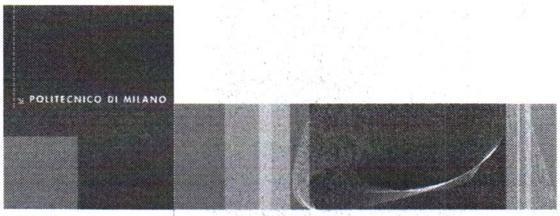
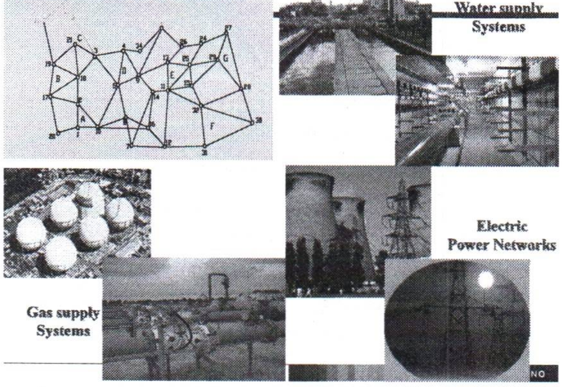


Reliability, Safety and Risk

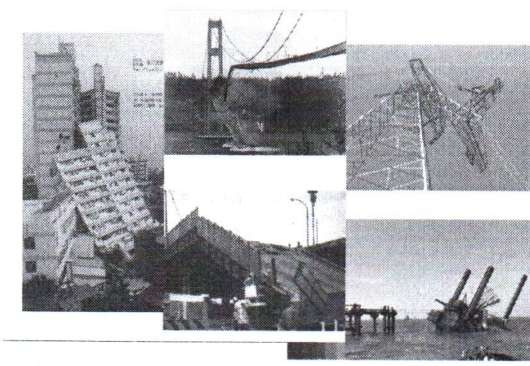
Enrico Zio

Technological systems

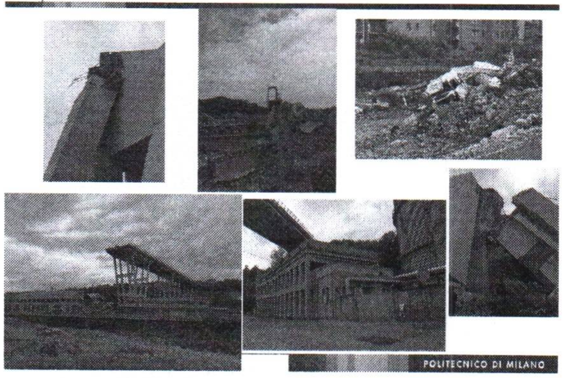
Critical infrastructures



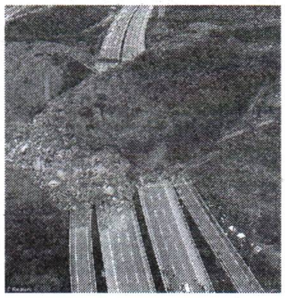
Failures



Failures



Failures (external events)

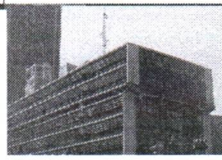


Taiwan News

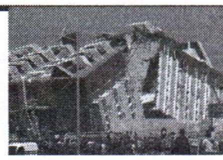
LANDSLIDE CUTS OFF TAIWAN FREEWAY, 2 TO 4 CARS FEARED BURIED.
25 APRIL 2010.

... LANDSLIDE BURIED A 300-M STRETCH OF NO. 3 FREEWAY BETWEEN TAIPEI AND KEELUNG

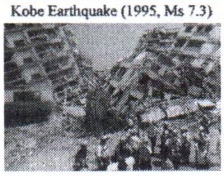
Failures (external events)



Kobe Earthquake (1995, Ms 7.3)



Chile Earthquake (2010, Ms 8.8)



Chi-Chi Earthquake (1999, Ms 7.6)

Gaoxiong Earthquake (2016, Ms 6.7)

Failures (external events)

Lifeline failures in Wenchuan Earthquake

In Dujiangyan City, the damaged pipelines length was 300km (more than 90%)

Failures (external events)

Extreme weather in January 2018

Failures and consequences

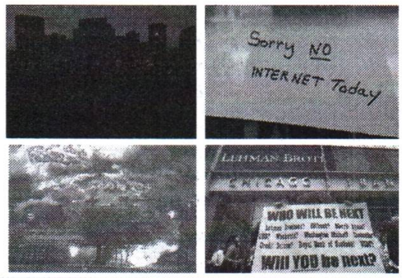
Loss of revenues

Unplanned shut-down, D.C. Cook NPP

Fatalities and contaminations

Oil rig explosion in 2010, Gulf of Mexico

Failures and consequences

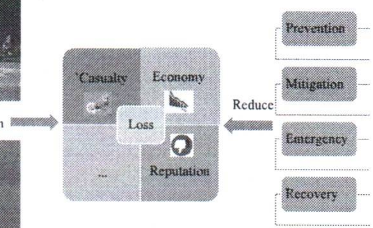


Crisis, service/business interruption, asset loss...

Failures and consequences: the problem

2018, Oklahoma Rig Explosion

2019, Nyonoksa radiation accident



Reliability

RELIABILITY: WHAT?

<u>Reliability</u>: an appreciable attribute of a person or artifact

Samuel T. Coleridge

"He inflicts none of those small pains and discomforts which irregular men scatter about them and which in the aggregate so often become formidable obstacles both to happiness and utility; while on the contrary he bestows all the pleasures, and inspires all that ease of mind on those around him or connected with him, with perfect consistency, and (<u>if such a word might be framed</u>) absolute reliability

<u>Reliability</u>: a pervasive concept...

Web of science (science citation) 9512

Library of congress 3253

Google 12,500,000

RELIABILITY: WHAT?

<u>Reliability</u>: ability to perform an assigned task for a given time

- Always present in human activities
- Increased importance with industrial revolution

⬇

From reasonable to rational solutions

⬇

Reliability Engineering

(Reliability engineering:)
It's a matter of what can happen, being able to measure it, being able to design against what can happen and being able to maintain

RELIABILITY ENGINEERING

An ensemble of formal methods to investigate the (uncertain) limits of systems

- *Why systems fail (**reliability physics to discover causes and mechanisms of failure and to identify consequences)***
- *How to develop reliable systems*
- *How to measure/test* **reliability** ***(in design, operation and management)***
- *How to maintain systems reliable* ***(fault diagnosis and prognosis, maintainability)***

RELIABILITY ENGINEERING

- System representation and modeling
- System model quantification
- Uncertainty modeling & quantification

RELIABILITY: Uncertain limits

- ***Uncertainty in system representation and modeling***
- ***Uncertainty in components behavior and relationships***
- ***Uncertainty on values of components parameters in time***

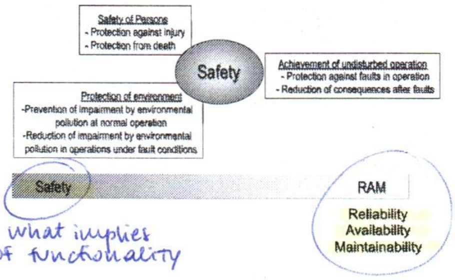
Safety

Safety

PROTECT LIVES & PROPERTY

PROTECT NATURE

Safety



looks at what implies the loss of functionality

looks at the systems' functionality

Safety and accident analysis

SAFETY ≡ freedom from unaffordable harm

• **Explanatory** (a posteriori, reactive)

Accident analysis

⇩

Difficulty/challenges:

– When something has happened, we try to find the cause.

⇩

When the cause has been found, we try to eliminate it or reduce it.

How can we find out what went wrong in complex socio-technical systems living in an uncertain environment

We live in an uncertain world → **Coping with uncertainties**

Subject (decision maker) → lack of complete knowledge (epistemic)

Object (aleatory) → Bernoulli

Safety and risk assessment

SAFETY ≡ freedom from unaffordable harm

• **Anticipative** (a priori, pro-active)

Accident analysis

⇩

Difficulty/challenges:

– Risk assessment: predicting what can happen

⇩

Elimination or prevention of potential risks

How can we predict what may go wrong?

"Freedom from unaffordable harm"

⇩

Models, methods, concepts must be compatible and able to describe "reality" in an adequate fashion

RISK=(A,C,L(U)) **True Risk**

Risk=(a,c,l(u),k) **Modeled Risk**

Epistemic → Model of l(u) → PRA + epistemic model

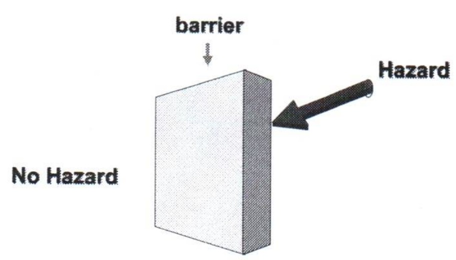
Aleatory

Uncertainty

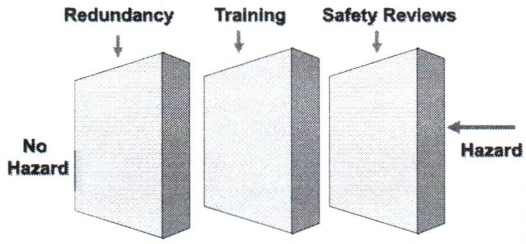
Aleatory Uncertainty
- irreducible uncertainty
- property of the system
- random fluctuations / variability / stochasticity

Epistemic Uncertainty
- reducible uncertainty
- property of the analyst
- lack of knowledge or perception

The 'parmesan cheese' model



Multiple Barriers

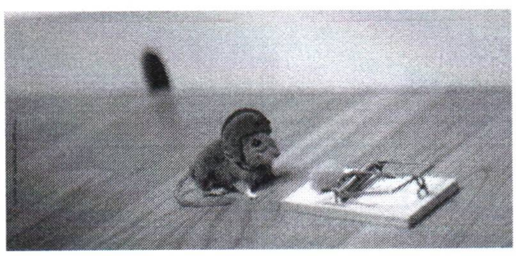


Redundancy: Example

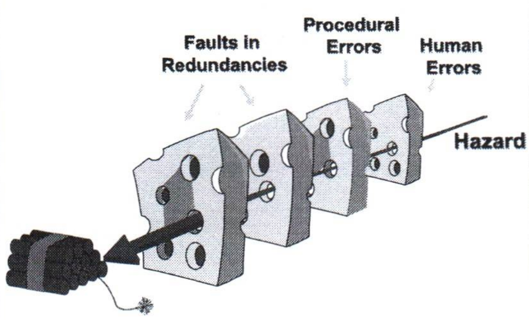
Risk

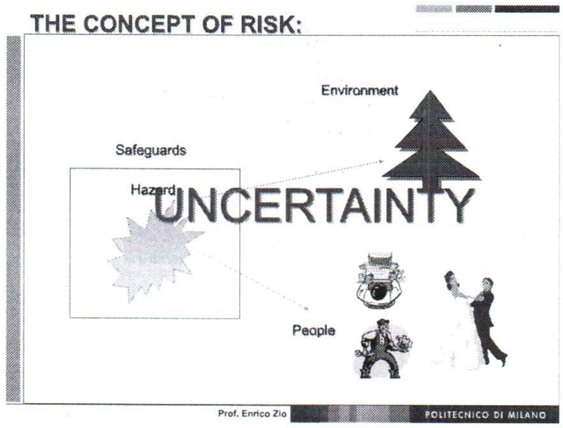
Reality: An example of a protection barrier

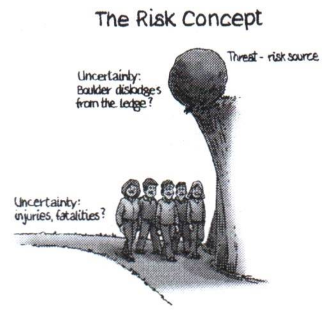
Not all risk mitigation strategies work...

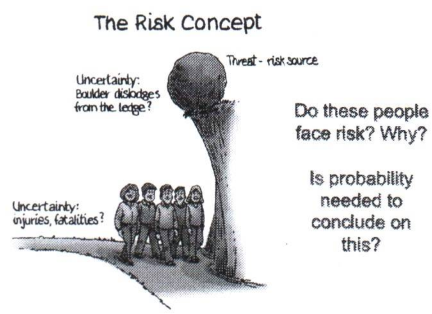


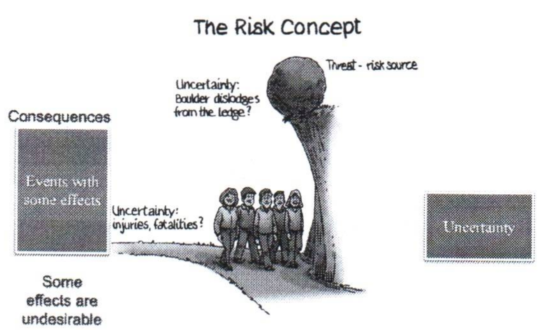
The 'swiss cheese' model

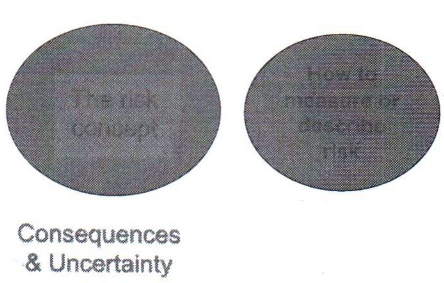



THE CONCEPT OF RISK:
Environment
Safeguards
Hazard
UNCERTAINTY
People
Prof. Enrico Zio
POLITECNICO DI MILANO


The Risk Concept
Threat - risk source
Uncertainty: Boulder dislodges from the ledge?
Uncertainty: injuries, fatalities?


The Risk Concept
Threat - risk source
Uncertainty: Boulder dislodges from the ledge?
Uncertainty: injuries, fatalities?
Do these people face risk? Why?
Is probability needed to conclude on this?


The Risk Concept
Threat - risk source
Uncertainty: Boulder dislodges from the ledge?
Consequences
Events with some effects
Uncertainty: injuries, fatalities?
Uncertainty
Some effects are undesirable


The risk concept
How to measure or describe risk
Consequences & Uncertainty

RISK = POTENTIAL DAMAGE + UNCERTAINTY

Dictionary: RISK = possibility of damage or injury
to people or things

1) What undesired conditions may occur? ➡ Accident Scenario, S
2) With what probability do they occur? ➡ Probability, p
3) What damage do they cause? ➡ Consequence, x

$$\text{RISK} = \{S_i, p_i, x_i\}$$

S. Kaplan, B.J. Garrick, On the quantitative definition of risk, Risk Analysis, 1981

RISK ASSESSMENT

1) What undesired conditions may occur? ➡ Accident Scenario, S
2) With what probability do they occur? ➡ Probability, p
3) What damage do they cause? ➡ Consequence, x

$$\text{RISK} = \{S_i, p_i, x_i\}$$

RISK ASSESSMENT:

Systemic Analysis of system performance under undesired conditions (uncertain space)

⬇

System/Man/Environment interactions under uncertainty

⬇

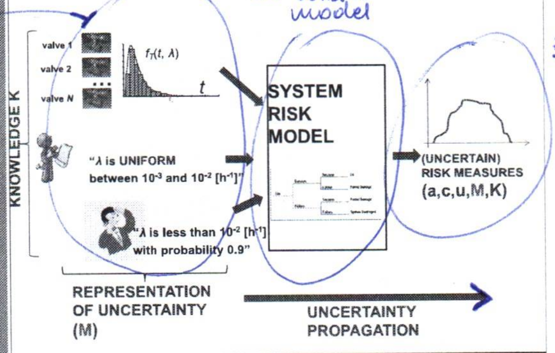
PROBABILISTIC RISK ASSESSMENT *

(QUANTITATIVE RISK ASSESSMENT)

Risk Assessment

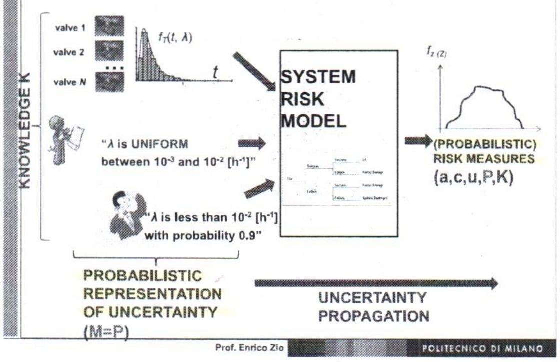
1. build a model

2. feed the model with what we know (with uncertainties)

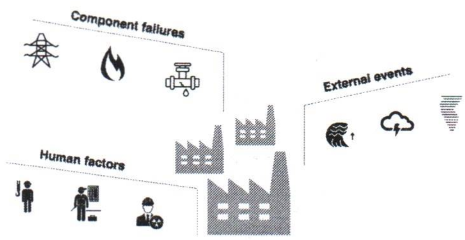


3. output: risk evaluation (if the representation of the uncertainty is probabilistic then we get probabilistic risk assessment *)

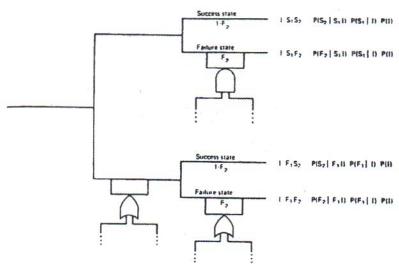
Probabilistic Risk Assessment



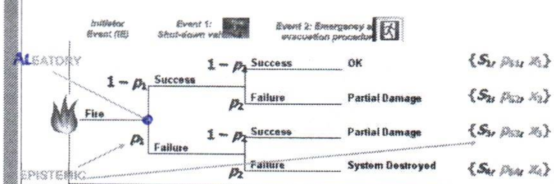
HAZARDS



Event Trees/Fault Trees



(aleatory and epistemic) Uncertainty



Aleatory: variability, randomness (in occurrence of the events in the scenarios)
Epistemic: lack of knowledge/information (probability and consequence models)

PROBABILISTIC RISK ASSESSMENT

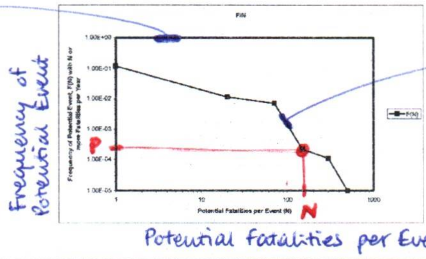
PRA results:

$$\{S_i, p_i, x_i\}$$

S SCENARIO	p PROBABILITY	x CONSEQUENCE
S_1	p_1	x_1
…	…	…
S_N	p_N	x_N

Example of F/N graph

Scenario	Number (N) of Potential Fatalities	Frequency of Scenario per Year	Frequency of Incidents with Potential (N) or more Fatalities per Year
1	1	0.1	0.12021
2	20	0.014	0.01141
3	70	0.0075	0.00713
4	150	0.00023	0.00032
5	300	0.00009	0.00011
6	500	0.00001	0.00001



There is a line somewhere representing the acceptable risk: if we're below the line we're good
(PROBABILISTIC FRAMEWORK OF RISK GOVERNANCE: we set a probabilistic limit curve and we compare where we stand)

Note: if we're close to the limit it's still not good: we want a probabilistic safety margin (let's be far from the curve)

:= COMPLEMENTARY CUMULATIVE DISTRIBUTION FUNCTION

Due to the accident we have probability P of having N deaths (N or more)

RISK ASSESSMENT

Risk Assessment is conditioned on the Knowledge

Possible Accident Scenarios

Knowledge Available

$$Risk = (\mathcal{A}, \mathcal{C}, \mathcal{Q}; \mathcal{K})$$

Consequences

Uncertainty

Risk-Informed Decision Making (1)

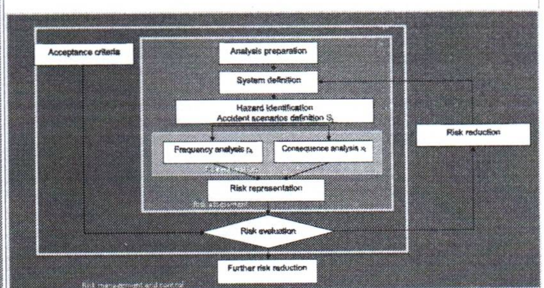
- **Decision making must be based on the current state of knowledge of the decision maker (DM)**
  - **The current state of knowledge regarding design, operation, and regulation is key.**
  - **The current state of knowledge is informed by science, engineering and operating experience, including past incidents.**
- **What we know about plant behavior is not easily available to the DM**
  - **Accident sequences, human performance, risk significance of systems, structures, and components, etc**

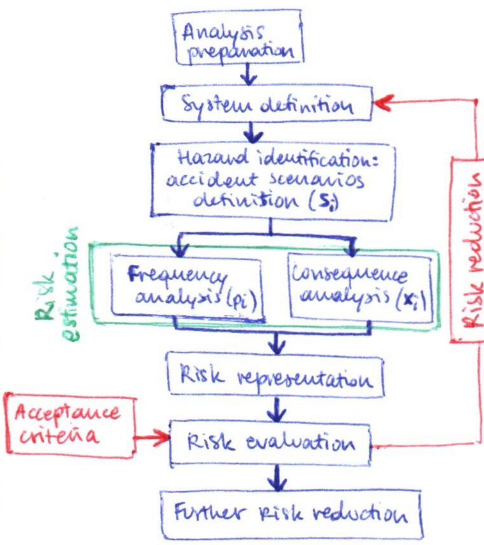
Risk-Informed Decision Making (2)

- **PRAs provide this information to the DM**
  - **PRAs do not predict the future** : it just analyzes what could possibly happen
  - **PRAs evaluate and assess potential accident scenarios to inform the decision makers' current state of knowledge.**

PRA = Probabilistic Risk Assessment

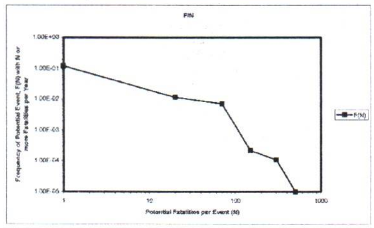
Risk Assessment and Management





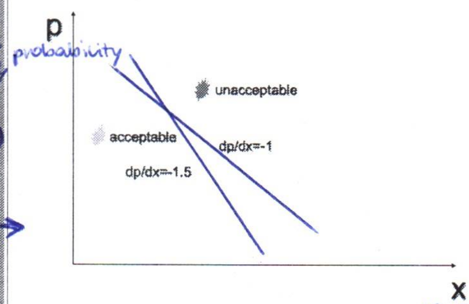
Example of F/N graph

Scenario	Number (N) of Potential Fatalities	Frequency of Scenario per Year	Frequency of Incidents with Potential (N) or more Fatalities per Year
1	1	0.1	0.12021
2	20	0.014	0.01141
3	70	0.0075	0.00713
4	150	0.00023	0.00032
5	300	0.00009	0.00011
6	500	0.00001	0.00001



The level of acceptance is defined by:
the idea is to look not only at the consequences but also at their probabilities. Then regulate the acceptability by looking at the whole picture (scenarios, consequences & probabilities)

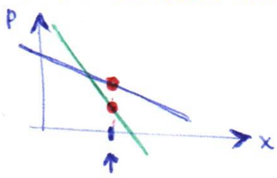
FARMER'S CURVE:



We need to put somewhere a line for which if we're sufficiently below the line with our risk assesment then we can accept the operation of the plant. We have to be able to manage the consequences "and the probabilities"

It's a responsability of the industries/society to decide the slope and intercept.

If it gives frequently accidents the accidents must give small consequences. If it can give large consequences then the probability must be low. We can inject more worries on consequences varying the slope (increasing). More worried about consequences:

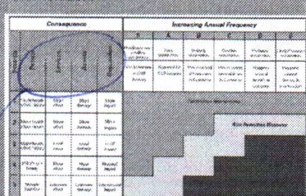


Large consequence: with the green line it has lower probability (consequences-driven → green)

RISK MATRIX: Discrete formulation of Farmer's curve

: basically the same concept but we're not looking at continuous values of consequences and probabilities, but discrete (and so we have categories).

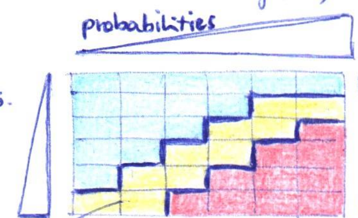
The level of risk is broadly acceptable and generic control measures are required aimed at avoiding deterioration.



The level of risk can be tolerable only once a structured review of risk-reduction measures has been carried out

The level of risk is not acceptable and risk control measures are required to move the risk figure to the previous regions.

consequences are viewed by different point of views



events that never happened
frequent events

BOUNDARIES OF ▭ :
ALARP: as low as reasonably practicable
ALARA: as low as reasonably achievable
We would like to be always blue.

Main strategies for handling risk

CODES AND STANDARDS – simple problems

RISK ASSESMENT INFORMED

ROBUSTNESS – RESILIENCE BASED STRATEGIES

DIALOGUE

cautionary/precautionary principles

BALANCING OTHER CONSTRAINTS

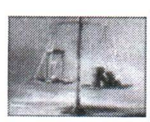
Balance

Development and protection

"DEVELOP, CREATING VALUES. TAKE RISK"

Develop, creating values

Take risk



Reduce the risks and uncertainties

"REDUCE THE RISKS AND UNCERTAINTIES"

Cost-benefit analyses

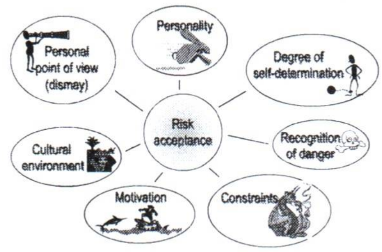
ALARP

cautionary-precautionary

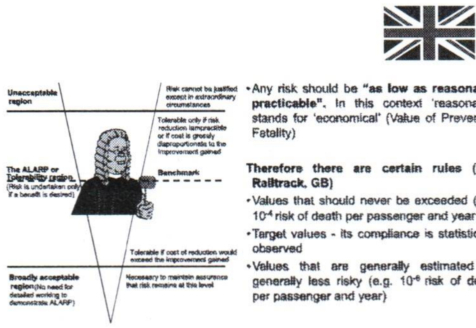
Risk acceptance criteria

There are different aspects that are considered in risk government:

Risk Acceptance



Risk Acceptance: ALARP



- Any risk should be **"as low as reasonably practicable"**. In this context 'reasonable' stands for 'economical' (Value of Prevented Fatality)

Therefore there are certain rules (e.g. Railtrack, GB)

- Values that should never be exceeded (e.g. 10^{-4} risk of death per passenger and year)
- Target values - its compliance is statistically observed
- Values that are generally estimated as generally less risky (e.g. 10^{-6} risk of death per passenger and year)

CLASSICAL TECHNIQUES OF RISK ASSESSMENT

!

Risk Assessment: main steps

1. System description and modeling
2. Historical analysis of past accidents
3. Hazard identification
4. Selection of most critical hazards and identification of Initiating Events (IEs)
5. Analysis of the accident sequences deriving from the IEs
6. Evaluation of risk → decision-making process

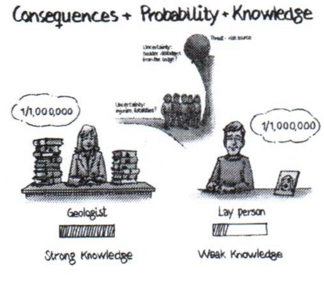
we consider all: past incidents, past risk assessments, everything, hazard, similar plants

(Qualitative analysis)
We end up with a lot of hazards, we cannot consider them all. In this step we concentrate all the most dangerous hazards. We have to see what the different hazards "cost": "this is dangerous", "this is frequent", "this is frequent and dangerous", ...

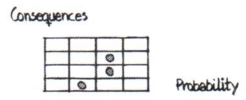
Expressing risk

Consequences + Probability + Knowledge

: when we do the risk assessment, how can we say how much is important an accident? How much do we know about it?



Consequences + Probability + Knowledge

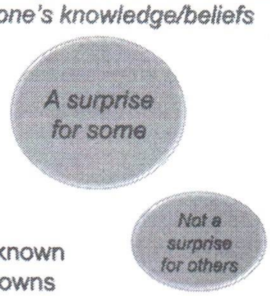


- Poor background knowledge
- Medium strong background knowledge
- Strong background knowledge

Black swans

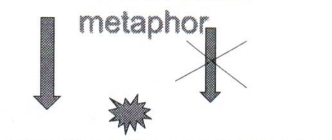
What is a black swan and how can it be taken into account in the risk assessment?

A surprising, extreme event relative to one's knowledge/beliefs



Unknown knowns

The black swan metaphor



Surprise

Focus on the knowledge
Assumptions
Signals and warnings
How can the knowledge be strengthened

Classical Techniques for Risk Assessment

- **Hazard identification:** FMEA & HAZOP
- **Accident Scenarios Identification:** ETA, FTA
- **System Failure Probabilty Assessment:** ETA, FTA

FMEA: Failure mode and effect analysis

HAZOP: Hazard and operability analysis

ETA: event trees analysis

FTA: fault trees analysis

FAILURE MODES AND EFFECTS ANALYSIS

(FMEA)

FMEA

- Qualitative
- Inductive

We look at the system, we list all the components and we analyze each component. We simulate the failure component by component and we look at the effects (what happens to a subsystem, to a system)

to understand the consequences of a failed component on a system we have to propagate the error (propagate, induct)

AIM:

Identification of those component failure modes which could fail the system (reliability) and/or become accident initiators (safety)

FMEA: Procedure steps

composed by probability and severity and detection

if we use a safety system which is not able to detect problems then we have a problem

(a same level of probability and severity but different ability of detection lead to different criticality)

component	Failure mode	Effects on other components	Effects on subsystem	Effects on plant	Probability*	Severity +	Criticality	Detection methods	Protection and mitigation
Description	Failure modes relevant for the operational mode indicated	Effects of failure mode on adjacent components and surrounding environment	Effects on the functionality of the subsystem	Effects on the functionality and availability of the entire plant	Probability of failure occurrence (sometimes qualitative)	Worst potential consequences (qualitative)	Criticality rank of the failure mode on the basis of its effects and probability (qualitative estimation of risk)	Methods of detection of the occurrence of the failure event	Protections and measures to avoid the failure occurrence

Failure mode: The manner by which a failure is observed. Generally, it describes the observable effect of the mechanism through which the failure occurs (e.g., short-circuit, open-circuit, fracture, excessive wear)

HAZARD OPERABILITY ANALYSIS

(HAZOP)

HAZOP

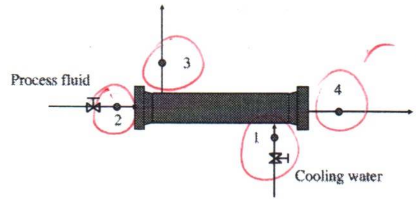
- Initially developed to analyze chemical process systems; later extended to complex operations and other types of systems (e.g., software)
- It is a qualitative, structured and systematic examination of a planned or existing process or operation in order to identify and evaluate problems that may represent risks to personnel or equipment, or prevent efficient operation
- Deductive (search for causes)
- Inductive (consequence analysis)

We start from the whole structure, we decompose in components and we look at what happens if a certain component fails. How can the process deviates? Once the possible deviation is identified (and its consequences) we can deduce the causes of the accidents.

We can go both ways: from component-failure to whole system effects and from whole system problem to component-fault.

Hazop: example

SYSTEM: shell & tube heat exchanger
Study Node: 1
Operational Mode: Nominal Conditions
Design Intent: P= 2bar, T=20°C, Flow=1l/sec



we look at some points of interest where the process can deviate (entrance/exit points)

HAZOP: Table

Study title:							Page: of		
Drawing no.:		Rev no.:					Date:		
HAZOP team:							Meeting date:		
Part considered:									
Design intent:		Material: Source:			Activity: Destination:				
No.	Guide Word	Element	Deviation	Possible Causes	Consequences	Safeguards	Comments	Actions Required	Actions Assigned to
Assign each entry a unique tracking number	Insert deviation guide word used	Describe what the guide word pertains to (material, process step, etc.)	Describe the deviation	Describe how the deviation may occur	Describe what may happen if the deviation occurs	List controls (preventive or reactive) that reduce deviation likelihood or severity	Capture key relevant rationale, assumptions, data, etc	Identify any hazard mitigation or control actions required	Record who is responsible for actions

Source: IEC 61882

FAULT TREE ANALYSIS

(FTA)

Fault Tree Analysis (FTA)

- **Systematic and quantitative**
- **Deductive**

What combination of failures of the components make the system fail? We start from defying the system fail, look at the system logic diagram and find out which are the components that, combined among each others, make the system fail. Then we see componentwise the probability of the failure of each component and we recompose to get the probability of failure of the system.

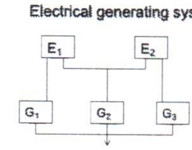
AIM:

1. **Decompose the system failure in elementary failure events of constituent components**
2. **Computation of system failure probability, from component failure probabilities**

FT construction: Procedure steps

1. Define top event (system failure)

Electrical generating system

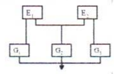


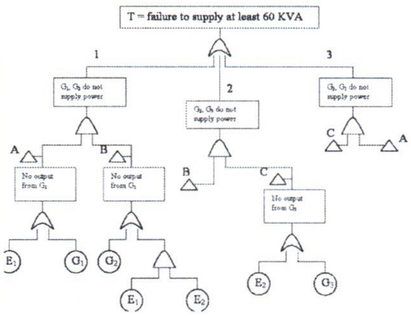
E1, E2 = engines

G1, G2, G3 = generators, each one is rated at 30 KVA

T = Failure to supply at least 60 kVA

FT Result





FT qualitative analysis

FT qualitative analysis

Introducing:

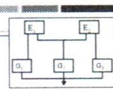
X_i : binomial indicator variable of i-th component state (basic event)

$$X_i = \begin{cases} 1 \text{ failure event } \underline{\text{true}} \\ 0 \text{ failure event } \underline{\text{false}} \end{cases}$$

- **FT = set of boolean algebraic equations (one for each gate) => structure (switching) function Φ:**

$$X_T = \Phi(X_1, X_2, \ldots, X_n)$$

FT mcs: Example



$$X_{T_1} = X_{E_1}X_{G_2} + X_{E_1}X_{E_2} + X_{G_1}X_{G_2} - X_{E_1}X_{E_2}X_{G_2} - X_{E_1}X_{G_1}X_{G_2}$$

$$= 1 - [1 - X_{E_1}X_{G_2} - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_2} + X_{E_1}X_{G_1}X_{G_2}] =$$
$$= 1 - [1 - X_{E_1}X_{G_2} - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_2} + X_{E_1}X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2} - X_{E_1}X_{E_2}X_{G_1}X_{G_2}] =$$
$$= 1 - [1 - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2} - X_{E_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_2} + X_{E_1}X_{G_1}X_{G_2} - X_{E_1}X_{E_2}X_{G_1}X_{G_2}] =$$
$$= 1 - [1 - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2} - X_{E_1}X_{G_2}(1 - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2})] =$$
$$= 1 - [(1 - X_{E_1}X_{G_2})(1 - X_{E_1}X_{E_2} - X_{G_1}X_{G_2} + X_{E_1}X_{E_2}X_{G_1}X_{G_2})] =$$
$$= 1 - [(1 - X_{E_1}X_{G_2})(1 - X_{E_1}X_{E_2})(1 - X_{G_1}X_{G_2})]$$

$$\Downarrow$$

3 minimal cut sets: $\begin{cases} M_1 = \{E_1 G_2\} \\ M_2 = \{E_1 E_2\} \\ M_3 = \{G_1 G_2\} \end{cases}$

FT quantitative Analysis

FT quantitative analysis

Compute system failure probability from primary events probabilities by:

1. using the laws of probability theory at the fault tree gate
2. using the mcs found from the qualitative analysis

$$P[\Phi(\underline{X})=1]=\sum_{j=1}^{mcs}P[M_j]-\sum_{i=1}^{mcs-1}\sum_{j=i+1}^{mcs}P[M_iM_j]+\cdots+(-1)^{mcs+1}P[\prod_{j=1}^{mcs}M_j]$$

It can be shown that:

$$\sum_{j=1}^{mcs}P[M_j]-\sum_{i=1}^{mcs-1}\sum_{j=i+1}^{mcs}P[M_iM_j]\le P[\Phi(\underline{X})=1]\le\sum_{j=1}^{mcs}P[M_j]$$

EVENT TREE ANALYSIS

(ETA)

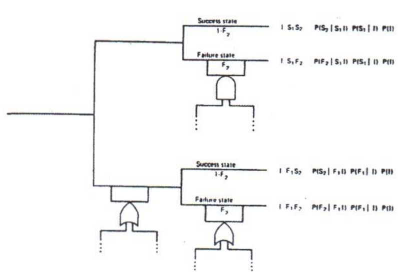
Event Tree Analysis (ETA)

- **Systematic and quantitative**
- **Inductive**

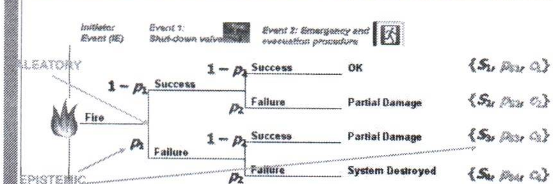
AIM:

1. **Identification of possible scenarios (accident sequences), developing from a given accident initiator**
2. **Computation of accident sequence probability**

ETA+FTA



(aleatory and epistemic) Uncertainty

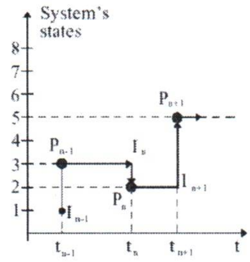


Aleatory: variability, randomness (in occurrence of the events in the scenarios)

Epistemic: lack of knowledge/information (on the values of the parameters of the probability and consequence models)

System life: random walk

Random walk = realization of the system life generated by the underlying state-transition stochastic process.

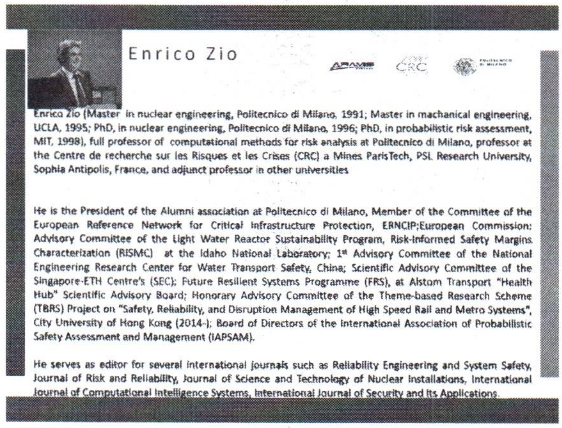


The lectures

24/02/2020 M	08:15-12:15	Introduction - Definition of Safety, Risk; Structure of Risk Analysis of Complex Engineering Systems Method of Hazard Identification
28/02/2020 F	08:15-12:15	Basics of probability theory
02/03/2020 M	08:15-12:15	Stochastic variables, Distributions, Failure time distributions, Hazard function
06/03/2020 F	08:15-12:15	Exercises - Probabilistic models
09/03/2020 M	08:15-12:15	Analytical calculations of simple system reliability
13/03/2020 F	08:15-12:15	Exercises - Probabilistic models of failure processes, Failure time distributions
16/03/2020 M	08:15-12:15	Analytical calculations of system availability
20/03/2020 F	08:15-12:15	Exercises - Analytical calculations of system reliability and availability
23/03/2020 M	08:15-12:15	Fault Tree Analysis
27/03/2020 F	08:15-12:15	Hazop and FMECA
30/03/2020 M	08:15-12:15	Fault Tree and Event Tree Analysis
03/04/2020 F	08:15-12:15	Exercises- Fault Tree and Event Tree Analysis
06/04/2020 M	08:15-12:15	Markov Chains
17/04/2020 F	08:15-12:15	Markov Chains

20/04/2020 M	08:15-12:15	Bayesian Belief Networks
24/04/2020 F	08:15-12:15	Bayesian Belief Networks
27/04/2020 M	08:15-12:15	Monte Carlo simulation
04/05/2020 M	08:15-12:15	Monte Carlo simulation
08/05/2020 F	08:15-12:15	Dependent Failures
11/05/2020 M	08:15-12:15	Exercises - Markov Chains
15/05/2020 F	08:15-12:15	Importance Measures
18/05/2020 M	08:15-12:15	Life tests and parameter estimates
22/05/2020 F	08:15-12:15	Exercises-Life tests and parameter estimates
25/05/2020 M	08:15-12:15	Exam practice
29/05/2020 F	08:15-12:15	Exam practice
05/06/2020	08:15-12:15	Exercise Monte Carlo simulation or sensitivity

The team



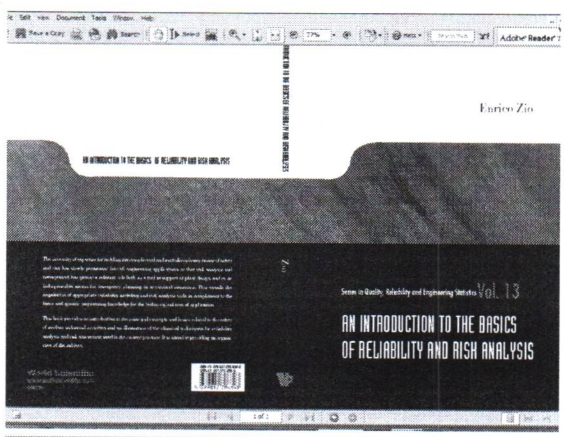
Dario VALCAMONICO
[illegible]
ITALY
MSc: Nuclear Engineering
PhD Candidate (Cycle XXXIV)
Laboratory of Signal Analysis and Risk Analysis
Department of Energy, Politecnico di Milano
Research Topic: Data Mining and Machine Learning Techniques for Fault Diagnosis and Failure Prognosis in Complex Industrial Components and Systems

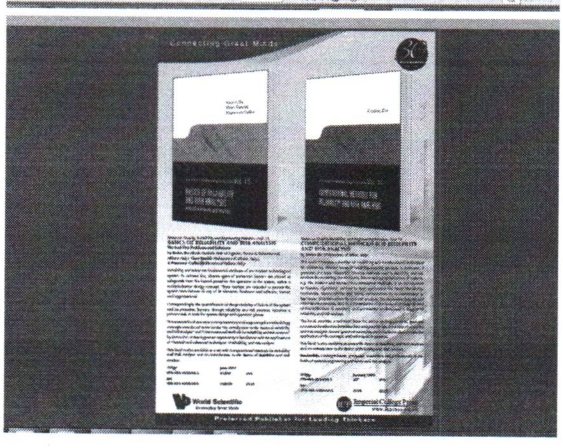
Federico ANTONELLO
[illegible]
ITALY
MSc: Nuclear Engineering
PhD Candidate (Cycle XXXIII)
Laboratory of Signal Analysis and Risk Analysis
Department of Energy, Politecnico di Milano
Research topic: Data Mining and Artificial Intelligence applications for reliability and risk analyses in complex technical infrastructures. Research collaboration with CERN (*Conseil Européen pour la Recherche Nucléaire, Geneva, Switzerland*)

[illegible]
IRAN
MSc: Earthquake Engineering
PhD Candidate (Cycle XXXII)
Laboratory of Signal Analysis and Risk Analysis
Department of Energy, Politecnico di Milano.
Research Topic: Condition-Based Probabilistic Safety Assessment (CB-PSA) for risk monitoring and life extension of aging facilities.

Bingsen WANG
bingsen.wang@polimi.it
CHINA
MSc: Engineering Mechanics
PhD Candidate (Cycle XXXIV)
Laboratory of Signal Analysis and Risk Analysis
Department of Energy, Politecnico di Milano
Research topic: Study and development of methods based on optimal transport theory and deep learning for prognostics and health management of industrial components

The books





2013, 2015, XIV, 198 p. 69 illus., 28 in color.

Printed book

Hardcover

- [illegible]
- [illegible]

eBook

For individual purchases buy at a lower price on springer.com. A free preview is available. Also available from libraries offering Springer's eBook Collection.

- springer.com/ebooks

MyCopy

Printed eBook exclusively available to patrons whose library offers Springer's eBook Collection.***

- € | $ 24.95
- springer.com/mycopy

E. Zio, Ecole Centrale Paris, Chatenay-Malabry, France

The Monte Carlo Simulation Method for System Reliability and Risk Analysis

Series: Springer Series in Reliability Engineering

- Illustrates the Monte Carlo simulation method and its application to reliability and system engineering to give the readers the sound fundamentals of Monte Carlo sampling and simulation
- Explains the merits of pursuing the application of Monte Carlo sampling and simulation methods when realistic modeling is required so that readers may exploit these in their own applications
- Includes a range of simple academic examples in support to the explanation of the theoretical foundations as well as case studies provide the practical value of the most advanced techniques so that the techniques are accessible

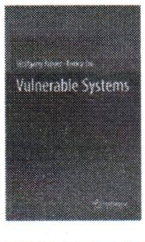
Monte Carlo simulation is one of the best tools for performing realistic analysis of complex systems as it allows most of the limiting assumptions on system behavior to be relaxed. The Monte Carlo Simulation Method for System Reliability and Risk Analysis comprehensively illustrates the Monte Carlo simulation method and its application to reliability and system engineering. Readers are given a sound understanding of the fundamentals of Monte Carlo sampling and simulation and its application for realistic system modeling.

Whilst many of the topics rely on a high-level understanding of calculus, probability and statistics, simple academic examples will be provided in support to the explanation of the theoretical foundations to facilitate comprehension of the subject matter. Case studies will be introduced to provide the practical value of the most advanced techniques.

This detailed approach makes The Monte Carlo Simulation Method for System Reliability and Risk Analysis a key reference for senior undergraduate and graduate students as well as researchers and practitioners. It provides a powerful tool for all those involved in system analysis for reliability, maintenance and risk evaluations.

Springer
the language of science

springer.com



2011, XIV, 204 p. 63 illus., 6 in color. Hardcover

- 99.95 €
- $129.00
- SFr. 143.50
- £90.00

ISBN 978-0-85729-654-2

W. Kröger, ETH Zürich, Zürich, Switzerland; E. Zio, Ecole Central Paris and Supelec, Châtenabry, France

Vulnerable Systems

The safe management of the complex distributed systems and critical infrastruct which constitute the backbone of modern industry and society entails identifyin quantifying their vulnerabilities to design adequate protection, mitigation, and e gency action against failure. In practice, there is no fail-safe solution to such pro and various frameworks are being proposed to effectively integrate different me of complex systems analysis in a problem-driven approach to their solution. Vul Systems reflects the current state of knowledge on the procedures which are bei forward for the risk and vulnerability analysis of critical infrastructures. Classic ods of reliability and risk analysis, as well as new paradigms based on network a tems theory, including simulation, are considered in a dynamic and holistic way of Vulnerable Systems will benefit from its structured presentation of the curren edge base on this subject. It will enable graduate students, researchers and safety analysts to understand the methods suitable for different phases of analysis and tify their criticalities in application. ... *more on http://springer.com/978-0-85729-*