_2\} \cdot \Pr\{B_3\} = Q^2 \cdot Q = Q^3$$
$$C \equiv \Pr\{d_1 \cap d_2 \cap d_3\} = Q^3$$

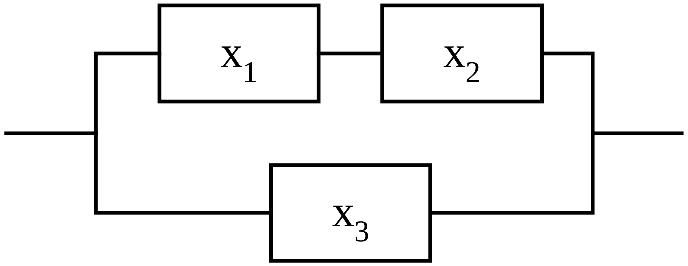
A Basic Event probability of 0.6 gives:

$$A = 1.08, \quad B = 0.648, \quad C = 0.216, \quad \boxed{Q_s = 0.648}$$

Computation of highly complicated systems

Approach

• Identification of those units which must at least operate for total system operability or units whose failure result in the total system failure.
→Minimal Paths and Minimal Cut Sets respectively.

Minimal Cut Sets	**Minimal Path Sets**
Smallest set of failed units, which blocks the path from input to output in a reliability block diagram.	Smallest set of (operating) units, that leaves open a path from input to output in a reliability block diagram.
Example 	
Cuts s_i: $\sigma_1 = \{\overline{x}_1; \overline{x}_3\}$; $\sigma_2 = \{\overline{x}_2; \overline{x}_3\}$	Paths p_j: $\pi_1 = \{x_1; x_2\}$; $\pi_2 = \{x_3\}$

Notation

State x_i of unit *I, where:*

$$x_i = \begin{cases} 0: \text{Unit state "failure" (in short: } \overline{x}_i\text{)} \\ 1: \text{Unit state "in operation" (in short: } x_i\text{)} \end{cases}$$

Each **cut set *i*** consists of the intersection of the minimum number of failed units required to cause the system failure, i.e. $\sigma_i = \bigcap_{k=1}^{l} \bar{x}_k$	Each **path set *j*** consists of the intersection of the minimum number of operating units required to ensure system operation, i.e. $\pi_j = \bigcap_{m=1}^{r} x_m$
System failure: union of cut sets σ_i $\bar{y} = \bigcup_{i=1}^{n} \sigma_i$	**System operation**: union of paths π_j $y = \bigcup_{j=1}^{s} \pi_j$
Boolean algebra: De Morgan's Theorem	
$\bar{y} = 1 - \bigcap_{j=1}^{n} (1-\sigma_j) = 1 - \left[(1-\bar{x}_1\bar{x}_3)(1-\bar{x}_2\bar{x}_3)\right]$	$\bar{y} = \bigcap_{j=1}^{s} (1-\pi_j) = (1-x_1x_2)(1-x_3)$
Multiply, Idempotent law ...	
$\bar{y} = 1 - \left[(1-\bar{x}_1\bar{x}_3)(1-\bar{x}_2\bar{x}_3)\right]$ $= 1-(1-\bar{x}_1\bar{x}_3 - \bar{x}_2\bar{x}_3 + \bar{x}_1\bar{x}_3\bar{x}_2\bar{x}_3)$ $= \bar{x}_1\bar{x}_3 + \bar{x}_2\bar{x}_3 - \bar{x}_1\bar{x}_2\bar{x}_3$	$\bar{y} = 1 - x_1x_2 - x_3 + x_1x_2x_3$
Applying of failure probabilities *$q_i(t)$*	**Applying of survival probabilities *$p_i(t)$***
…	*Note:* Calculations in order to get the same formal representation as for cut sets. $\bar{y} = 1-(1-\bar{x}_1)(1-\bar{x}_2)-(1-\bar{x}_3)+(1-\bar{x}_1)(1-\bar{x}_2)(1-\bar{x}_3)$ $=$...multiply... $= \bar{x}_1\bar{x}_3 + \bar{x}_2\bar{x}_3 - \bar{x}_1\bar{x}_2\bar{x}_3$
System failure probability	
$F = q_1q_3 + q_2q_3 - q_1q_2q_3$	$F = q_1q_3 + q_2q_3 - q_1q_2q_3$

Advantages of a FTA

- Well suited for modelling of binary (Boolean) mechanical processes, e.g. valve fails to open/close.
- Events occurring on component level due to interaction of multiple failures are easy to represent.
- Provides reliability figures of a system (if adequate data is available).
- FTA leads to improved understanding of system characteristics. Design flaws and insufficient operational and maintenance procedures may be revealed and corrected during the Fault Tree construction.
- Encourages a methodical way of thinking.
- Applicable to a wide field of systems and processes.

Disadvantages

- FTA is not (fully) suitable for modelling dynamic scenarios.
- FTA is binary (fail – success) and may therefore fail to address some problems.
- Complicated systems usually result in an unmanageable amount of basic events and branches.
- Reliability figures are often difficult to get.

Event Tree Analysis (ETA)

• An event tree analysis (ETA) is an inductive procedure that begins with an initiating (triggering, accidental) event and “propagate” this event through the system under study by considering all possible ways in which it can effect the behaviour of the system. The nodes of an event tree represent the possible functioning or malfunctioning of a (sub)system.

• By studying all relevant accidental events (that have been identified by a preliminary hazard analysis, a HAZOP, or some other technique), the ETA can be used to identify all potential accident scenarios and sequences in a complicated system.

• Design and procedural weaknesses can be identified, and probabilities of the various outcomes from an accidental event can be determined.

Working steps of a ETA

1. Identify (and define) a relevant accidental (initial) event that may give rise to unwanted consequences.
2. Identify the events that are relevant to the initiating event and can affect the propagation of the latter through the system. These events can be barriers, safety functions, protection layers, etc. and may be technical and/or administrative (organizational).
3. Construct the event tree.
4. Describe the (potential) resulting accident sequences.
5. Determine the frequency of the accidental event and the (conditional) probabilities of the branches in the event tree.
6. Calculate the probabilities/frequencies for the identified consequences (outcomes).
7. Compile and present the results from the analysis.

1. Identify (and define) a relevant accidental (initial) event

When defining an accident event, we should answer the following questions:

- What type of event is it (e.g., leak, fire)?
- Where does the event take place (e.g., in the control room)?
- When does the event occur (e.g., during normal operation, during maintenance)?

In practical applications there are sometimes discussions about what should be considered an accidental event (e.g., should we start with a gas leak, the resulting fire or an explosion).

Whenever feasible, we should always start with the first significant deviation that may lead to unwanted consequences.

An accidental event may be caused by:

- System or equipment failure.
- Human error.
- Process upset.

The accidental event is normally “anticipated”. The system designers have put in barriers that are designed to respond to the event by terminating the accident sequence or by mitigating the consequences of the accident.

2. Identify the events

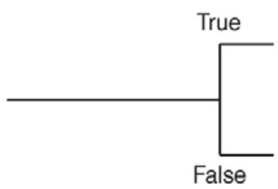
The events that are relevant to a specific triggering (initiating) event should be listed in the sequence they will be activated. Examples include:

- Automatic detection systems (e.g., fire detection).
- Automatic safety systems (e.g., fire extinguishing).
- Alarms warning personnel/operators.
- Procedures and operator actions.
- Mitigating barriers.

Each event should be described by a (negative) statement, e.g., " X does not function" (This means that X is not able to perform its required function(s) when the specified accidental event occurs in the specified context).

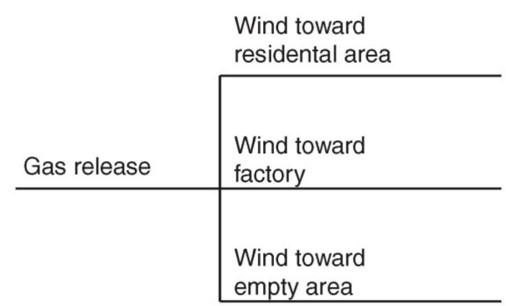
Additional events and factors should also be described by (worst case) statements, e.g., gas is ignited, wind blows toward dwelling area.

	B_1	B_2	B_3	B_4	B_5	
Accidental event	Additional event I occurs	Event I	Event II	Event III	Additional event II occurs	Outcome / consequence



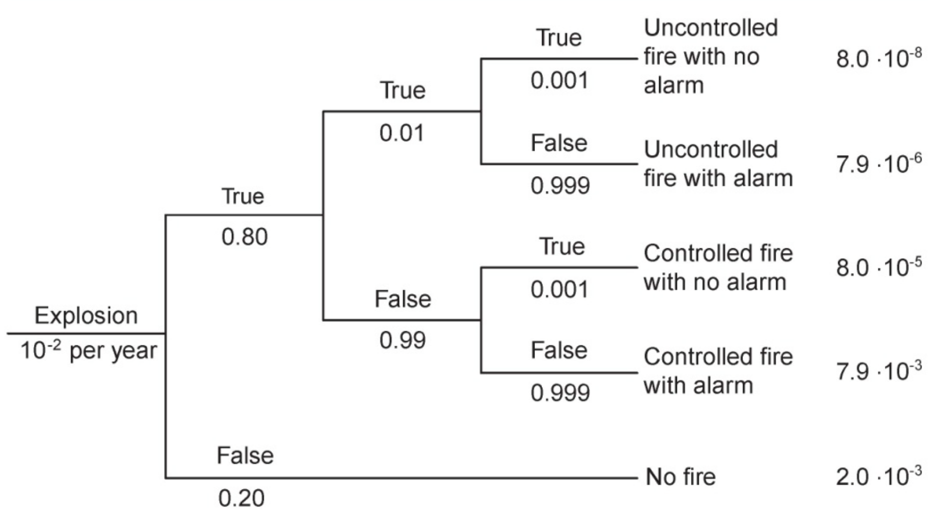
By this way the most severe consequences will come first

In most applications only two alternatives ("true" and "false") are considered. It is, however, possible to have three or more alternatives:

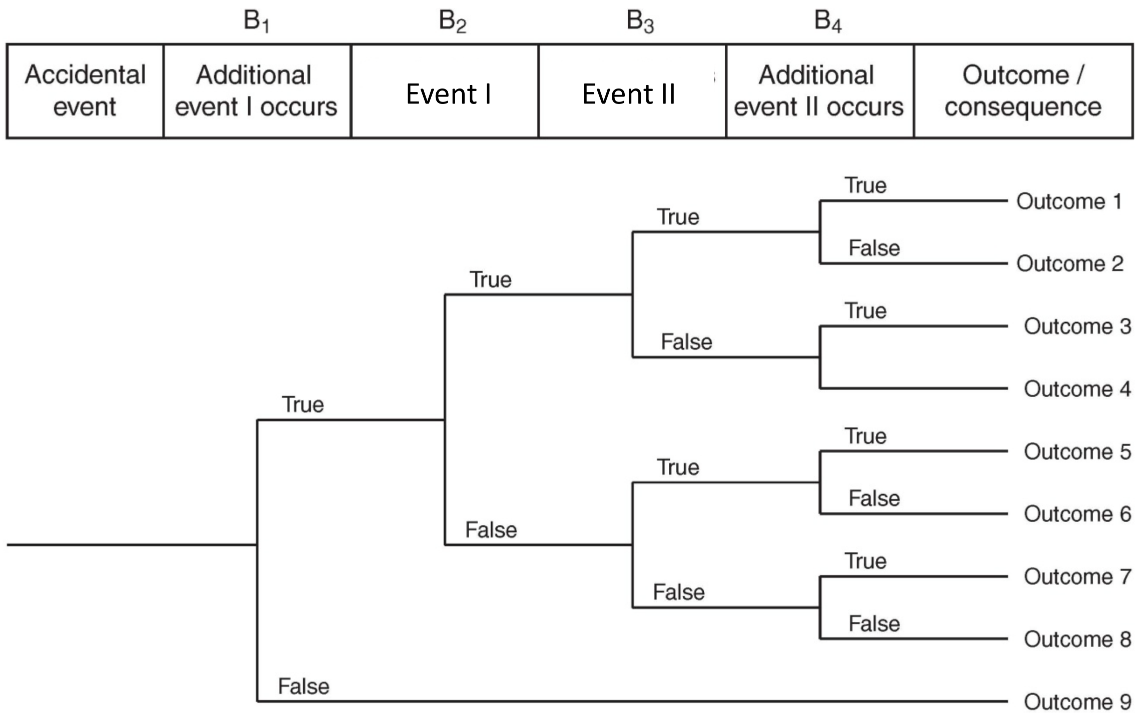


Example

Initiating event	Start of fire	Sprinkler system does not function	Fire alarm is not activated	Outcomes	Frequency (per year)



Generic Example



$$\Pr(Outcome\ \ 1 \mid Initiating\ \ \ Event) = \Pr(B1 \cap B2 \cap B3 \cap B4)$$
$$= \Pr(B1) \cdot \Pr(B2 \mid B1) \cdot \Pr(B3 \mid B1 \cap B2) \cdot \Pr(B4 \mid B1 \cap B2 \cap B3 \cap B4)$$

Note that all the probabilities are conditional given the result of the process until "Barrier i" is reached.

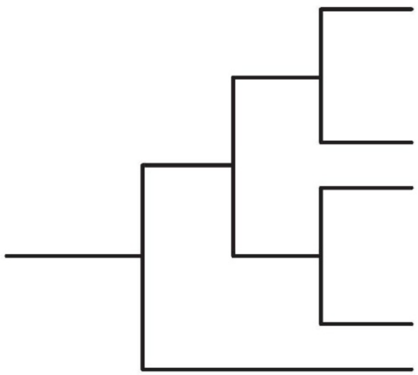
The frequency of the Outcome 1 is : $\Pr(Initiating\ \ \ Event) \cdot \Pr(B1 \cap B2 \cap B3 \cap B4).$

$where\ \ \Pr(Initiating\ \ Event)\ \ is\ \ the\ \ frequency\ \ of\ \ the\ \ initiating\ \ event.$

The frequencies of the other outcomes are determined in a similar way.

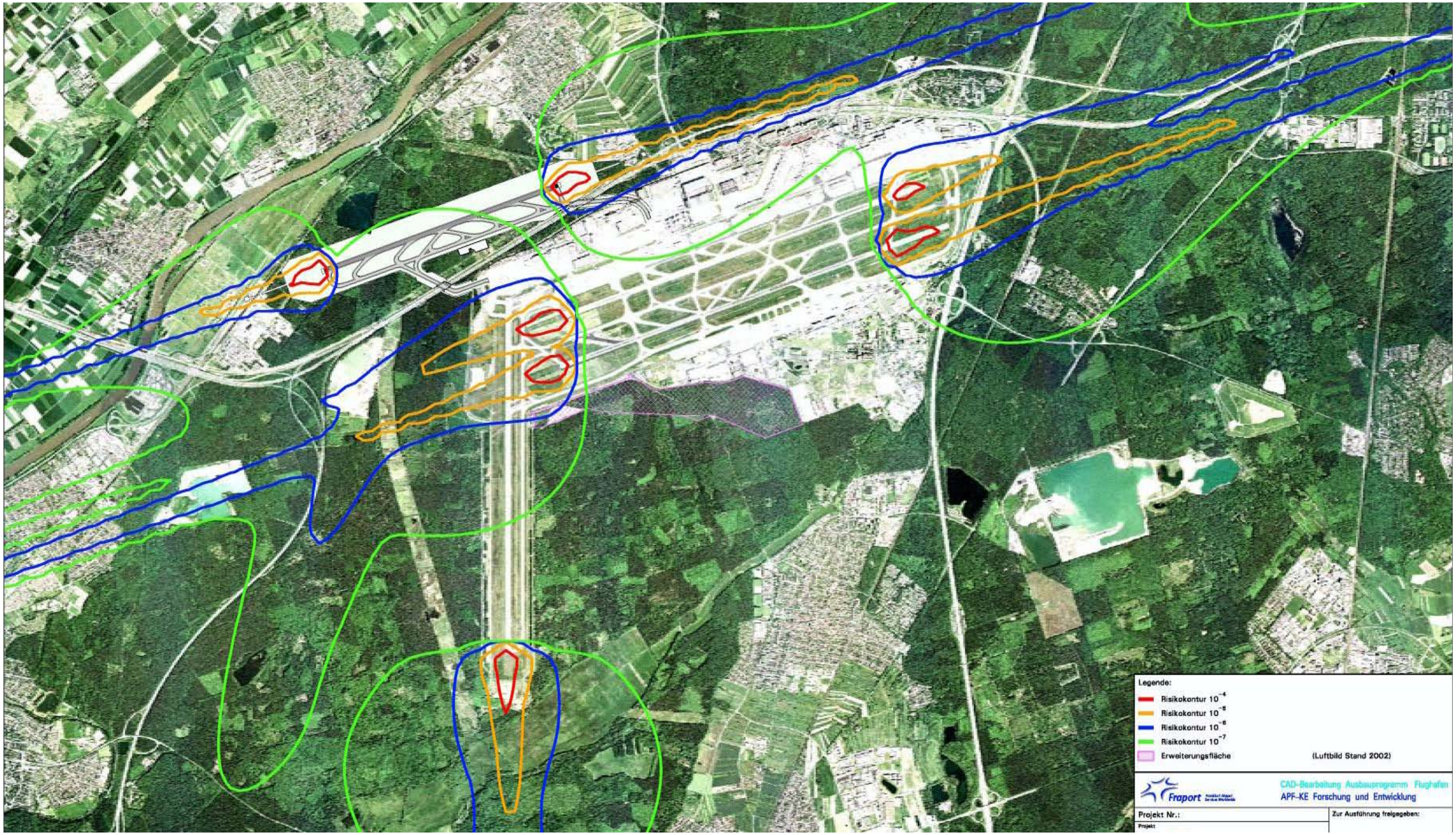
7. Present the results

Consequences Analysis



Out-come descr.	Freq-uency	Loss of lives					Material damage				Environmental damage			
		0	1-2	3-5	6 - 20	> 20	N	L	M	H	N	L	M	H

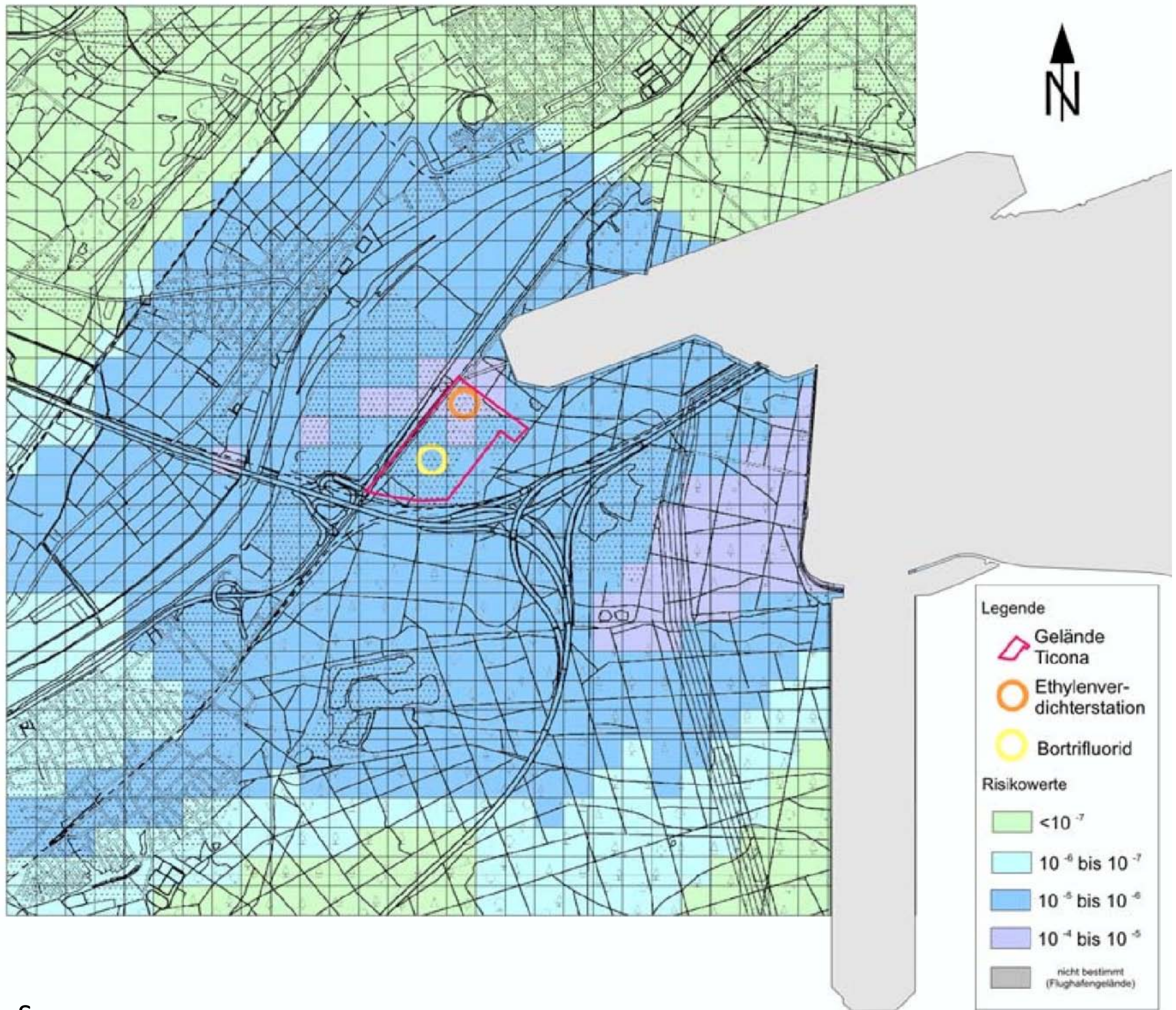
Example: Expansion of Frankfurt Airport (I) - Situation



Source:
http://www.ausbau.fraport.de/cms/default/dok/44/44526.neue_landebahn_und_ticona_sind_vereinbar.htm

Example: Expansion of Frankfurt Airport (II)

Risk zones, including the risk of toxic gas dispersion:



Source:
http://www.ausbau.fraport.de/cms/default/dok/44/44526.neue_landebahn_und_ticona_sind_vereinbar.htm

Example: Expansion of Frankfurt Airport (III) – Event Tree

Eintrittsfrequenz flugbetriebliches Primärereignis bei Tag [1/Jahr]: IF: 1,2E-06; PF: 1,7E-06

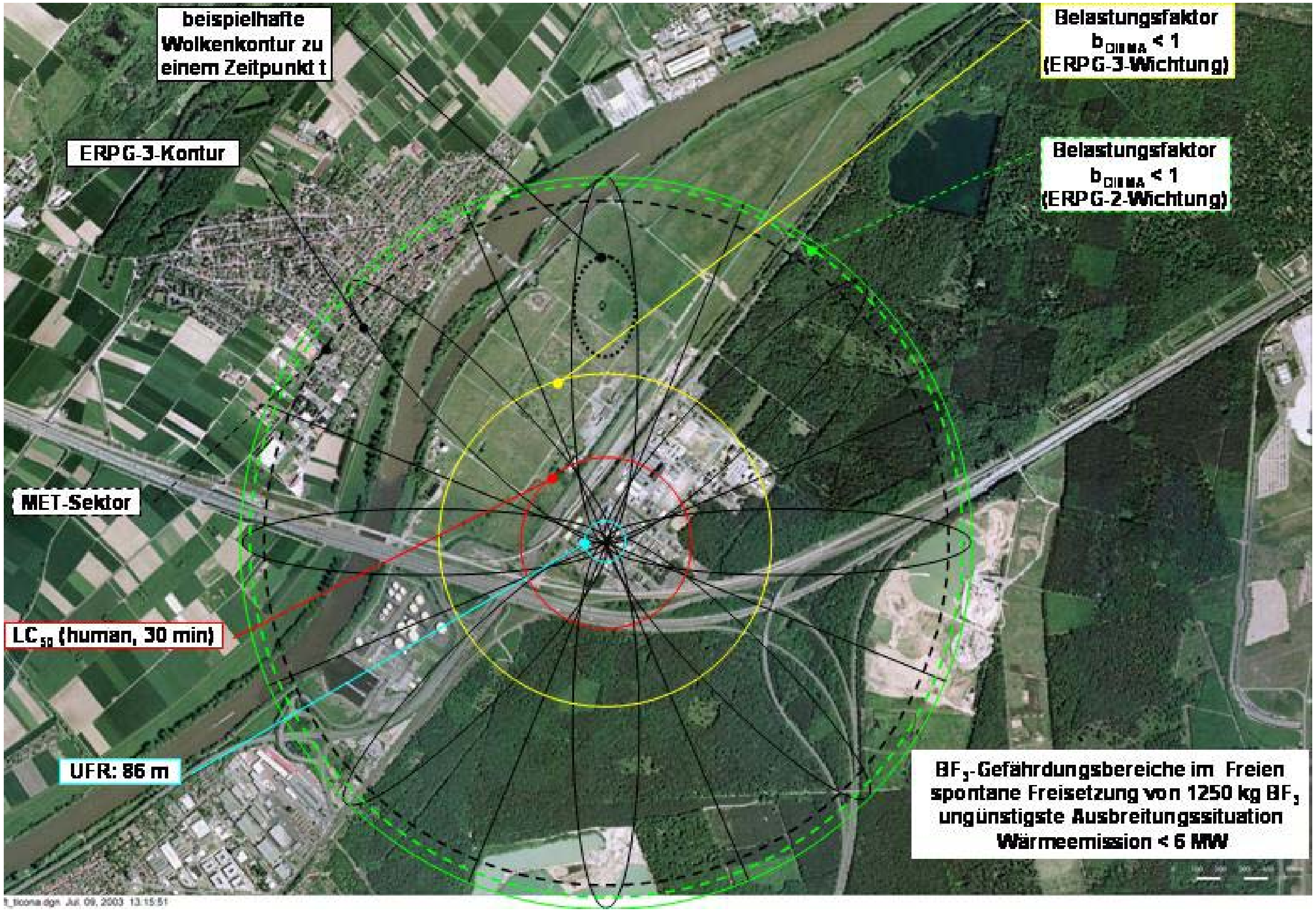
Folgeereignis / Sekundärereignis	Brandeinfluss	Ausbreitungs-situation	Ausbreitungs-richtung	Eintrittsfrequenz Schadensereignis [1/Jahr]		Gesamtbetroffenheit Anzahl Todesopfer: gesamt	exkl. Anlagen-personal	exkl. Gewerbe-gebiet	exkl. Gewerbe-gebiet + Anl.-Pers.
50% Direkt-einwirkung: BF_3-Freisetzung 1250 kg	10% Wärmeemission < 6 MW	40% ungün-stigste	10% N	IS:	2,4E-09	IS: 21	5	21	5
				PF:	3,4E-09	PF: 115	91	29	5
			26% NO	IS:	6,4E-09	IS: 30	0	30	0
				PF:	8,8E-09	PF: 47	0	47	0
			6% O	IS:	1,5E-09	IS: 23	0	23	0
				PF:	2,0E-09	PF: 35	0	35	0
			8% SO	IS:	2,0E-09	IS: 30	5	30	5
				PF:	2,7E-09	PF: 43	5	43	5
			4% S	IS:	9,8E-10	IS: 49	30	49	30
				PF:	1,4E-09	PF: 59	30	59	30
			30% SW	IS:	7,3E-09	IS: 39	23	39	23
				PF:	1,0E-08	PF: 49	23	49	23
			9% W	IS:	2,2E-09	IS: 21	8	21	8
				PF:	3,1E-09	PF: 92	72	28	8
			5% NW	IS:	1,2E-09	IS: 21	8	21	8
				PF:	1,7E-09	PF: 166	146	28	8
		60% mittlere	31% 10°-70°	IS:	1,1E-08	IS: 22	0	22	0
				PF:	1,6E-08	PF: 32	0	32	0
			10% 70°-130°	IS:	3,7E-09	IS: 22	0	22	0
				PF:	5,1E-09	PF: 32	0	32	0
			7% 130°-190°	IS:	2,6E-09	IS: 19	0	19	0
				PF:	3,6E-09	PF: 28	0	28	0
			32% 190°-250°	IS:	1,2E-08	IS: 17	0	17	0
				PF:	1,6E-08	PF: 25	0	25	0
			11% 250°-310°	IS:	4,0E-09	IS: 13	0	13	0
				PF:	5,6E-09	PF: 30	11	19	0
			8% 310°-10°	IS:	2,9E-09	IS: 13	0	13	0
				PF:	4,1E-09	PF: 23	4	19	0
50% Trümmerwurf: BF_3-Freisetzung 500 kg	90% Wärmeemission >= 6 MW	44% ungün-stigste	10% N	IS:	2,4E-09	IS: 12	0	12	0
				PF:	3,4E-09	PF: 19	0	19	0
			26% NO	IS:	6,4E-09	IS: 12	0	12	0
				PF:	8,8E-09	PF: 19	0	19	0
			6% O	IS:	1,5E-09	IS: 12	0	12	0
				PF:	2,0E-09	PF: 19	0	19	0
			8% SO	IS:	2,0E-09	IS: 12	0	12	0
				PF:	2,7E-09	PF: 19	0	19	0
			4% S	IS:	9,8E-10	IS: 12	0	12	0
				PF:	1,4E-09	PF: 19	0	19	0
			30% SW	IS:	7,3E-09	IS: 12	0	12	0
				PF:	1,0E-08	PF: 19	0	19	0
			9% W	IS:	2,2E-09	IS: 11	0	11	0
				PF:	3,1E-09	PF: 19	1	18	0
			5% NW	IS:	1,2E-09	IS: 11	0	11	0
				PF:	1,7E-09	PF: 20	2	18	0
		56% mittlere	in Relation zu den Primärfolgen vernachlässigbare BF_3-Schadenswirkung						

Boron Trifluoride (BF_3)- Storage:

Direct impact of an airplane crash (medium sized airplane), total release (1.25 tons).

Source:
http://www.dfld.de/PFV_Landebahn/PFV/Ordner57/002_G16_3.pdf

Example: Expansion of Frankfurt Airport (IV) – Risk Regions



BF_3-Storage:

BF_3-Risk regions,
total release (1.25 tons),
worst case dispersion,
heat emission < 6 MW.

Sources:
http://www.dfld.de/PFV_Landebahn/PFV/Ordner57/002_G16_3.pdf
http://www.ausbau.fraport.de/cms/default/dok/44/44526.neue_landebahn_und_ticona_sind_vereinbar.htm

Advantages of an ETA

- Visualize event chains following an accident event.
- Visualize barriers and sequence of applications.
- Good basis for evaluating the need for new/improved procedures and safety functions.
- Applicable to all kind of (technical) systems, specially for larger facilities with active and passive security measures and unknown physical/chemical system states.
- Scenarios and event sequences are listed and analysed.
- Combination of function and failure.

Disadvantages

- Difficulty in application: practical knowledge and a detailed system analysis needed.
- Only one initiating event can be studied in each analysis.
- Easy to overlook subtle system dependencies.
- Not well suited for handling common cause failures in the quantitative analysis.
- Reduced readability of large event trees.
- Modifications of an event tree (by inserting a new subsystem) are difficult.

References

1. Papazoglou, I.A. and O.N. Aneziris, *Master Logic Diagram: method for hazard and initiating event identification in process plants.* Journal of Hazardous Materials, 2003. **97**(1-3): p. 11-30.

2. Kletz, T., *HAZOP & HAZAN: Notes on the Identification and Assessment of Hazards*. Loss Prevention: Hazard Workshop Modules. 1983, Rugby (GB): The Institution of Chemical Engineers.

3. Pitt, M.J., *Hazard and Operability Studies: A Tool for Management Analysis.* Facilities, 1994. **12**(13): p. 5-8.

4. VDI-2075, *Eissportanlagen - Technische Gebäudeausrüstung*. 2003, VDI Verlag GmbH: Düsseldorf. p. 1-93.

5. ISO-9001, *Quality Management Systems - Requirements*. 2000, International Organization for Standardization (ISO): Geneva.

6. MIL-STD-1629A, *Military Standard Procedures for Performing a Failure Mode, Effects and Criticality Analysis*. 1980, US Department of Defense. p. 1-32.

7. DIN-25424T1, *Fehlerbaumanalyse: Methode und Bildzeichen*. 1981, Beuth Verlag: Berlin. p. 1-15.

8. DIN-25424T2, *Fehlerbaumanalyse: Handrechenverfahren zur Auswertung eines Fehlerbaumes*. 1990, Beuth Verlag: Berlin. p. 1-8.

9. Roberts, N.H., et al., *Fault Tree Handbook (NUREG-0492)*. 1981, Washington, D.C.: U.S. Nuclear Regulatory Commission. 1-209.

10. Lewis, E.E., *Introduction to Reliability Engineering*. 1987, New York: John Wiley & Sons.

11. *System Safety Analysis Hand Book*. First Edition ed. 1993: System Safety Society.

12. DIN-25419, *Ereignisablaufanalyse: Verfahren, graphische Symbole und Auswertung*. 1985, Beuth Verlag: Berlin. p. 1-5.

13. NASA Fault Tree Handbook with Aerospace Applications, 2002.

14. Tim Bedford and Roger Cooke. Probabilistic Risk Analysis: Foundations and Methods. Cambridge University Press, 2001.

15. Mohammad Modarres. Risk Analysis in Engineering : Techniques, Tools, and Trends. Taylor & Francis, Inc., 2006.

16. Ian Lerche and Walter Glaesser. Environmental Risk Assessment: Quantitative Measures, Anthropogenic Influences, Human Impact. Springer, 2006.

17. Hiromitsu Kumamoto. Satisfying safety goals by probabilistic risk assessment. Springer, 2007.

Laboratory for Safety Analysis
INSTITUTE FOR ENERGY TECHNOLOGY

Course material:

http://www.lsa.ethz.ch/education/vorl

HAZOP - Form

Guide word	Deviation	Possible cause	Consequences	Action required
Less	Pressure in the piping system (1.0)	Compressor is running to low (1.1)	Reduced cooling	Install surveillance equipment
Less	Pressure	Pipe leakage (1.0)	Release	Higher inspection intervals
More	Pressure	Compressor is running to high (1.1)	Potential of pipe break	Install surveillance equipment
No	Mass flow in the piping system (1.0)	Compressor are out of order (1.1)	No cooling	Higher maintenance intervals
Reduced	Mass flow	One Compressor broken (1.1)	Reduced cooling	Install redundancy
Reduced	Mass flow	Pipe break inside building (1.0)	Release, risk of harm, loss of cooling	Regular visual inspection
…				

FMEA - Form

System: Skating rink		
Initial state: Normal daily routine	Environmental conditions: Temperature 8°	Documentation: Plans, system specifications, …

Nr.	**Unit**	**Failure mode of *(b)***	**Class: Frequency of *(c)***	**Failure recognition of *(c)***	**Countermeasures against *(c)***	**Failure effect of *(c)* on the adjoined units**	**Comments *(g)***	**Class: Effect / facility state**
(a)	***(b)***	***(c)***	*(d)*	*(e)*	*(f)*	***(g)***	*(h)*	*(i)*
1	Pipe (1.0)	Blockage	Reasonable probable	Loss of cooling	Instruction maintenance personal	Overpressure at the pumps (1.1)		Marginal
		Break	Rare	Loss of cooling	Adequate position of pipes, visual inspection	Underpressure at the pumps,		Critical
2	Compressor(1.1)	Stops pumping	Reasonable probable	Loss of cooling / pressure	Install redundancy	No flow		Minor
		More pressure	Reasonable probable		Higher maintenance intervals	Expansion of the cooling liquid		Marginal
	…							