Risk assessment methodologies of hydrogen applications in a socio-technological context

Frank Markert
Systems Analysis Department
Risø National Laboratory
Technical University of Denmark

2nd European Summer School on Hydrogen Safety
Belfast, 30.7 – 8.8.2007

Introduction

New technologies have to be at least as safe as the well known alternatives.

Testing and systems analysis is required
to achieve high
level of safety

The lecture is dealing with methodologies that describe the
hydrogen applications as being
part of a socio-technological system.

Outline of lecture

- Accident model, scenarios, basic measures
- The role of risk analysis
- Hazard identification
- Functional modelling
- Barrier diagrams
- Short about GIS-systems
- Uncertainty in the results

Definition of risk and hazard

The "Seveso-II-directive" includes definitions for hazard and risk:

Hazard shall mean the intrinsic property of a dangerous substance or physical situation, with a potential for creating damage to human health and/or the environment.
Risk shall mean the likelihood of a specific effect occurring within a specified period or in specified circumstances.

As such,
RISK is a complex function of:
- the *hazards* connected with a certain system,
- the *probability* that a hazard results in an undesired event,
- the *consequences* of this event and
- the *vulnerability* of the environment that is exposed.

- *Perceived* risk, or risk as interpreted by the general public, as well as the acceptability of certain risks appear to depend on many aspects like control, dread, knowledge and trust.

Historical development of Risk Analysis

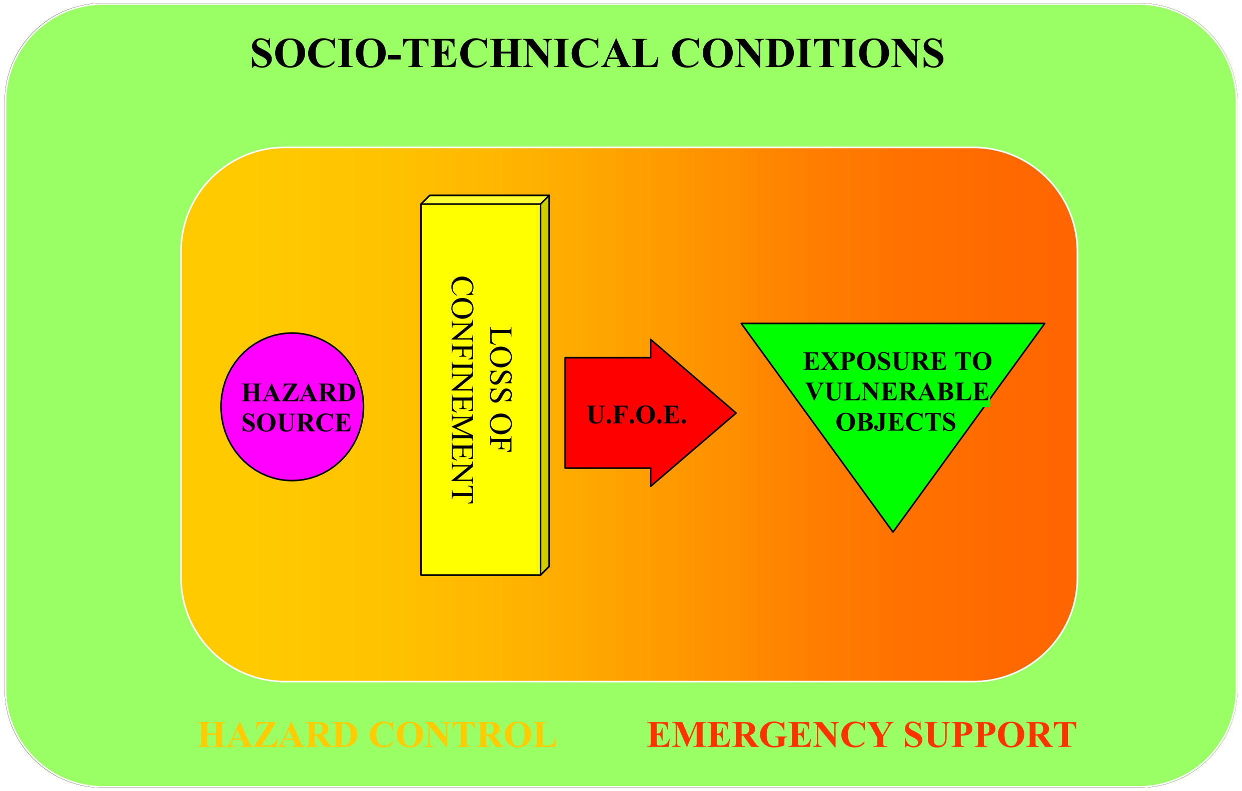
Of methodologies and techniques for complex systems

1. **Technical age:**
   - *Fokus on operational & engineering methods to ”combating” hazards*

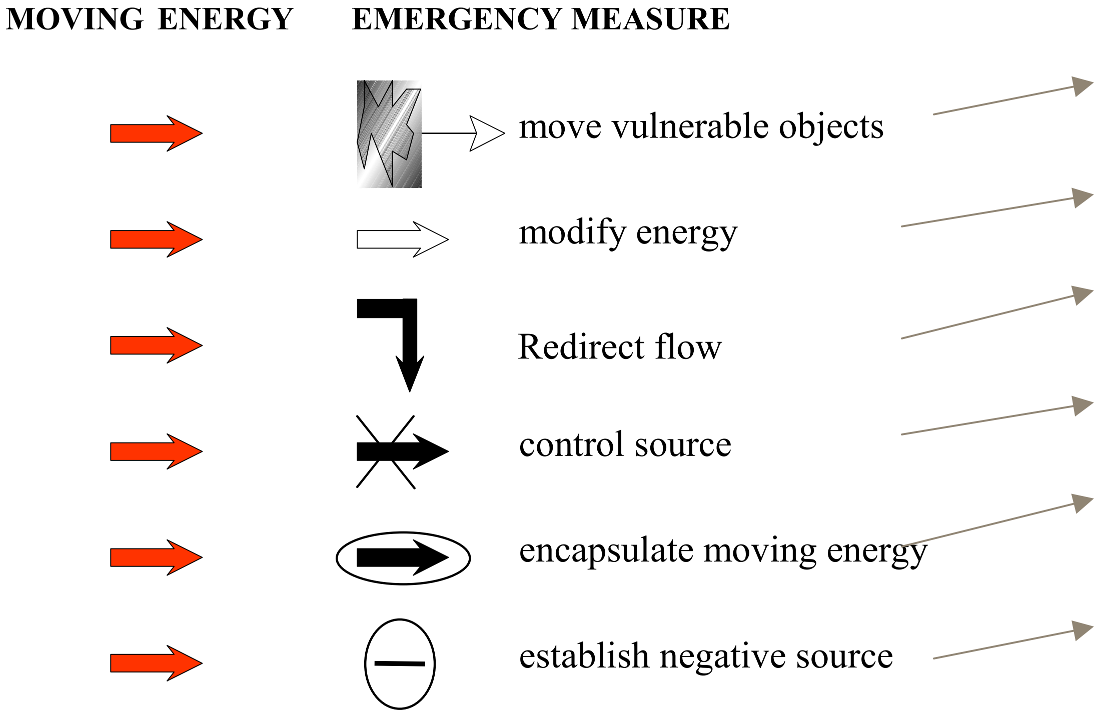
2. **Human error age**:
   - *Human beings are capable of circumventing even the most advanced engineered safety device*

3. **Socio-technical age:**
   - *Recognition that the major residual safety problems do not exclusively belong to technical or operational factors, but that the interactions between the technical and social aspects of the system are important*

A GENERAL Accident MODEL



Basic emergency measures



Evacuate plant staff & neighbors, traffic control, remove valuable objects
Water curtain (absorb heat)
lead outflow away from sensitive areas
Extinguish fire, cover leak
Cover with foam
Lead spills to sewer, add chemical agents that react with dangerous substance

A GENERAL ACCIDENT MODEL

Any accident can be described as one or more sequences of "energy transfer", influenced by more or less successful confinements.

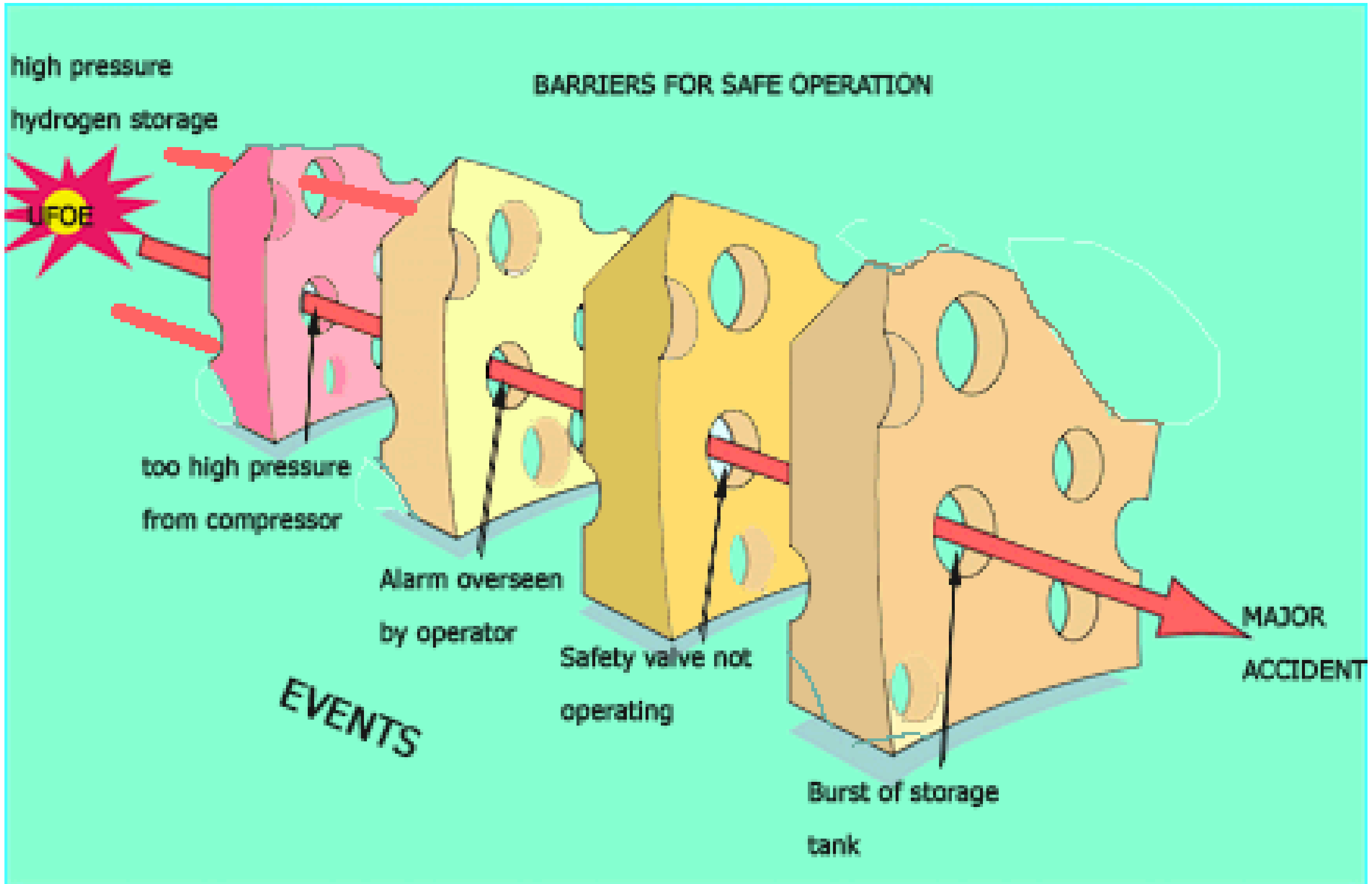
•A confined amount of energy can constitute a hazard source. If sufficient energy is present, the prerequisites for an accident are present. It is essential to ensure that all hazard sources of the considered activity are identified and evaluated.

•Central factors of the model is confinement and loss of confinement. Confinements involve containing systems and control systems. In order to control the hazard source possibilities for confinements must be identified and realised.

•The combination of sufficient energy and inadequate confinement results in uncontrolled flow of energy (UFOE).

•If a vulnerable object is exposed to an energy flow without sufficient barriers then the accidental consequence becomes a fact. There is a near-miss incident if a UFOE occurs without hitting a vulnerable target. Vulnerable objects can be human beings, environment and property.

Barriers & Events
Swiss-cheese model



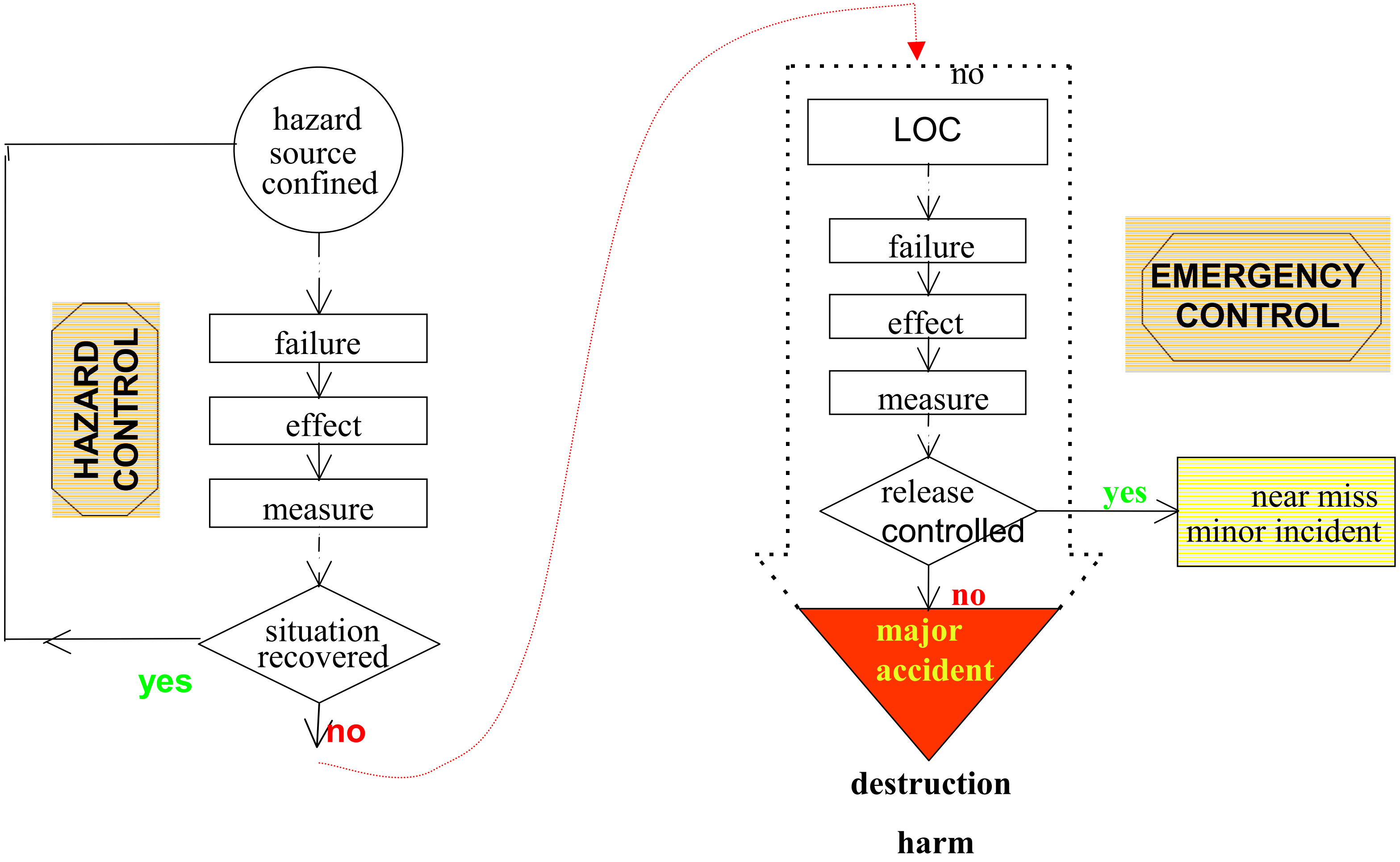
What is a scenario?

An **Accident** is a specific, unplanned sequence of events

For each EVENT the following has to be analysed:

FAILURE:	Not intended condition or event
EFFECT:	Consequences, impact, change-of-state, change-of-condition, domino effects, failure propagation
MEASURE:	Protective, preventive, operation, equipment, decision, alarm

SCENARIO MODEL

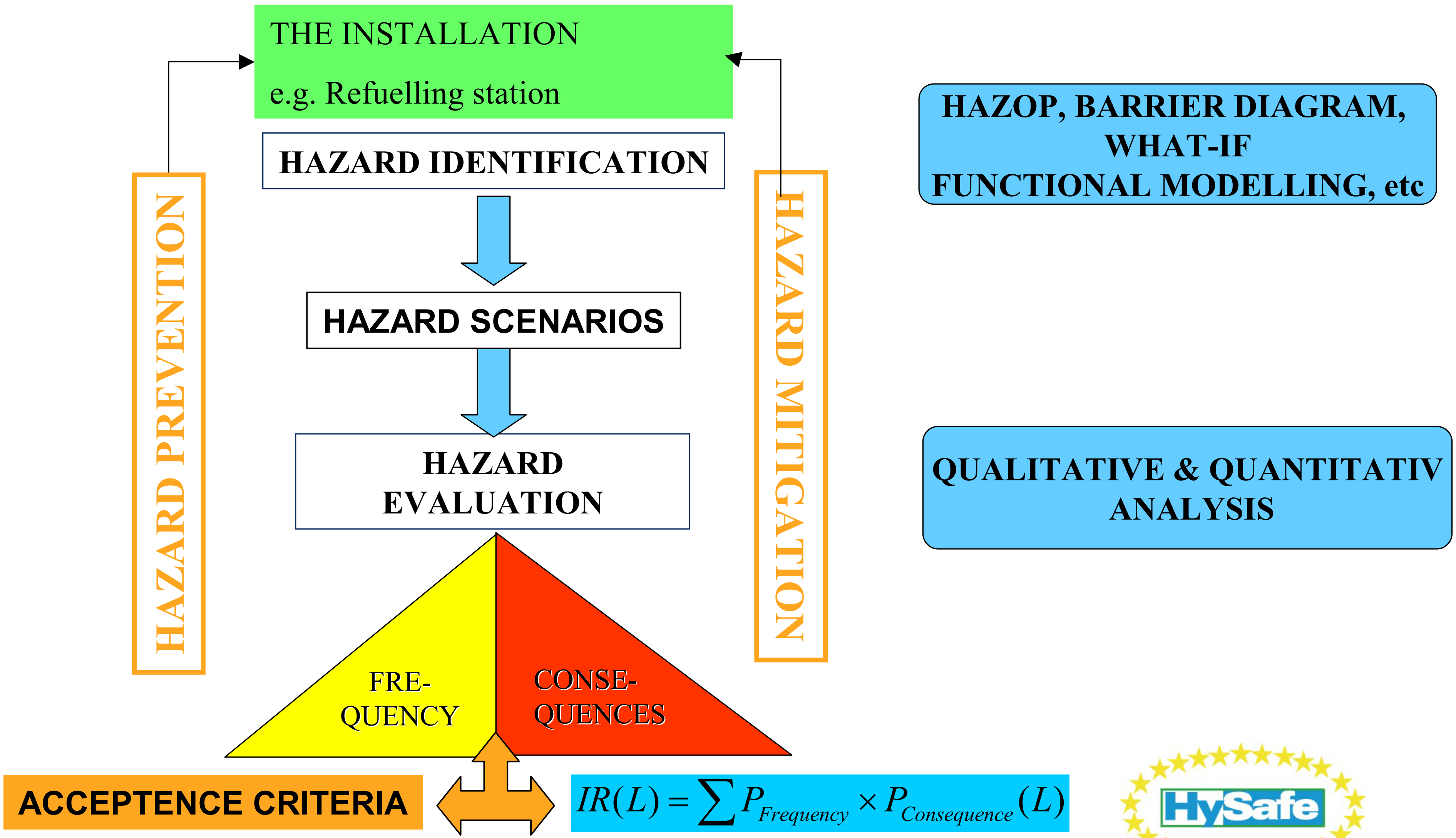


LOOP for each source and event (dependent on: time, geography and other rel. factors)

SCENARIO MODEL - TABLE

loop	failure	effect	measure
0	-	-	storage conditions, smoke/gas detectors and alarms, packing materials, facility
1	insufficient storage tests, temperature too high	wrong storage conditions, decomposition, heat generation	smoke detection
2	smoke detection too slow	escalation of decomposition, damage to packing materials	fire alarm
3	release of burning chemicals	domino effect, ignition of part of the storage	on-site emergency operation (extinguish fire, cover with foam)
4	bad access to fire source	insufficient fire fighting, developing fire	on-site emergency operation (extinguish fire, cover with foam), alarm to police and fire brigade
5	fire fighting insufficient	fully developed fire, damage to building, release of toxic fumes	evacuate plant staff, evacuate neigh-bours, stop traffic to area, remove valu-able objects
6	evacuation too slow	harm to people	hospitals, ambulances
7	insufficient collection of water from fire fighting	contamination of recipients	cleaning of contaminated areas
8	fire fighting insufficient	damage to property	build new storage

Elements of a Risk Analysis



HAZARD IDENTIFICATION

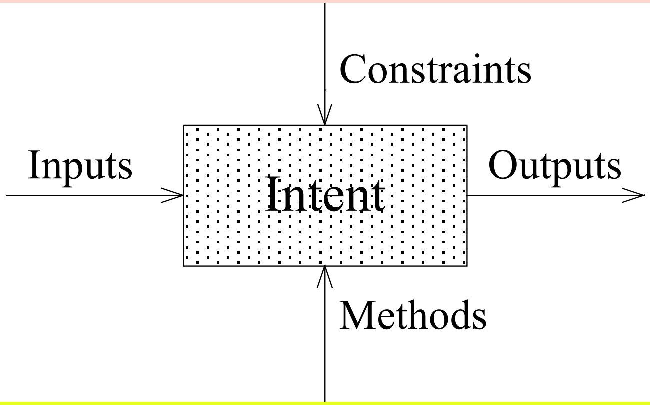
- Methods based on a *top-down analysis*,
  - *start from a top event and going down to basic events*
    - e.g. Fault Trees, Functional analysis, Hazard and Consequences Analysis
- Methods based on a *bottom-up analysis*,
  - *starts with deviations of the process variables/failures of devices investigating the consequences*
    - e.g. HAZOP, Structured What-If Technique (SWIFT), Hazard Screening Analysis (HAZSCAN) and FMEA
- Methods based on the *systematic use of standard checklists*, after division of the plant in areas, lessons learnt from past accidents/detailed studies.

HAZARD IDENTIFICATION
Functional modelling – basic object

Intents - the functional goals of the specific plant activity

Constraints
items to supervise or restrict the Intent.
(*physical laws, work organisation, con-trol & protective systems)*

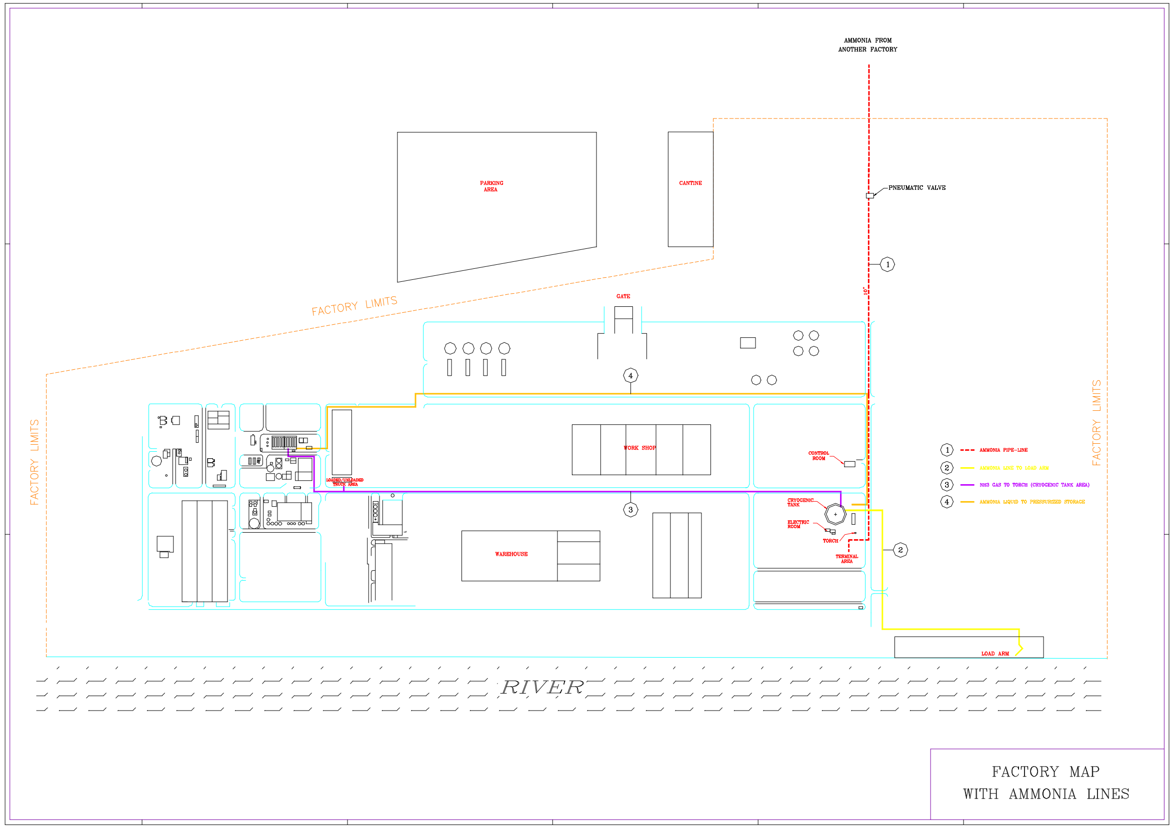
Inputs
the necessary con-ditions to perform the Intent & the link to the previous Intent



Outputs
the outcome from the Intent & the link to subsequent Intent.

Methods
hardware, procedures, software to carry out the Intent

An example – large gas storage



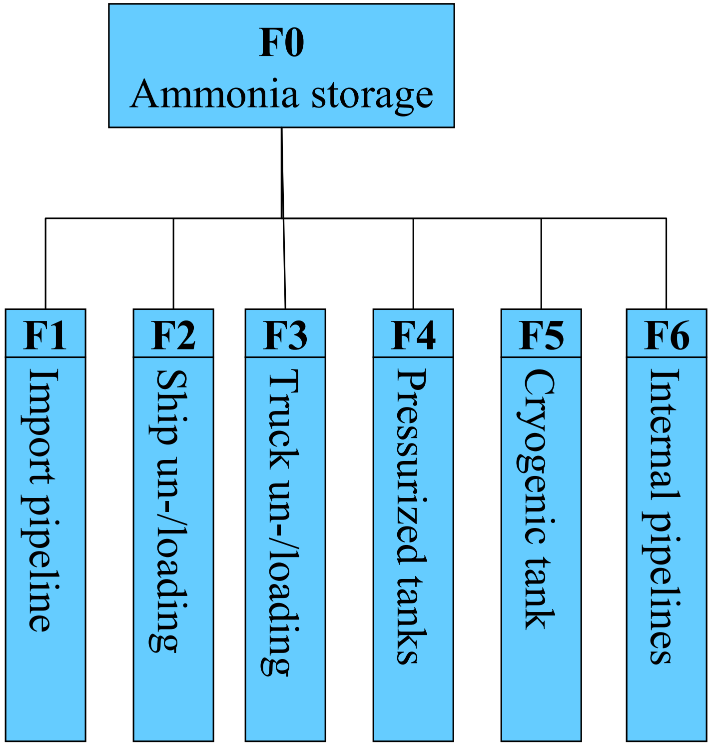
INSTALLATIONS:

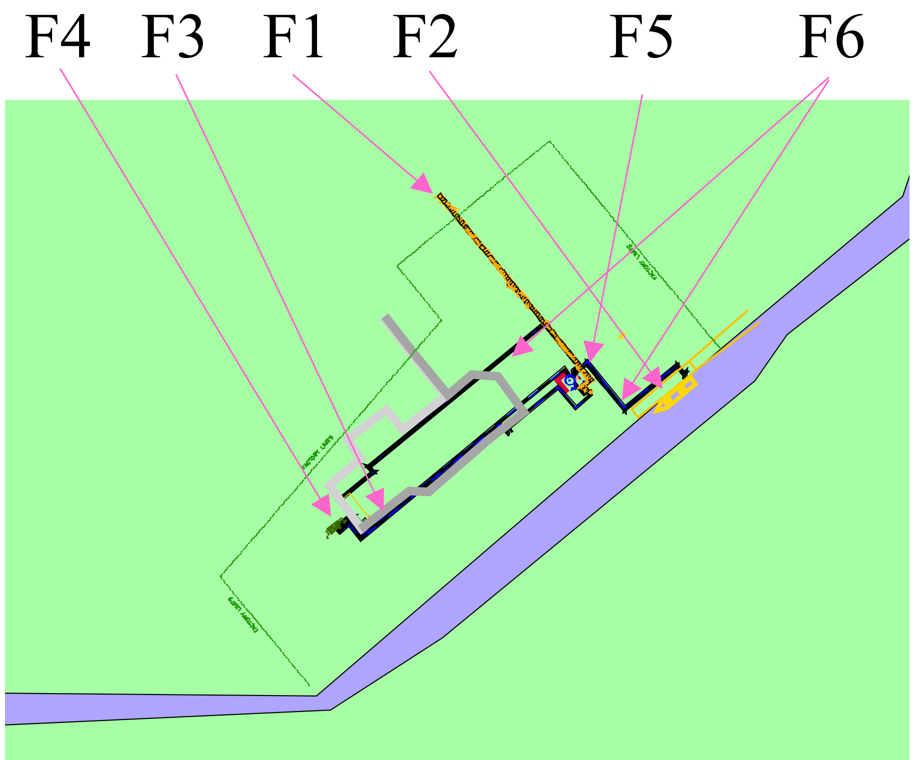
Pressurized storage
Cryogenic storage
Pipelines (delivery)
Pipelines (connecting)

Example plant subdivision into functions 1

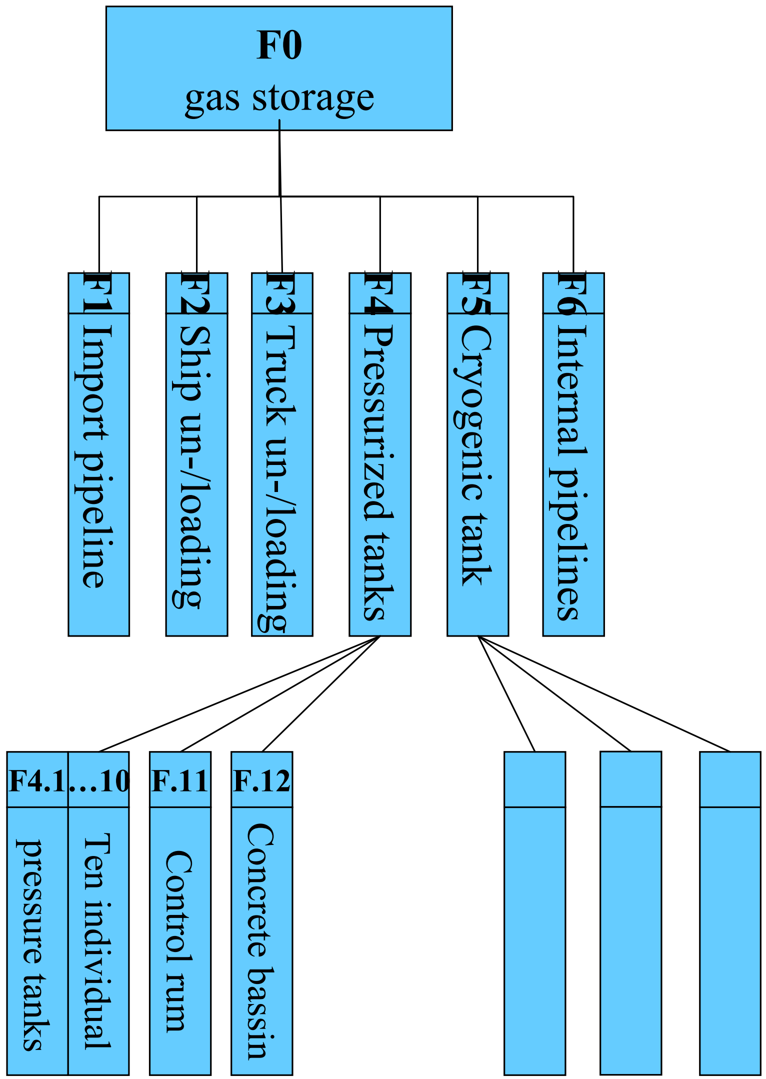
F0
gas storage facility

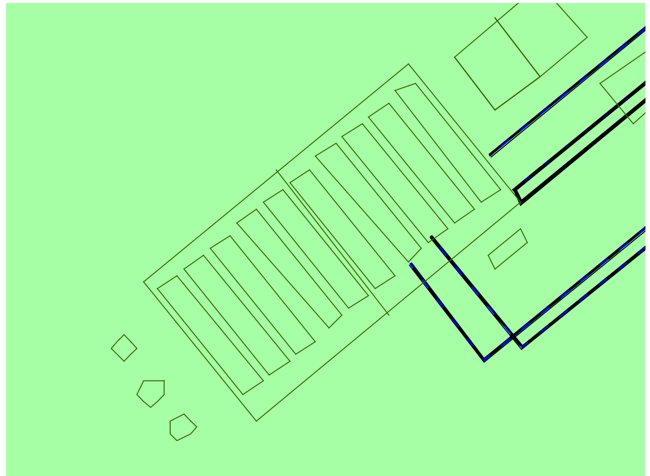
Example plant subdivision into functions 2

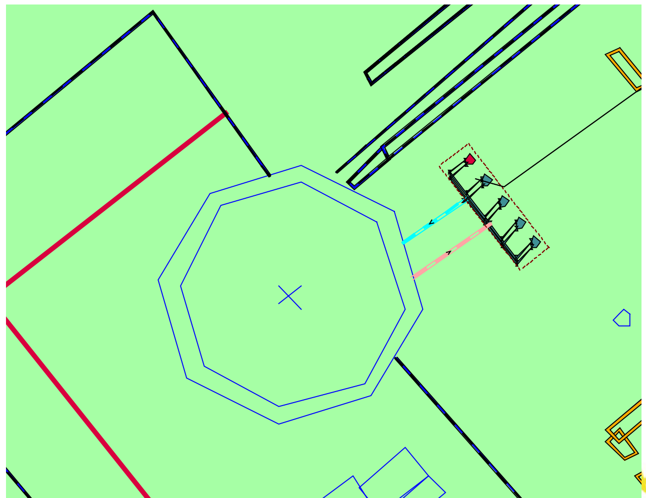




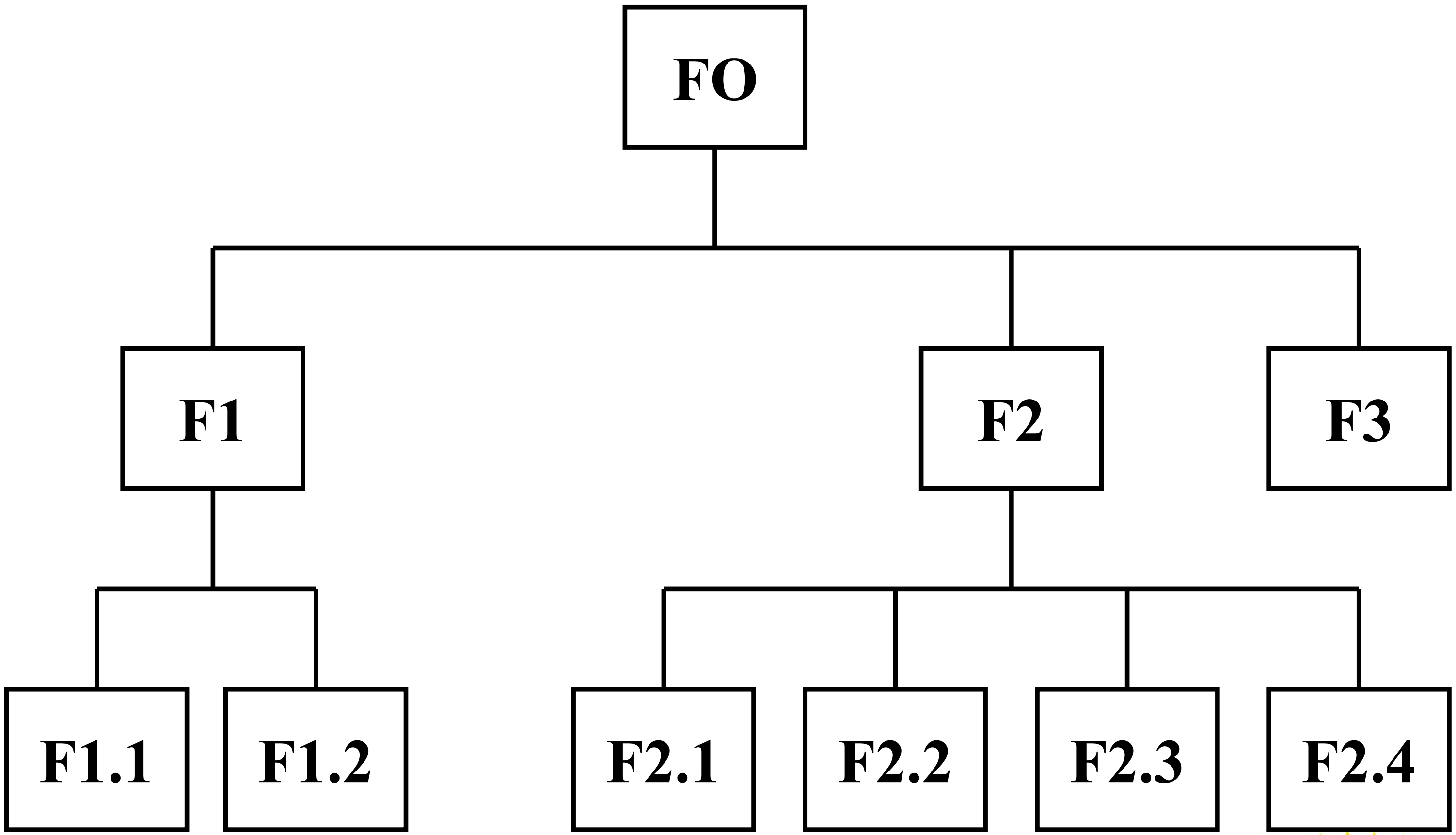
Example plant subdivision into functions 3







Hazard identification – Functional modelling

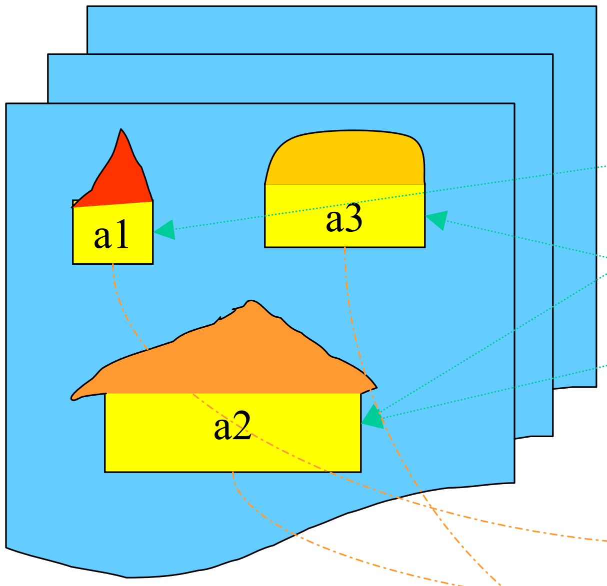


Output example for functional modelling

Intent		Storage of chemicals
Methods	Safety	Alarms (e.g. gas, smoke) Fire engines and equipment
	Operation	Coordination of activities Safety culture Maintenance and repair Construction Inspection Manuals, procedures and instructions
Constraints	Safety	Prevent fire ignition Manage fire Manage exposure Protect storage from external damage
	Operation	Logistics Inspection and supervision Manuals, procedures and instructions

What is a Geographical Information System?

- Database
- Map
- Advanced analysis of data linked to geographical information
- Data management system



key	substance	Max. Storage Date
B1	TNT	2/2-2002
B2	C6H6	4/2-2002
B3	HCN	12/11-2001
B4	Ether	12/07-1999

key	Industry	staff	hazards	chemicals
a1	Name 1	2	Explosion	TNT
a2	Name 2	10	Flam.	C6H6
a3	Name 3	20	Tx	HCN

Advenatges of a GIS

- GIS database will preserve the geographical data
- Visualisation of exact locations of the equipments.
- Easier to assess possible domino effects
- Application of (regional) maps
- Correlation with population densities or vulnerable environments etc. to supports the analyses of the consequences,
- Present IR curves around the facility or to calculate more easily F-N curves.

BARRIER DIAGRAMS

Barriers can be defined as measures present to interrupt an accident event sequence,
(i.e. prevent the end-event of the accident scenario in occurring.)

Examples of barriers:

- An alarm for instance for high level in a tank.
- A sprinkler system in a building to prevent fires in developing.
- A dike surrounding a tank, designed to contain accidental spillage from the tank.

Barriers can be of different types.

- Active versus passive barriers
- Automatic versus manual barriers

Barrier diagrams serve two main purposes:

1) Evaluation of adequateness of safety measures (part of accident prevention)
(Are the barrieres reasonable and independent? Are barriers missing?)

2) Communication to all stakeholders
(Illustrating the possible accident scenarios and safety measures taken to prevent them)

CONSTRUCTION OF BARRIER DIAGRAMS

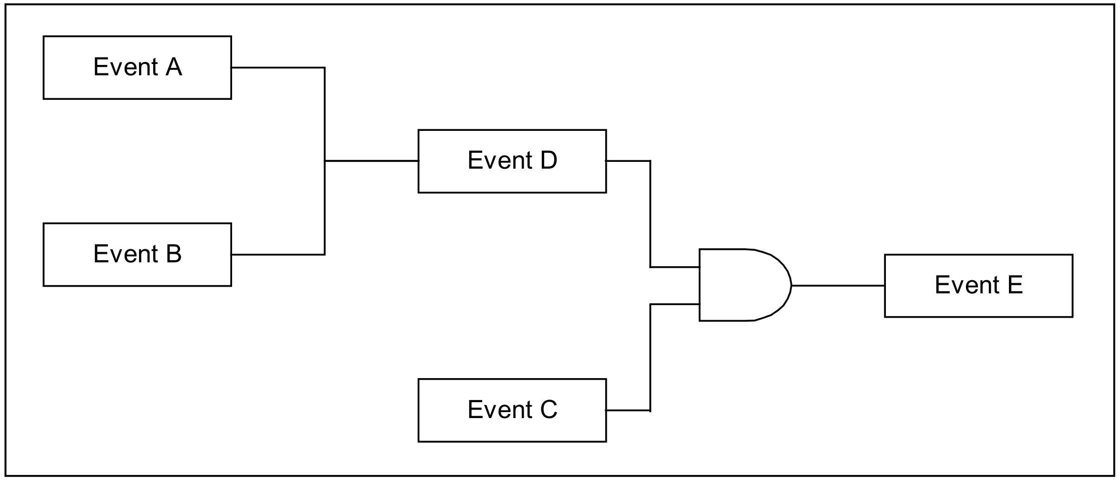
The construction of barrier diagrams consists of 4 steps:

1. Construction of the event chains
2. Inclusion of the barriers.
3. Evaluation for each barrier of what would happen assuming that the barrier is effective and construction of relevant event chains from the evaluation.
4. Classification of barriers according to type or evaluated reliability of the barrier (optional).

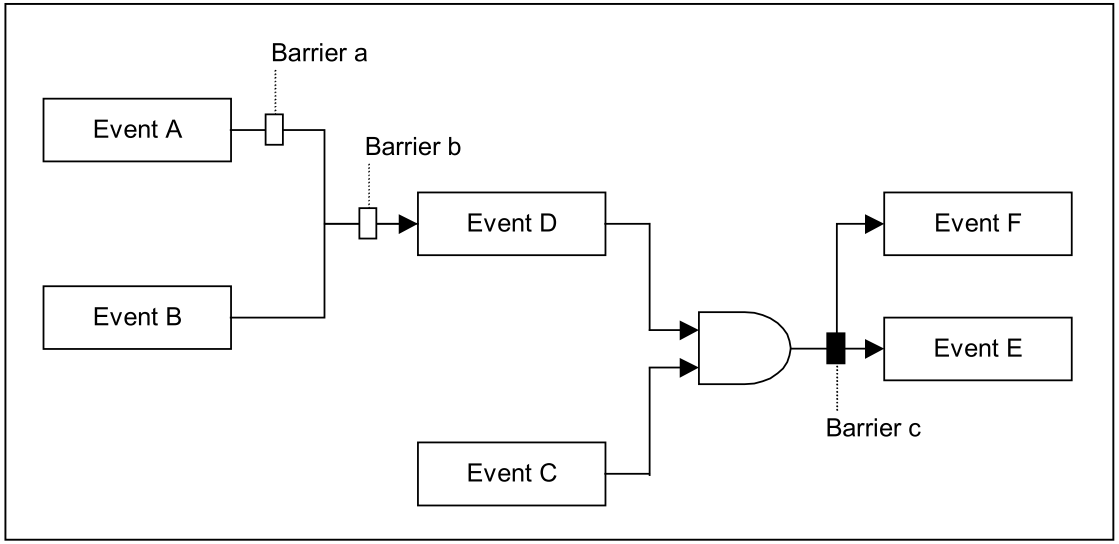
When constructing barrier diagrams one must start with ignoring all the existing barriers! The main structure of the barrier diagram is the event chains, which may consist of elements from both the event tree and the fault tree method. An example the event (cause-consequence) chains of a barrier diagram is given below. The events most to the left may be called the initiating events (causes) and those most to the right the consequences.

STEPS IN CONSTRUCTING BARRIER DIAGRAMS

STEP 1



STEP 2



Evaluation of barrier diagrams

Once the barrier diagram is finished, the level of safety should be evaluated.

The purpose of evaluating the barrier diagrams is to determine whether there are sufficient barriers against the undesired events happening, i.e. is the design sufficiently safe.

When evaluating the diagram one must consider:

- The frequency/probability of the initiating events
- The severity of the end events (consequence assessment)
- The number, coverage and reliability of barriers in each of the event chains in the diagram

TYPES OF UNCERTAINTY

- Aleatory, also known as stochastic uncertainty or due to randomness.

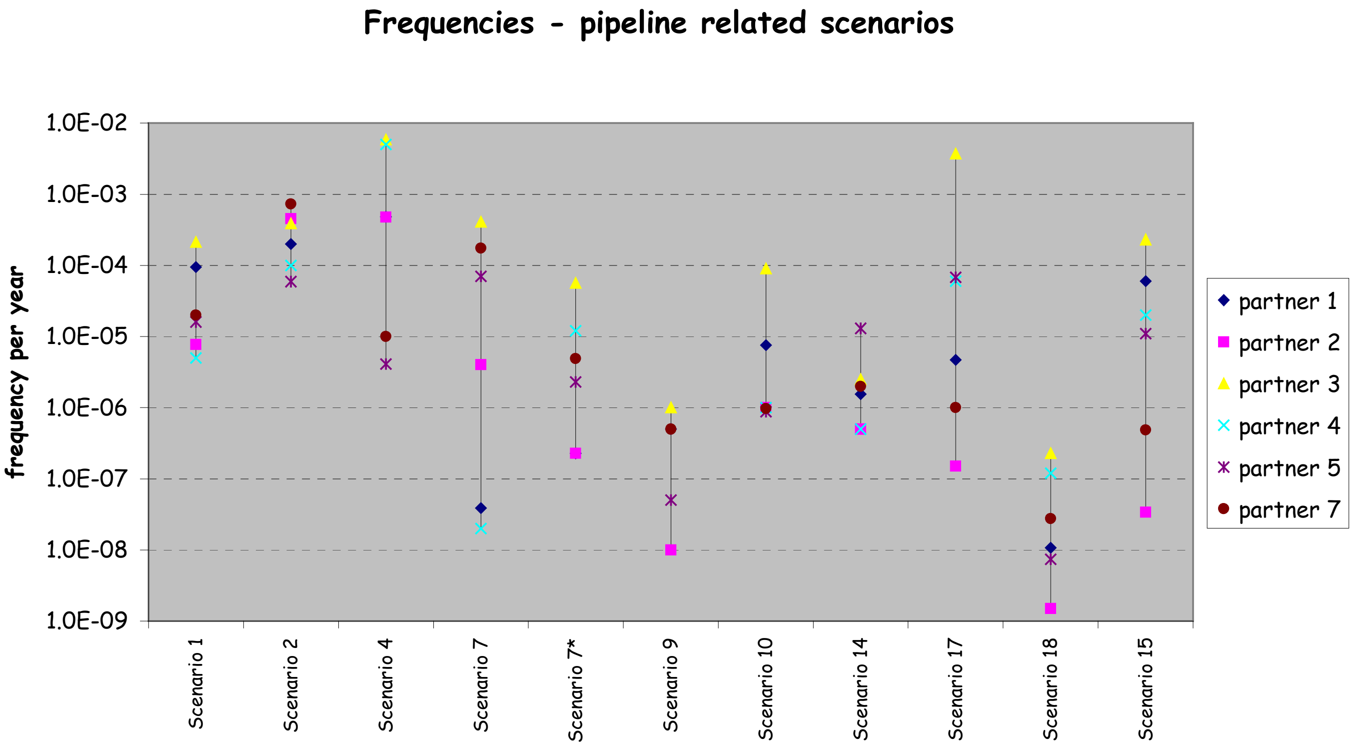
  This can be called irreducible. Even if a certain narrowing of the range in which the risk figures are defined can be achieved through a better knowledge of their distributions, quantities such as failure rates, and meteorological conditions at the time of a release, size of a breakage etc. can only be defined through probability distributions.

  Aleatory uncertainties can be treated by well-established methods, e.g. propagated through the analysis by Monte Carlo simulation.

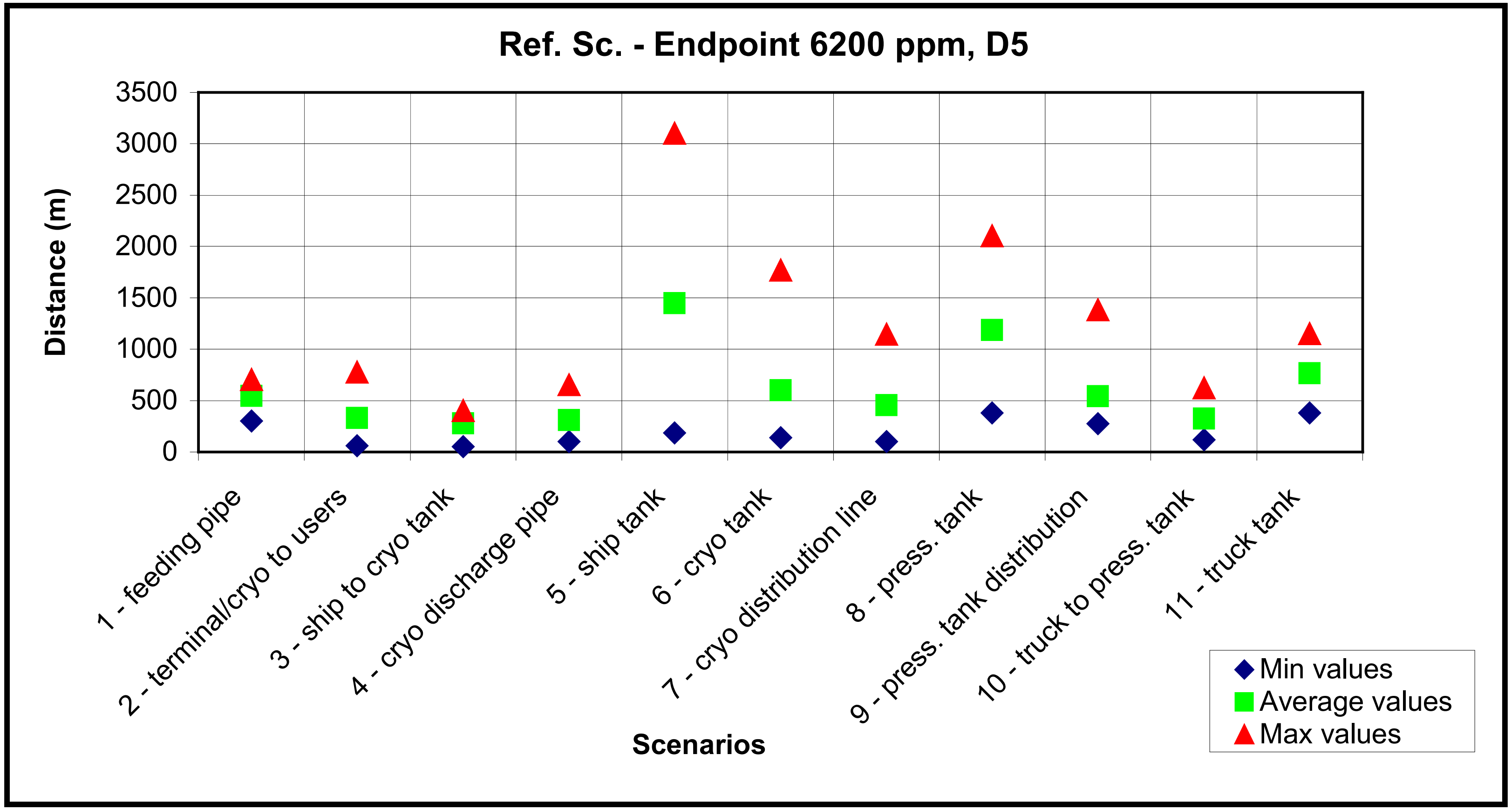
- Epistemic (also called reducible uncertainty) is related to incomplete knowledge about phenomena of concern and inadequate matching of available databases to the case under assessment, etc.

UNCERTAINTY for FREQUENCIES

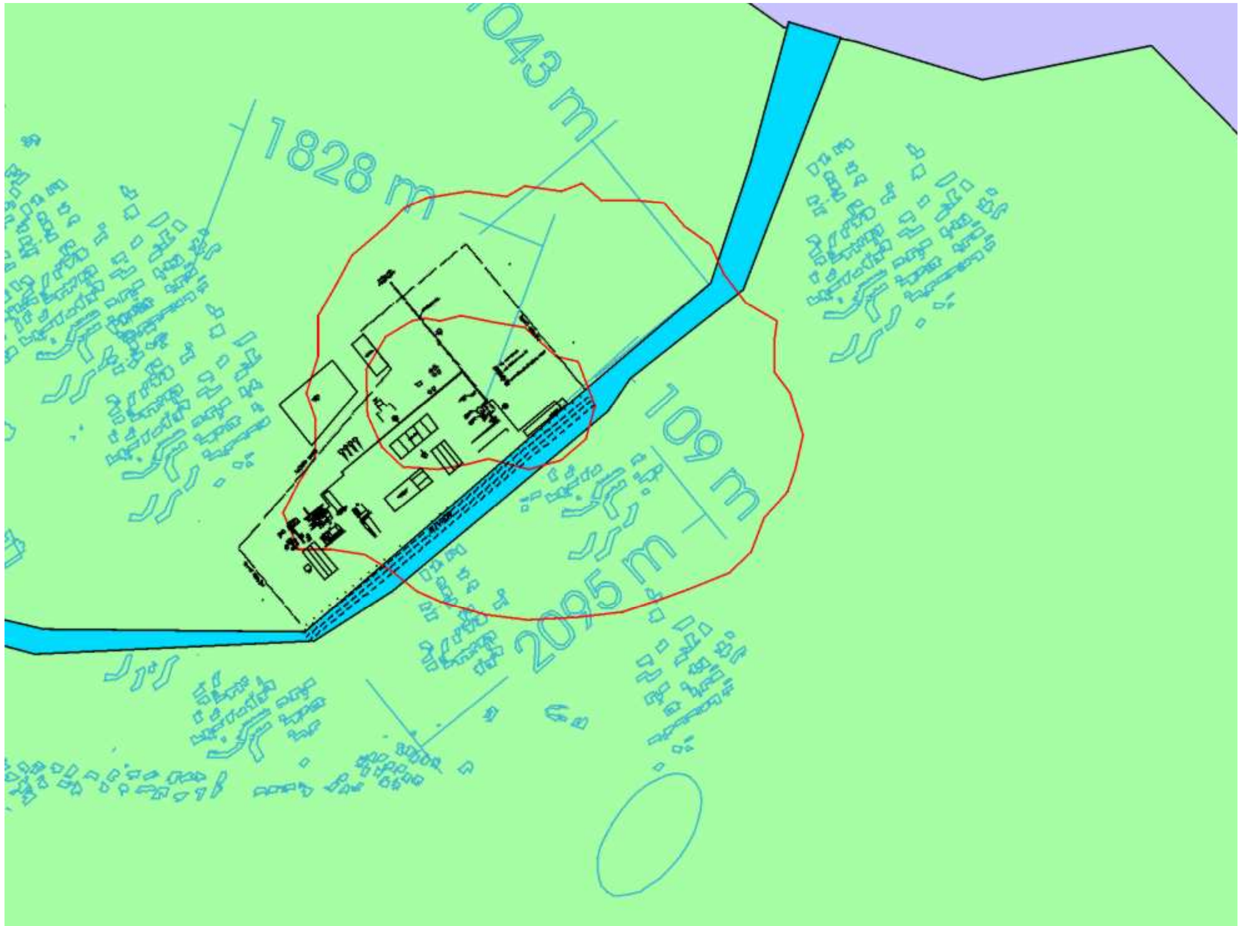
The EU ASSURANCE project - Sources and magnitudes of uncertainties in risk analysis of chemical establishments



UNCERTAINTY for CONSEQUENCES I



UNCERTAINTY for Individual risk contours



Min - max for IR = 10^{-5} per year

UNCERTAINTY IN COMMUNICATION
Ranking - Frequencies

Partner	category 1 *range (year^{-1})*	category 2 *range (year^{-1})*	category 3 *range (year^{-1})*	category 4 *range (year^{-1})*	category 5 *range (year^{-1})*
1	improbable $< 10^{-6}$	remote $< 5 \times 10^{-5}$	occasional $< 10^{-3}$	probable $< 5 \times 10^{-2}$	
2	very unlikely $< 10^{-9}$	unlikely $< 10^{-7}$	likely $< 10^{-5}$	very likely $< 10^{-3}$	
3	1 $< 10^{-2}$	2 $< 3 \times 10^{-2}$	3 $< 10^{-1}$	4 < 1	5 > 1
4	significant $> 10^{-9}$				
5	very low $< 10^{-6}$	low $< 10^{-5}$	medium $< 10^{-4}$	high $> 10^{-4}$	
7	extremely unlikely $< 10^{-5}$	very unlikely $< 10^{-4}$	unlikely $< 10^{-3}$	likely $< 10^{-2}$	probable $> 10^{-2}$

Range of ”labels” assigned to a frequency of 10^{-5} /year

UNCERTAINTY IN COMMUNICATION
Ranking - Consequences

Partner	category 1	category 2	category 3	category 4	category 5
1	marginal *transitory health problem/damage inside the plant*	dangerous *injuries/minor damage inside the plant*	critical *minor injuries outside the plant. Fatalities/major damage inside the plant*	catastrophic *injuries/ severe damage outside the plant*	
2	class 4 *no fatalities consequences < 100m*	class 3 *some fatalities cons 100 – 500 m*	class 2 minor fatalities cons. >500 – 1000 m	class 1 *many fatalities consequences> 1000 m*	
3	rate *< 3 kg/s* release *< 3 min*	*3 – 10 kg/s 3 –10 min*	*10 – 30 kg/s 10 – 30 min*	*30–100 kg/s 30–100 min*	*>100 kg/s >100 min*
4	*a large number of release categories have been defined*				
5	minor *on-site effects only*	severe *injuries offsite*	major *few fatalities offsite*	catastrophic *many fatalities offsite*	
6	*ordered after: length of reversible effect thresholds and max effect distances*				
7	negligible *<0.5t NH_3*	low *0.5 – 5 t*	medium *5 – 50 t*	high *> 50 t NH_3*	

Definitions of a catastrophic event

Sources for uncertainty

- the implicit or explicit assumptions about the "nature" of probability, and choices among databases, and within the same data base
- the choice of the modelling (e.g. by Fault tree method) for hazards identification, for structuring the quantification of the event frequencies,
- the choice and the use of the physical models (which only in part derive from epistemic uncertainty)
- the bias introduced by the context (e.g. in a regulatory environment which in some way prescribes certain parameters, models)
- the completeness of the analysis, which can derive from practical constraints but also choices in the boundaries
- the basic experience of the analysts and his operational background etc. Lack of knowledge/misunderstandings about plant lay-out and operation

THANK YOU FOR YOUR ATTENTION