



## Reliability, Safety and Risk



Enrico Zio



# QS World University Rankings 2023

\*World | 139°

•Italia | 1°

# Employer Reputation 2023

World | 80°

Italia | 1°

# Academic Reputation 2023

World | 96°

Italy | 1°





# The team



**Stefano MARCHETTI**  
[stefano.marchetti@polimi.it](mailto:stefano.marchetti@polimi.it)  
ITALY

MSc: Nuclear Engineering  
PhD Candidate (Cycle XXXVIII)  
**Laboratory of Signal Analysis and Risk Analysis**  
Department of Energy, Politecnico di Milano  
**Research topic:** Condition-Informed Dynamic Risk  
Assessment of complex systems



**Ibrahim AHMED**  
[Ibrahim.ahmed@polimi.it](mailto:Ibrahim.ahmed@polimi.it)  
ITALY

PhD Nuclear Engineering – Kyung Hee University, South Korea  
Assistant Professor  
**Laboratory of Signal Analysis and Risk Analysis**  
Department of Energy, Politecnico di Milano



## Enrico Zio



POLITECNICO  
DI MILANO

MSc degree in nuclear engineering from Politecnico di Milano in 1991 and in mechanical engineering from UCLA in 1995

Ph.D. degree in nuclear engineering from Politecnico di Milano and in probabilistic risk assessment at MIT in 1996 and 1998

Full professor at the Centre for research on Risks and Crises (CRC) of Ecole de Mines, ParisTech, PSL University, France  
Full professor and President of the Alumni Association at Politecnico di Milano, Italy,  
Distinguished guest professor at Tsinghua University, Beijing, China, adjunct professor at City University of Hong Kong, Beihang University and Wuhan University, China and Co-Director of the Center for RELiability and Safety of Critical Infrastructures (CRESCI) and the sino-french laboratory of Risk Science and Engineering (RISE), at Beihang University, Beijing, China.

He is IEEE and Sigma Xi Distinguished Lecturer.

In 2020, he has been awarded the prestigious international Humboldt Research Award in Germany.

In 2021, he has been appointed as 4TU.Resilience Ambassador by the 4TU Centre for Resilience Engineering of the four Dutch Technical Universities.

In 2021, he has been named Fellow of the of the Prognostics & Health Management Society.

In 2023, he has been appointed as Scientific Director of Research and Development of Datrix AI Solutions group.

In 2023 he has been elected fellow of Asia-Pacific Artificial Intelligence Association

In 2024 he has been elevated to the status of IEEE fellow

In 2024 he has been nominated Vice-President of Fondazione Politecnico di Milano, Italy

His Google Scholar H-index is 93 and he is in the top 2% of the World scientists, according to Stanford ranking.



Zio  
Enrico

10



*signed for Panthers: July 1998*

Better known "***Little knee***" for his ease in running.

After the much talked retirement of the "*Divine Ponytail*" (Roberto Baggio), he stands as the last true and pure artist of the Italian soccer. He remains a patrimony to be safeguarded, in spite of the "*tactical problem*" he represents for the Panthers team.

Fancy on the field and even brilliant off the field: meeting him disguised as Santa Claus at weddings or as deejay in popular Milano's bars, one would never realize that he is an internationally renowned luminary.

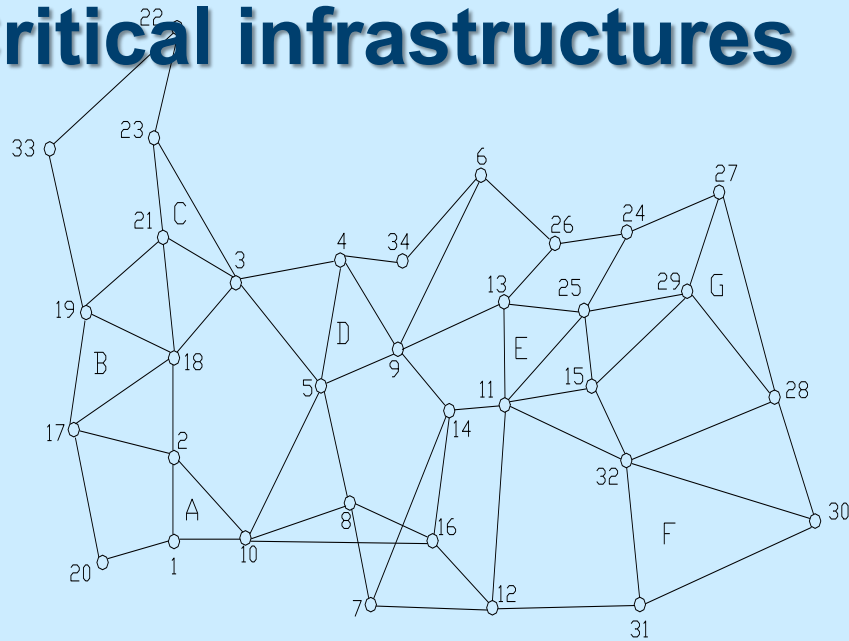




# Technological systems



# Critical infrastructures



## Water supply Systems



## Gas supply Systems



## Electric Power Networks







# Failures







# Failures







# Failures (external events)



**Taiwan News**  
台湾英文新聞  
VOICE OF THE PEOPLE - BRIDGE TO THE WORLD ESTABLISHED IN 1949

**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)



'Bomb cyclone' smashes eastern US: Power outages and flight cancellations...



Tempest Eleanor: disrupted transport (3 Jan 2018, Paris)



Avalanche cut the access to the village. (10 Jan 2018, Bonneval-sur-Arc)

## 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...**



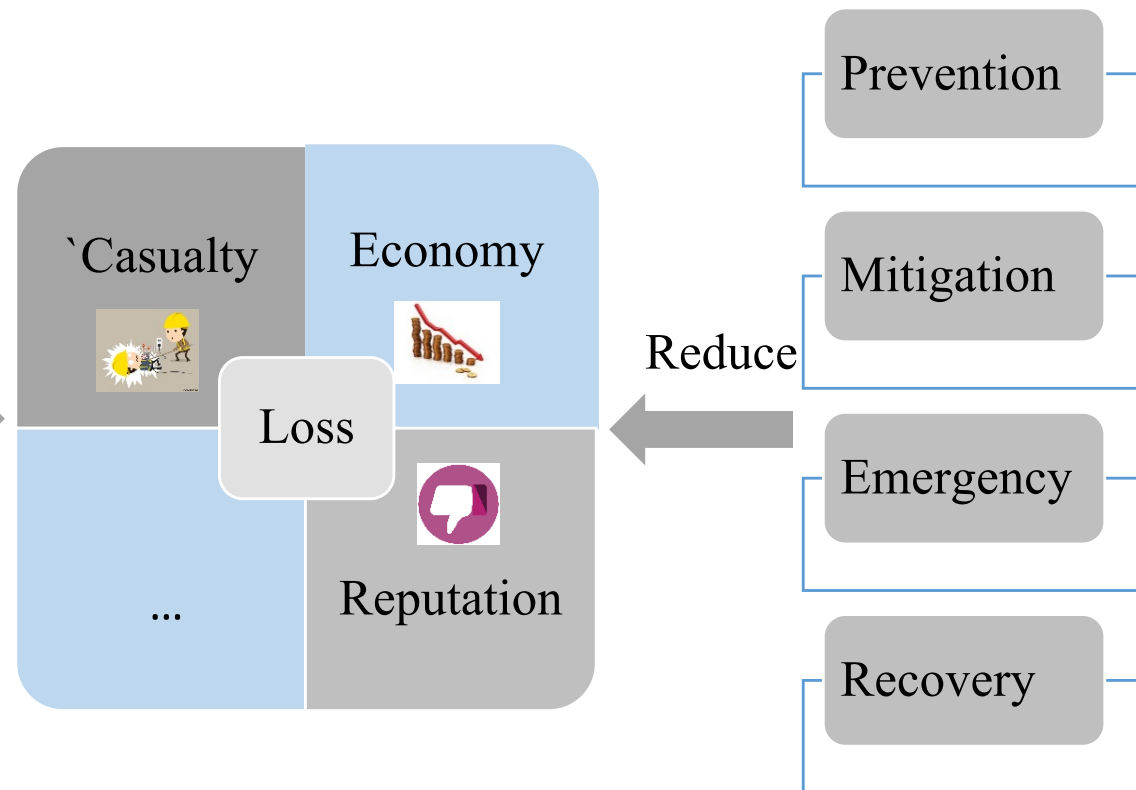
# Failures and consequences: the problem



2018, Oklahoma Rig Explosion



2019, Nyonoksa radiation accident



Reduce



# Reliability





# RELIABILITY: WHAT?

Reliability: 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 (if such a word might be framed) absolute *reliability*”*

**Reliability: a pervasive concept...**

**Web of science (science citation) 9512**

**Library of congress 3253**

**Google 12,500,000**



# RELIABILITY: WHAT?

Reliability: 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



*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)

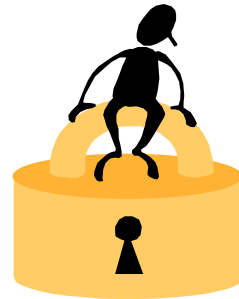


- **System representation and modeling**
- **System model quantification**
- **Uncertainty modeling & quantification**



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

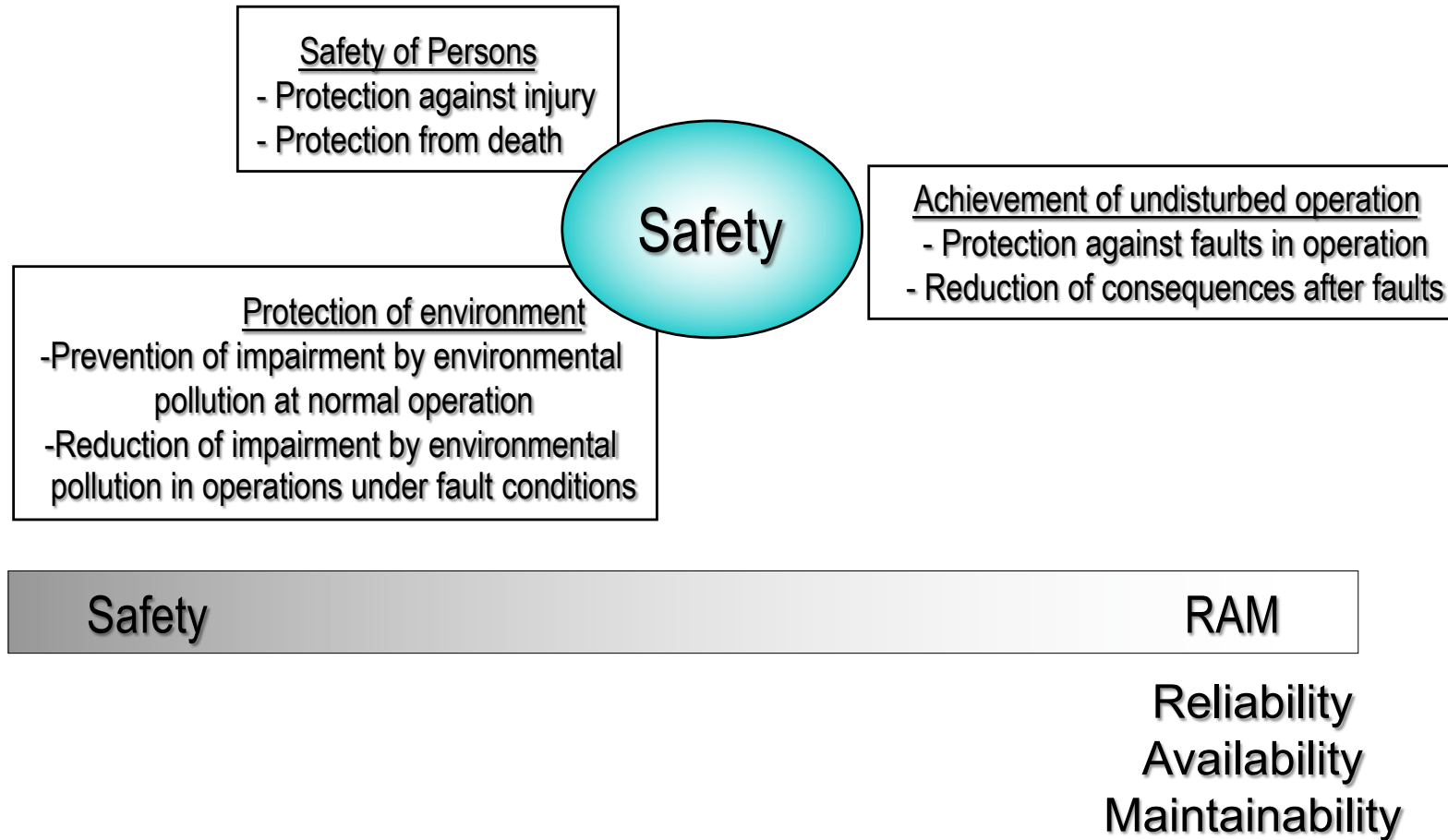
# Safety





**PROTECT LIVES &  
PROPERTY**

**PROTECT  
NATURE**





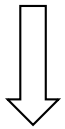


**SAFETY  $\equiv$  freedom from unaffordable harm**



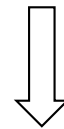
- Explanatory (a posteriori, reactive)

**Accident analysis**



**Difficulty/challenges:**

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

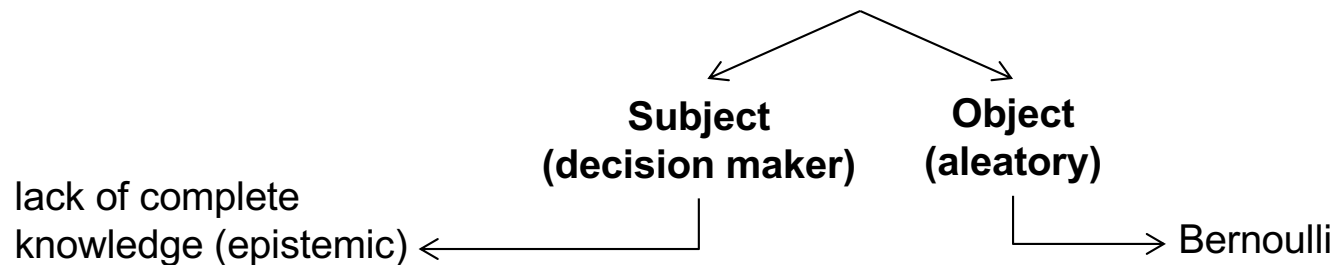


When the cause has been found, we try to eliminate it or reduce it.

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**

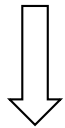




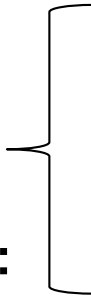
## SAFETY ≡ freedom from unaffordable harm

• Anticipative ( a priori, pro-active)

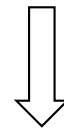
Accident analysis



Difficulty/challenges:



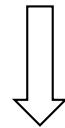
- Risk assessment: predicting what can happen



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

Aleatory

Model of I(u)

PRA +

epistemic model

# Uncertainty

---

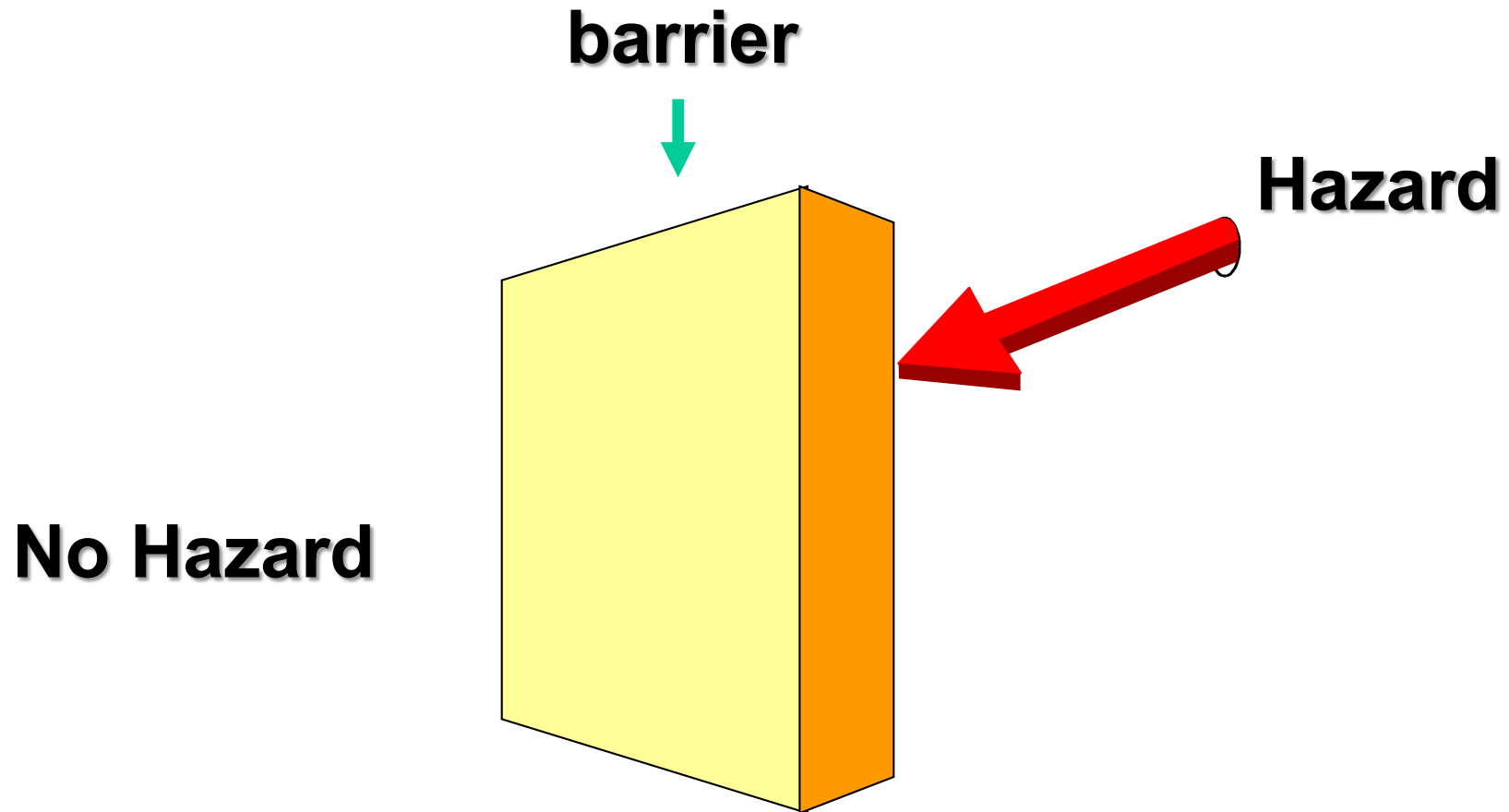
## **Aleatory Uncertainty**

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

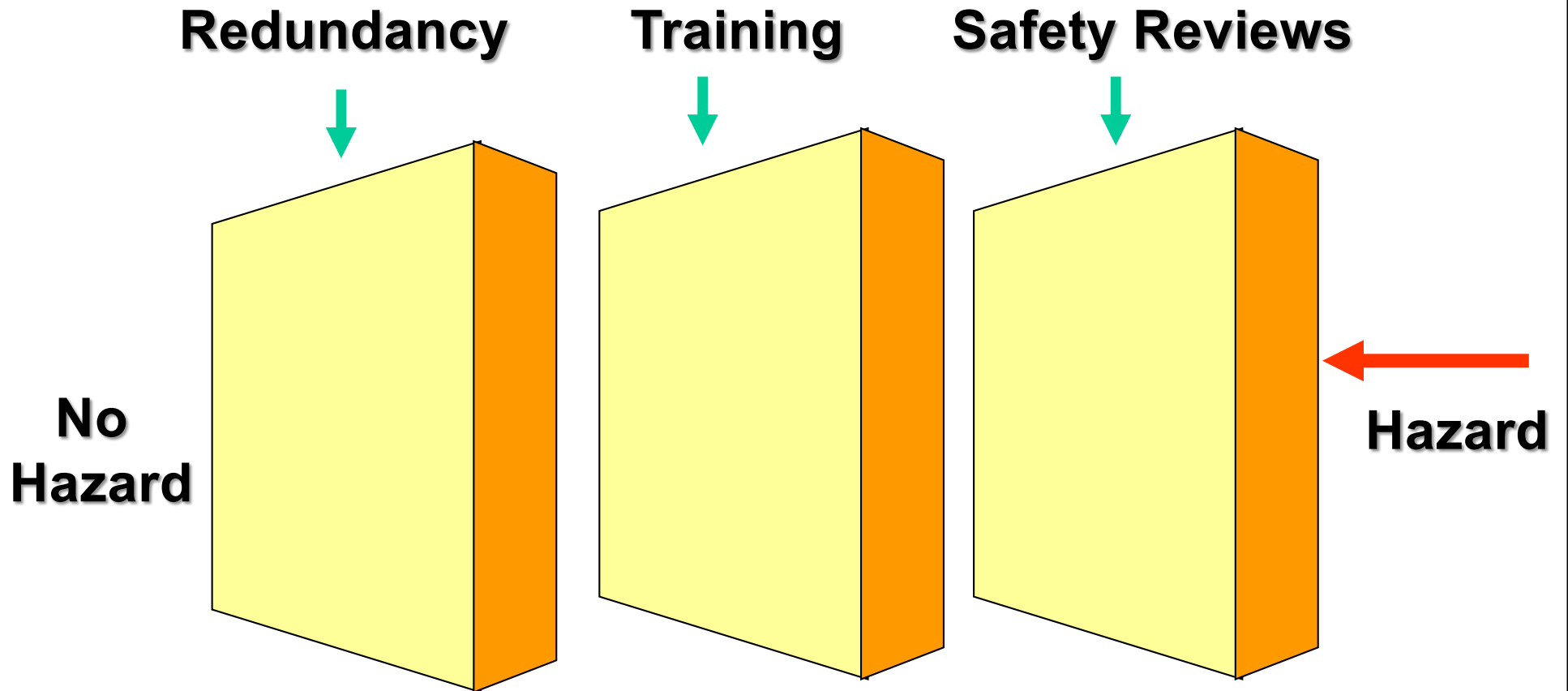
## **Epistemic Uncertainty**

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

# The 'parmesan cheese' model



# Multiple Barriers



# Redundancy: Example



# Risk

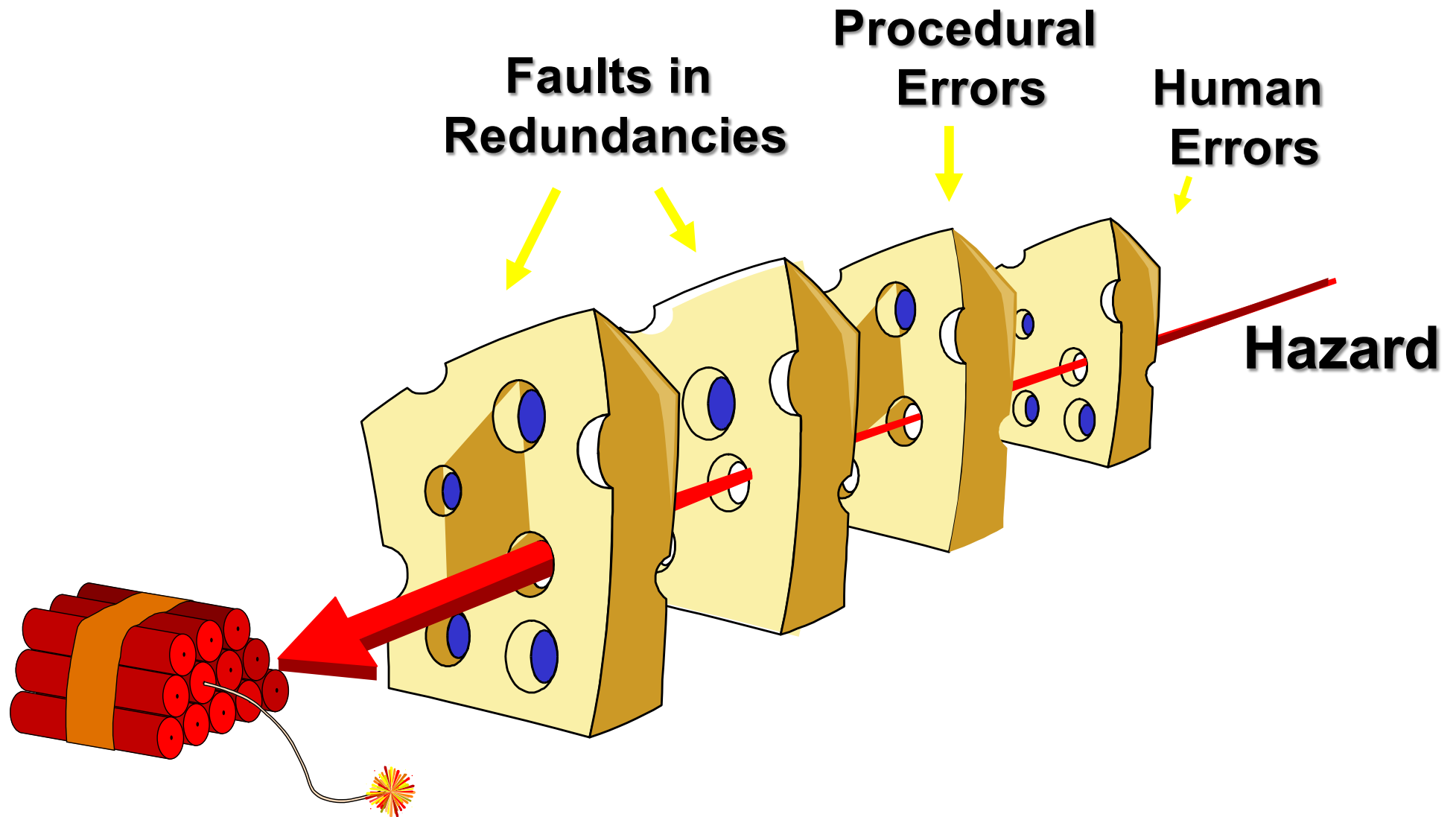
# Reality: An example of a protection barrier

Not all risk mitigation strategies work...

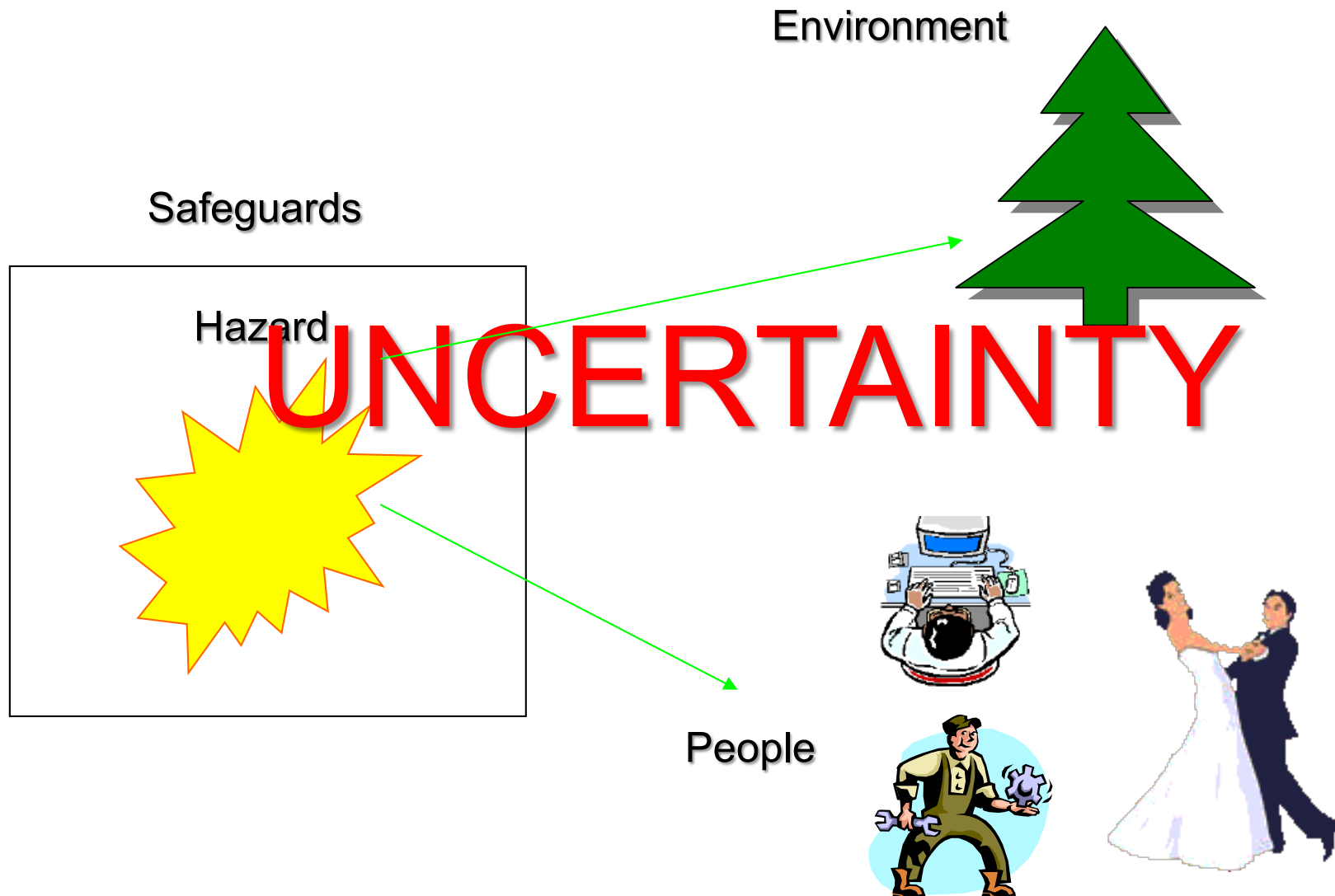




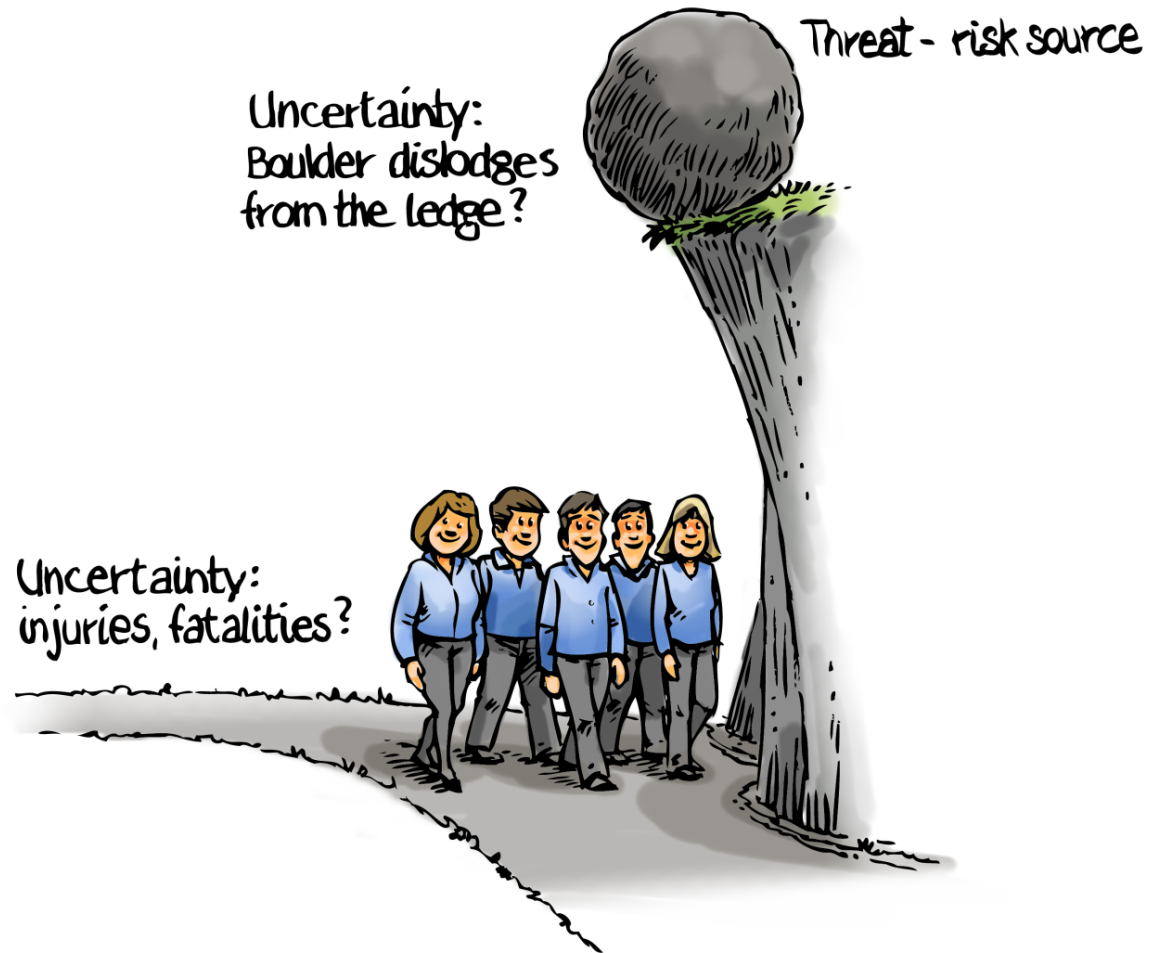
# The 'swiss cheese' model



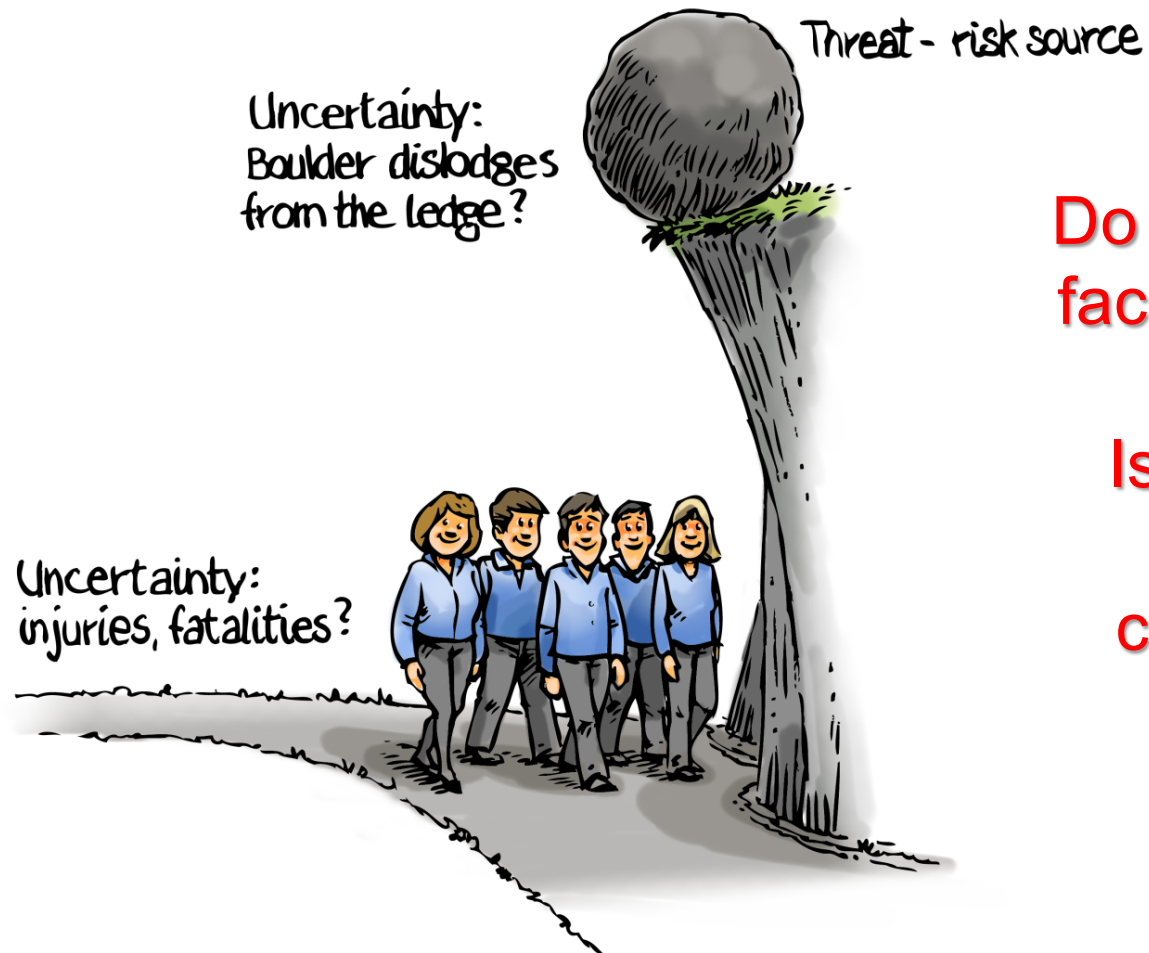
# THE CONCEPT OF RISK:



# The Risk Concept



# The Risk Concept



Do these people  
face risk? Why?

Is probability  
needed to  
conclude on  
this?

# The Risk Concept

## Consequences

Events with  
some effects

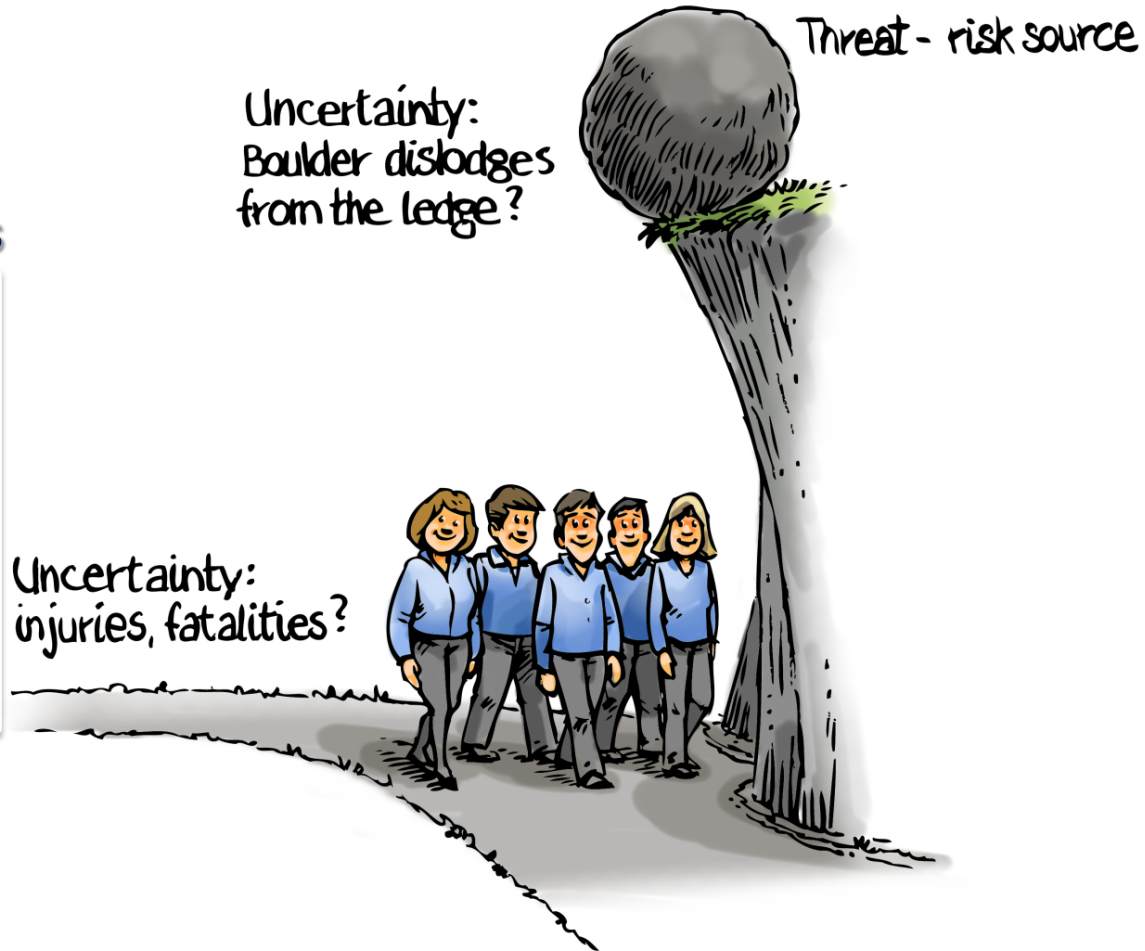
Some  
effects are  
undesirable

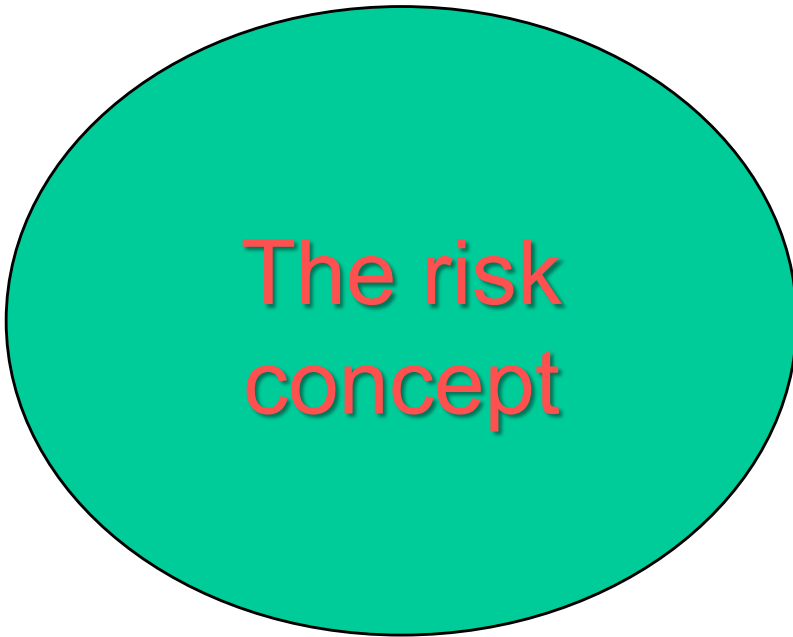
Uncertainty:  
Boulder dislodges  
from the ledge?

Threat - risk source

Uncertainty:  
injuries, fatalities?

Uncertainty





Consequences  
& Uncertainty

# Risk

---

**RISK = POTENTIAL DAMAGE + UNCERTAINTY**

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

- |   |   |                             |
|---|---|-----------------------------|
| 1) What undesired conditions may occur? | ➔ | Accident Scenario, <b>S</b> |
| 2) With what probability do they occur? | ➔ | Probability, <b>p</b>       |
| 3) What damage do they cause?           | ➔ | Consequence, <b>x</b>       |


$$\mathbf{RISK} = \{\mathbf{S}_i, \mathbf{p}_i, \mathbf{x}_i\}$$

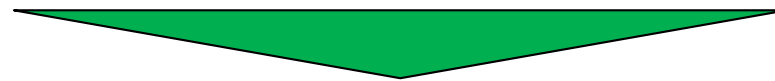
# RISK ASSESSMENT



# Risk

---

- 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**



$$\text{RISK} = \{\mathbf{S}_i, \mathbf{p}_i, \mathbf{x}_i\}$$

# RISK ASSESSMENT:

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



**System/Man/Environment  
interactions under uncertainty**



**PROBABILISTIC RISK ASSESSMENT  
(QUANTITATIVE RISK ASSESSMENT)**

KNOWLEDGE K

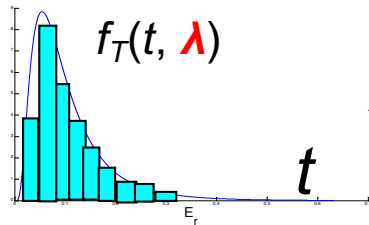
valve 1



valve 2



valve N

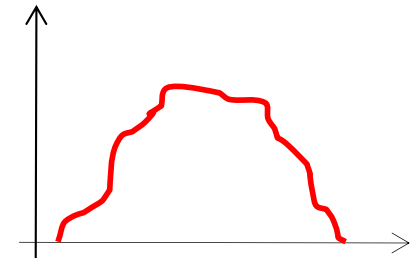
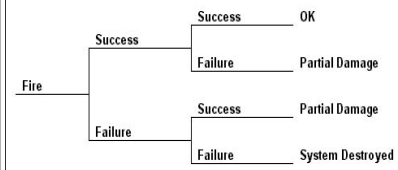


“ $\lambda$  is **UNIFORM** between  $10^{-3}$  and  $10^{-2}$  [h<sup>-1</sup>]”



“ $\lambda$  is less than  $10^{-2}$  [h<sup>-1</sup>] with probability 0.9”

**SYSTEM RISK MODEL**



**(UNCERTAIN) RISK MEASURES (a,c,u,M,K)**

**REPRESENTATION OF UNCERTAINTY (M)**

**UNCERTAINTY PROPAGATION**

KNOWLEDGE K

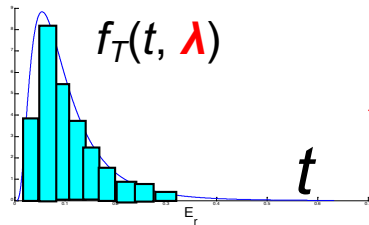
valve 1



valve 2



valve N

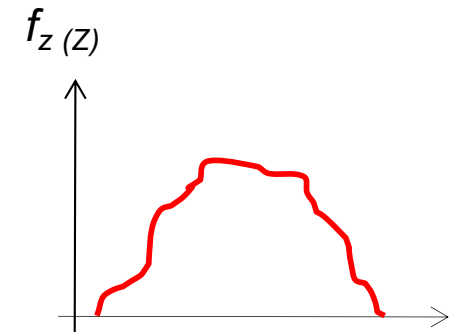
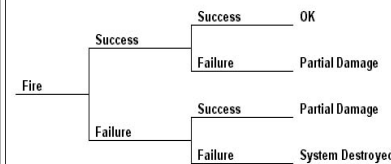


“ $\lambda$  is **UNIFORM** between  $10^{-3}$  and  $10^{-2}$  [h<sup>-1</sup>]”



“ $\lambda$  is less than  $10^{-2}$  [h<sup>-1</sup>] with probability 0.9”

**SYSTEM RISK MODEL**

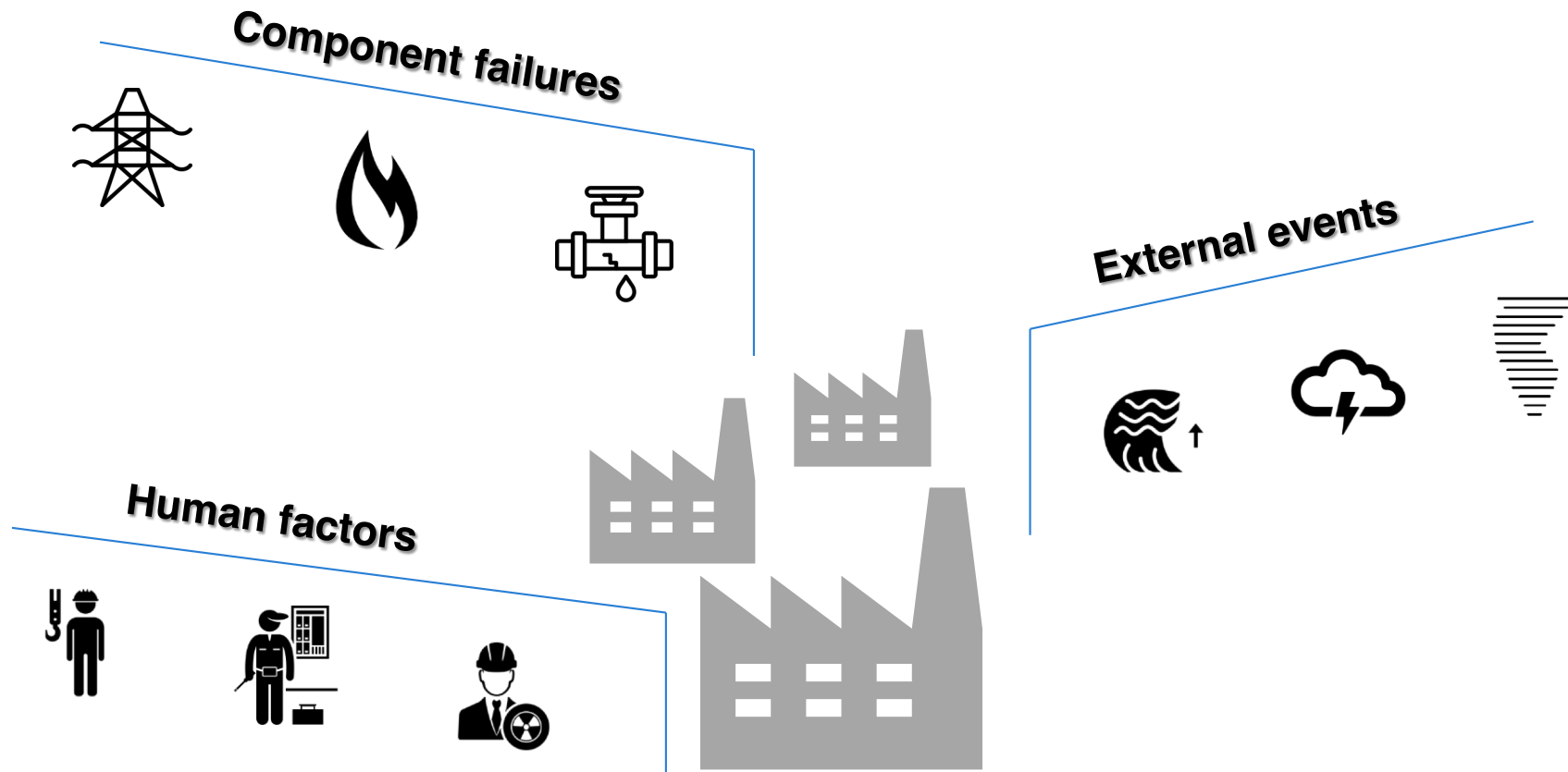


**(PROBABILISTIC) RISK MEASURES (a,c,u,P,K)**

**PROBABILISTIC REPRESENTATION OF UNCERTAINTY (M=P)**

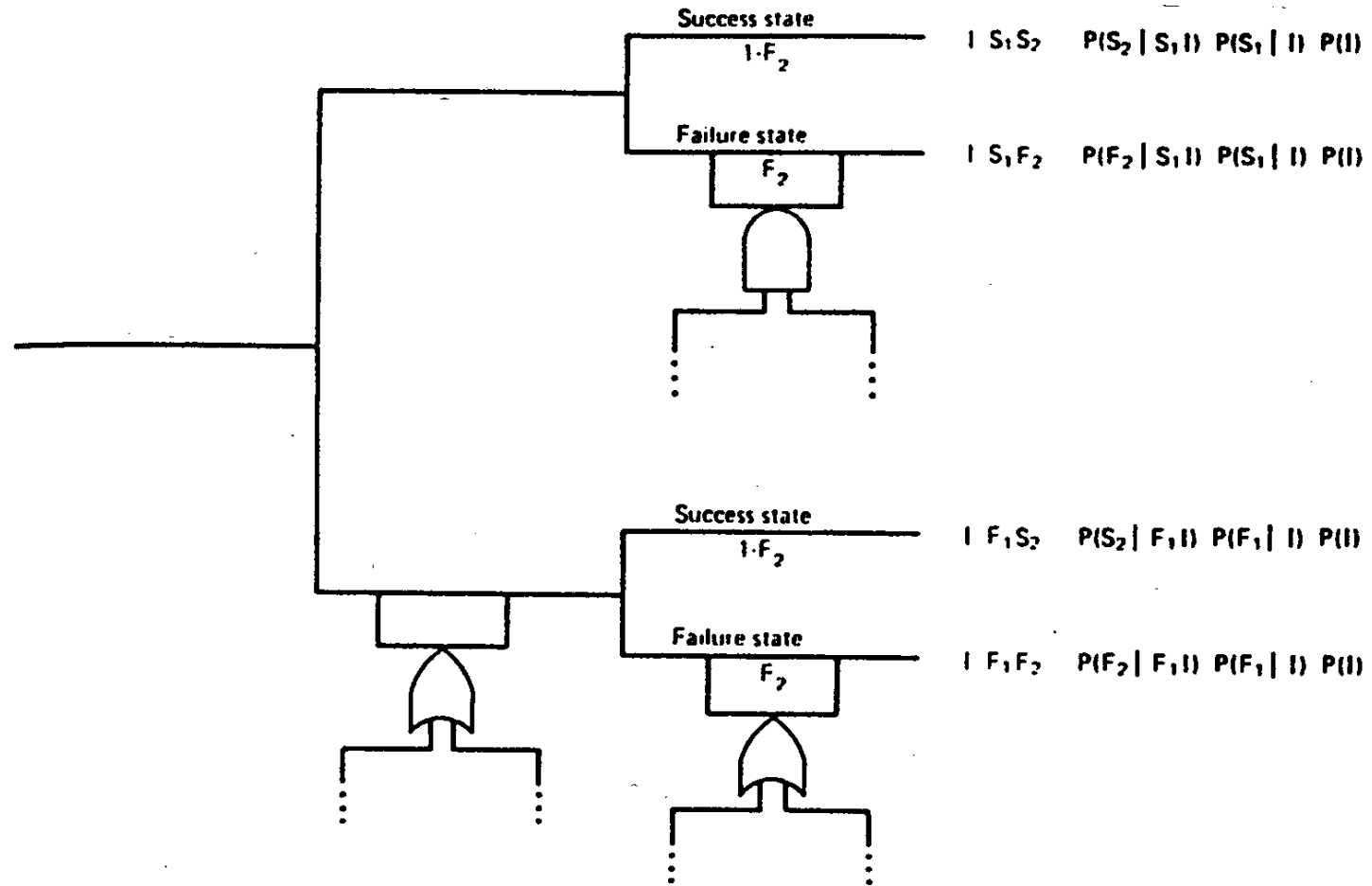
**UNCERTAINTY PROPAGATION**

# HAZARDS

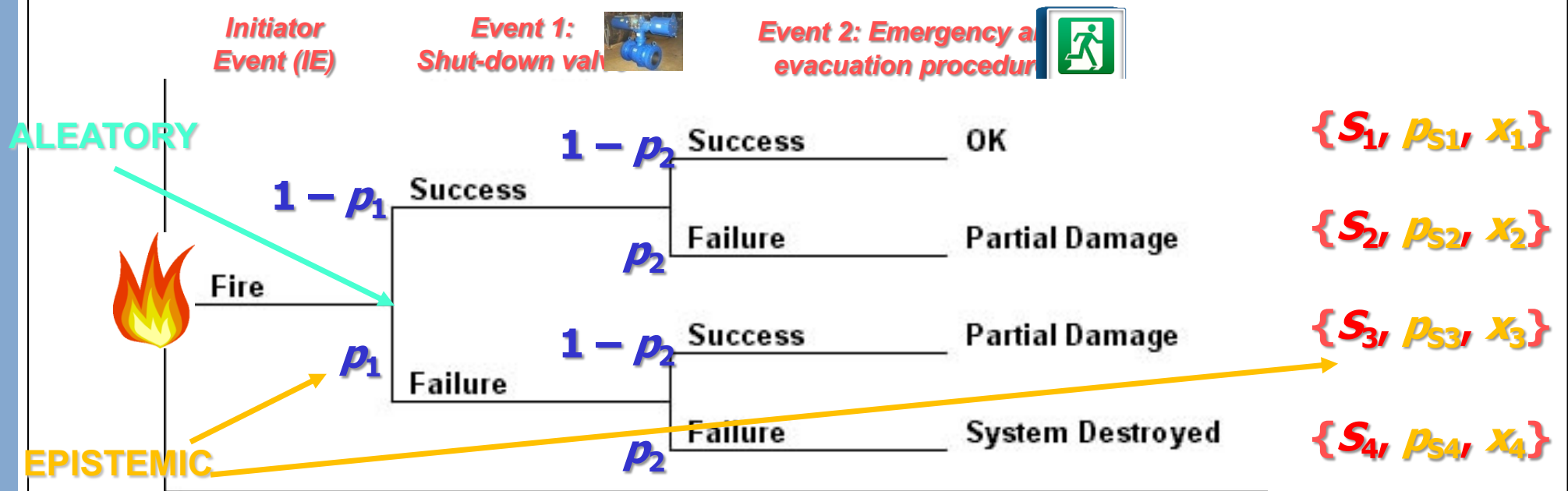




# Event Trees/Fault Trees



# (aleatory and epistemic) Uncertainty



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

**Epistemic: lack of knowledge/information** (probability and consequence models)

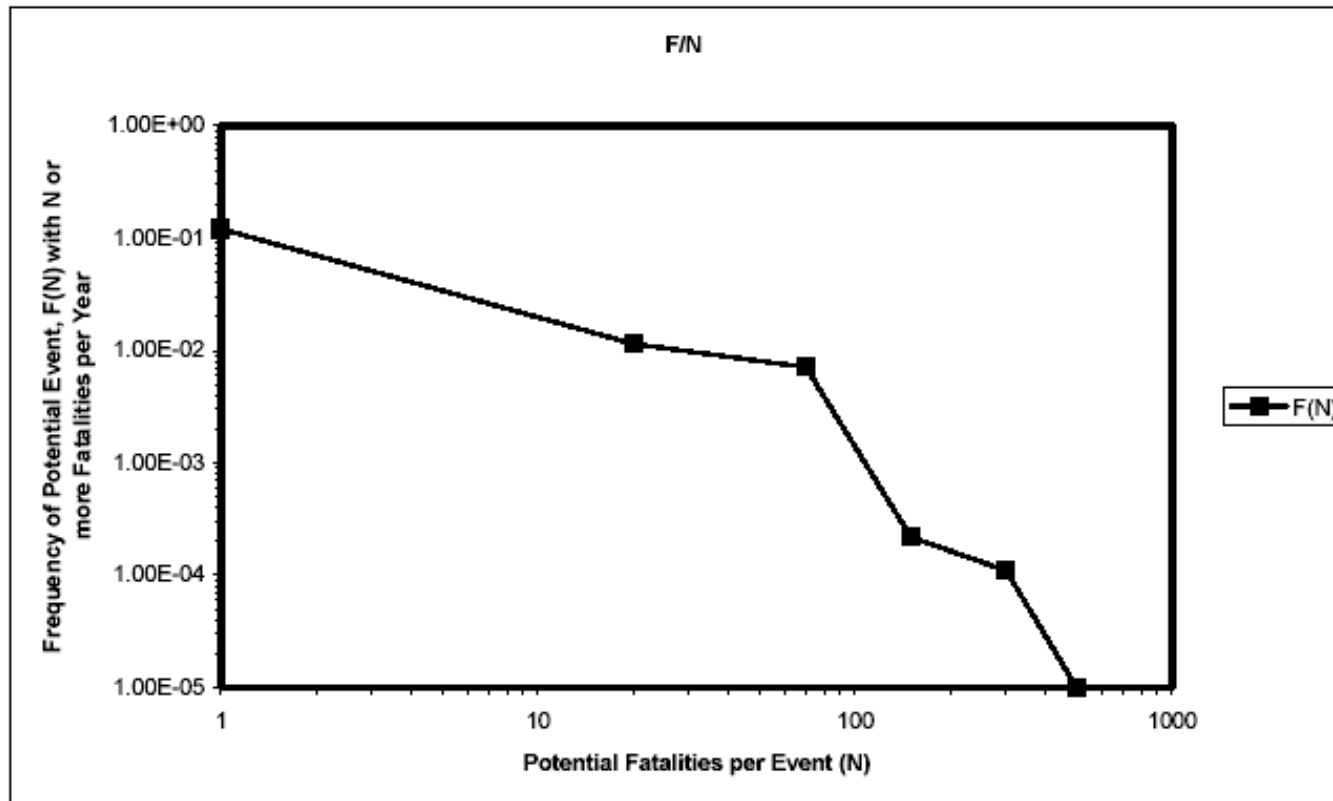
# PRA results:

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

<b>S</b>	<b>p</b>	<b>x</b>
<b>S<sub>1</sub></b>	<b>p<sub>1</sub></b>	<b>x<sub>1</sub></b>
<b>...</b>	<b>...</b>	<b>...</b>
<b>S<sub>N</sub></b>	<b>p<sub>N</sub></b>	<b>x<sub>N</sub></b>

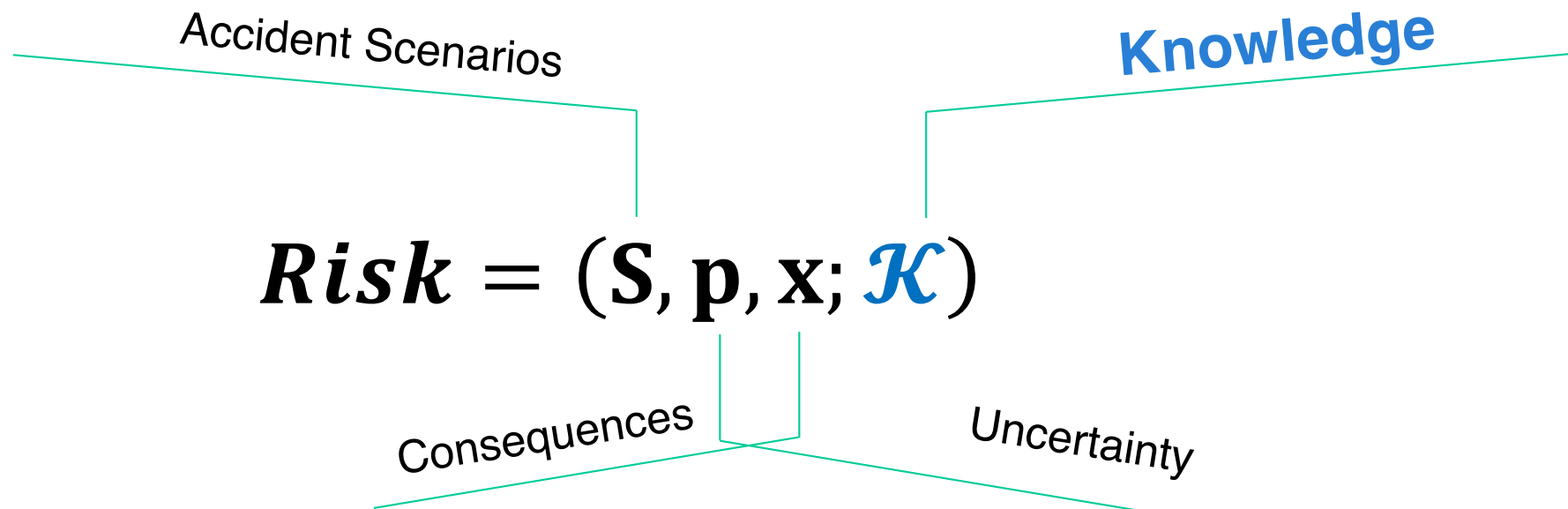
# Example of F/N graph

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	0.00022
5	300	0.00009	0.00011
6	500	0.00001	0.00001





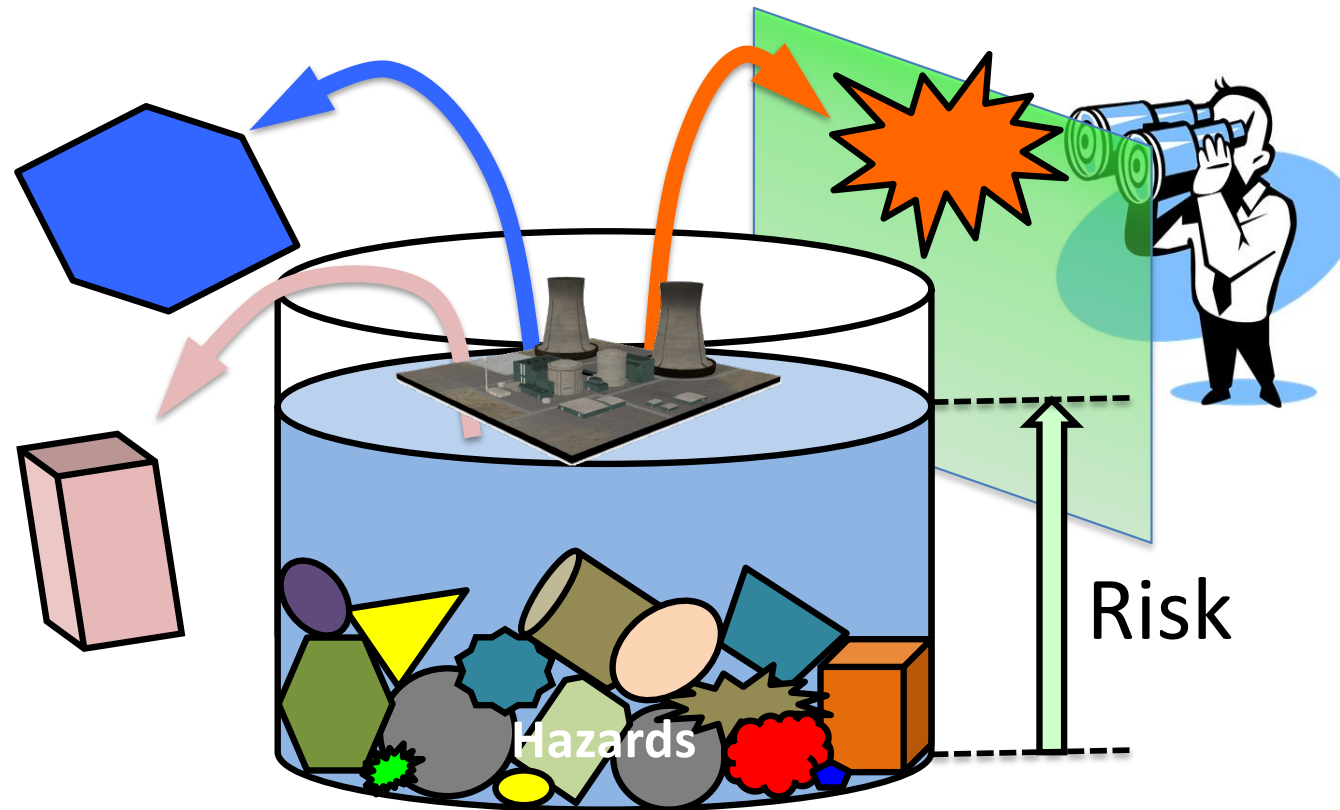
# Risk assessment – a knowledge “exercise”



Apostolakis G. The concept of probability in safety assessments of technological systems. Science. 1990  
Aven T, Zio E, Knowledge in Risk Assessment and Management, Wiley; 2018.

# Risk management

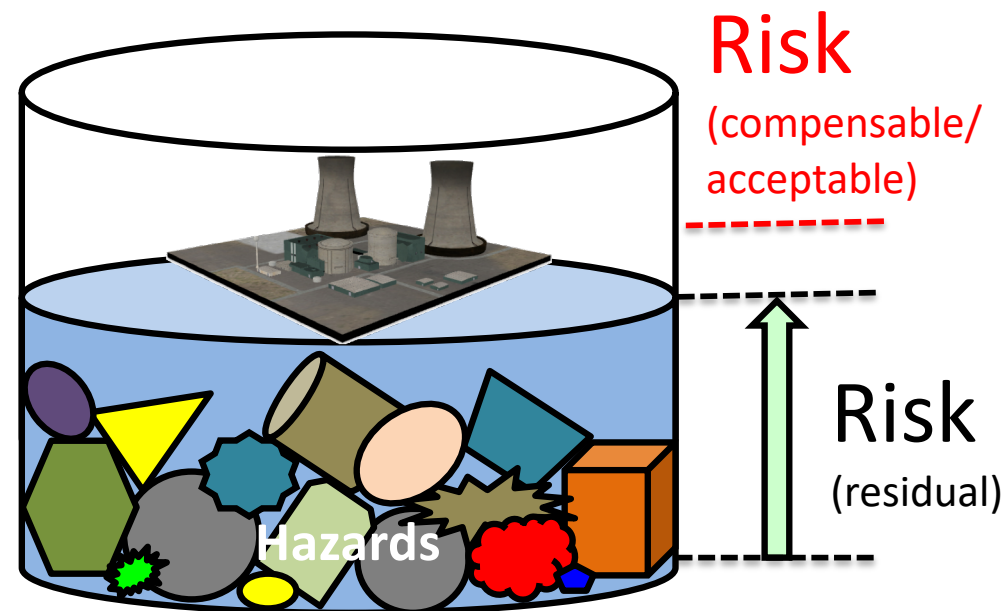
# Risk management



A. Yamaguchi, PSAM 12, 2016

T. Aven and E. Zio, Foundational Issues in Risk Assessment and Risk Management, Risk Analysis, Vol. 34(7), 2014

# Risk management



A. Yamaguchi, PSAM 12, 2016

T. Aven and E. Zio, Foundational Issues in Risk Assessment and Risk Management, Risk Analysis, Vol. 34(7), 2014

# 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

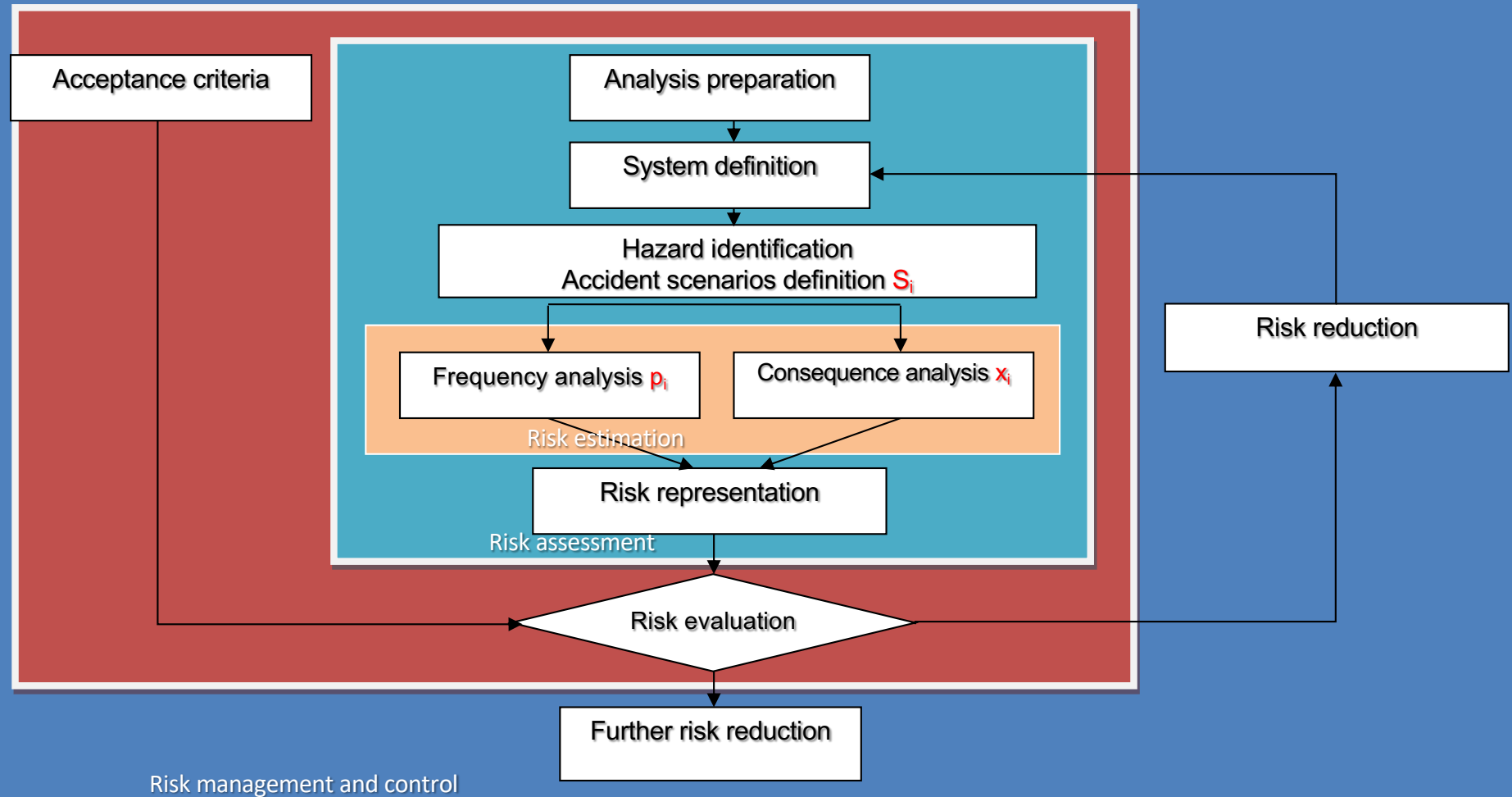


# Risk-Informed Decision Making (2)

- **PRA**s provide this information to the DM
  - PRA
s do not predict the future
- PRA
s evaluate and assess potential accident scenarios to **inform the decision makers' current state of knowledge.**

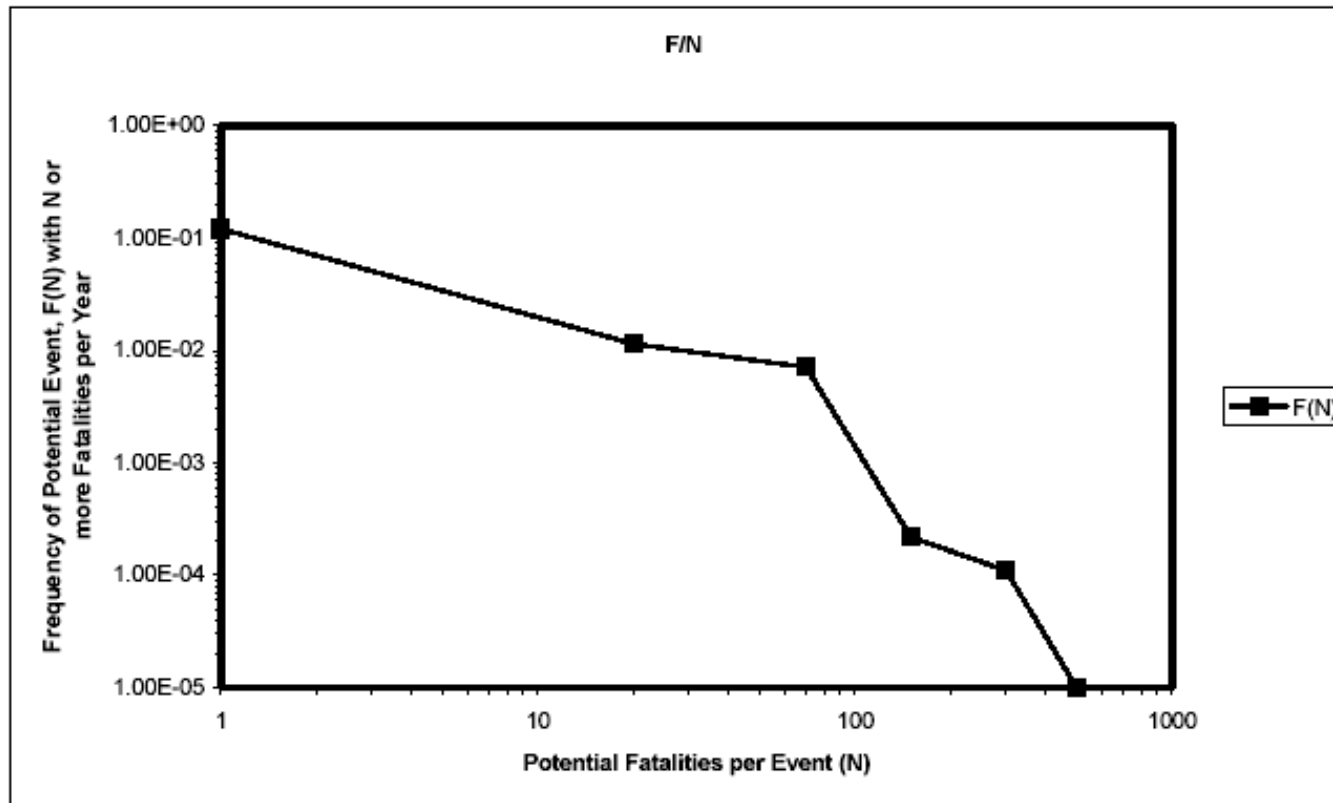
**PRA = Probabilistic Risk Assessment**

# Risk Assessment and Management

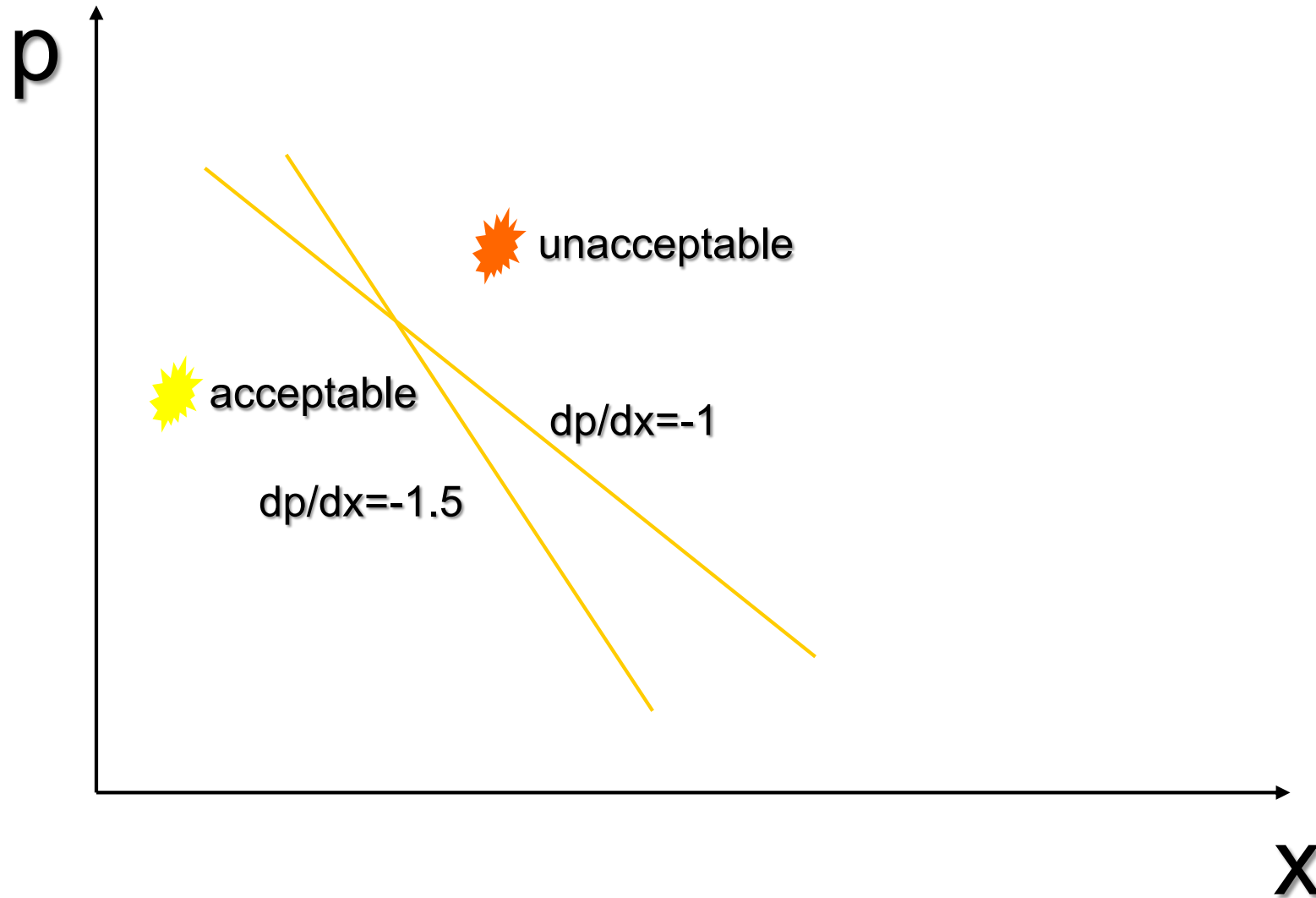


# Example of F/N graph

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	0.00022
5	300	0.00009	0.00011
6	500	0.00001	0.00001



# FARMER'S CURVE:



# RISK MATRIX:

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

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	<b>Continuous Improvement</b>					
2	Minor health effect / injury	Minor effect	Minor damage	Minor impact						
3	Major health effect / injury	Local effect	Local damage	Local impact	<b>Intolerable Risk</b>					
4	PTD(*) or 1 fatality	Major effect	Major damage	National impact						
5	Multiple fatalities	Extensive effect	Extensive damage	International impact						

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



# Main strategies for handling risk

Codes and standards – simple problems

Risk assessment  
informed

Robustness, resilience-  
based strategies

Dialogue

Cautionary/  
precautionary  
principles

Balancing other concerns

# Balance

## Development and protection

Develop,  
creating values  
  
Take risk



Reduce the risks  
and uncertainties

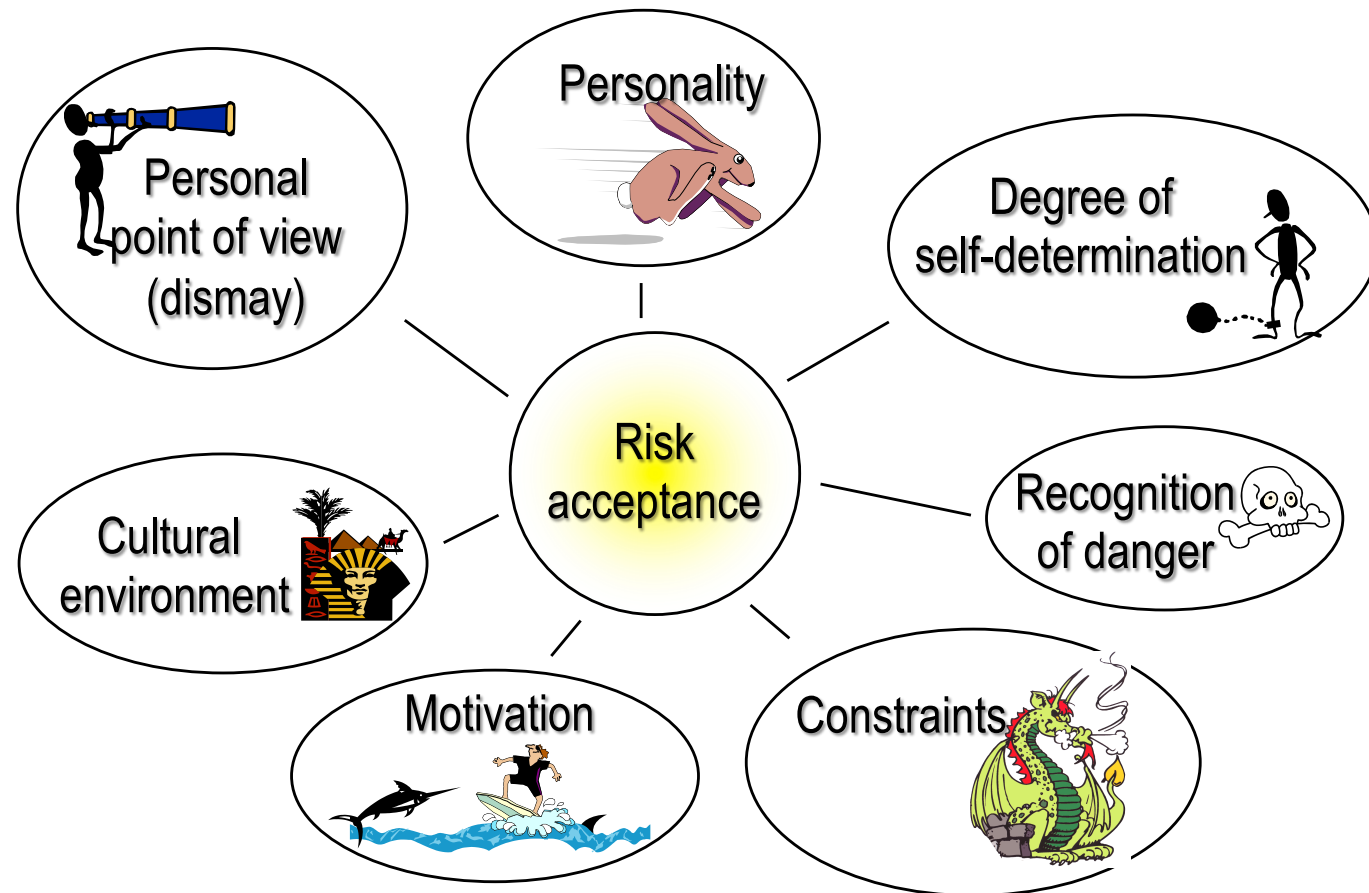
Cost-benefit analyses

ALARP

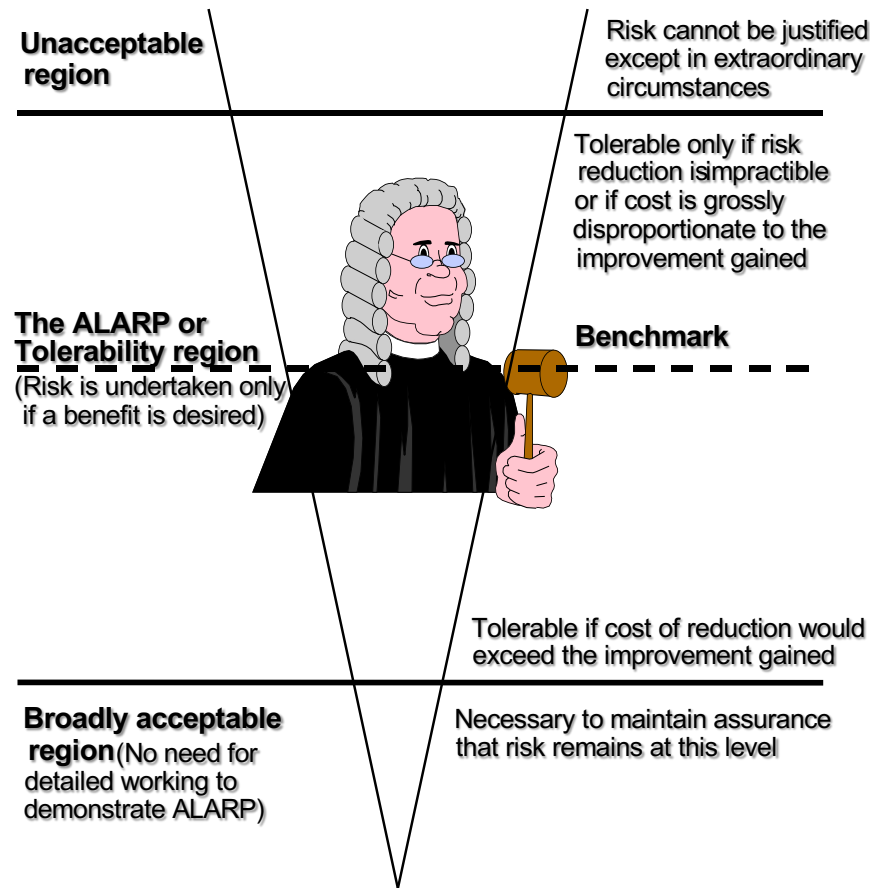
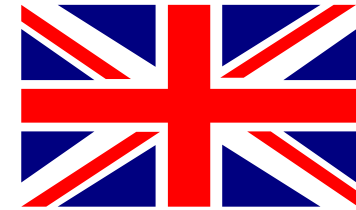
cautionary-  
precautionary

Risk acceptance criteria

# Risk Acceptance



# Risk Acceptance: ALARP



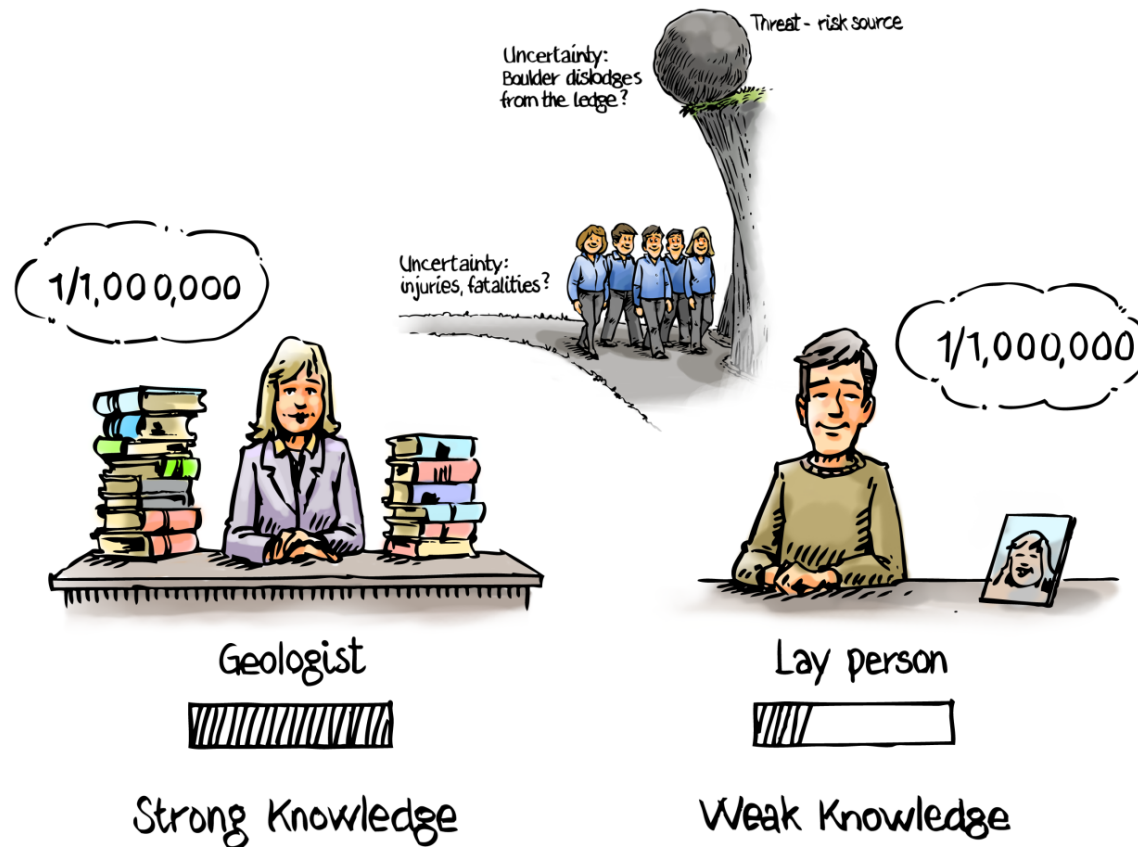
- Any risk should be “as low as reasonably practicable”. In this context ‘reasonable’ stands for ‘economical’ (Value of Prevented Fatality)

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)

# Expressing risk

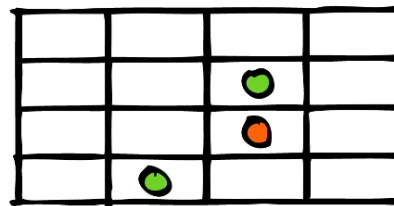
Consequences + Probability + Knowledge





# Consequences + Probability + Knowledge

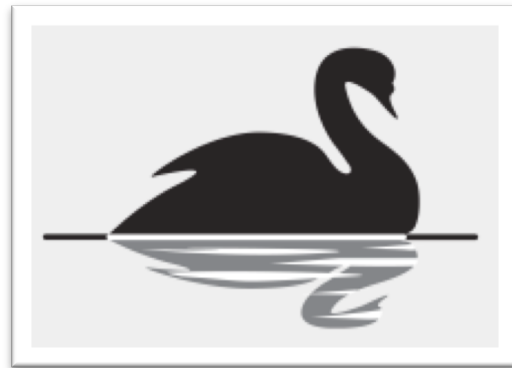
Consequences



Probability

- 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?

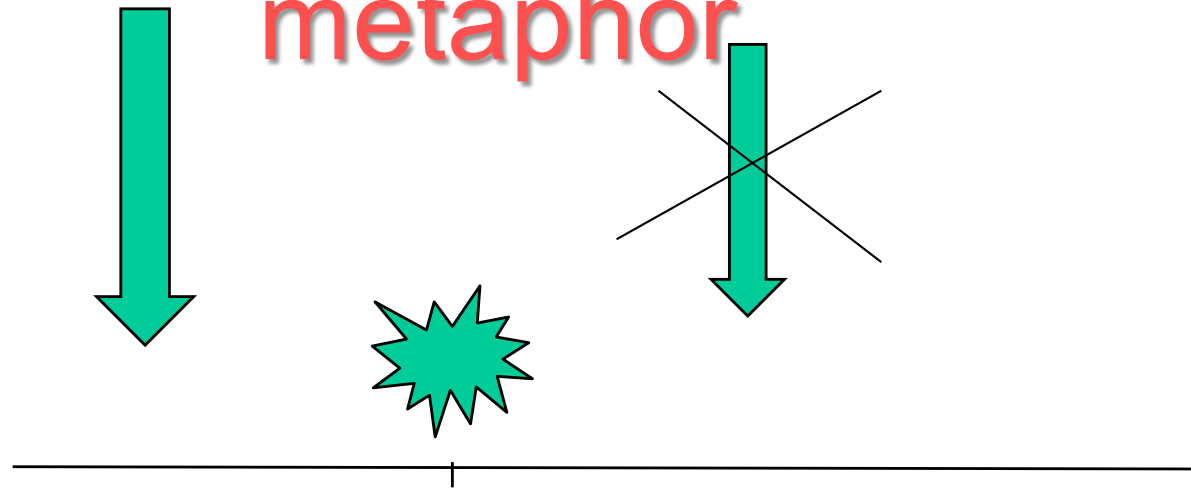
*A surprising, extreme event relative to  
one's knowledge/beliefs*

*A surprise  
for some*

*Not a  
surprise  
for others*

**Unknown  
knowns**

# The black swan metaphor



## Surprise

Focus on the knowledge  
Assumptions

Signals and warnings

How can the knowledge be strengthened



# 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

# Classical Techniques for Risk Assessment

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

# FAILURE MODES AND EFFECTS ANALYSIS

- **Qualitative**
- **Inductive**

## **AIM:**

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

# FMEA: Procedure steps

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



- 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)

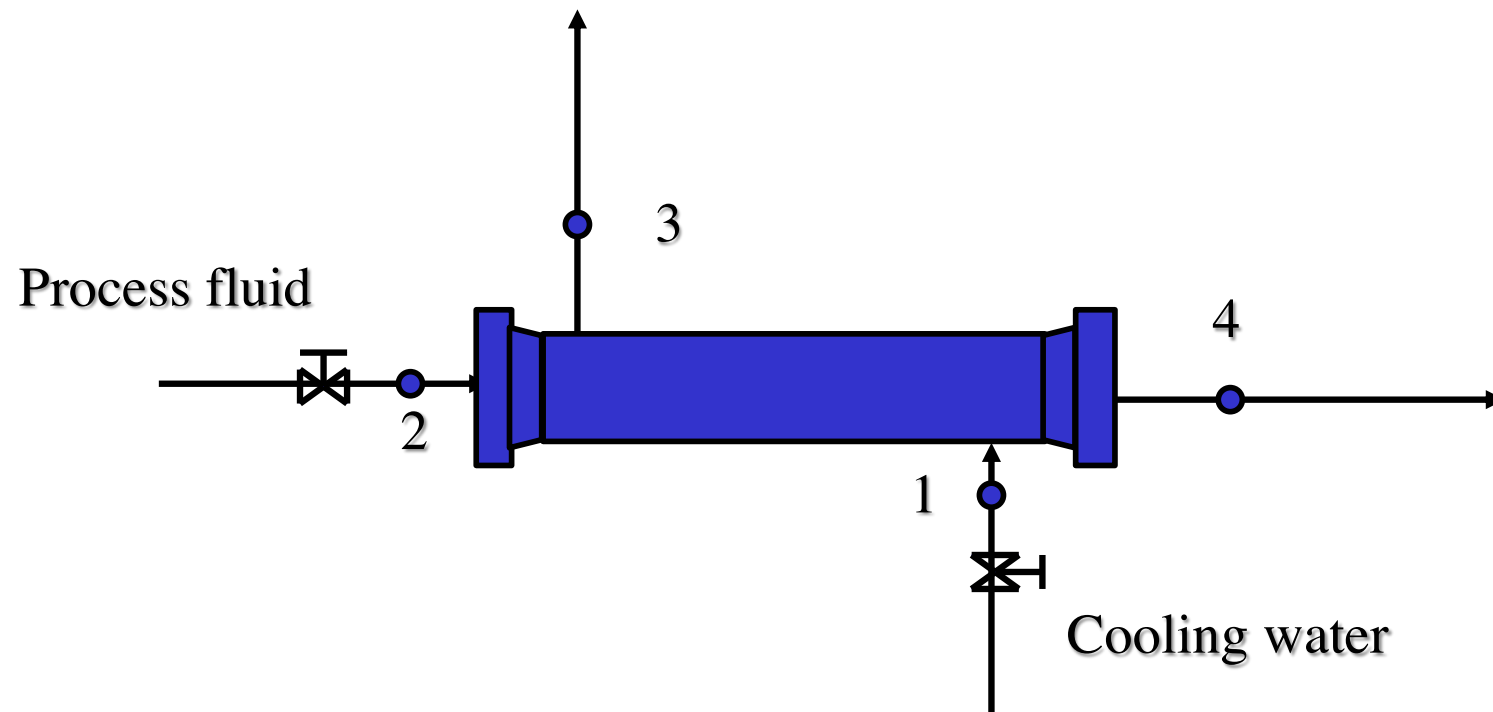
## Hazop: example

**SYSTEM: shell & tube heat exchanger**

**Study Node: 1**

**Operational Mode: Nominal Conditions**

**Design Intent:  $P=2\text{bar}$ ,  $T=20^\circ\text{C}$ ,  $\text{Flow}=1\text{l/sec}$**



# HAZOP: Table

Study title:				Page:        of					
Drawing no.:		Rev no.:		Date:					
HAZOP team:				Meeting date:					
Part considered:									
Design intent:		Material:		Activity:					
		Source:		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



# FAILURES



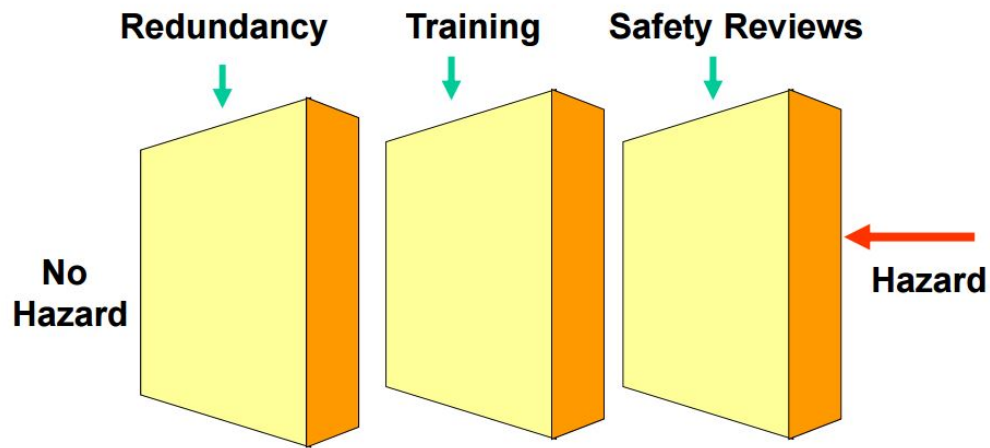


## Failures

Prevented by

Design for Reliability/Availability

Maintenance

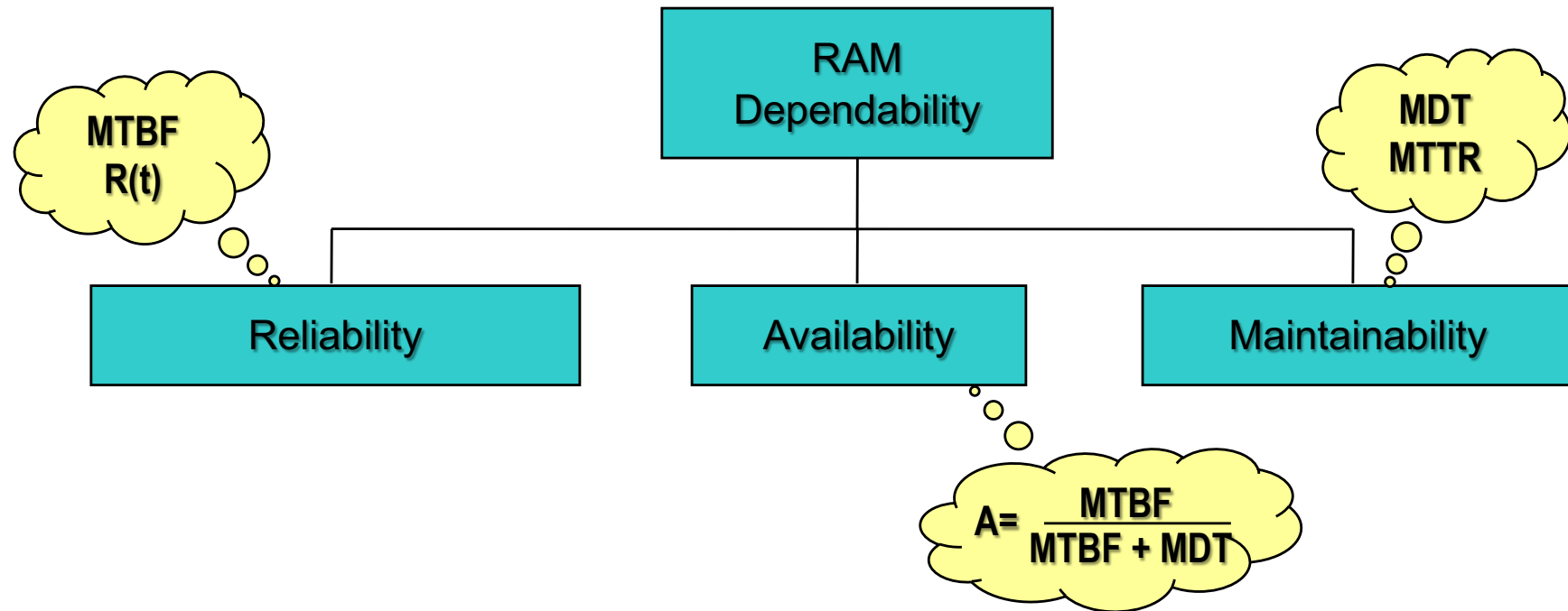




- RAM background:

RAM = Reliability, Availability, Maintainability





- Definition under IEC 50 (191):
- Summarising expression to describe **availability** and its influencing factors, **reliability** and **maintainability**.
- *Note:* Dependability is only used for general descriptions of non-quantitative character.
- Broad definition:
- Dependability is the methodical approach of **estimating**, **analysing** and **avoiding** failures in the future.

- **Reliability and availability:** important performance parameters of a system, with respect to its ability to fulfill the required mission in a given period of time



- Two different system types:
  - Systems which must satisfy a specified mission within an assigned period of time: **reliability** quantifies the ability to achieve the desired objective without failures
  - Systems maintained: **availability** quantifies the ability to fulfill the assigned mission at **any** specific moment of the life time

## Maintainability:

Ability of a unit, under given circumstances, to maintain or respectively to reset its actual state so that the desired requirements are met, provided that maintenance is carried out using the specified resources and stated procedures.



- RAM background:  
Component reliability

***Reliability* is the ability of an item to perform a required function under stated conditions for a stated period of time.**

**Therefore....  
the *failure* is an event whereby a unit or component under consideration is no longer capable of fulfilling a required function under stated conditions for a stated the period of time.**

## Basic definitions (2)

The *required function* includes the specification of satisfactory operation as well as unsatisfactory operation. For a complex system, unsatisfactory operation may not be the same as failure.

The *stated conditions* are the total physical environmental including mechanical, thermal, and electrical conditions.

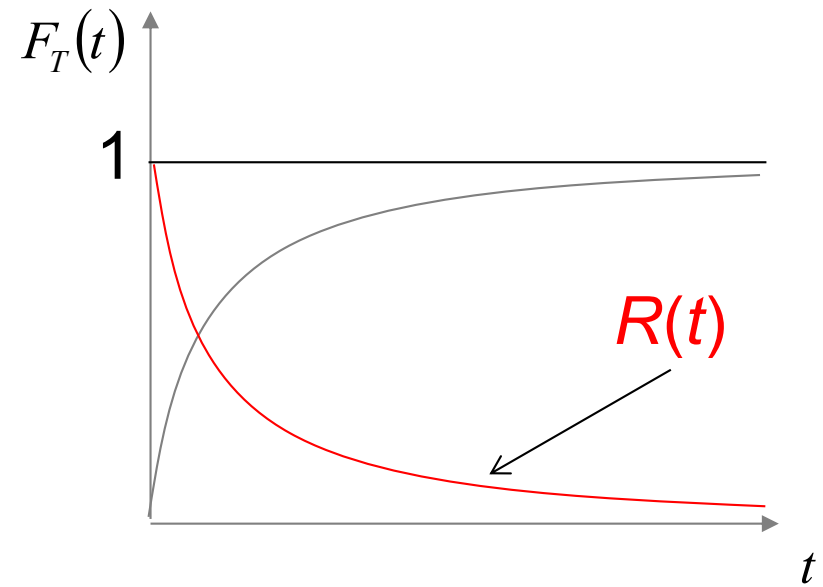
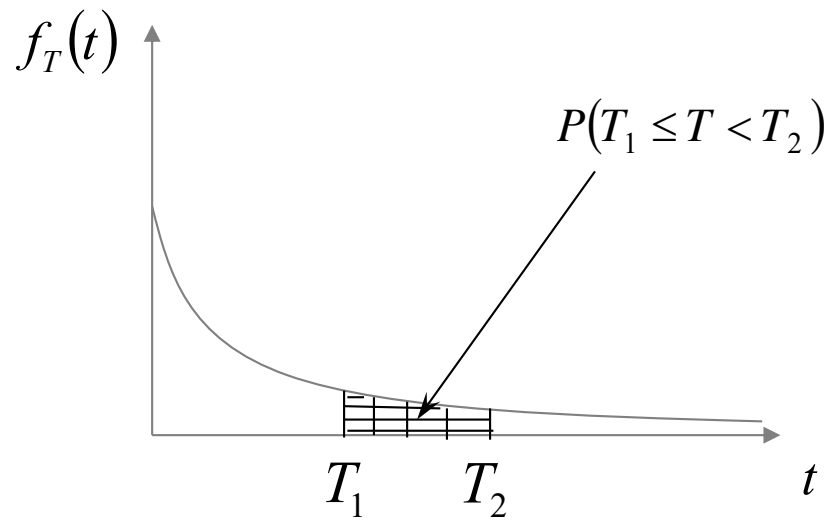
The *stated period of time* is the time during which satisfactory operation is desired, commonly referred to as service life.

- $T$  = Time to failure of a component (random variable)
  - cdf =  $F_T(t)$  = probability of failure before time  $t$ :  $P(T < t)$
  - pdf =  $f_T(t)$  = probability density function at time  $t$ :  
$$f_T(t)dt = P(t < T < t + dt)$$
  - ccdf =  $R(t) = 1 - F_T(t)$  = reliability at time  $t$ :  $P(T > t)$
  - $h_T(t)$  = **hazard function** or failure rate at time  $t$

$$h_T(t)dt = P(t < T \leq t + dt \mid T > t) = \frac{P(t < T \leq t + dt)}{P(T > t)} = \frac{f_T(t)dt}{R(t)}$$



# Basic definitions (4)



# Hazard function: the bath-tub curve

## Three types of failures:

- **Early failures** (Infant mortality), caused by errors in design, defects in manufacturing, etc..

Characteristic: The failure rate is initially high, but rapidly decreases.

- **Wear-out failures**, caused by ageing.

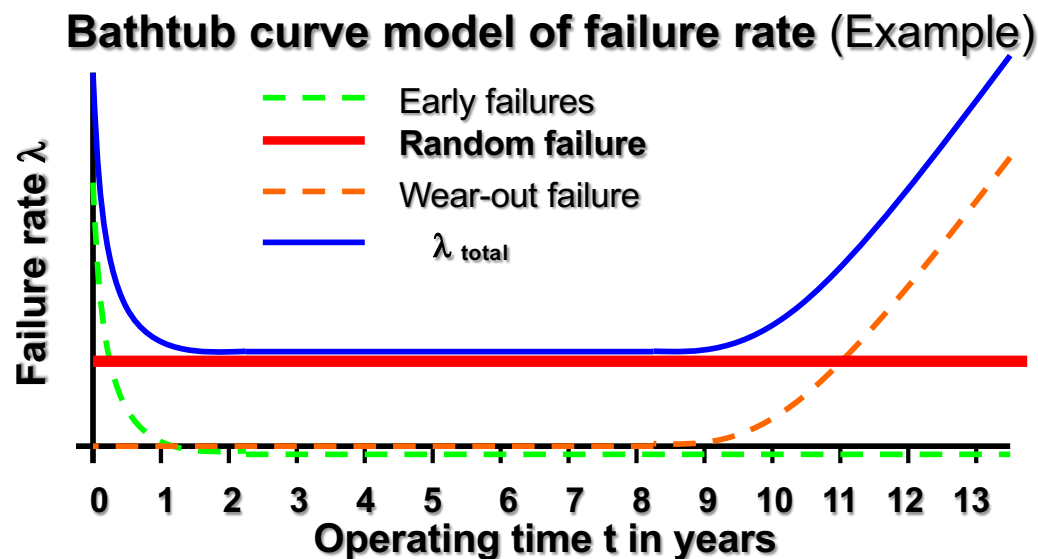
Characteristic: The failure rate increases monotonically.

(Both types are systematic failures and could be prevented by improvement in design, manufacturing, maintenance).

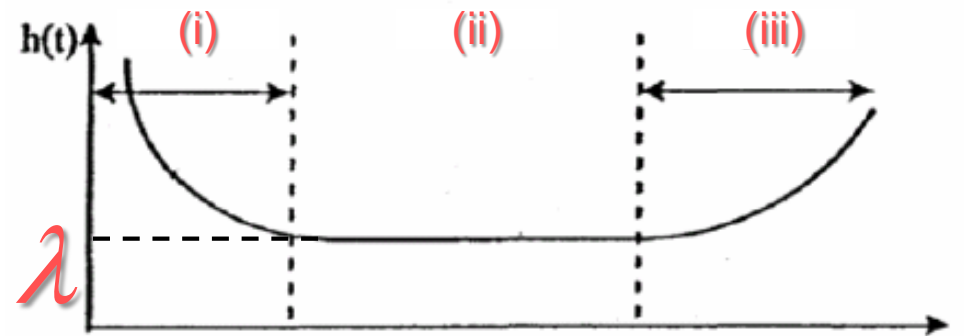
- **Random failure**: appear spontaneously and purely by chance.

Characteristic: Constant failure rate during the whole lifetime of the units.

**These types of failure rates result in the traditional bathtub curve**



- The hazard function shows three distinct phases:
  - i. Decreasing - *infant mortality* or *burn in period*
  - ii. Constant - *useful life*
  - iii. Increasing - *ageing*

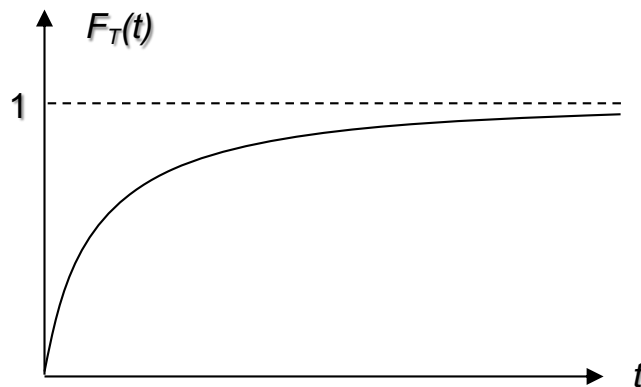


The unit of the failure rate  $\lambda$  is failure/time, often indicated as FIT (Failure in Time).  
e.g. 1 FIT = 1 Failure per  $10^9$ h in FRU (Field Replaceable Unit) employed in the railway industry

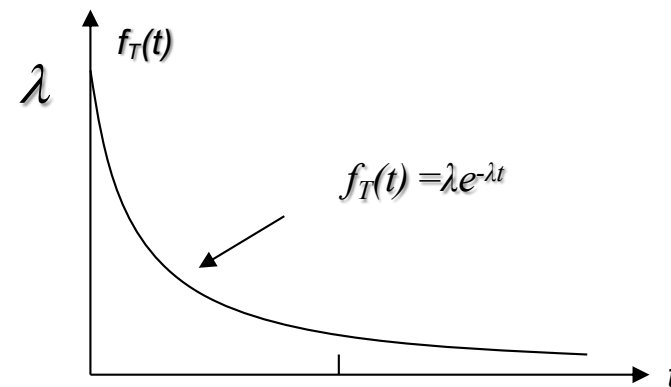
# The exponential distribution (1)

- $h_T(t) = \lambda, t \geq 0$

$$F_T(t) = P(T \leq t) = 1 - e^{-\lambda t}$$



$$\begin{cases} f_T(t) = \lambda e^{-\lambda t} & t \geq 0 \\ = 0 & t < 0 \end{cases}$$



- Only distribution characterized by a constant hazard rate
- Widely used in reliability practice to describe the constant part of the bath-tub curve

# The exponential distribution (2)

- The expected value and variance of the distribution are:

$$E[T] = \frac{1}{\lambda} = MTTF \quad ; \quad Var[T] = \frac{1}{\lambda^2}$$

- Failure process is **memoryless**



$$\begin{aligned} P(t_1 < T < t_2 | T > t_1) &= \frac{P(t_1 < T < t_2)}{P(T > t_1)} = \frac{F_T(t_2) - F_T(t_1)}{1 - F_T(t_1)} = \\ &= \frac{e^{-\lambda t_1} - e^{-\lambda t_2}}{e^{-\lambda t_1}} = 1 - e^{-\lambda(t_2 - t_1)} \end{aligned}$$

- In practice, the age of a component influences its failure process so that the hazard rate does not remain constant throughout the lifetime

$$F_T(t) = P(T \leq t) = 1 - e^{-\lambda t^\alpha}$$

$$\begin{cases} f_T(t) = \lambda \alpha t^{\alpha-1} e^{-\lambda t^\alpha} & t \geq 0 \\ = 0 & t < 0 \end{cases}$$

$$E[T] = \frac{1}{\lambda} \Gamma\left(\frac{1}{\alpha} + 1\right) \quad ; \quad Var[T] = \frac{1}{\lambda^2} \left( \Gamma\left(\frac{2}{\alpha} + 1\right) - \Gamma\left(\frac{1}{\alpha} + 1\right)^2 \right)$$

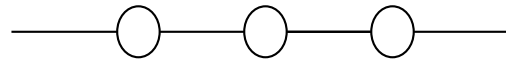
$$\Gamma(k) = \int_0^{\infty} x^{k-1} e^{-x} dx \quad k > 0$$





- RAM background:  
System reliability  
(simple)

- **Objective:**
  - Computation of the system reliability  $R(t)$
- **Hypotheses:**
  - $N$  = number of system components
  - The components' reliabilities  $R_i(t)$ ,  $i = 1, 2, \dots, N$  are known
  - The system **configuration** is known

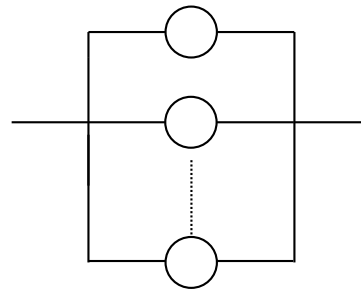


- All components must function for the system to function

$$R(t) = \prod_{i=1}^N R_i(t)$$

- For  $N$  **exponential** components:

$$\boxed{R(t) = e^{-\lambda t}} \longrightarrow \begin{cases} \lambda = \sum_{i=1}^N \lambda_i & \longrightarrow \text{System failure rate} \\ E[T] = \frac{1}{\lambda} & \longrightarrow \text{MTTF} \end{cases}$$



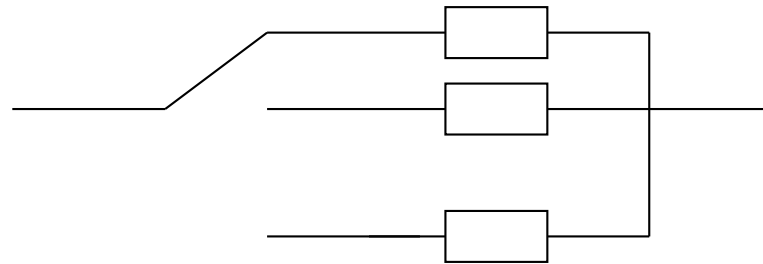
- All components must fail for the system to fail

$$R(t) = 1 - \prod_{i=1}^N [1 - R_i(t)]$$

- For  $N$  exponential components:

$$R(t) = 1 - \prod_{i=1}^N [1 - e^{-\lambda_i t}]$$

$$\left\{ \begin{aligned} MTF &= \sum_{i=1}^N \frac{1}{\lambda_i} - \sum_{i=1}^{N-1} \sum_{j=i+1}^N \frac{1}{[\lambda_i + \lambda_j]} + \\ &+ \sum_{i=1}^{N-2} \sum_{j=i+1}^{N-1} \sum_{k=j+1}^N \frac{1}{[\lambda_i + \lambda_j + \lambda_k]} - \dots + (-1)^{N-1} \frac{1}{\sum_{i=1}^N \lambda_i} \end{aligned} \right.$$



- One component is functioning and when it fails it is replaced immediately by another component (sequential operation of one component at a time)
- The system configuration is **time-dependent**  $\Rightarrow$  the story of the system from  $t = 0$  must be considered
- Two types of standby:
  - **Cold**: the standby unit cannot fail until it is switched on
  - **Hot**: the standby unit can fail also while in standby



- **RAM background:**  
System reliability and availability  
(complicated)

# FAULT TREE ANALYSIS



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

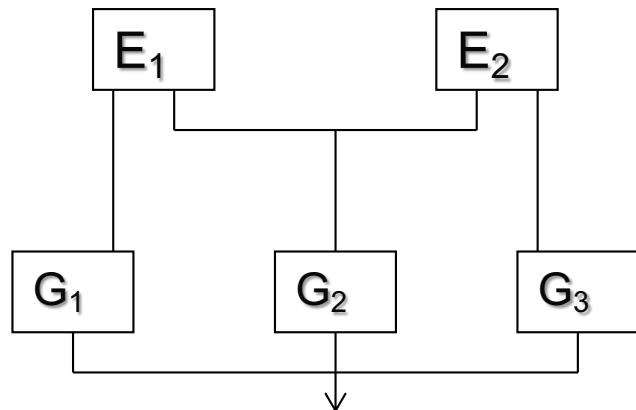
## **AIM:**

- 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

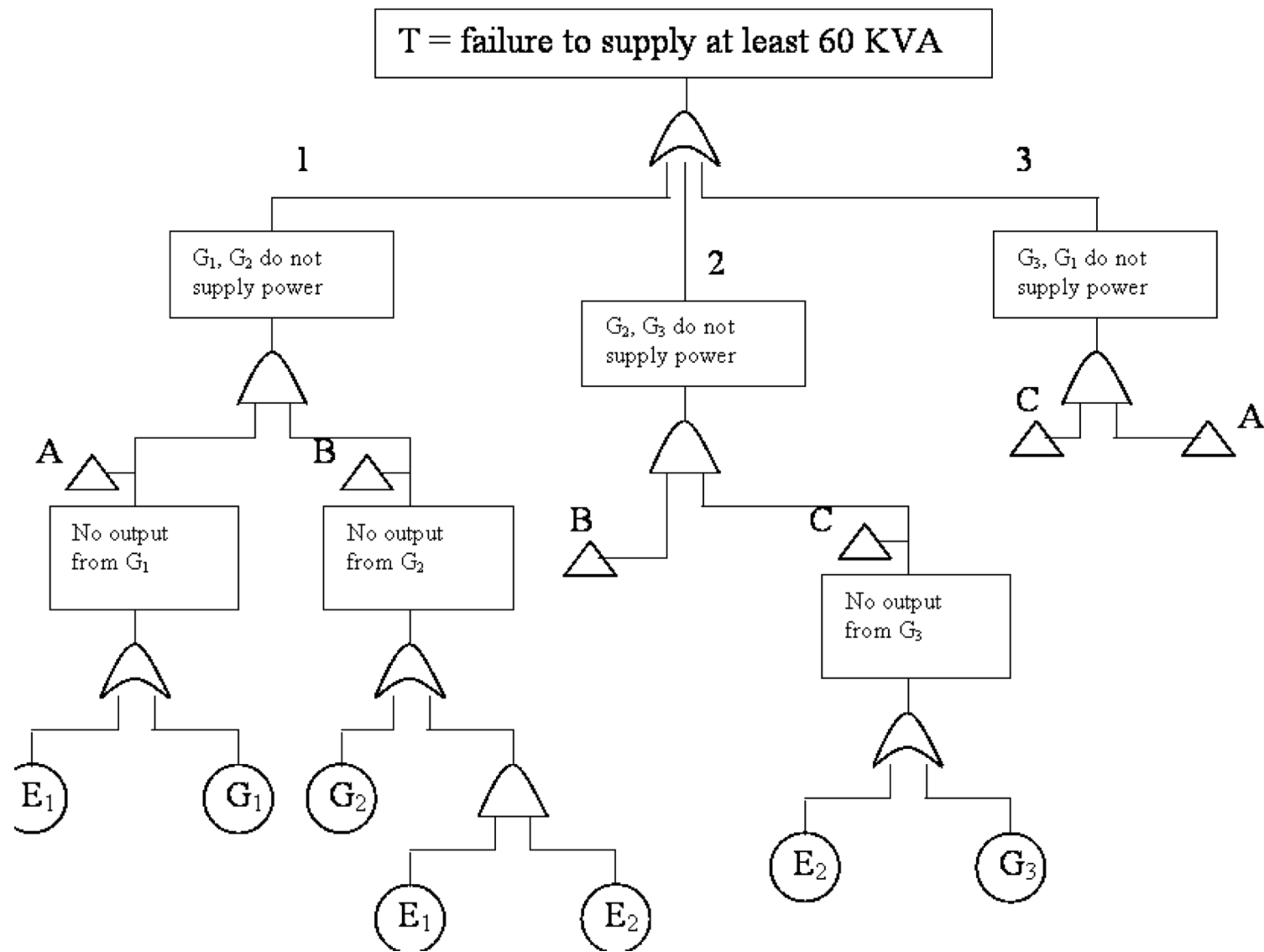
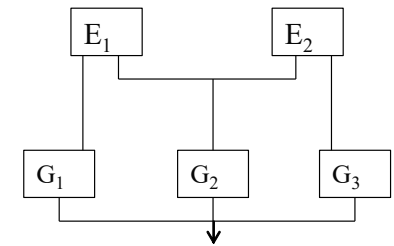


E1, E2 = engines

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:

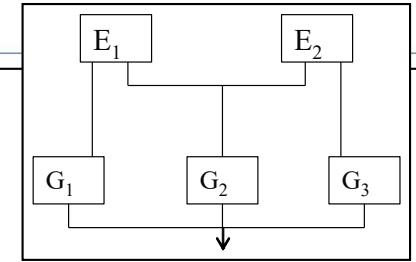
$X_i$  : binomial indicator variable of i-th component state (basic event)

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

- FT = set of boolean algebraic equations (one for each gate) => structure (switching) function  $\Phi$ :

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

# FT mcs: Example



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

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

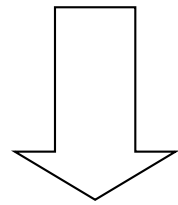
$$= 1 - [1 - X_{E_1} X_{G_2} - X_{E_1} X_{E_2} - X_{G_1} X_{G_2} + X_{E_1} X_{E_2} X_{G_2} + X_{E_1} X_{G_1} X_{G_2} + X_{E_1} X_{E_2} X_{G_1} X_{G_2} - X_{E_1} X_{E_2} X_{G_1} X_{G_2}] =$$

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

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

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

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



3 minimal cut sets:

$$M_1 = \{E_1 G_2\}$$

$$M_2 = \{E_1 E_2\}$$

$$M_3 = \{G_1 G_2\}$$

# 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**

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

**It can be shown that:**

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

# EVENT TREE ANALYSIS

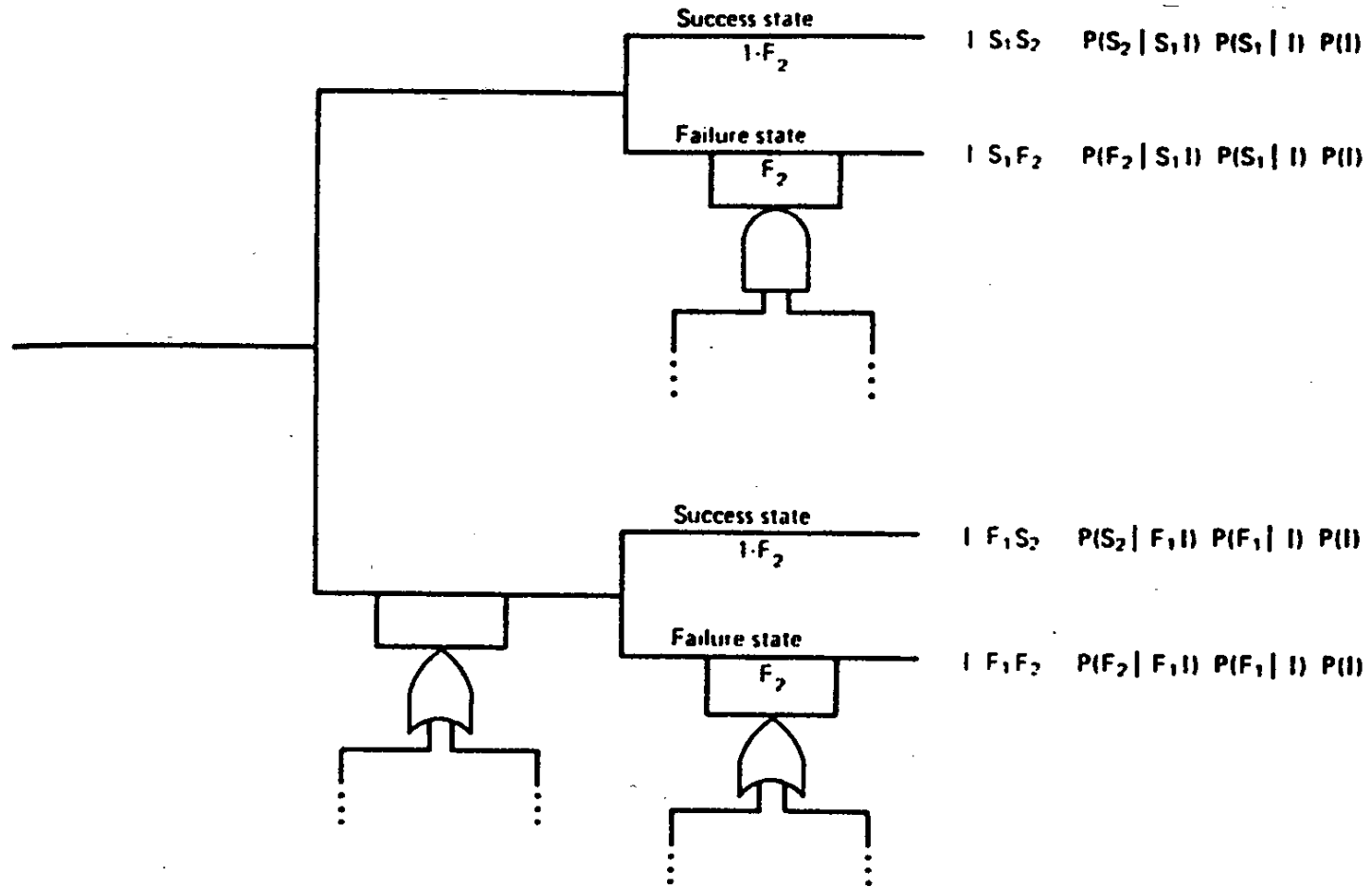
# Event Tree Analysis (ETA)

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

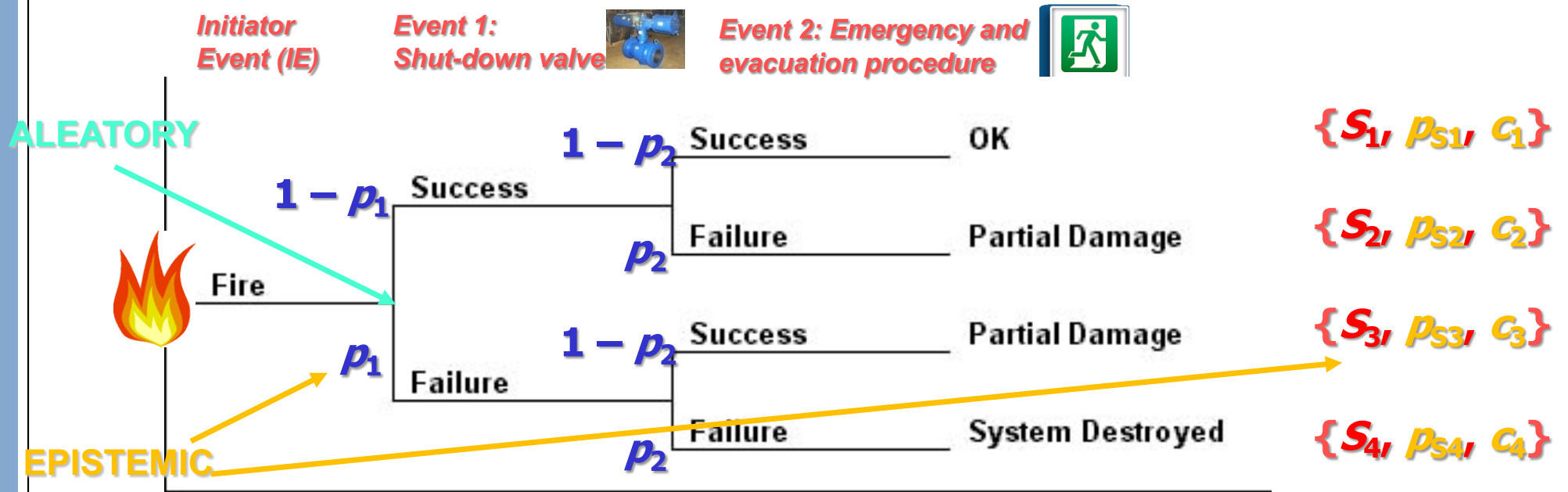
## **AIM:**

- 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)



- **RAM background:**  
System reliability and availability  
(complex)

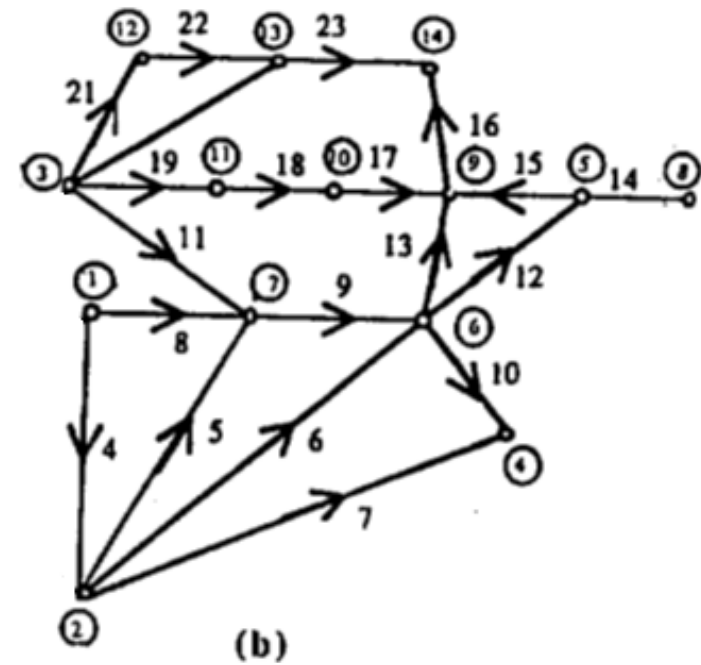
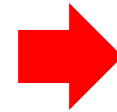
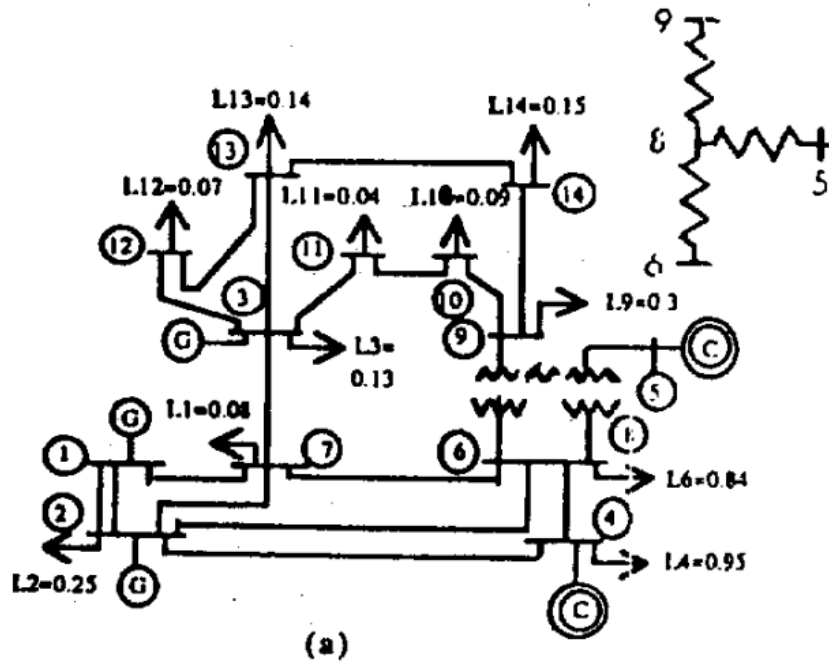


# Complex System (IEEE 14)

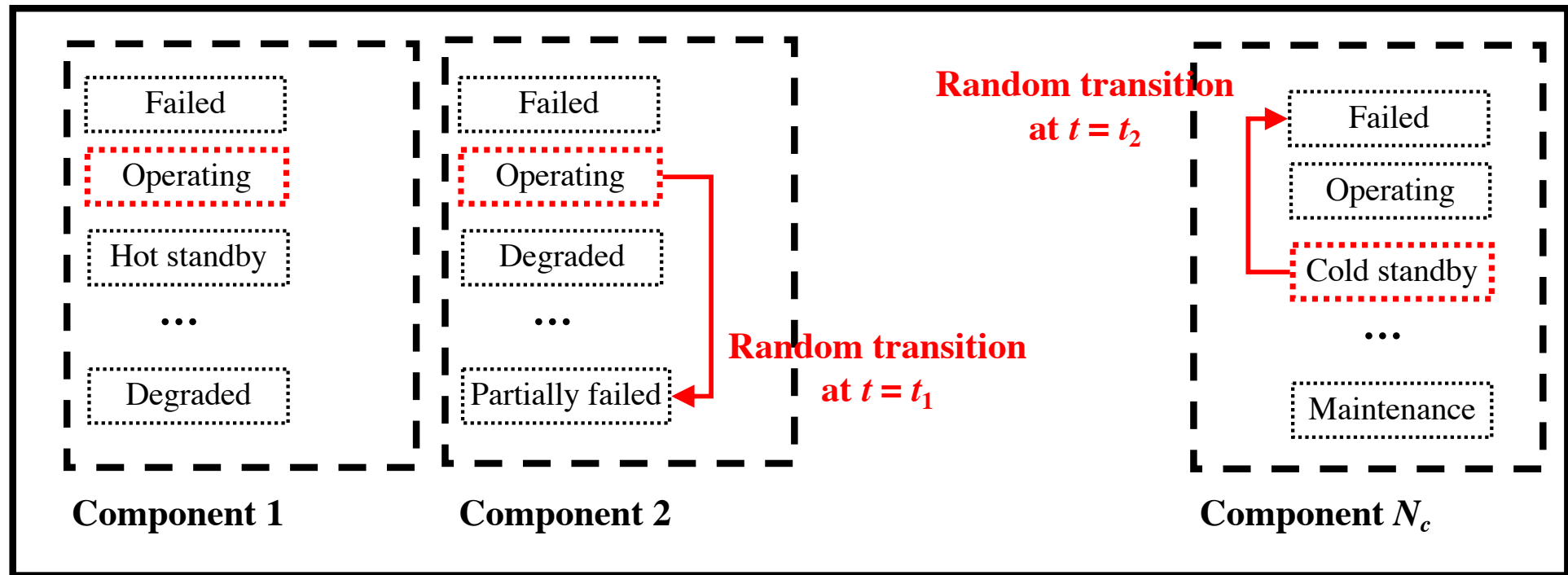
Generators (G1, G2, G3)

Loads (2, 3, 4, 6, 7, 9, 10, 11, 12, 13, 14)

Power delivery paths: lines (L) and buses (B).



## SYSTEM



Under specified conditions:

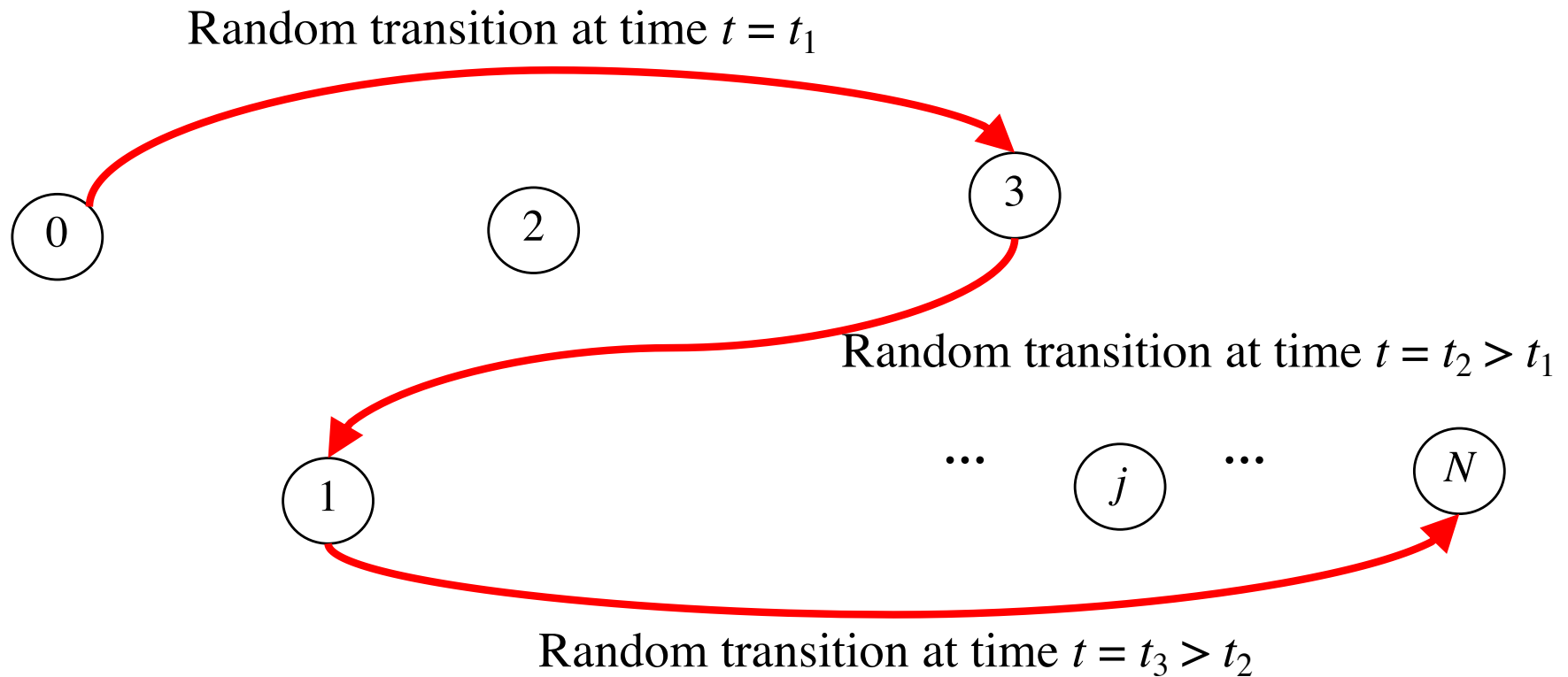
**Stochastic process** of system evolution

=

**MARKOV PROCESS**



- **Transitions** from one state to another occur **stochastically** (i.e., **randomly in time**)



- Extending to the other equations:

$$\frac{d\underline{P}}{dt} = \underline{P}(t) \cdot \underline{A}, \quad \underline{A} = \begin{pmatrix} -\sum_{j=1}^N \alpha_{0j} & \alpha_{01} & \dots & \alpha_{0N} \\ \alpha_{10} & -\sum_{\substack{j=0 \\ j \neq 1}}^N \alpha_{1j} & \dots & \alpha_{1N} \\ \dots & \dots & \dots & \dots \end{pmatrix}$$

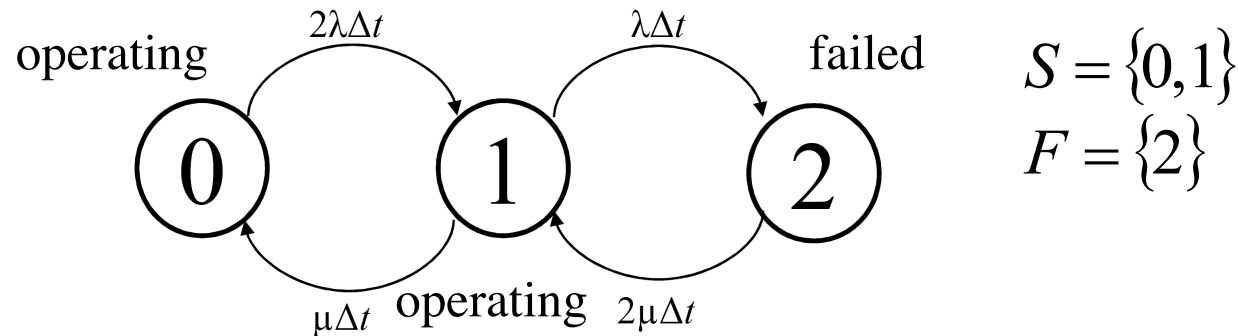
TRANSITION RATE MATRIX



System of **linear, first-order differential equations** in the unknown state probabilities

$$P_j(t), j = 0, 1, 2, \dots, N, t \geq 0$$

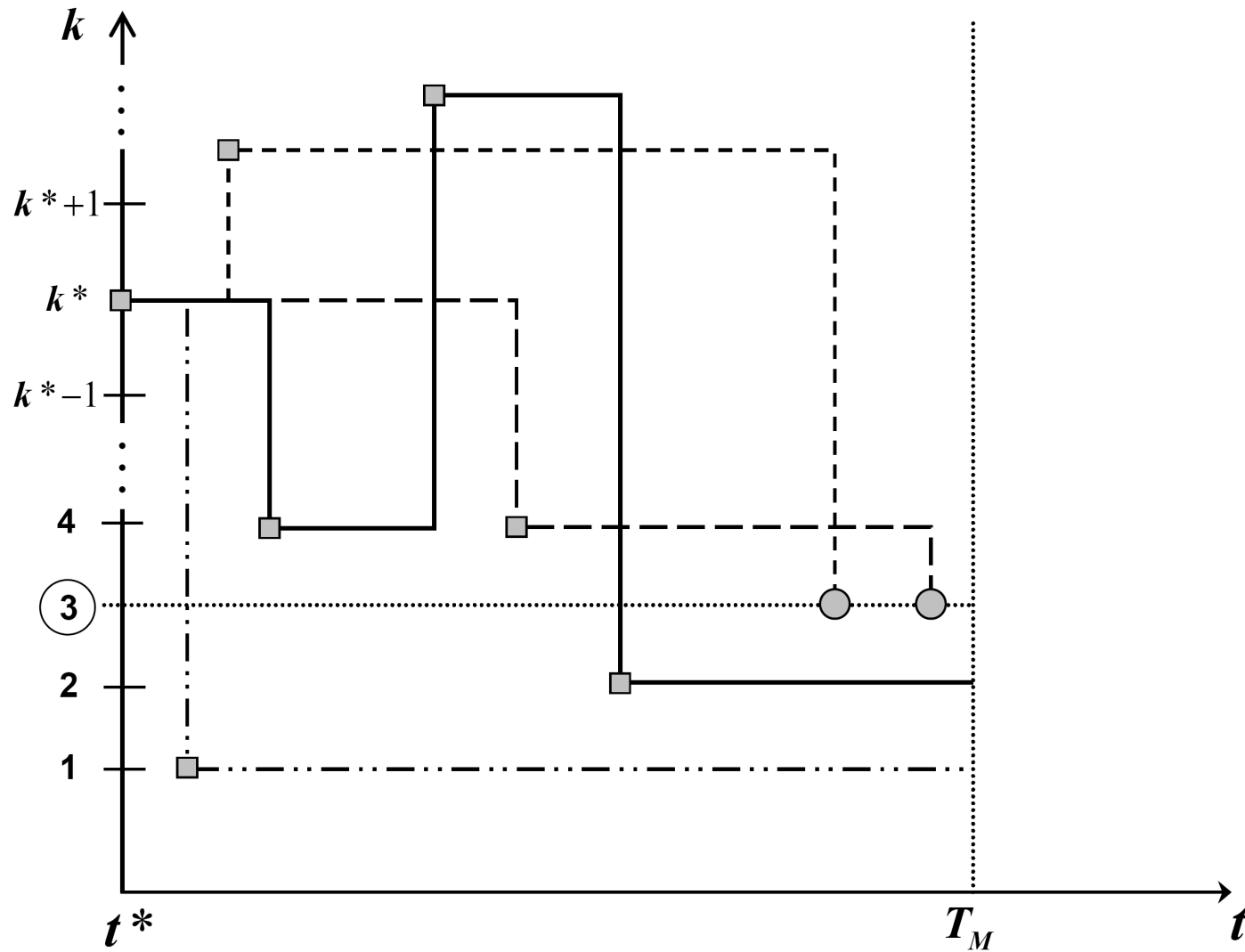
1. Exclude all the failed states  $j \in F$  from the transition rate matrix  $\underline{\underline{A}}$



$$\underline{\underline{A}} = \begin{pmatrix} -2\lambda & 2\lambda & 0 \\ \mu & \mu + \lambda & \lambda \\ 0 & 2\mu & -2\mu \end{pmatrix} \quad \rightarrow \quad \underline{\underline{A}} = \left( \begin{array}{cc|c} -2\lambda & 2\lambda & 0 \\ \mu & -(\mu + \lambda) & \lambda \\ \hline 0 & 2\mu & -2\mu \end{array} \right) \Rightarrow \underline{\underline{A}}' = \begin{pmatrix} -2\lambda & 2\lambda \\ \mu & -(\mu + \lambda) \end{pmatrix}$$

The new matrix  $\underline{\underline{A}}'$  contains the transition rates for transitions **only among the success states**  $i \in S$   
 (the “reduced” system is virtually functioning continuously with no interruptions)

# Monte Carlo Simulation

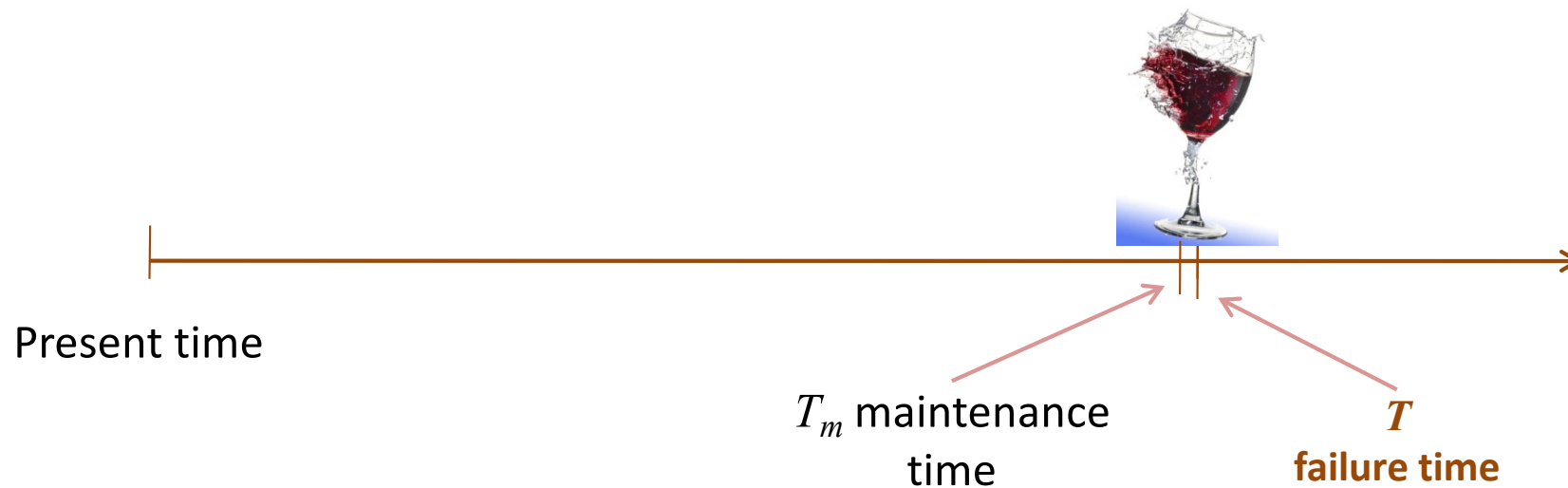


# Maintenance

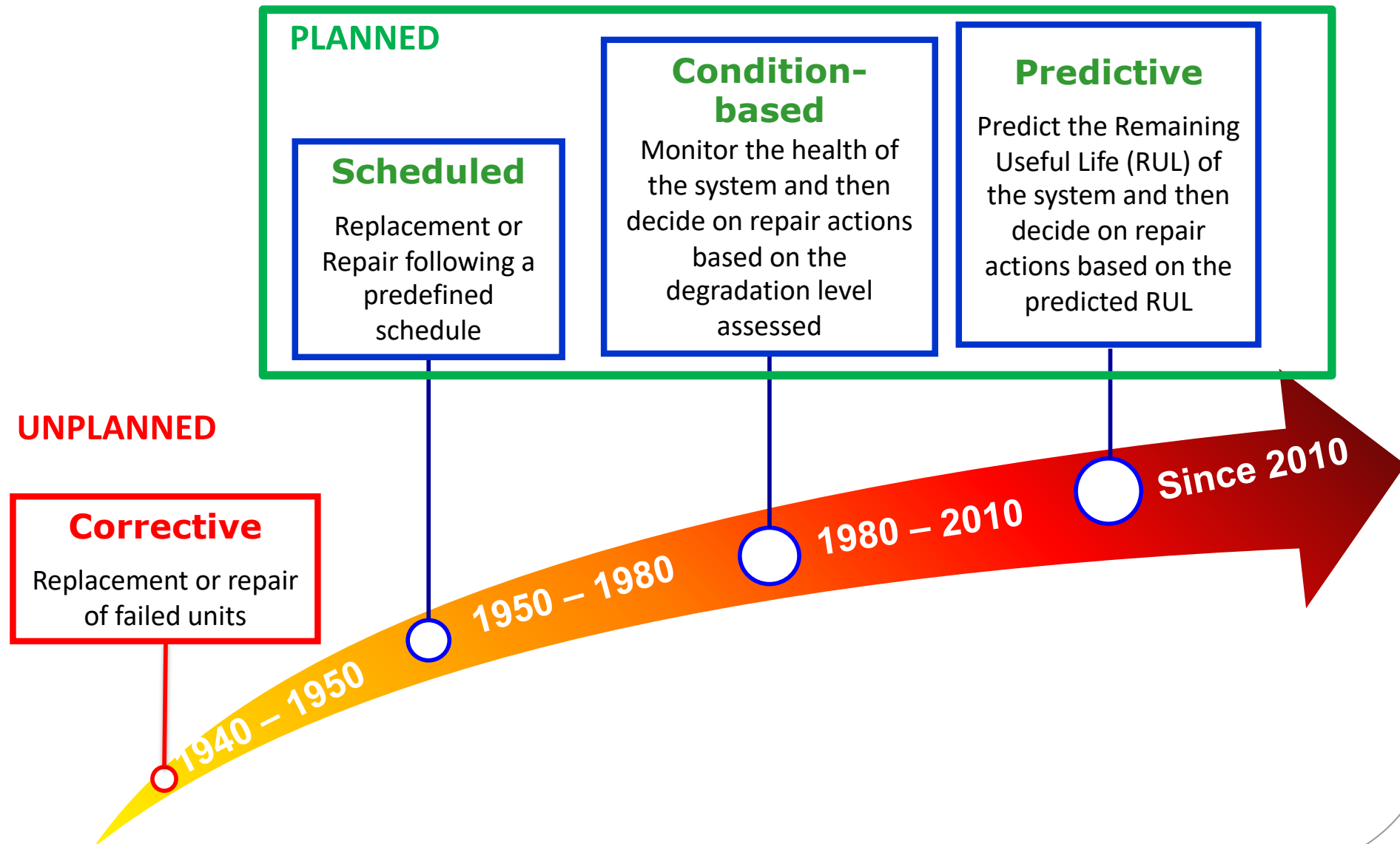
# Ideal Maintenance: When?

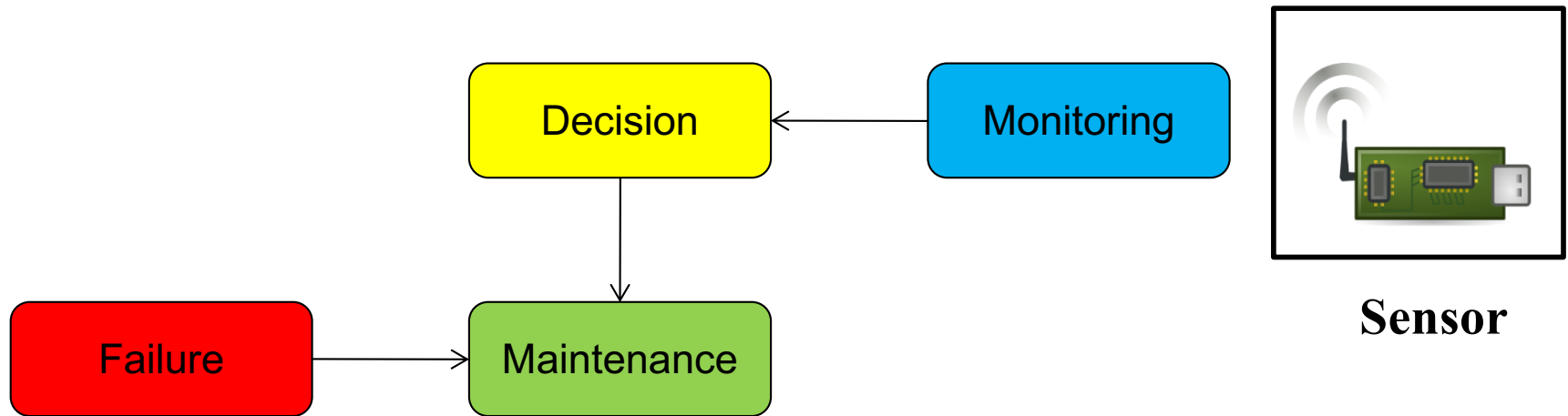
$$T_m = T - dt$$

- Component's life fully exploited
- Unavailability due to maintenance actions are avoided

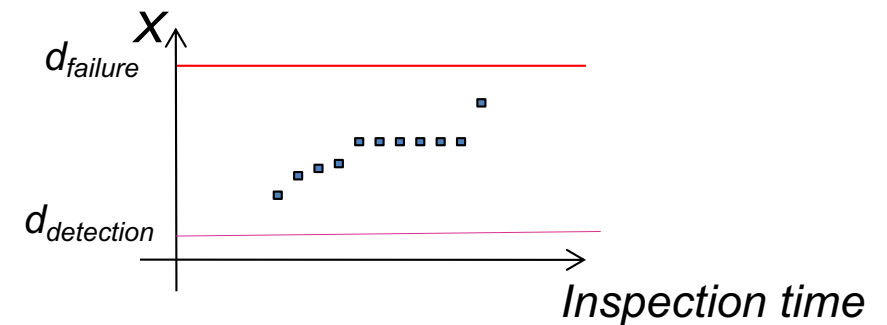
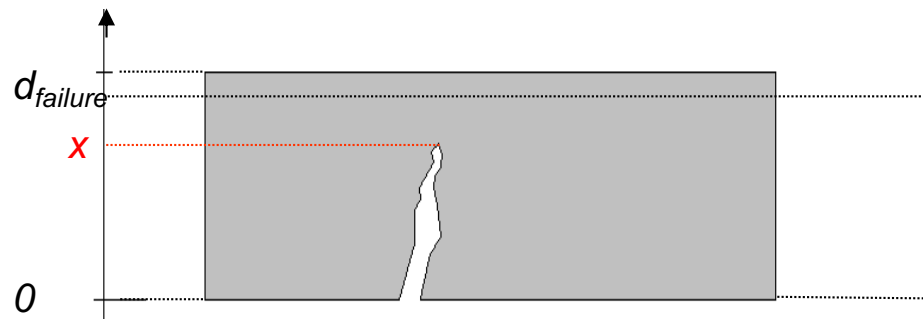


# Maintenance Intervention Approaches

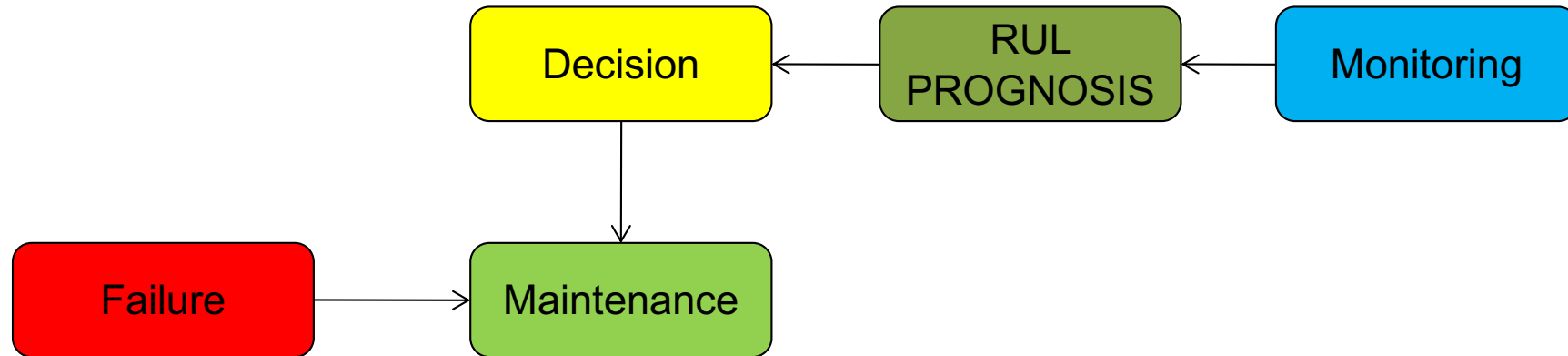




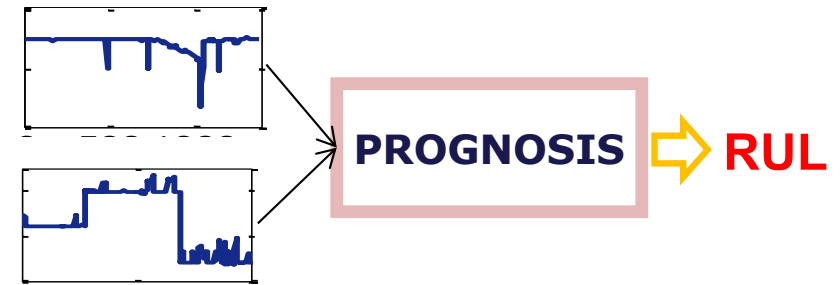
- Equipment degradation monitoring:
  - Periodic inspection by manual or automatic systems







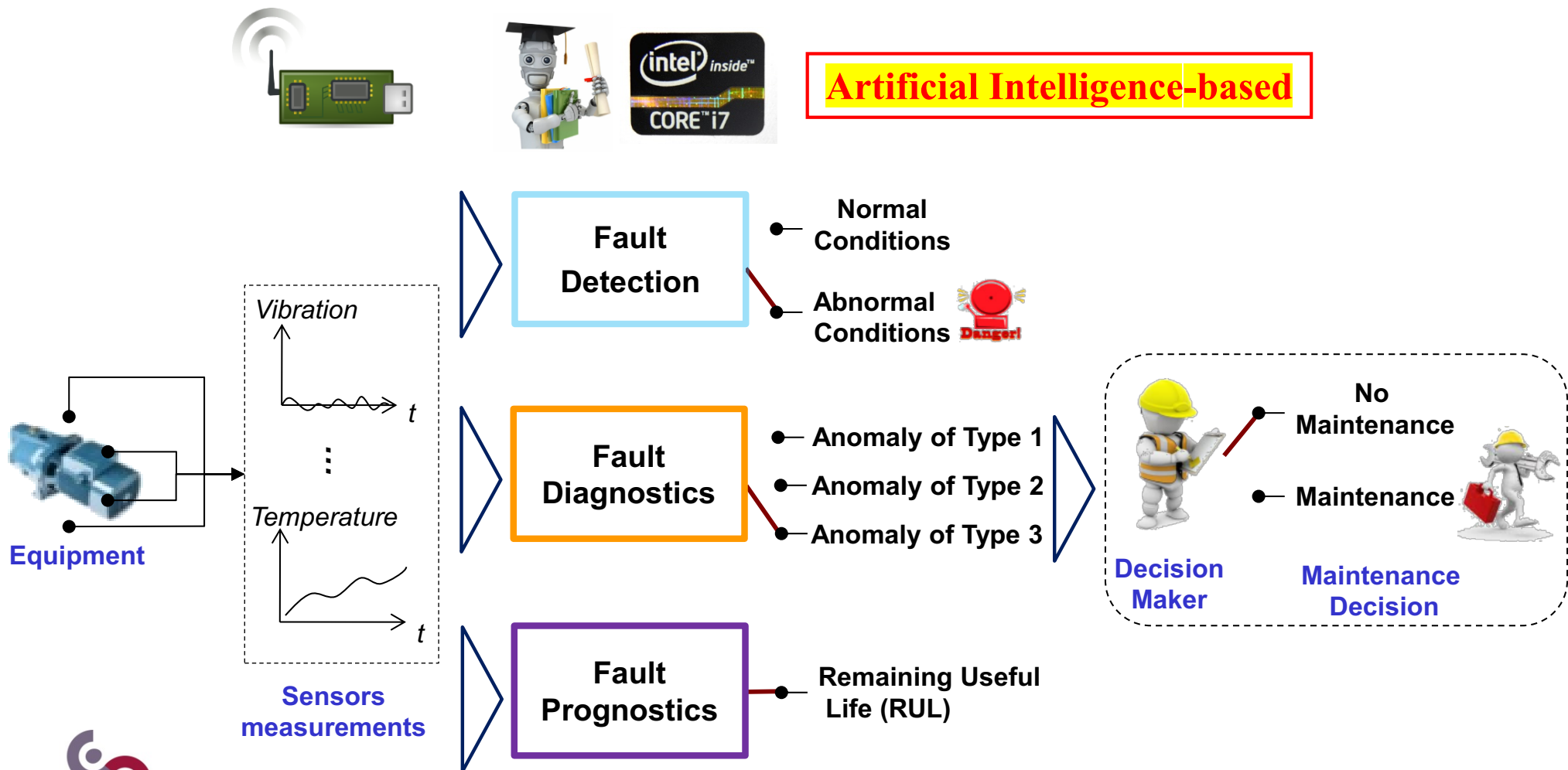
- Equipment degradation monitoring:  
    ▼
- Remaining Useful Life (RUL) prediction  
    ▼
- Maintenance Decision



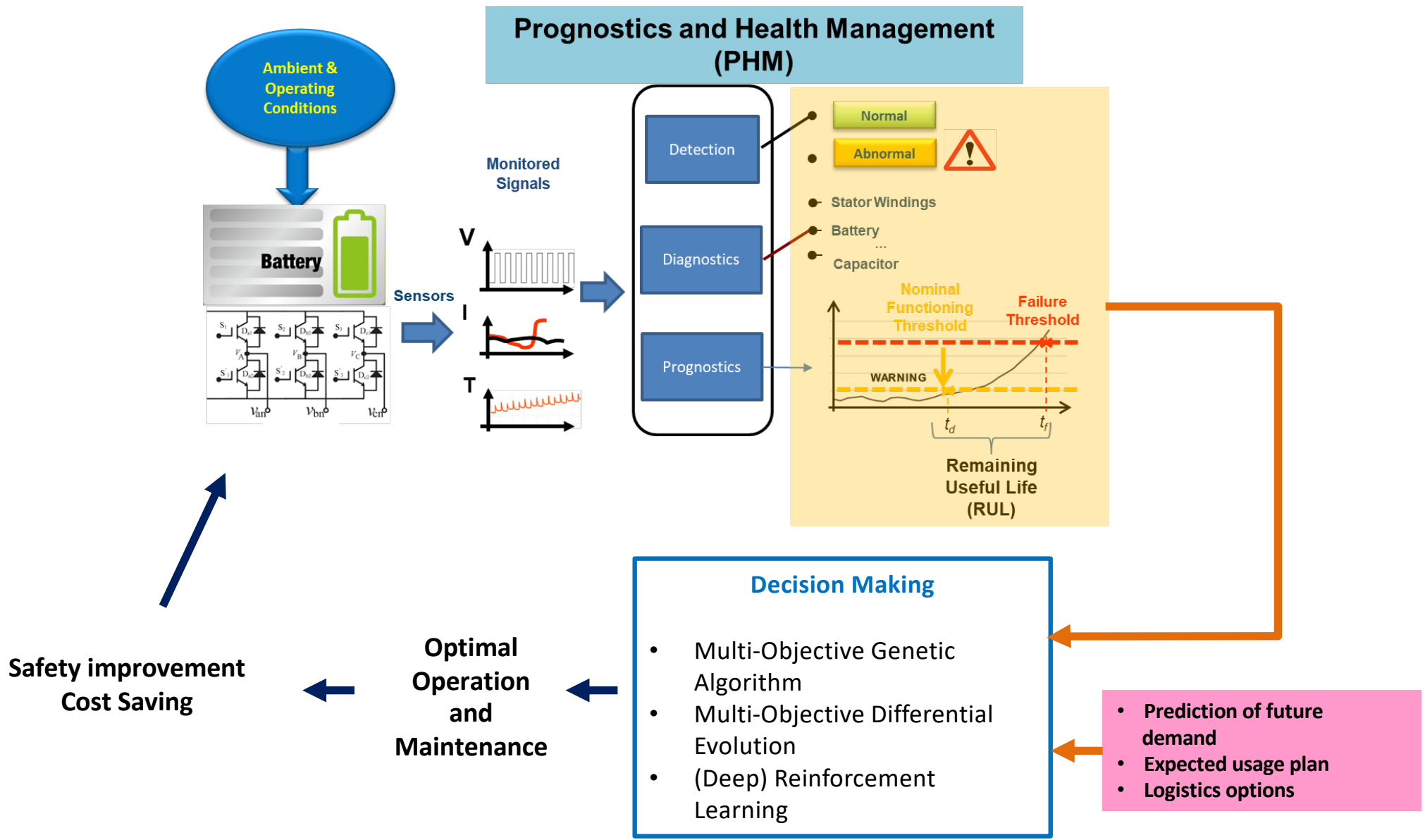
**Prognostics and Health  
Management (PHM) for  
Predictive (PrM) and Condition-  
based (CBM) Maintenance**



## PHM in support to CBM and PrM



# Predictive O&M



# **The lectures**

Introduction - Definition of Safety, Risk; Structure of Risk Analysis of Complex Engineering Systems Method of Hazard Identification

Analytical calculations of simple system reliability

Analytical calculations of system availability

Fault Tree Analysis

Event Tree Analysis

Markov Models

Prognostics and Health Management

Monte Carlo simulation

Seminar

Importance Measures
Bayesian Belief Networks
Dependent Failures
Life tests and parameter estimates
Lecture on advanced risk assessment
Exam Practice
Seminar

# The books



PRODUCTION TO THE BASICS OF RELIABILITY AND RISK ANALYSIS

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.

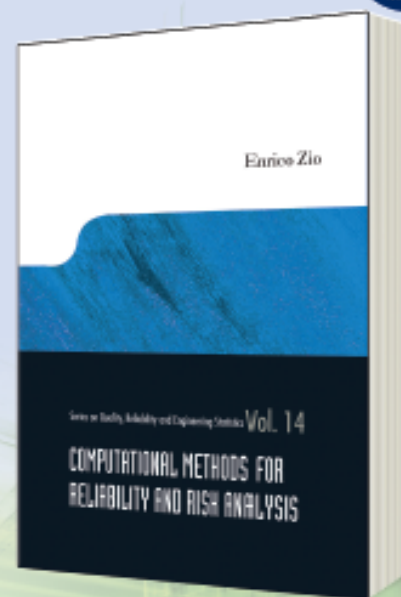
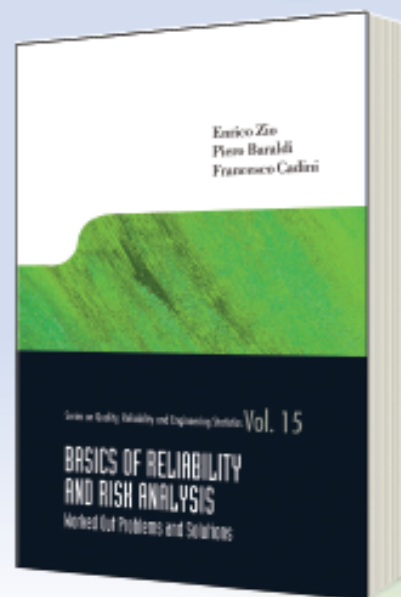
Zio

Series in Quality, Reliability and Engineering Statistics Vol. 13

AN INTRODUCTION TO THE BASICS OF RELIABILITY AND RISK ANALYSIS

World Scientific www.worldscientific.com 8442 hc





Series on Quality, Reliability and Engineering Statistics - Vol. 15  
**BASICS OF RELIABILITY AND RISK ANALYSIS**  
 Worked Out Problems and Solutions

by Enrico Zio (Ecole 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*.

220pp	June 2011	
978-981-4255-03-2	US\$66	£44
Set		
978-981-4360-66-5	US\$199	£129

Series on Quality, Reliability and Engineering Statistics - Vol. 14  
**COMPUTATIONAL METHODS FOR RELIABILITY AND RISK ANALYSIS**

by Enrico Zio (Politecnico di Milano, Italy)

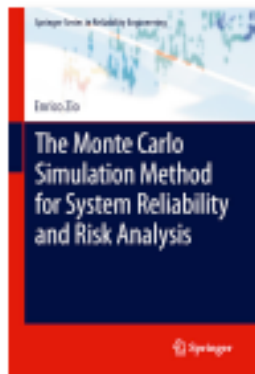
This book illustrates a number of modelling and computational techniques for addressing relevant issues in reliability and risk analysis. In particular, it provides: i) a basic illustration of some methods used in reliability and risk analysis for modelling the stochastic failure and repair behaviour 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 a set with *Basics of Reliability and Risk Analysis* and *An Introduction to the Basics of Reliability and Risk Analysis*.

**Readership:** Undergraduates, graduates, academics and professionals in the fields of systems engineering and safety and risk analysis.

264pp	January 2009	
978-981-263-901-5	£57	\$92
Set		
978-981-4360-68-5	£129	\$225



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](http://springer.com).  
A free preview is available.  
Also available from libraries offering Springer's eBook Collection.

- ▶ [springer.com/ebooks](http://springer.com/ebooks)

#### MyCopy

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

- ▶ € | \$ 24.95
- ▶ [springer.com/mycopy](http://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

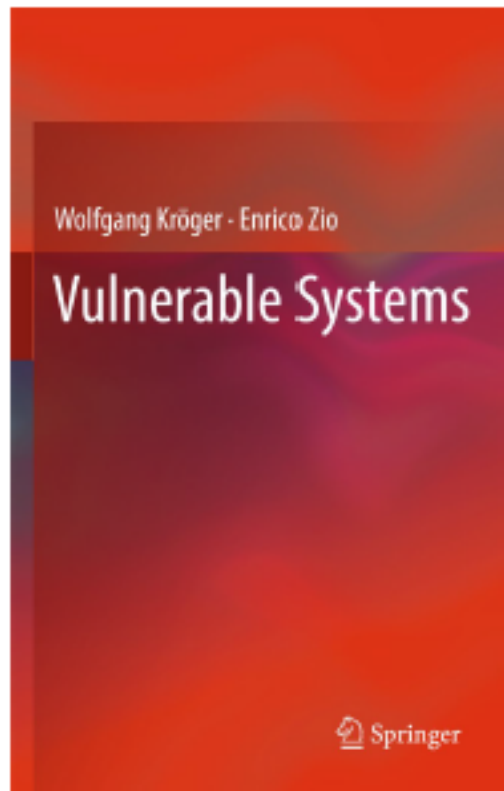
- ▶ **Illustrates the Monte Carlo simulation method and its application to reliability and system engineering to give the readers the sound fundamentals of Monte Carlo sampling and simulation**
- ▶ **Explains the merits of pursuing the application of Monte Carlo sampling and simulation methods when realistic 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.





2011. XIV, 234 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 infrastructure which constitute the backbone of modern industry and society entails identifying and quantifying their vulnerabilities to design adequate protection, mitigation, and emergency action against failure. In practice, there is no fail-safe solution to such problems and various frameworks are being proposed to effectively integrate different methods of complex systems analysis in a problem-driven approach to their solution. *Vulnerable Systems* reflects the current state of knowledge on the procedures which are being developed for the risk and vulnerability analysis of critical infrastructures. Classical methods of reliability and risk analysis, as well as new paradigms based on network and systems theory, including simulation, are considered in a dynamic and holistic way. *Vulnerable Systems* will benefit from its structured presentation of the current state of knowledge on this subject. It will enable graduate students, researchers and safety analysts to understand the methods suitable for different phases of analysis and to identify their criticalities in application. ... *more on* <http://springer.com/978-0-85729-654-2>

MATHEMATICS &  
STATISTICS

WILEY

Connect with  
us:



Wiley Statistics and Mathematics



@Wiley\_Stats



Statistics by Wiley

# Uncertainty in Risk Assessment

Representation and  
Treatment of  
Uncertainties by  
Probabilistic and  
Non-Probabilistic  
Methods

By Terje Aven, Enrico Zio, Piero Baraldi  
and Roger Flage

**Uncertainty in Risk Assessment:**

- Illustrates the need for seeing beyond probability to represent uncertainties in risk assessment contexts.
  - Provides simple explanations (supported by straightforward numerical examples) of the meaning of different types of probabilities including interval probabilities, and the fundamentals of possibility theory and evidence theory.
  - Offers guidance on when to use probability and when to use an alternative representation of uncertainty.
  - Presents and discusses methods for the representation and characterization of uncertainty in risk assessment.
  - Uses practical examples to clearly illustrate ideas and concepts.
- The theories and methods studied in the book have wide ranging applications from engineering and medicine to environmental impacts and natural disasters to security and financial risk management.

*Uncertainty in Risk Assessment* can be read with profit by a broad audience of professionals in the field, including researchers and graduate students in specialized courses within risk analysis, statistics, engineering and the physical sciences.

Hardback | 184 pages | 2014 | ISBN 978-1-118-48958-1  
\$95.00 £55.00 €66.70 \*E-book versions also available

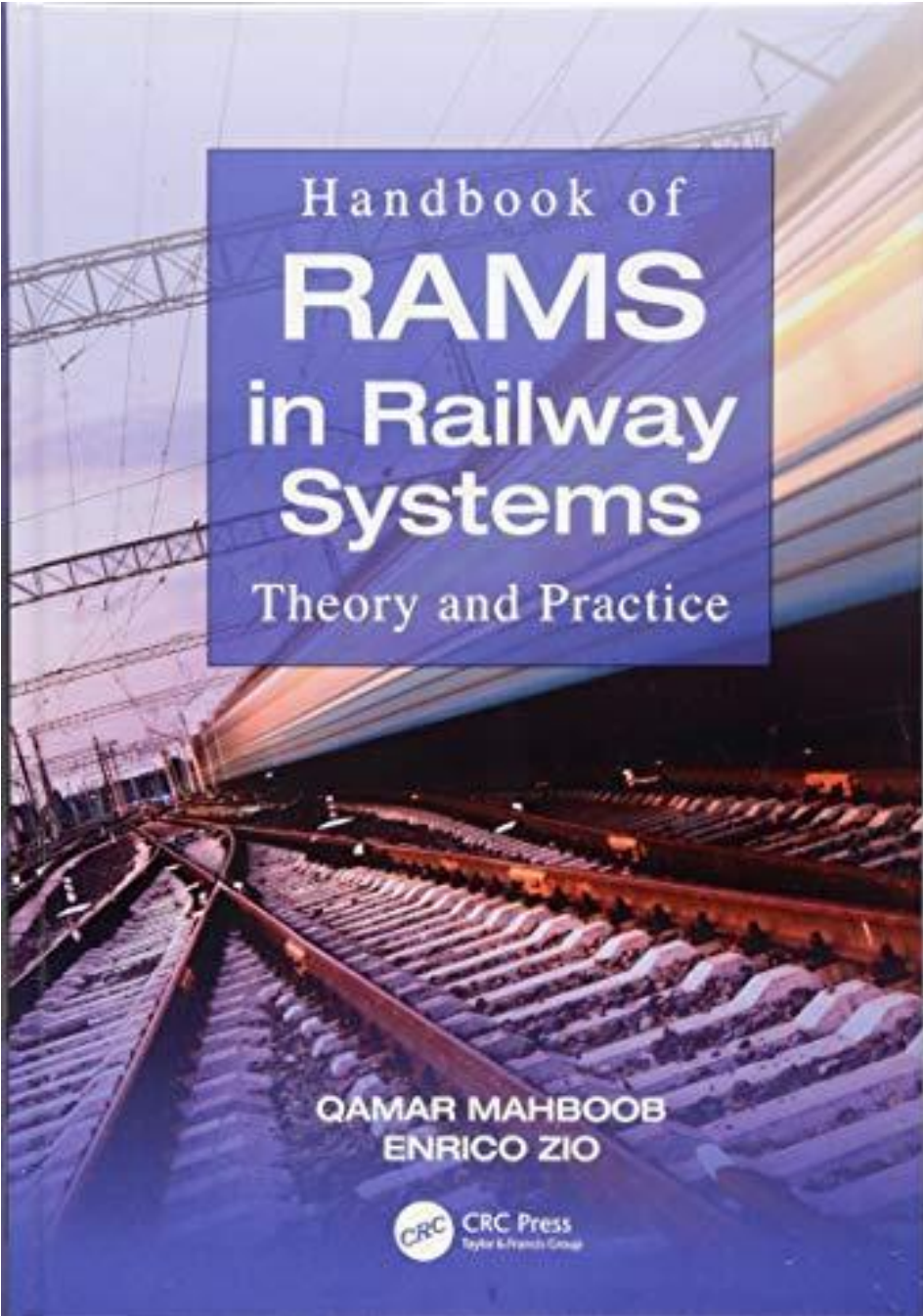


## Wiley-Blackwell E-Books and Online Books

Digital editions of the books featured are available for download to your computer or e-book reader. Please visit [wiley.com](http://wiley.com) or your preferred e-book retailer for further details.

A collection of online books are also available for libraries and institutions. To learn more visit [wileyonlinelibrary.com/onlinebooks](http://wileyonlinelibrary.com/onlinebooks) and contact your librarian to ensure you have access.





Handbook of  
**RAMS**  
in Railway  
Systems

Theory and Practice

QAMAR MAHBOOB  
ENRICO ZIO



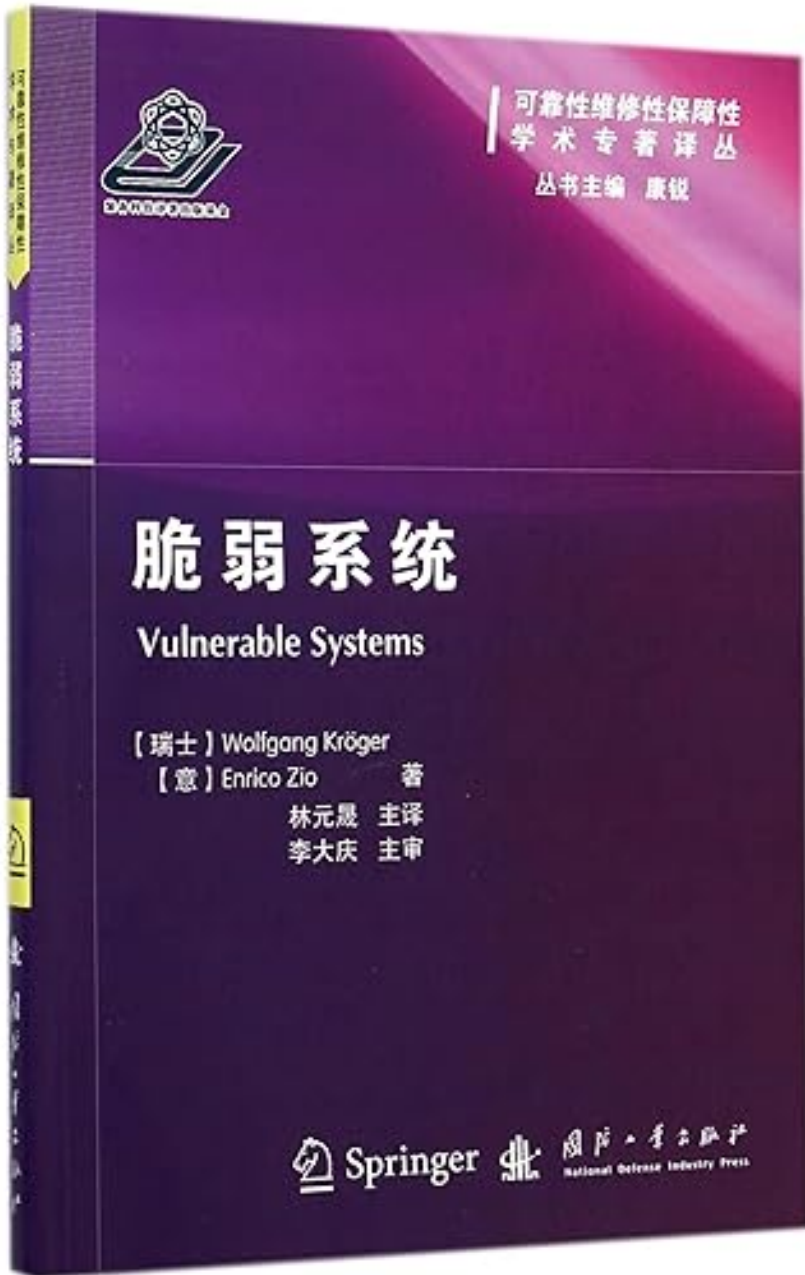
SPRINGER NATURE  
Reference 

Michel Fathi  
Enrico Zio  
Panos M. Pardalos  
*Editors*

# Handbook of Smart Energy Systems

 Springer





Paperback

**Currently unavailable.**

We don't know

when or if this

item will be back

in stock.