



“RELIABILITY, SAFETY AND RISK ANALYSIS”

Lecture 1: Introduction to the Course

Piero Baraldi (piero.baraldi@polimi.it)



Introduction to the course:

- Reliability
- Safety
- Risk Analysis

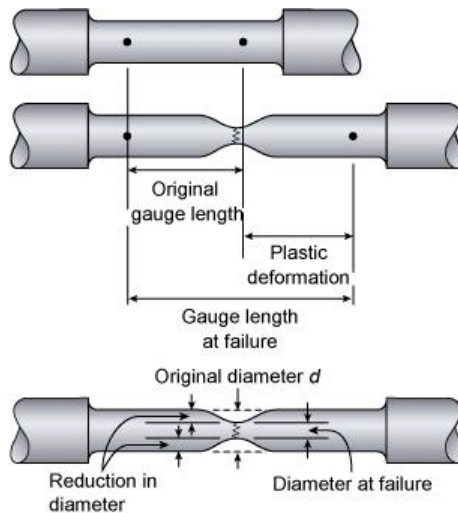
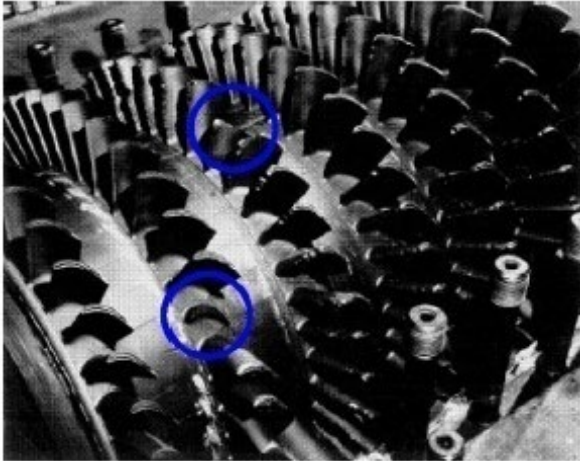


Evolution to... failure



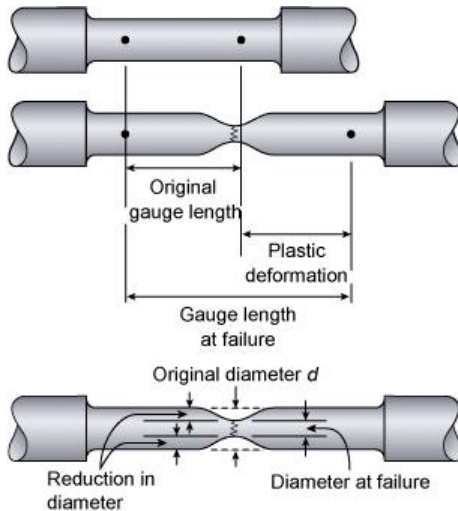
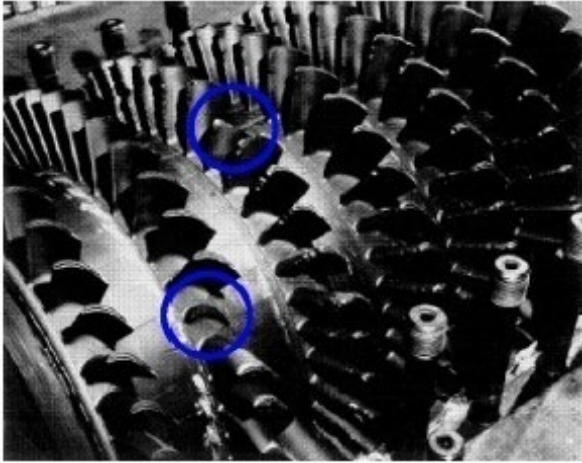
Degradation (some examples)

Creeping of turbine blades



Degradation (some examples)

Creeping of turbine blades

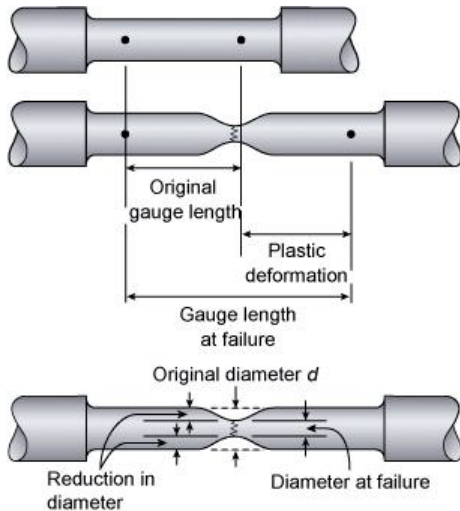
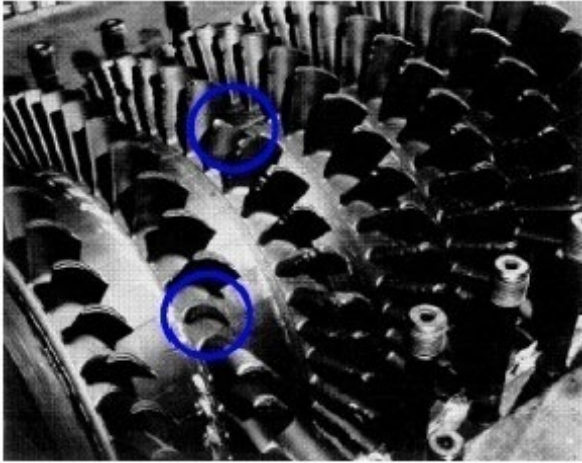


Erosion of choke valves

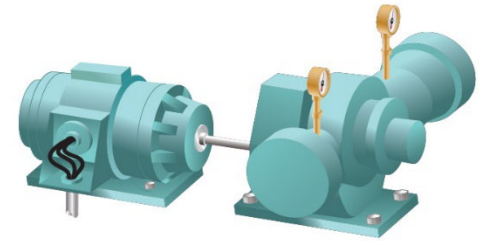


Degradation (some examples)

Creeping of turbine blades



Erosion of choke valves



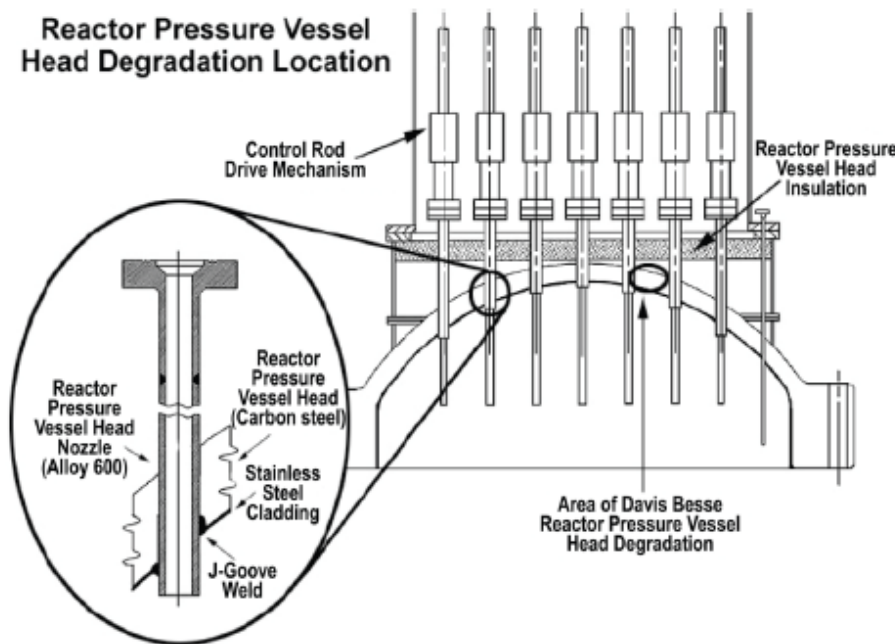
Crack propagation in bearings



FAILURES: SOME EXAMPLES



- Davis-Besse accident (February 2002):
 - Refueling outage → a cavity of the size of an American football in the reactor pressure vessel head. Only a layer of cladding of 7.6 mm thick was left by the corrosion.



Consequences

Possible consequences in case of rupture

Loss of coolant accident (LOCA)

Emergency safety procedures to protect from core damage or meltdown

The jet of reactor coolant might have damaged adjacent control rod drive mechanisms, hampering or preventing reactor shut-down.

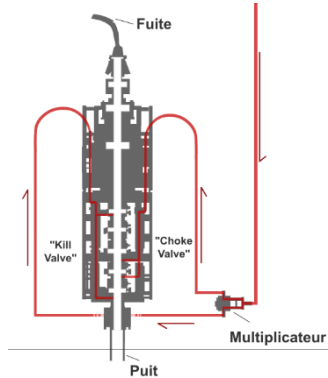
Core melt down

- Repair Action: new lid (600M \$)
- Stop operation until March 2004 (2 years)

Failure: an Example from the Oil and Gas Industry



Explosion of the platform Deepwater Horizon (Gulf of Mexico), April 2010
(source: sciencesetavenir.fr)



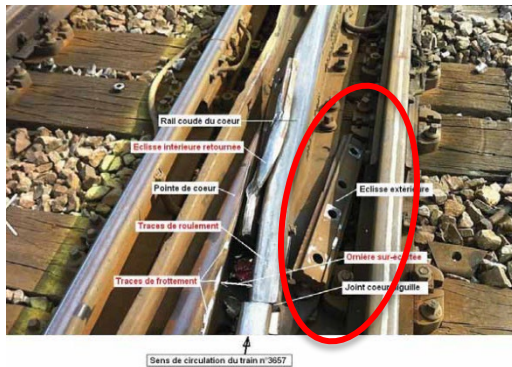
Probable cause: leakage in the oil pumping system due to a bad cement job and other factors

Consequences

- 11 fatalities
- 4.9 billion barrels of oil spilled into Gulf of Mexico
- Reputation → Reputation Repair efforts:
 - ❖ 1 billion dollars spent in Google, Adwords, and Youtube advertising
 - ❖ New CEO



Train derailment in Brétigny-sur-Orge in July 2013



Cause: failure of a fishplate (source: Bureau d'enquêtes sur les accidents de transport terrestre)

Consequences

- 7 fatalities
- 21 people were seriously injured
- 180 people were injured

Failure costs (Some Numbers)

- According to Network Rail (UK), rail infrastructure failures and defects are responsible for **14 million minutes of delay per year**



- In **automobile domain**, failures cost around **288 millions US \$ per day**





- Failure definition: *the termination/loss of ability of an item to perform its required function*
- Failure examples:
 - ❖ Total cessation of function
 - An engine stops running
 - A structure collapses
 - ❖ Deterioration/instability of function
 - a motor that is no longer capable of delivering a specified torque
 - a structure that exceeds a specified deflection





Failures

Prevented by

Design for Reliability

Maintenance

Normal



Degradation
onset



Repair



Time



Reliability (ISO8402): ability to perform an assigned task for a given time under given environmental and operational conditions



Reliability (ISO8402): ability to perform an assigned task for a given time under given environmental and operational conditions

- Always present in human activities



- From reasonable to rational solutions





II World War:

- USA

Radar



Vacuum tubes



- lot of failures
- poor system performance
- high maintenance costs



first reliability studies

- GERMAN

V1 Missile



first 10 launches were all fiascos



first reliability studies



Lusser (German Mathematician):
“the reliability of a chain of components is determined by the reliability of the weak link”



- Why do 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 and operation)?
- How to maintain systems reliable (maintenance)?



Our Big Problem...

*lamp of my wife's
bedside table*



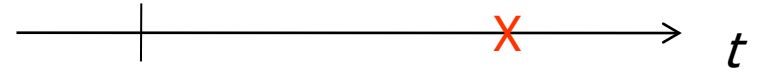
*lamp of my
bedside table*



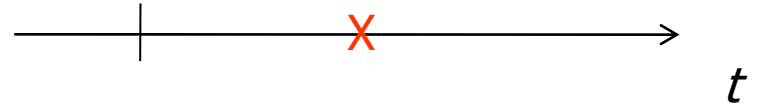


Our Big Problem...

*lamp of my wife's
bedside table*



*lamp of my
bedside table*

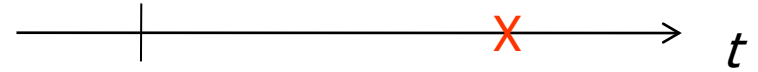


UNCERTAINTY!

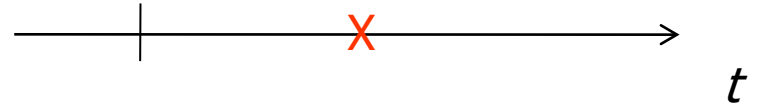


Our Big Problem...

*lamp of my wife's
bedside table*



*lamp of my
bedside table*



The failure time is a random variable!

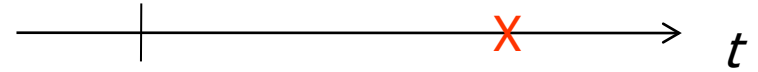


How to represent the failure time?

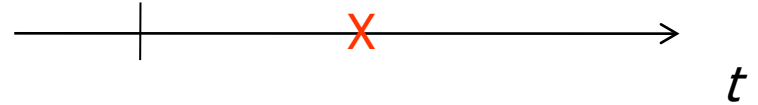


Our Big Problem...

*lamp of my wife's
bedside table*



*lamp of my
bedside table*



The failure time is a random variable!



How to represent the failure time?



Probability distribution: $f_T(t)$







Definition of reliability (ISO8402): the ability to perform an assigned task for a given time under given environmental and operational conditions



Operative definition of reliability: *Probability* that an item performs its assigned task for a given time under given environmental and operational conditions



- Objective: design and build product for **improved performance**
 - Faster aircraft
 - Thermodynamically more efficient energy conversion devices
- Increase 'load'
 - Aircraft → decrease weight
 - Energy conversion devices → work at larger temperature
- Approach the physical limit of the system
 - Aircraft → Increase stress level in its components
 - Energy conversion devices → heat-induced losses of strengths and more rapid corrosion
- Number of failures increases (**reliability decreases**)
- Countermeasures should be taken (**cost increases**)
 - Purer material
 - Tighter dimensional tolerance
 - Monitoring & improved maintenance



- Objective: design and build product for **improved performance**

- Faster aircraft
- Thermodynamically more efficient energy conversion devices



- Increase 'load'
 - Aircraft → decrease weight
 - Energy conversion devices → work at higher temperature



- Approach the physical limit of the system
 - Aircraft → Increase stress level in its components
 - Energy conversion devices → heat-induced losses of strengths and more rapid corrosion



- Number of failures increases (**reliability** decreases)



- Countermeasures should be taken (**cost** increases)
 - Purer material
 - Tighter dimensional tolerance
 - Monitoring & improved maintenance



Use new-design components, thanks to new technologies (e.g. iron instead of wood in structures)



Potentially, in the long term:

- Better performance
- Lower costs
- Larger reliability

But in the early stage of introduction of the new technology:

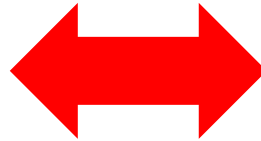
- Lower reliability

e.g. iron instead of wood in structures:

- Problem of brittle fractures



Failure



Maintenance

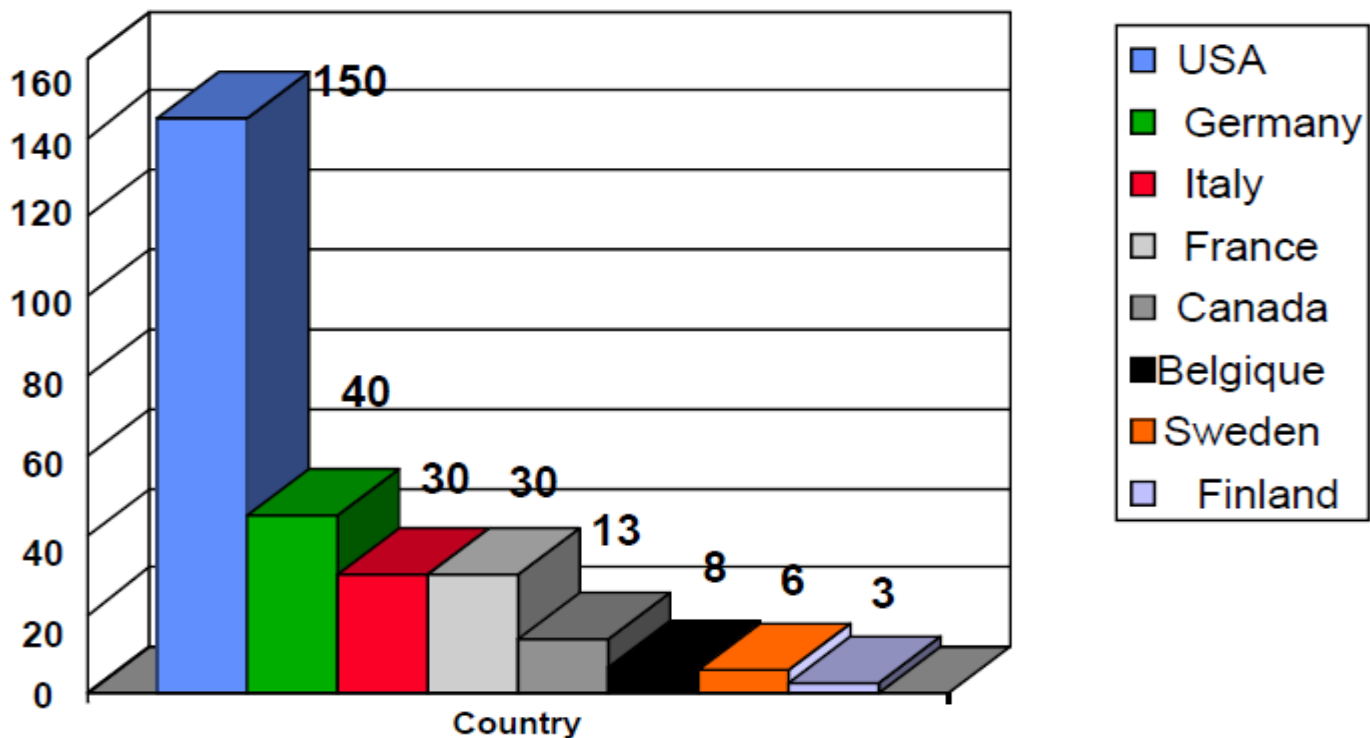
- **Maintenance (IEC60300):** set of actions that ensure the ability of an item to be retained in (preventive maintenance) or restored to (corrective maintenance) the functional state required by the purpose for which it was conceived.





Maintenance Costs

G\$/year



Derived from M. Garetti

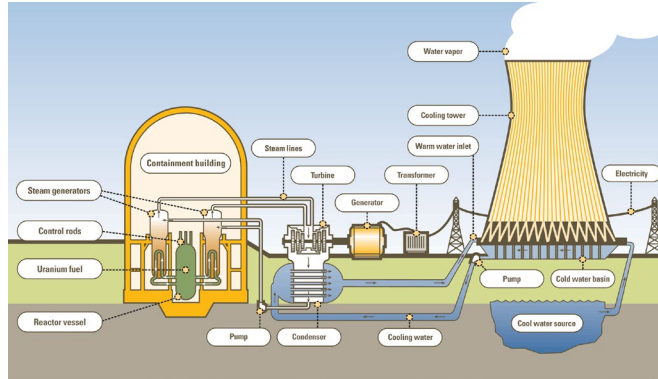


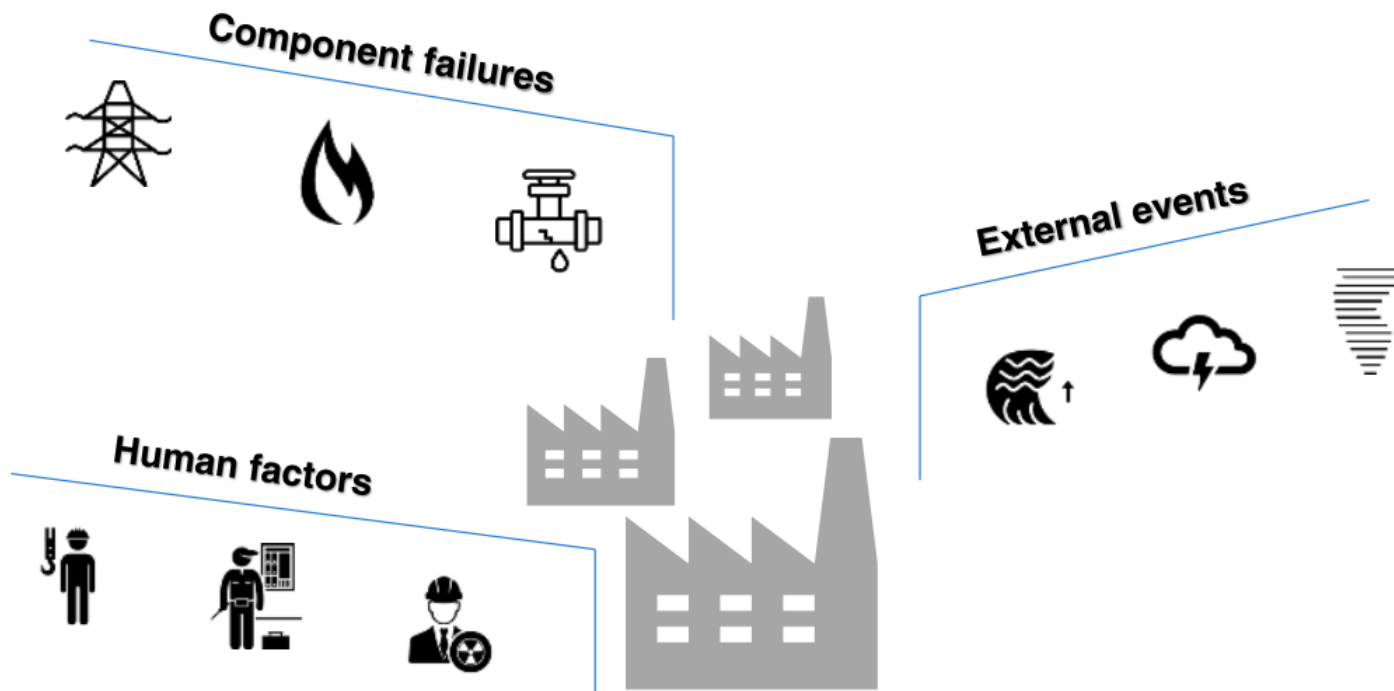
Introduction to the course:

- Reliability
- Safety
- Risk Analysis



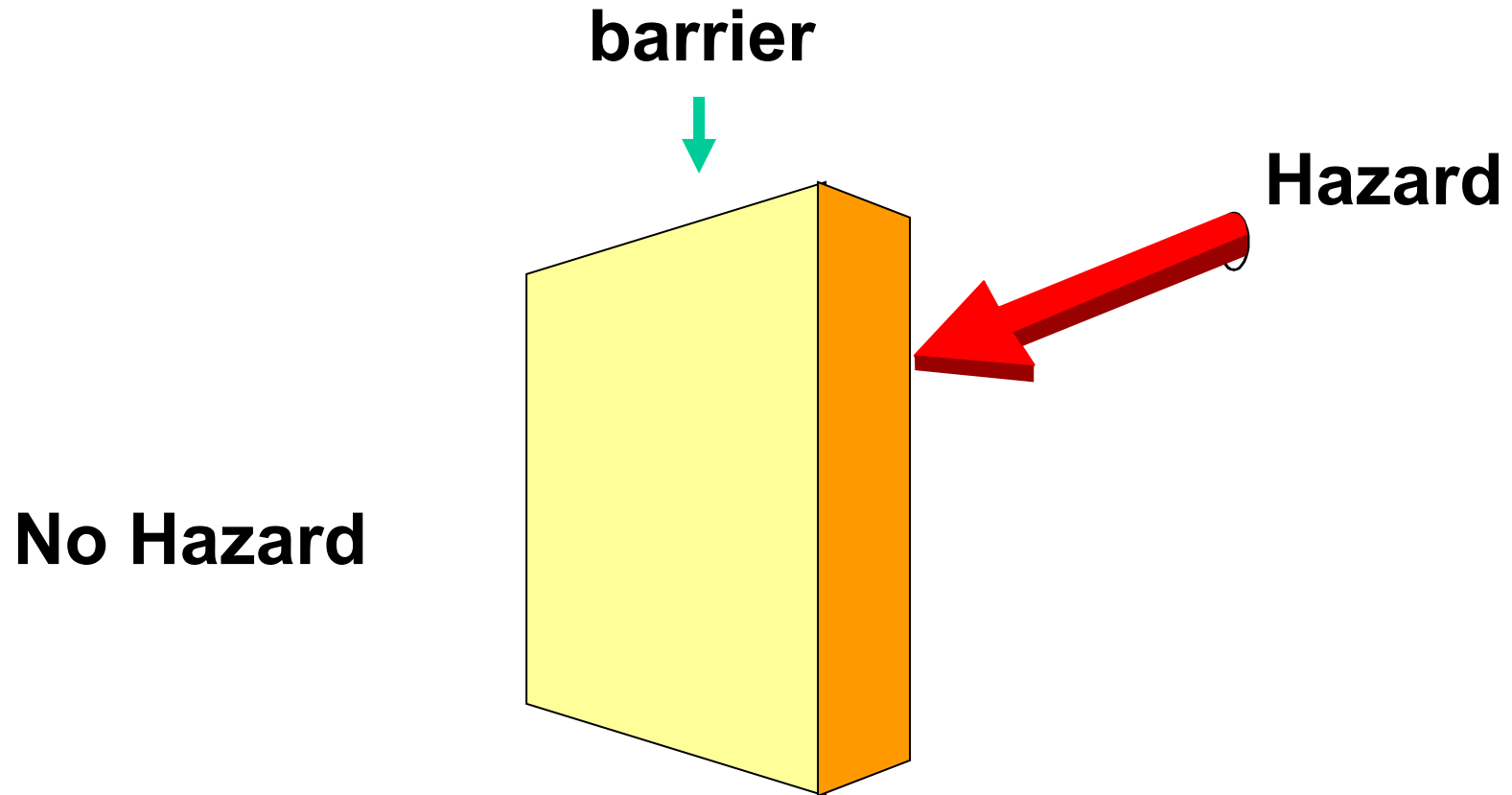
- **SAFETY** \equiv freedom from unaffordable harm







- **SAFETY \equiv freedom from unaffordable harm**
- **The 'parmesan cheese' model**



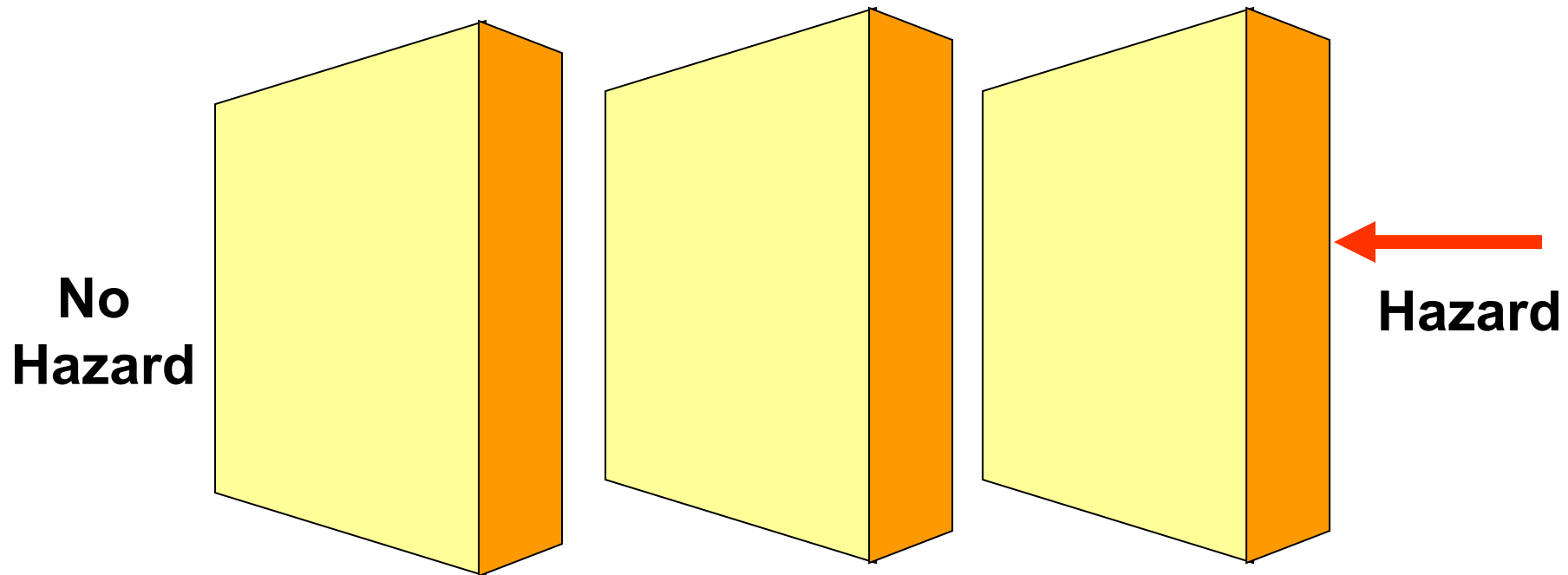


Not all barriers work...





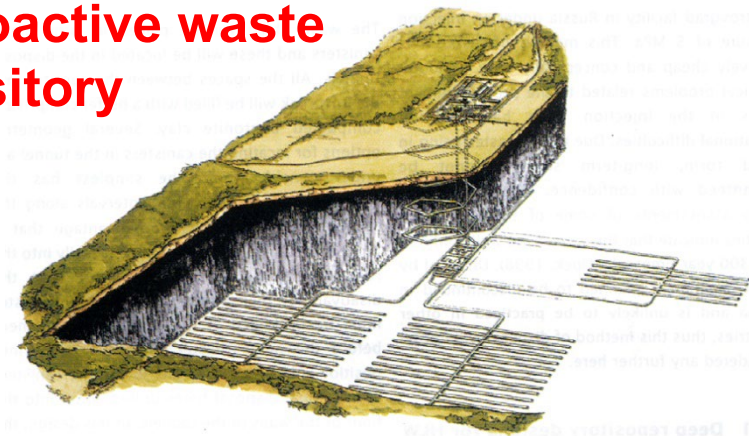
Safety: Multiple Barriers





Safety: Multiple Barriers - Example

Radioactive waste repository





Safety: Multiple Barriers - Example

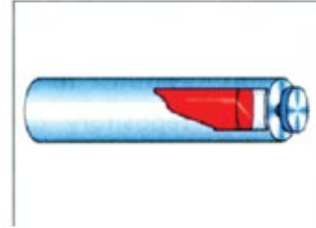


Radioactive waste repository



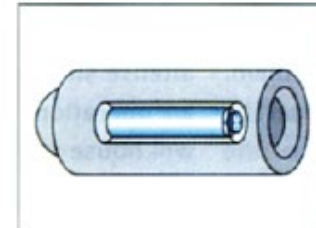
Glass Matrix

- Low corrosion rate of glass
- High resistance to radiation damage
- Homogeneous radionuclide distribution



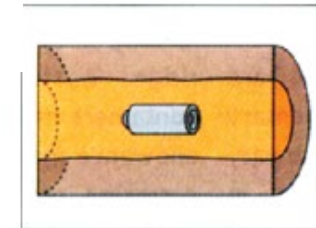
Steel Canister

- Completely isolates waste for > 1000 years
- Corrosion products act as a chemical buffer
- Corrosion products take up radionuclides



Betonite Backfill

- Long resaturation time
- Low solute transfer rates (diffusion)
- Retardation of radionuclide transport (sorption)
- Chemical buffer
- Low radionuclide solubility in leachate
- Colloid filter
- Plasticity (self-healing following physical disturbance)

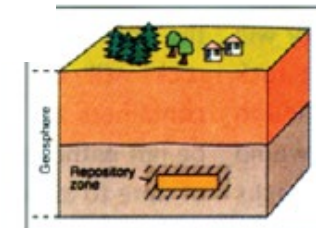


Geological Barrier

- Low water flux
- Favourable geochemistry
- Mechanical stability

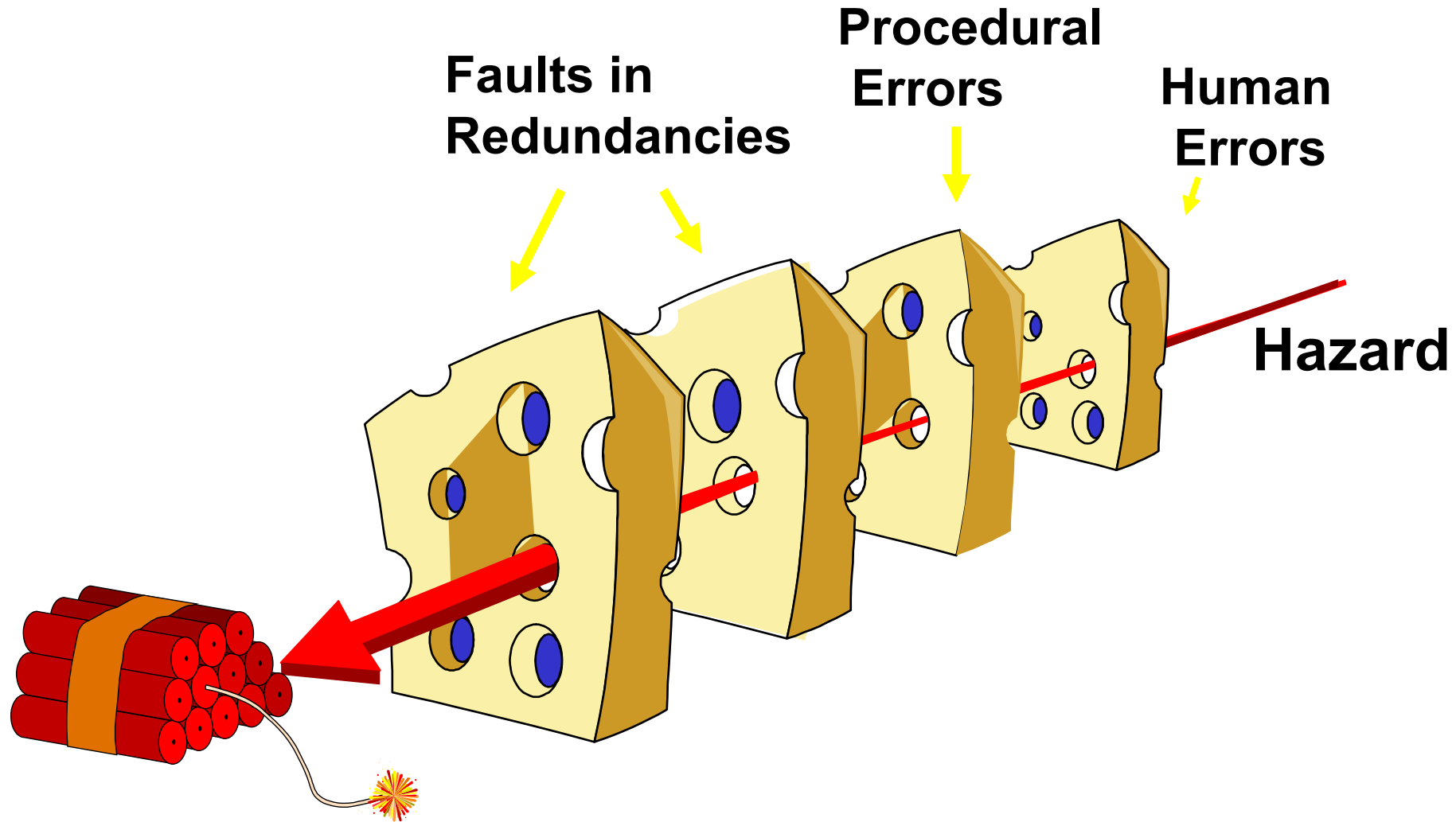
Geosphere:

- Retardation of radionuclides (sorption, matrix diffusion)
- Reduction of radionuclide concentration (dilution, radioactive decay)
- Physical protection of the engineered barriers (e.g. from glacial erosion)





Safety: the Swiss Cheese Model



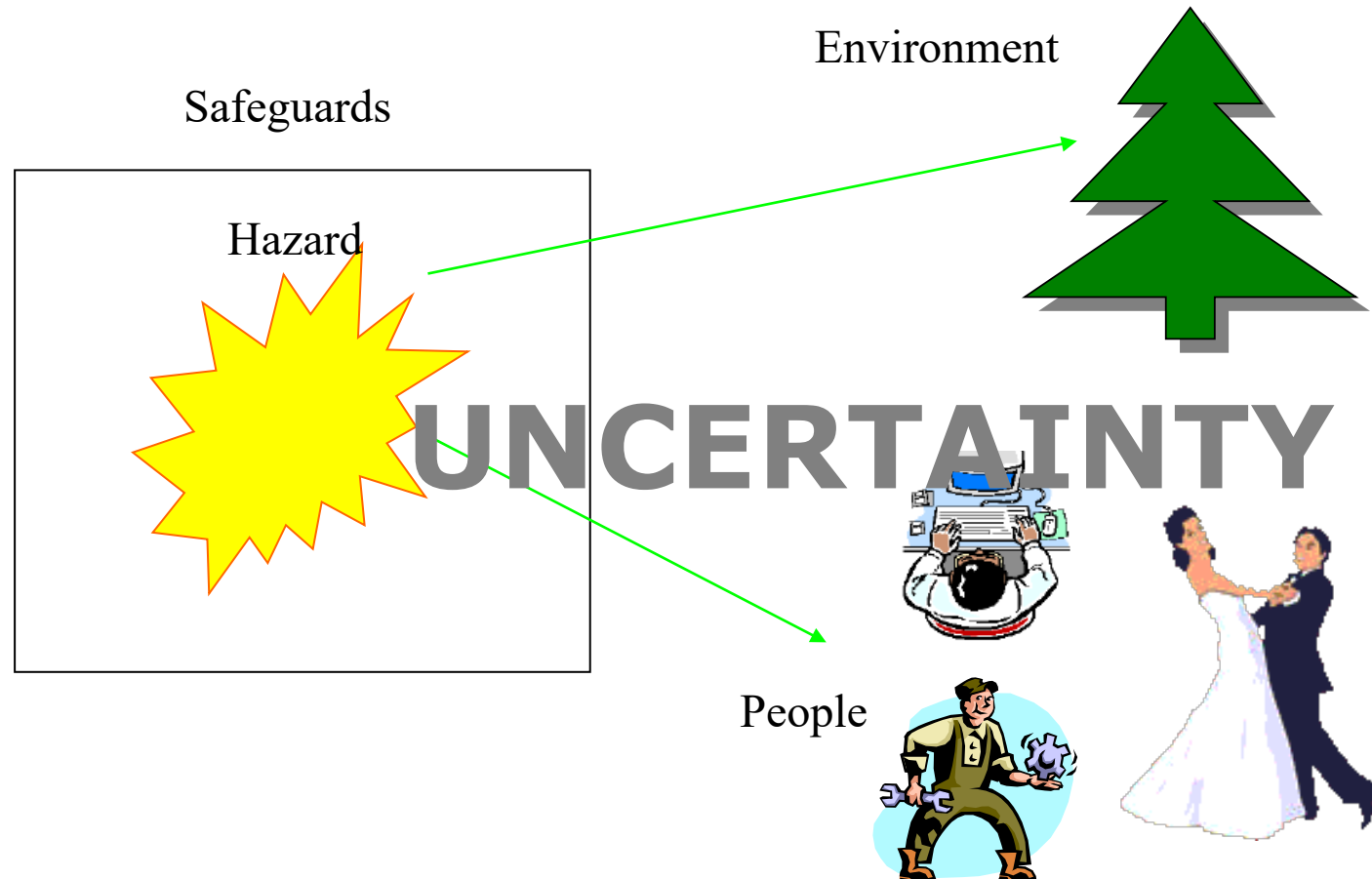


Introduction to the course:

- Reliability
- Safety
- Risk Analysis



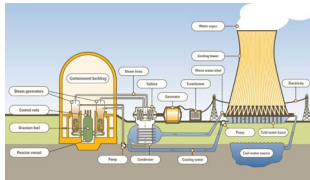
The Concept of Risk

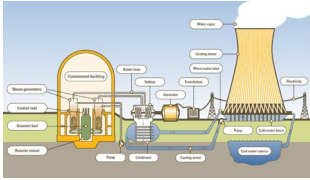




RISK = POTENTIAL DAMAGE + UNCERTAINTY

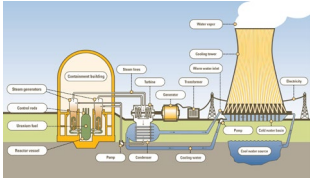
Dictionary: RISK = possibility of damage or injury to people or things





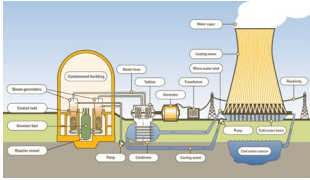
1. What undesired conditions may occur? ➡ Accident Scenario, S

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



1. What undesired conditions may occur? ➡ Accident Scenario, S
2. With what probability do they occur? ➡ Probability, p

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



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**



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



Probabilistic Risk Assessment (PRA): Results

$\{S_i, p_i, x_i\}$

S	p	x
S₁	p₁	x₁
...
S_N	p_N	x_N



$$\text{RISK} = p \cdot x$$



$$\text{RISK} = p \cdot x \cdot k(>1)$$



$$\text{RISK} = \sum_i p_i x_i^{k(>1)}$$

WARNING:

RISK (A) = RISK (B)

A=(P, x); B=(p, X)



RISK REDUCTION:

A: Prevention

B: Mitigation, Protection



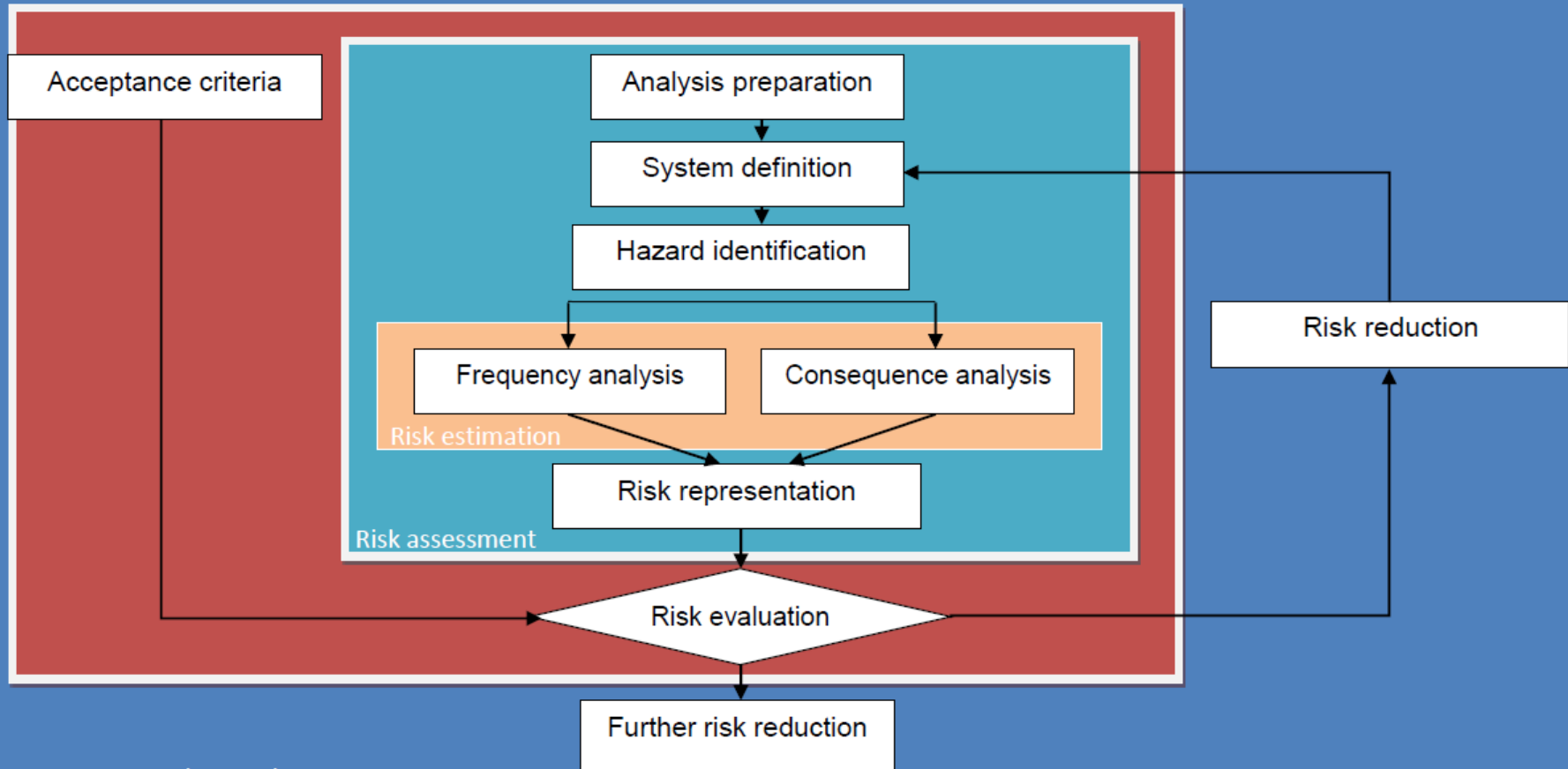
Risk Evaluation: Risk Matrix

Consequence					Increasing Annual Frequency					
Severity	People	Environ.	Assets	Reputation	0	A	B	C	D	E
					Practically non-credible occurrence	Rare occurrence	Unlikely occurrence	Credible occurrence	Probable occurrence	Likely/Frequent occurrence
					Could happen in E&P industry	Reported for E&P industry	Has occurred at least once in Company	Has occurred several times in Company	Happens several times/y in Company	Happens several times/y in one location
1	Slight health effect / injury	Slight effect	Slight damage	Slight impact	Continuous Improvement					
2	Minor health effect / injury	Minor effect	Minor damage	Minor impact						
3	Major health effect / injury	Local effect	Local damage	Local impact	Risk Reduction Measures					
4	PTD(*) or 1 fatality	Major effect	Major damage	National impact						
5	Multiple fatalities	Extensive effect	Extensive damage	International impact	Intolerable Risk					

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



Risk management and control

Course Syllabus



Part 1: Reliability

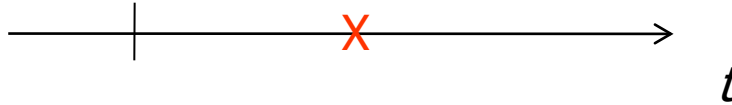
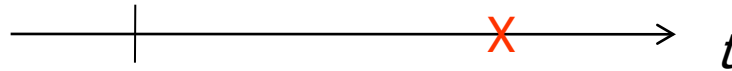
- Basics of probability
- Reliability of simple systems
- Markov processes for reliability and availability analysis of more complex systems
- Monte Carlo simulation method for reliability and availability analysis
- Estimation of reliability parameters from experimental data
- Maintenance in the energy industry

Part 2: Safety and Risk Assessment

- Probabilistic Risk Assessment
- Bayesian networks, fault and event tree analysis for identification and quantification of accidental sequences
- Dependent Failures
- Importance Measures



- Basics of probability



The failure time is a random variable!



How to represent the failure time?

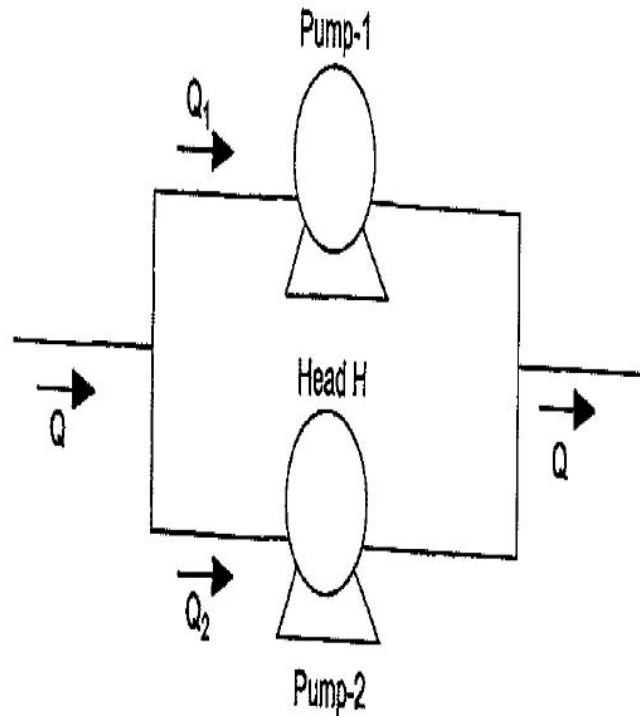


Probability distributions: $f_T(t|\lambda)$



Topics (Part 1)

- Basics of probability
- Reliability of simple systems

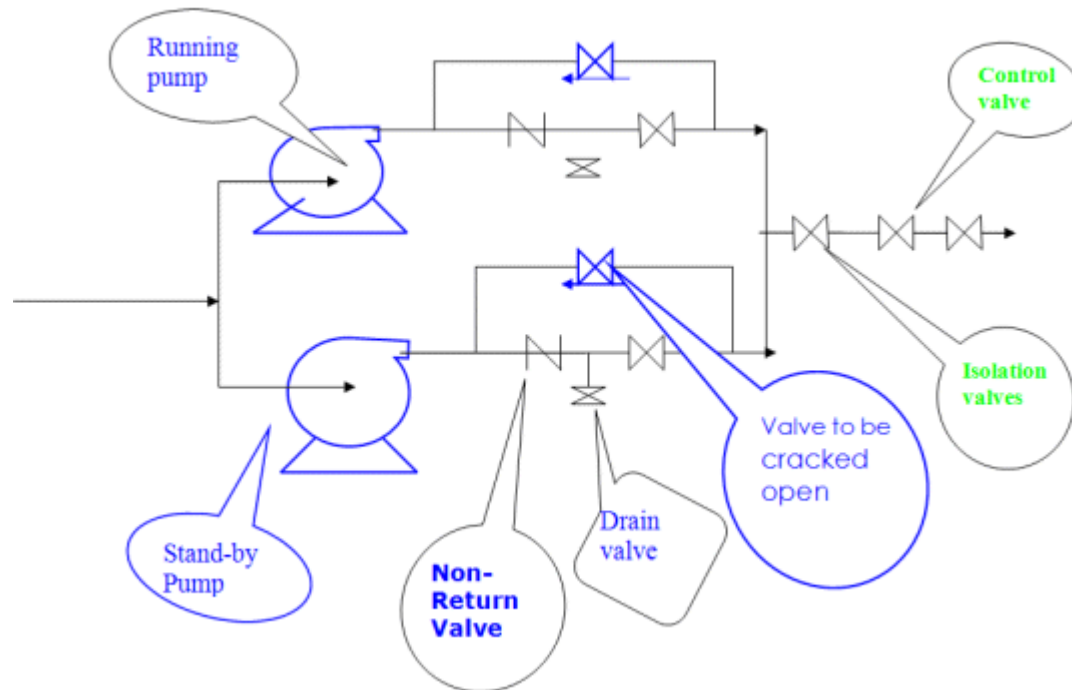


pumping system



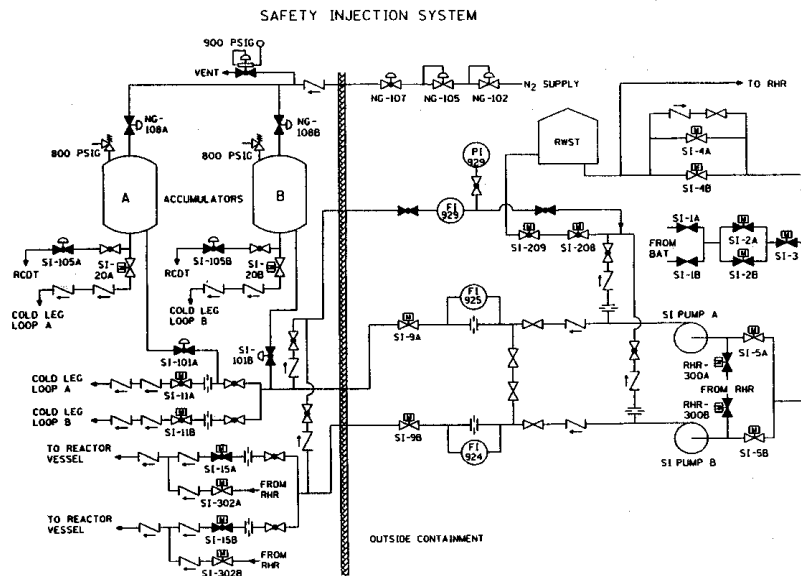
Topics (Part 1)

- Basics of probability
- Reliability of simple systems
- Markov processes for reliability and availability analysis of more complex systems





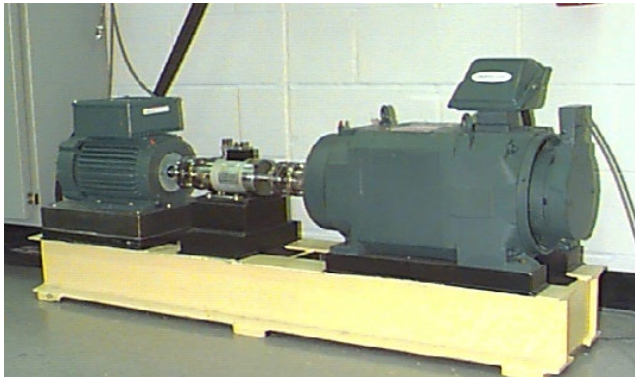
- # Monte Carlo Simulation for reliability and availability analysis





Topics (Part 1)

- Basics of probability
- Reliability of simple systems
- Markov processes for reliability and availability analysis of more complex systems
- Monte Carlo simulation method for reliability and availability analysis
- Estimation of reliability parameters from experimental data



(Accelerated) degradation tests

Failure times

15.8 h

15.9 h

15.1 h

17.2 h

...

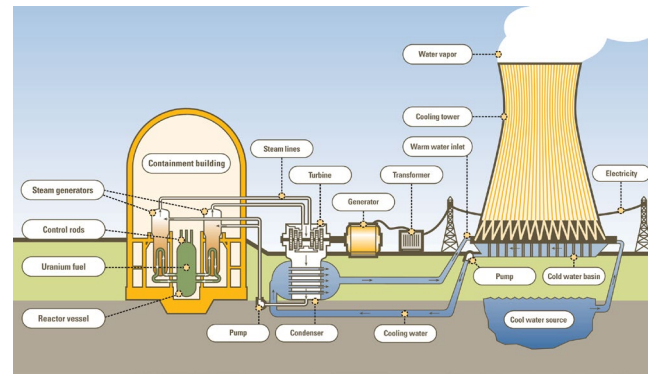
14.5 h

$f_T(t|\theta)$



Topics (Part 1)

- Basics of probability
- Reliability of simple systems
- Markov processes for reliability and availability analysis of more complex systems
- Monte Carlo simulation method for reliability and availability analysis
- Estimation of reliability parameters from experimental data
- Maintenance

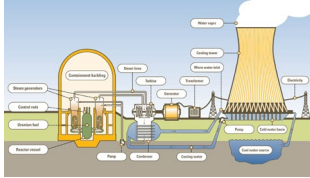




- (Probabilistic) Risk Assessment
- Bayesian networks, fault and event tree analysis for identification and quantification of accidental sequences
- Importance Measures
- Dependent Failures



- (Probabilistic) Risk Assessment

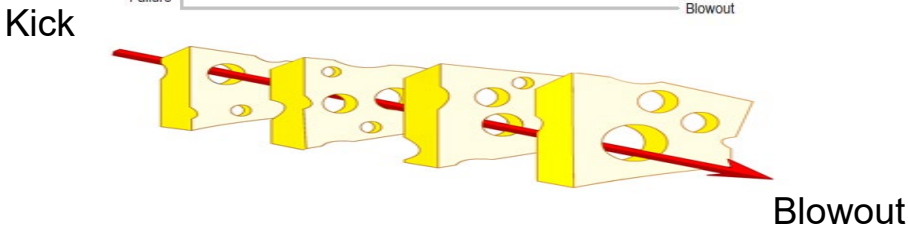
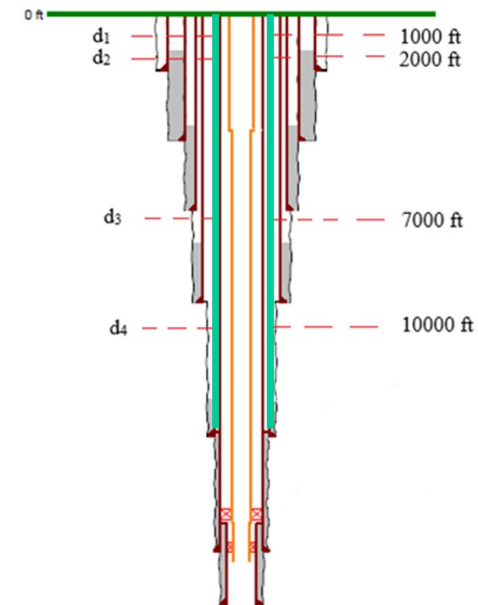
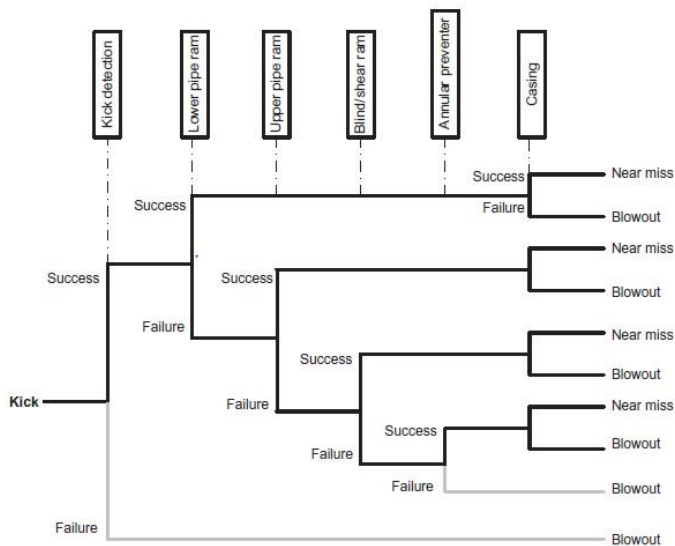


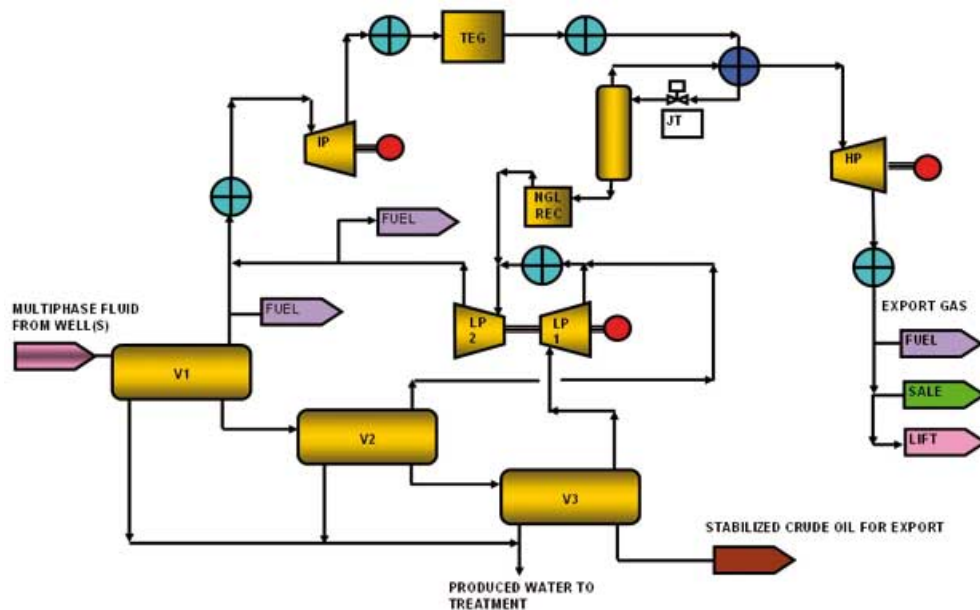
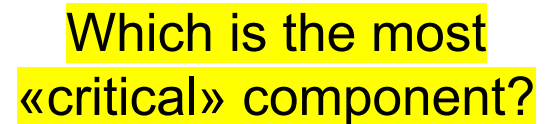
S	p	x
S₁	p₁	x₁
...
S_N	p_N	x_N



- Probabilistic Risk Assessment
- Bayesian networks, fault and event tree analysis for identification and quantification of accidental sequences

Blowout accident in oil and gas wells during drilling

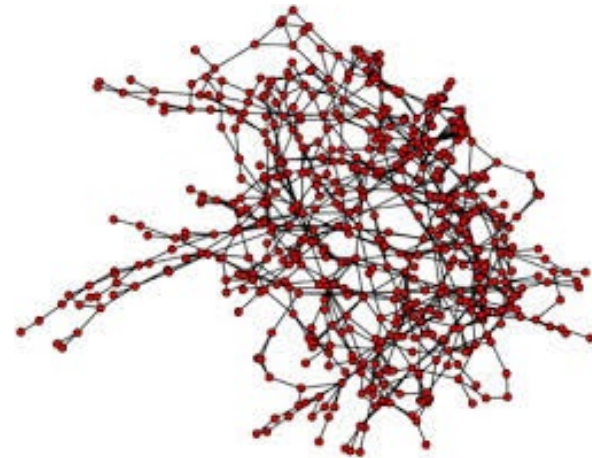






- Probabilistic Risk Assessment
- Fault and event tree analysis for identification and quantification of accidental sequences
- Importance Measures
- Dependent Failures

electric grid





- Probabilistic Risk Assessment
- Fault and event tree analysis for identification and quantification of accidental sequences
- Importance Measures
- Dependent Failures



- Lectures (traditional + flipped classes)
- Exercise sessions
- Tests during exercise sessions
- Multidisciplinary teams:
 - Development of a matlab/python* code for the estimation of reliability and availability of an energy system (Monte Carlo project)
 - Prepare a presentation and deliver a speech on a specific topic related to the latest advancement in the field of reliability, safety and risk analysis.
- Seminars

*Chance to take part in tutoring sessions organized by the study program



- Lecture slides (<http://www.lasar.polimi.it/> → Teaching)
- Course material (except lecture slides) → WeBeep:
 - Assignments (Monte Carlo project, Scientific Talk)
 - Course information and updates;
 - Exam results
- Books:
 - Zio E., An introduction to the basics of reliability and risk analysis, World Scientific, 2007.
 - Zio E., Computational methods of reliability and risk analysis, World Scientific, 2009.
 - Zio E., The Monte Carlo Simulation Method for System Reliability and Risk Analysis
 - Zio E., Baraldi P., Cadini F., “Basics of Reliability and Risk Analysis: Worked Out Problems and Solutions”. World Scientific, Singapore, 2011

Enrico Zio

AN INTRODUCTION TO THE BASICS OF RELIABILITY AND RISK ANALYSIS

The necessity of expertise for tackling the complicated and multidisciplinary issues of safety and risk has slowly permeated into all engineering applications so that risk analysis and management has gained a relevant role both as a tool in support of plant design and as an indispensable means for emergency planning in accidental situations. This entails the acquisition of appropriate reliability modeling and risk analysis tools as complement to the basic and specific engineering knowledge for the technological area of application.

This book provides an introduction to the principal concepts and issues related to the safety of modern industrial activities and an illustration of the classical techniques for reliability analysis and risk assessment used in the current practice. It is aimed at providing an organic view of the subject.

Zio

Series in Quality, Reliability and Engineering Statistics **Vol. 13**

AN INTRODUCTION TO THE BASICS OF RELIABILITY AND RISK ANALYSIS

World Scientific
www.worldscientific.com
6442 hc



Connecting Great Minds

30 Years World Scientific 1982-2012

Series on Quality, Reliability and Engineering Statistics - Vol. 15
BASICS OF RELIABILITY AND RISK ANALYSIS
Worked Out Problems and Solutions
 by Enrico Zio (École Centrale Paris et Supélec, France & Politecnico di Milano, Italy), Piero Baraldi (Politecnico di Milano, Italy), & Francesco Cadini (Politecnico di Milano, Italy)

Reliability and safety are fundamental attributes of any modern technological system. To achieve this, diverse types of protection barriers are placed as safeguards from the hazard posed by the operation of the system, within a multiple-barrier design concept. These barriers are intended to protect the system from failures of any of its elements, hardware and software, human and organizational.

Correspondingly, the quantification of the probability of failure of the system and its protective barriers, through reliability and risk analysis, becomes a primary task in both the system design and operation phases.

This exercise book serves as a complementary tool supporting the methodology concepts introduced in the books "An introduction to the basics of reliability and risk analysis" and "Computational methods for reliability and risk analysis" by Enrico Zio, in that it gives an opportunity to familiarize with the applications of classical and advanced techniques of reliability and risk analysis.

This book is also available as a set with *Computational Methods for Reliability and Risk Analysis* and *An Introduction to the Basics of Reliability and Risk Analysis*.

224pp	June 2011	
978-981-4355-03-2	US\$60	£44
Set		
978-981-4360-05-0	US\$109	£79

Series on Quality, Reliability and Engineering Statistics - Vol. 14
COMPUTATIONAL METHODS FOR RELIABILITY AND RISK ANALYSIS
 by Enrico Zio (Politecnico di Milano, Italy)

This book illustrates a number of modelling and computational techniques for addressing relevant issues in reliability and risk analysis. In particular, it provides: (i) a basic illustration of some methods used in reliability and risk analysis for modelling the stochastic failure and repair behaviour of systems, e.g. the Markov and Monte Carlo simulation methods; (ii) an introduction to Genetic Algorithms, tailored to their application for RAMS (Reliability, Availability, Maintainability and Safety) optimization; (iii) an introduction to key issues of system reliability and risk analysis, like dependent failures and importance measures; and (iv) a presentation of the issue of uncertainty and of the techniques of sensitivity and uncertainty analysis used in support of reliability and risk analysis.

The book provides a technical basis for senior undergraduate or graduate courses and a reference for researchers and practitioners in the field of reliability and risk analysis. Several practical examples are included to demonstrate the application of the concepts and techniques in practice.

This book is also available as part with *Basics of Reliability and Risk Analysis* and *An Introduction to the Basics of Reliability and Risk Analysis*.

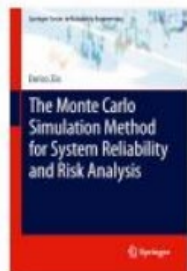
Readership: Undergraduate, graduate, academics and professionals in the fields of systems engineering and safety and risk analysis.

264pp	January 2009	
978-981-263-401-5	£27	\$83
Set		
978-981-4360-04-5	£129	\$225

World Scientific
 Connecting Great Minds

ICP Imperial College Press
 www.icpress.co.uk

Preferred Publisher for Leading Thinkers



2013, 2013, XIV, 198 p. 69 illus., 24 in color.

Printed book

Hardcover

- 129,95 € | £117.00 | \$179.00
- *139,05 € (D) | 142,94 € (A) | CHF 173.00

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.

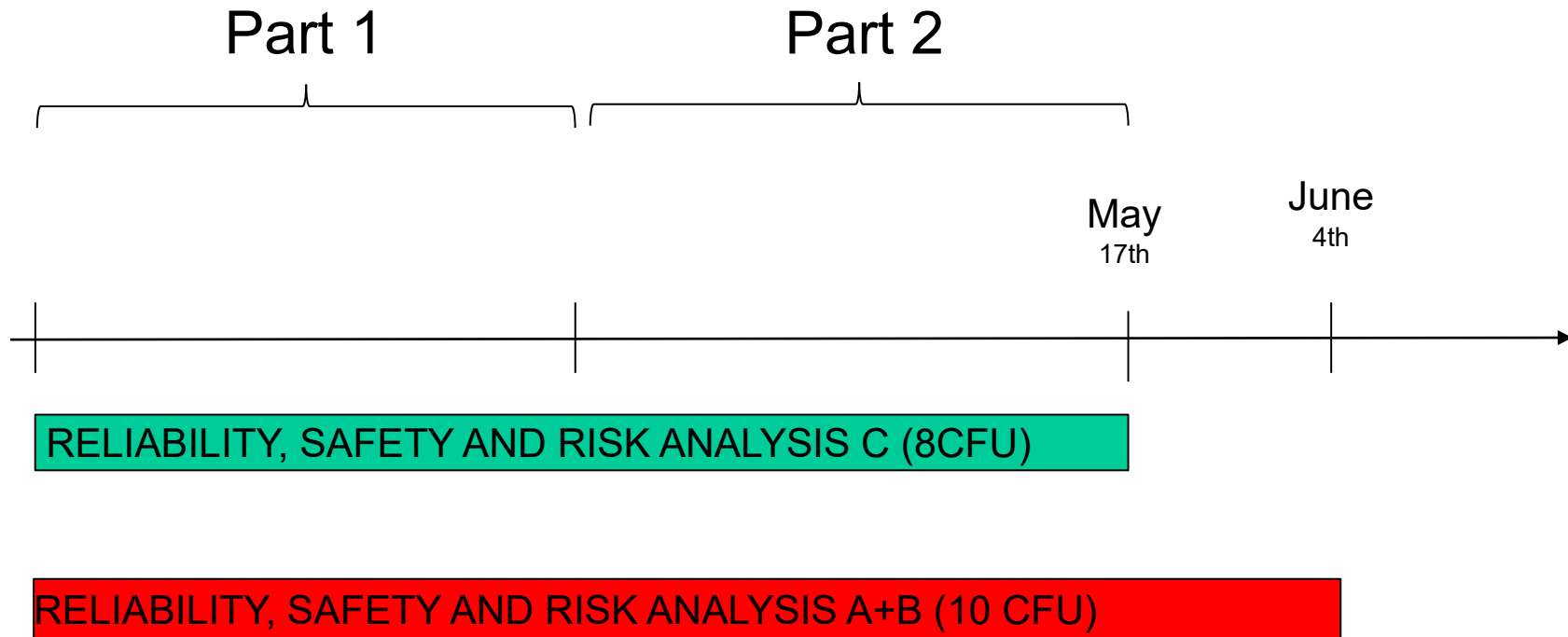


- Piero Baraldi
- Nicola Cardenas



- Giovanni Roma







- Project (15%)
- Scientific Talk (15%)
- 4 Hands-on exercises that will be done during 4 exercise sessions¹ (35%)
- Written exam on theory (35%)²
- Possibility to have an oral exam (+/- 3 points)

¹ It is necessary to have at least 18/30 in each one of the four hands-on exercises to be admitted to the written exam.

- Students that do not pass the hands-on exercises will have the possibility to do a written exam with 2 exercises

² It is necessary to have at least 18/30 in the written exam to pass the course.