“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
Degradation & Failure

Evolution to... failure

Healthy
Degradation initiation
Failure
Examples of degradation in industrial components

Creeping of turbine blades

Erosion of choke valves

Crack propagation
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.

Sources: Keynote of Pierre Dersin at PHM Europe 2014,
Failure Definition

➢ 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
Failure prevention

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

- Always present in human activities

- From reasonable to rational solutions
Reliability engineering: When?

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

http://www.centennialbulb.org/photos.htm

UNCERTAINTY!
Our big problem...

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
Reliability, performance and cost: the trade-off

- **Objective:** design and build product for **improved performance**
  - Faster aircraft
  - Thermodynamically more efficient energy conversion devices

- Increase ‘load’
  - Aircraft $\rightarrow$ decrease weight
  - Energy conversion devices $\rightarrow$ work at higher temperature

- Approach the physical limit of the system
  - Aircraft $\rightarrow$ Increase stress level in its components
  - Energy conversion devices $\rightarrow$ 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
Reliability, performance and cost: the trade-off

- **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

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
- **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 ≡ freedom from unaffordable harm
• The ‘parmesan cheese’ model
Not all barriers work...
Safety: Multiple Barriers

- Redundancy
- Training
- Safety Reviews

No Hazard → Hazard
Safety: Multiple Barriers - Example

- Glass matrix (in steel mould)
  - 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

- Bentonite 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 barriers
  - Repository zone:
    - Low water flux
    - Favourable geochemistry
    - Mechanical stability
  - Geospheres:
    - Retardation of radionuclides (sorption, matrix diffusion)
    - Reduction of radionuclide concentration (dilution, radioactive decay)
    - Physical protection of the engineered barriers (e.g., from glacial erosion)
Faults in Redundancies

Procedural Errors

Human Errors

Safety: the Swiss Cheese Model

Hazard
Introduction to the course:

- Reliability
- Safety
- Risk Analysis
The Concept of Risk

- Hazard
- Safeguards
- People
- Environment

UNCERTAINTY
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, $S$

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\}

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>p</td>
<td>x</td>
</tr>
<tr>
<td>S_1</td>
<td>p_1</td>
<td>x_1</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>S_N</td>
<td>p_N</td>
<td>x_N</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Severity</th>
<th>Consequence</th>
<th>People</th>
<th>Environment</th>
<th>Assets</th>
<th>Reputation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Slight health effect / injury</td>
<td>Slight effect</td>
<td>Slight damage</td>
<td>Slight impact</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Minor health effect / injury</td>
<td>Minor effect</td>
<td>Minor damage</td>
<td>Minor impact</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Major health effect / injury</td>
<td>Local effect</td>
<td>Local damage</td>
<td>Local impact</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>PT(1) or 1 fatality</td>
<td>Major effect</td>
<td>Major damage</td>
<td>National impact</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Multiple fatalities</td>
<td>Extensive effect</td>
<td>Extensive damage</td>
<td>International impact</td>
<td></td>
</tr>
</tbody>
</table>

#### Increasing Annual Frequency

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>Rare occurrence</td>
<td>Unlikely occurrence</td>
<td>Credible occurrence</td>
<td>Probable occurrence</td>
<td>Likely/Frequent occurrence</td>
</tr>
<tr>
<td>Example</td>
<td>Could happen in E&amp;P industry</td>
<td>Reported for E&amp;P industry</td>
<td>Has occurred at least once in Company</td>
<td>Has occurred several times in Company</td>
<td>Happens several times in Company</td>
</tr>
</tbody>
</table>

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 Assessment & Management Procedure

- Acceptance criteria
- Analysis preparation
  - System definition
  - Hazard identification
- Frequency analysis
- Consequence analysis
- Risk estimation
- Risk representation
- Risk assessment
- Risk evaluation
- Further risk reduction
- Risk management and control
- Risk reduction
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: Risk Assessment

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

Failure times

\[ f_T(t|\theta) \]

15.8 h
15.9 h
15.1 h
17.2 h

(Accelerated) degradation tests

\[ \ldots \]

14.5 h
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
Topics (Part 2)

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

<table>
<thead>
<tr>
<th>$S$</th>
<th>$p$</th>
<th>$x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_1$</td>
<td>$p_1$</td>
<td>$x_1$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>$S_N$</td>
<td>$p_N$</td>
<td>$x_N$</td>
</tr>
</tbody>
</table>
• Probabilistic Risk Assessment
• Fault and event tree analysis for identification and quantification of accidental sequences

Blowout Accident in Oil and Gas Wells during drilling
Topics (Part 2)

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

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

Which is the most «critical» component?
• Probabilistic Risk Assessment
• Fault and event tree analysis for identification and quantification of accidental sequences
• Dependent Failures
• Importance Measures
• Uncertainty and Sensitivity Analysis
Teaching Organization

- Lectures
- Exercise Sessions
- Seminars
Teaching Organization
(energy and nuclear engineering students)

Part 1
February 26th

Part 2
April 13th
May 21st
June 8th

ENERGY ENG. STUDENTS

NUCLEAR ENG. STUDENTS
Final Evaluation

You can choose between:

- **Path A**
  - First Midterm (1/3 of the final mark, April):
    - Exercises and questions on the first part of the course
  - Second Midterm (1/3 of the final mark, May):
    - Exercises and questions on the second part of the course
  - Oral Exam (1/3 of the final mark, first week of June or 1°)*:
    - 2 questions (on all the course topics)

- **Path B**
  - Written exam (2/3 of the final mark):
    - Exercises and questions on all the course topics
  - Oral exam (1/3 of the final mark)**:
    - 2 questions (on all the course topics)

* To be admitted to the oral it is necessary to have at least 18/31 in both midterms
** To be admitted to the oral it is necessary to have at least 18/31 in the written exam
Course Material

- Lecture slides (http://www.lasar.polimi.it/)
- Zio E., The Monte Carlo Simulation Method for System 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.
Connecting Great Minds

BASICS OF RELIABILITY AND RISK ANALYSIS

World Scientific Publishing Co. Pte. Ltd.

Computational Methods for Reliability and Risk Analysis

by Enrico Zio (Polytechnic of Milan, Italy)

Reliability and safety are fundamental attributes of any modern technological system. To achieve this, diverse types of protection barriers are placed in a system to ensure that the system operates without any failure. These barriers are intended to protect the system from failures of any of its elements, human and software, human and organizational.

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

This text book serves as a comprehensive tool supporting the methodology concepts introduced in the books "An Introduction to the Basics of Reliability and Risk Analysis" by Enrico Zio, in the design and operation phases of the systems.

The book is also available in a complete set with "Computational Methods for Reliability and Risk Analysis" and "An Introduction to the Basics of Reliability and Risk Analysis".
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 of 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 of 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.