ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Risk Analysis of Highly-integrated Systems

Dozent: Prof. Dr. W. Kröger, kroeger@mavt.ethz.ch

Assistenz: Konstantinos Trantopoulos, trantopoulos@mavt.ethz.ch
Patrick Probst, probst@mavt.ethz.ch

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Introduction to the topic with a specific case:

Italian Blackout, September 28, 2003

3:00 AM	Italy imports 6.9 GW, 25% of the country's total load, 300 MW more than scheduled
3:01	Trip of the 380 kV line Mettlen-Lavorgo (highly loaded) caused by tree flashover; overload of the adjacent 380 kV line Sils-Soazza
3:11	ETRANS (CH) informs GRTN (I): Request by phone to reduce the import by 300 MW (not enough)
3:21	GRTN reduces import by 300 MW
3:25	Trip of the Sils-Soazza line due to tree flashover (at 110% of its nominal capacity); the Italian grid loses its synchronism with the UCTE grid; almost simultaneous tripping of all the remaining connecting lines
3:27	Breakdown of the Italian system, which is not able to operate separately from the UCTE network (instabilities); loss of supply
9:40 PM	Restoration of the Italian system completed

Impact on Population - strong

- People affected: 56 Million
- Hundreds of people have been trapped in elevators.

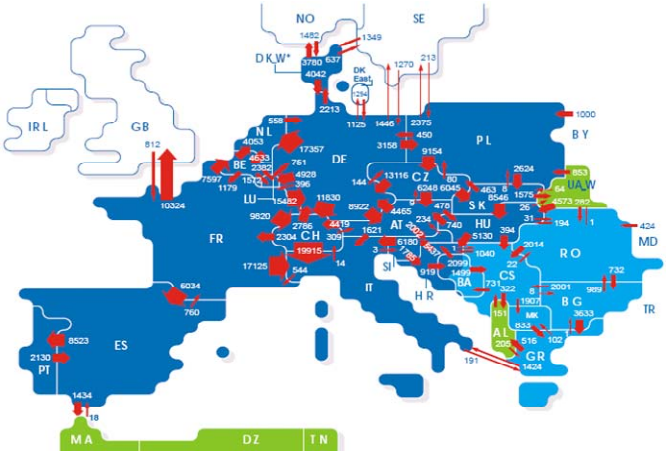
Economic Losses - moderate

- About 120 million €
- Several hundred k € due to the interruption of continuously working industries .

Impact on Dependent Critical Infrastructures - varying

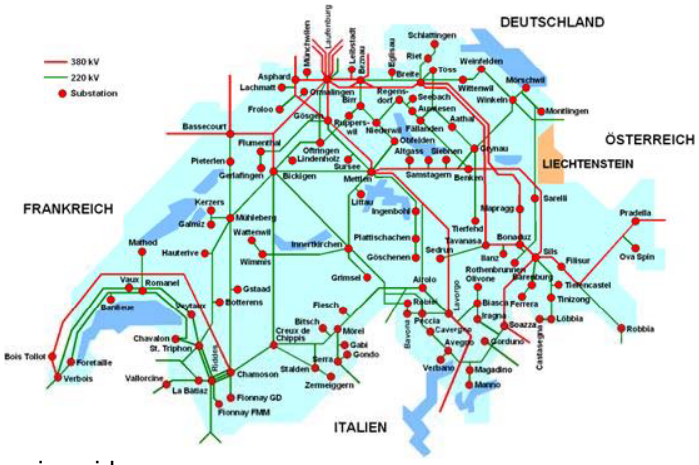
- Transportation: ~110 trains , 30'000 passengers, Subways in Rome and Milan. Flights cancelled or delayed. Outage of traffic lights partly led to chaotic situations in major cities, no severe accidents.
- Water supply: Interruptions for up to 12 hours.
- I & C: Telephone and mobile networks in a critical state. Internet providers shut down their servers (data transfer rate went down to 5% of normal).
- Hospitals: No serious problems due to the use of diesel-driven generators..

Highly integrated Systems: (1/2)



Transboundary energy flows (GWh) in 2004 [UCTE 2006]

Highly integrated Systems: (2/2)



swissgrid

Risk as a Central Term

Problems to solve:

- Identification
- Assessment
- Management

of **threats and risks** to technical installations in a context by applying methodologies of natural and engineering sciences.

Factual ("calculated") risk – as opposed to the perceived risk – calls for

- Verification
- High degree of independence from observer / analyst
- Proper application of a specific methodology
- Presentation of results with indication of uncertainties

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Definition of Factual (Mathematical) Risk

General

- Possibility that damage results from a state or process.

Risk

- Measure for hazards. It is a function of the frequency F of an undesirable event and the consequences C (ISO/IEC Guide 73, 2002: combination of the probability of an event and its consequence).

Usual calculation ("insurance formula") without aversion

- $Risk = f(F,C) = F \cdot C$ respectively $\sum_i F_i C_i$ (for more than one event)

Weighted risk

- In order to consider the so called aversion, the consequences are weighted above a certain threshold value a using a coefficient α > 1 (between 1.2 and 2)

$$Risk = \begin{cases} F \cdot C : C < c_i \\ F \cdot C^{\alpha} : C \geq c_i \end{cases}$$

- For infrastructures (in addition) also the frequency of service interruption with its resulting consequences for the people concerned.

Systematics of Factual ("calculated") Risks

Statistical risk

- Basis: available, directly usable data, e.g. [number of accidents/year];
- Experience from a large number of similar events.
- Collection of directly usable observations on system/event level.

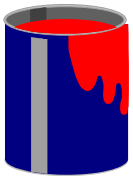
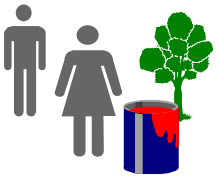
Real risk

- Basis: a complete sample of all possible information and data of an event
- After prolonged observation (infinite) a complete set of data is available, provided circumstances/conditions remain unchanged. Not determinable!

Predicted risk

- Basis: failure scenarios and models for the prediction of rare or not yet occurred events, e.g. fault tree analysis
- Events are assessable by using the probability of their occurrence
- Use of observations (statistical data) at component's level

More Precise Definition of Terms

Danger (Gefahr)	**Hazard (Gefährdung)**
A danger is a state, factor [circumstance], or action which may cause damage to persons, the environment and/or goods. **Examples**: tank filled with gasoline, a knife	A hazard is a tangible, concrete danger to persons or goods, specified in its nature, extent and course – a "specified potential".
	

Security

Control or isolation of a specified hazard (= active security) and/or the defence of a hazard (= passive security)

or

Reliability (DIN 40042, 12/90)

The ability of a system or component to perform its required functions under stated conditions for a specified period of time [IEEE 90] (mission without maintenance). Reliability is expressed as probability.

Availability (DIN 40042, 12/90)

The probability of a unit to be in working order at the time t (including maintenance work).

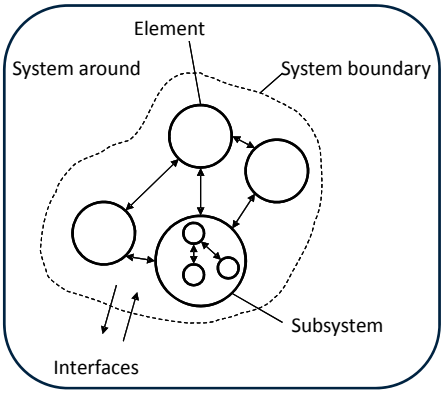
Definition of a System

Definition: „A system is a deterministic entity comprising an interacting collection of discrete elements“ [1].

<u>A System consists of:</u>

- Boundaries.
- Elements: notional or real units which can be a system themselves.
- Interactions: establish a structure between the elements.

One can distinguish between open and closed systems.



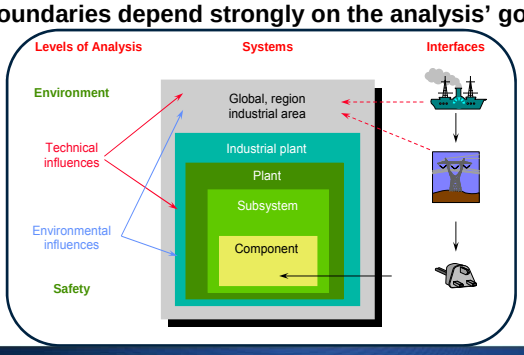
[1] Roberts, N.H., et al., *Fault Tree Handbook (NUREG-0492)*. 1981, Washington, D.C.: U.S. Nuclear Regulatory Commission. 1-209.

System Boundaries

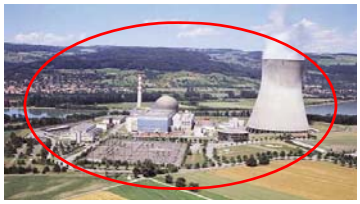
The boundaries of a system are not always obvious and per se given.

Example: In a technical system like an industrial plant the boundaries are not clearly definable. Moreover they are interconnected with other systems like transport infrastructure and the environment and may differ depending on the goals of the analysis.

→ **System boundaries depend strongly on the analysis' goals.**

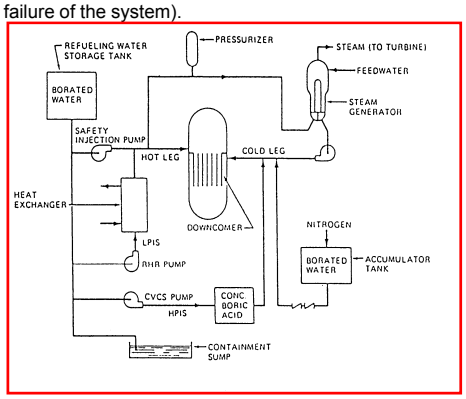


System Boundaries by Example



Risk due to operation of a nuclear power plant.

Reliability/availability of an emergency core cooling system (core damage frequency contribution due to failure of the system).



Complicated vs. Complex

Complicated Systems

- Large number of highly connected components.
- Components have well-defined roles and are governed by prescribed interactions.
- Structure remains stable over the time.
- Low dynamical behavior.
- No adaptation. One key defect may bring the system to a halt.
- Limited range of responses to changes in their environment.
- Decomposing the system and analyzing sub-parts can give us an understanding of the behavior of the whole, i.e. the whole can be reassembled from its parts.
- Problems can be solved through analytical thinking and diligence work.

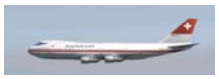
Complex Systems

- Large number of highly connected components.
- Rules of interaction between the components may change over time and may not be well understood.
- Connectivity of the components may be quite plastic and roles may be fluid. Interactions are not obvious.
- System responds to external conditions and evolves.
- Display organization without a central organizing principle (self-organization/emergence).
- Respond to and interact with their environment.
- Inadequate information about the state of the influencing variables.
- Nonlinearities.
- Tend to create surprise with their behavior.
- The overall behavior cannot be described simply in terms of their building blocks. The whole is much more than the sum of its parts.

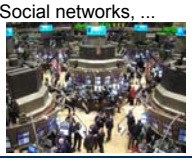
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Examples of Complicated and Complex Systems

Complicated Systems: Mechanical watches, Boeing 747, …



Complex Systems: Stock market, Power grids, Highways, World Wide Web, Natural ecosystems, Social networks, …



The nation's Power Grid is an example of a complex system that evolves continually.

It must respond to the challenges such as

- incorporating new, intermittent sources at new locations such as wind and solar,
- supporting a market in bulk electricity.
- accommodating new loads such as electric cars,
- exploiting the ongoing advances in communications, computer power, materials and devices.

Scrapping the Power Grid and redesigning it from scratch is not an option: advances must build on and coexist with components and technologies that are up to 50 years old. Any redesign or upgrade affects how the engineering system is used and this, in turn, affects the requirements. **This interaction with and adaptation to the changing environment makes the evolving system complex.**

Questions in risk analysis

- What can go wrong? (accident sequences, scenarios)
- What is the probability of these scenarios?
- What are the consequences?

Set of multiple threats disclosing vulnerabilities

- **Natural events** such as earthquakes, hurricanes, tornados, severe flooding, or other (increasing) extreme weather conditions
- **Accidents or technical factors** leading to the debilitation of plants, networks and operations
- **Human factors** such as unintended failures, physical or cyber-attacks
- **Market factors** e.g. economic pressure trading-off security factors
- **Policy factors** such as misusing "energy" for political purposes

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Analysis Preparation

Determination of the method, approach, available resources

- Framing of the problem
- Building the analysis team, responsibilities, method of operation, etc.

Definition of the protection goals

- Protection of persons, environment, vicinity and other assets
- Limits for certain event frequencies, risk goals

Definition of the objects to be analysed

- Documentation of the objects to be analysed and the system boundaries
- Optionally: Front-end and back-end („life cycle")

Analysis Preparation (cont.)

Specification of the system states and system modes

- Normal operation, startup and shutdown procedures, faults and failures, decommissioning
- Production, transport, storage

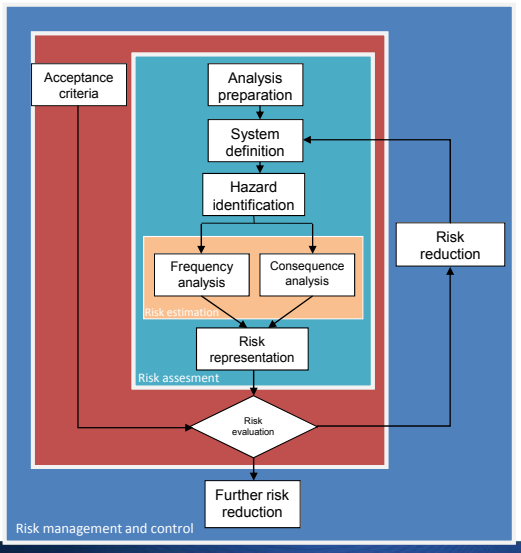
Specification of the analysis breadth and depth

- Cut-off criterion: Definition of a threshold (frequency of occurrence) limiting event chains

Specification of effects

- System inherent/internal:
  technical failure/breakdown and/or human factors
- External factors:
  natural (e.g. earthquake) and civilization causes (e.g. airplane crash)

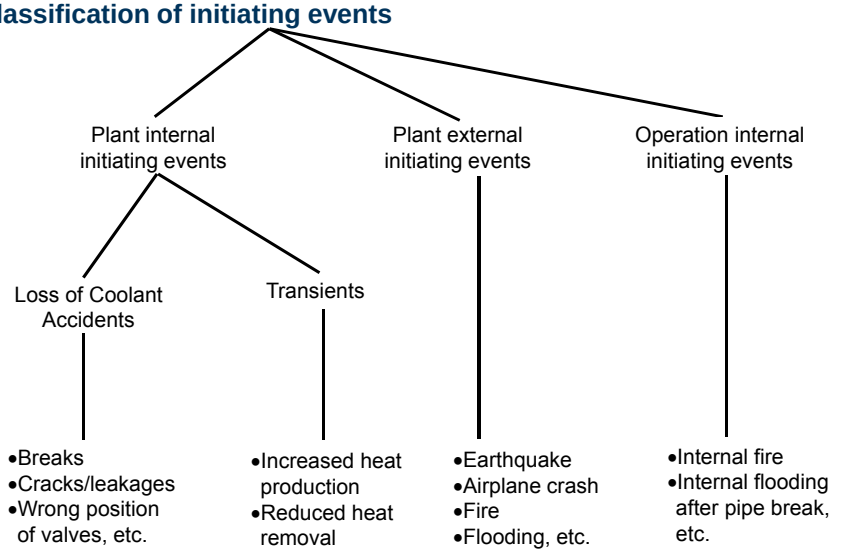
Risk analysis procedure



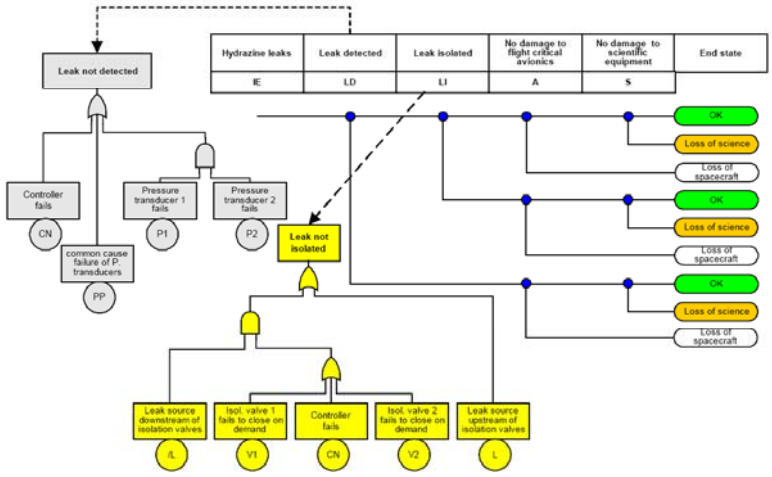
Structure and "Levels" of a PRA for Nuclear Power Plants

Plant response to initiating events	→ **Level 1**	Frequency of core damage (CDF)
Physical effects, containment response	→ **Level 2**	Frequency and amount of radionuclides released (source term, PDF)
Athmospheric dispersion, potential and expected doses, dose-effect/risk relation	→ **Level 3**	Frequency and quantities of environmental and health effects

Classification of initiating events



Combination of Fault Trees and Event Trees



Source: Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. 2002

Information requirement

Frequency of triggering Events

- Generic data (Publications)
- Plant specific knowledge

System response / System reliability

- Reliability data of single components
- Human factors (reliability of Operator)
- Common cause mechanisms

Renewal processes / Maintenance

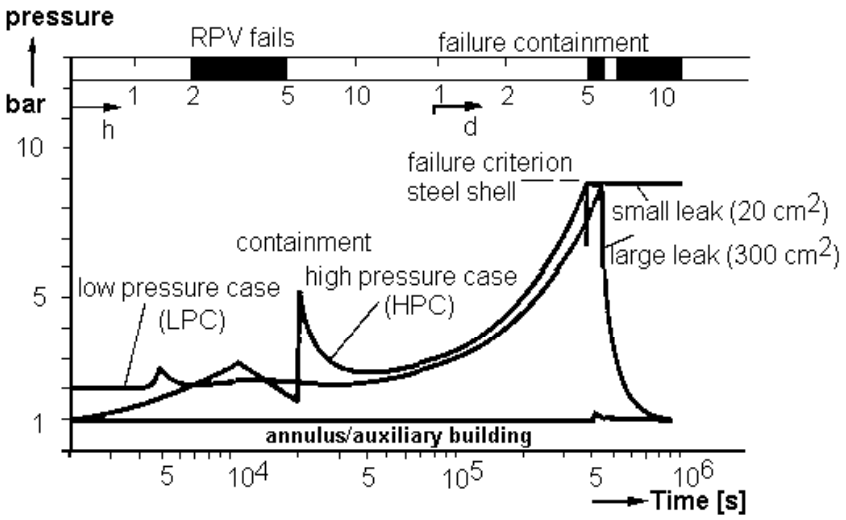
⇒ Actual plant / system description, operating handbooks

GRS-Results Level 1 PRA, German NPP GKN-II, Full Power

Initiating Events	System damage state	Core damage state
Loss of main feed water	26%	<5%
Loss of main heat sink	20%	<5%
Loss of preferred power	17%	10%
Very small primary leaks	16%	53%
SBLOCA via stuck-open SRV	5%	15%
Steam generator tube rupture	4%	7%
Total expected frequency of system damage state without AM: 8.5×10^{-6}/year Total expected frequency of core damage state with AM: 2.5×10^{-6}/year		

--	Expected frequency of system damage state / year	Expected frequency of core damage state / year
Mean	8.5×10^{-6}	2.5×10^{-6}
5% Fractile	1.6×10^{-6}	4.4×10^{-7}
50% Fractile (median)	4.6×10^{-6}	1.5×10^{-6}
95% Fractile	2.1×10^{-5}	7.3×10^{-6}
„Point Value“*	5.0×10^{-6}	1.7×10^{-6}

Pressure Curve in the Containment after a Core Melt Accident



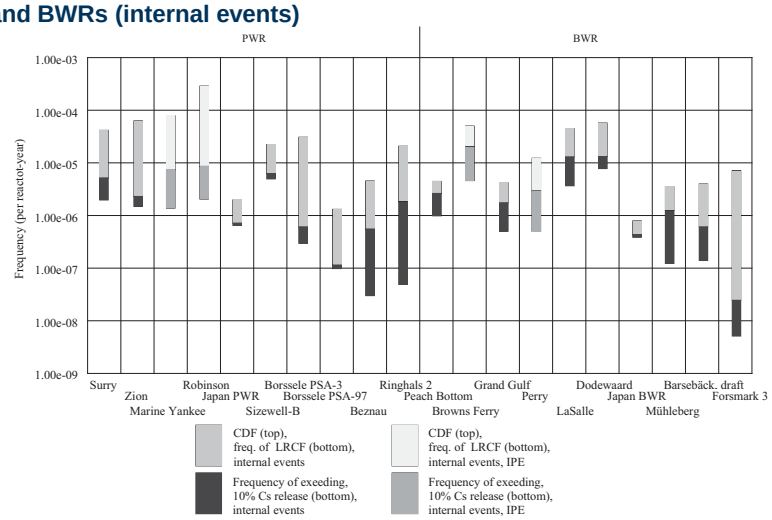
Sources

- The source term is defined by the amount, the physical and the chemical properties of each isotope released, thermal energy in the release plume/cloud, release rate over time and release height.
- The source term depends on the accident sequence.

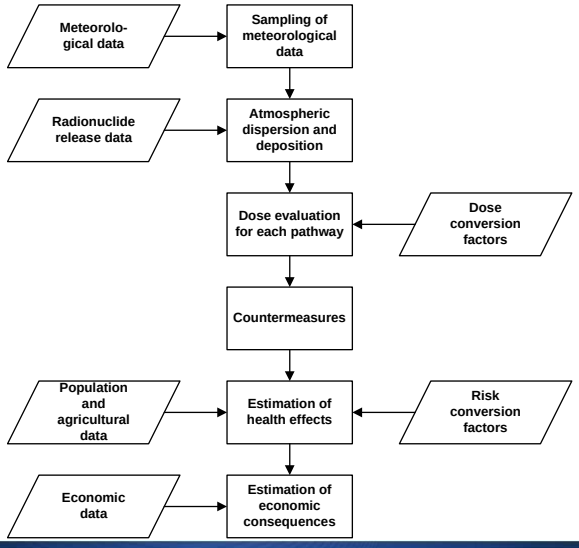
Examples of various source terms

Source term	Time before release [h]	Duration of release [h]	Release rate [MW]	Release height [m]	Time of alarm [h]	Released quantity						
						Xe-Kr	Org-I	I	Cs-Rb	Te-Sb	Ba-Sr, Ru	La
QT1	2.0 3.0	1.0 5.0	2.0 0.2	10 10	1.0 -	1.0 -	0.001 -	0.1 -	0.1 -	0.05 0.05	0 0.01	0 0.001
QT2	2.0	1.0	0	10	1.0	1.0	0.001	0.1	0.1	0.1	0.01	0.001
QT3	2.0	1.0	0	10	1.0	0.1	0.00001	0.001	0.001	0.001	0.0001	0.00001
QT4	2.0 3.0 5.0	1.0 1.0 1.0	0 0 0	10 10 10	1.0 - -	1.0 - -	0.00033 0.00033 0.00033	0.033 0.033 0.033	0.033 0.033 0.033	0.033 0.033 0.033	0.0033 0.0033 0.0033	0.00033 0.00033 0.00033
QT5	2.0	24.0	0	10	1.0	1.0	0.001	0.1	0.1	0.1	0.01	0.001

Frequencies of Core Damage of Large Release Containment Failure and of exceedance of 10% Cs release, Western PWRs and BWRs (internal events)



Basic Elements of Probabilistic Consequence Assessment



Result Representation