Aalto University
School of Science

POLITECNICO DI MILANO

Bayesian approach for safety barrier portfolio optimization

A. Mancuso[a,b], M. Compare[b], A. Salo[a], E. Zio[b,c]

a. Systems Analysis Laboratory, Department of Mathematics and Systems Analysis - Aalto University

b. Laboratory of Signal and Risk Analysis, Dipartimento di Energia - Politecnico di Milano

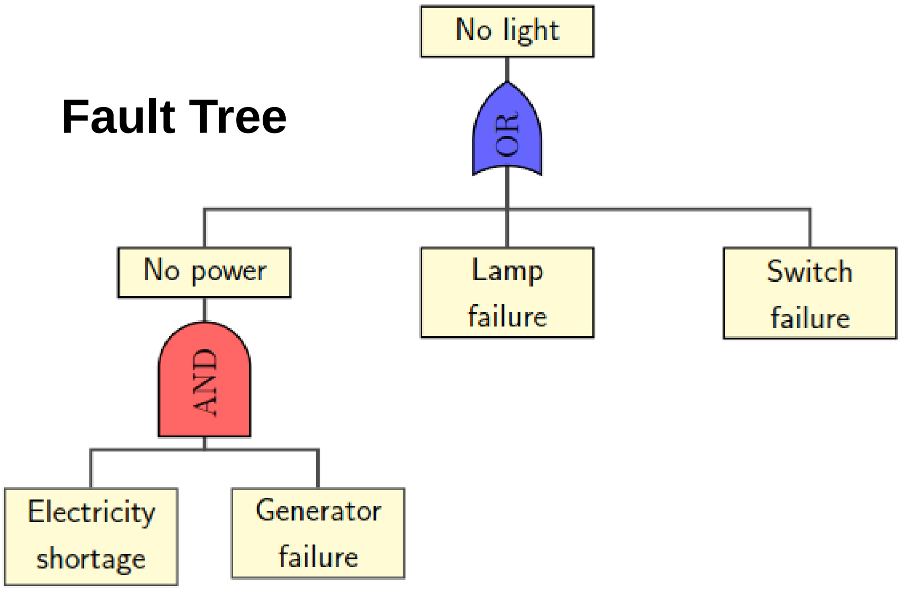
c. Chair on Systems Science and the Energetic Challenge - École Centrale Paris and Supelec

March 29, 2017

Risk-informed decision making in safety critical context

Based on **Probabilistic Risk Assessment (PRA)**

Fault Tree



$$RRW^{Gen} = \frac{R(No\ light)}{R(No\ light|No\ generator\ failure)}$$

$$RRW^{Lamp} = \frac{R(No\ light)}{R(No\ light|No\ lamp\ failure)}$$

$$RRW^{Switch} = \frac{R(No\ light)}{R(No\ light|No\ switch\ failure)}$$

<u>Concerns</u>

- Experts interpret these importance measures and choose actions
- Action costs and feasibility constraints considered only afterwards
- The results can be sub-optimal

Our methodology

The methodology identifies **portfolios of actions** for the whole system which minimize the residual risk of the system and the total cost of actions.

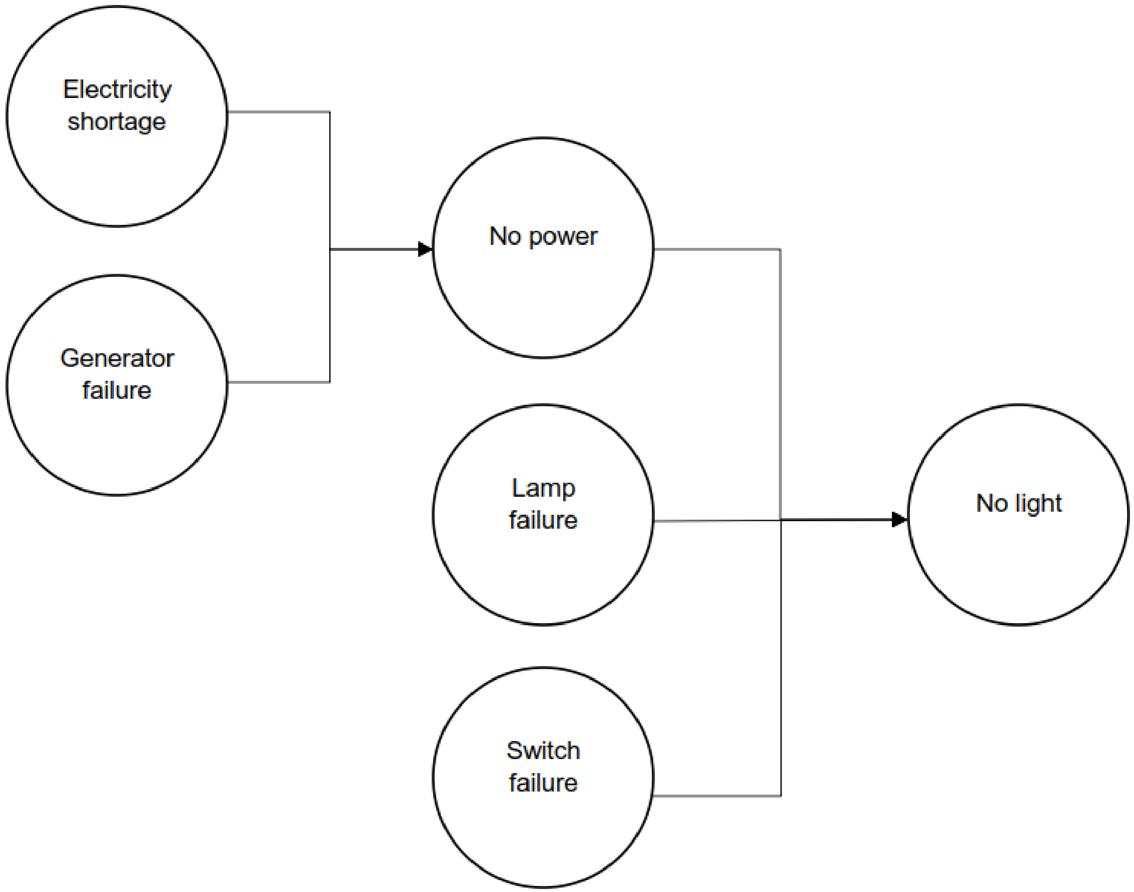
The methodology accounts for **risk**, **budget** and other **feasibility constraints**.

Methodology steps:

- **Step 1**: Failure scenario modeling
- **Step 2**: Definition of failure probabilities
- **Step 3**: Specification of actions
- **Step 4**: Optimization model

Step 1: Failure scenario modeling

Mapping of Fault Tree (FT) into **Bayesian Belief Network (BBN)**



Advantages

- Multi-state modeling
- Extension of concepts of AND/OR gates

Reference: *Khakzad N., Khan F., Amyotte P., Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network, Process Safety and Environmental Protection 91 (1-2), pp. 46-53 (2013).*

Step 2: Definition of failure probabilities

Information sources

- Information provided by AND/OR gates in FT
- Statistical analyses
- Expert elicitation

The probabilities of events are defined as follows:

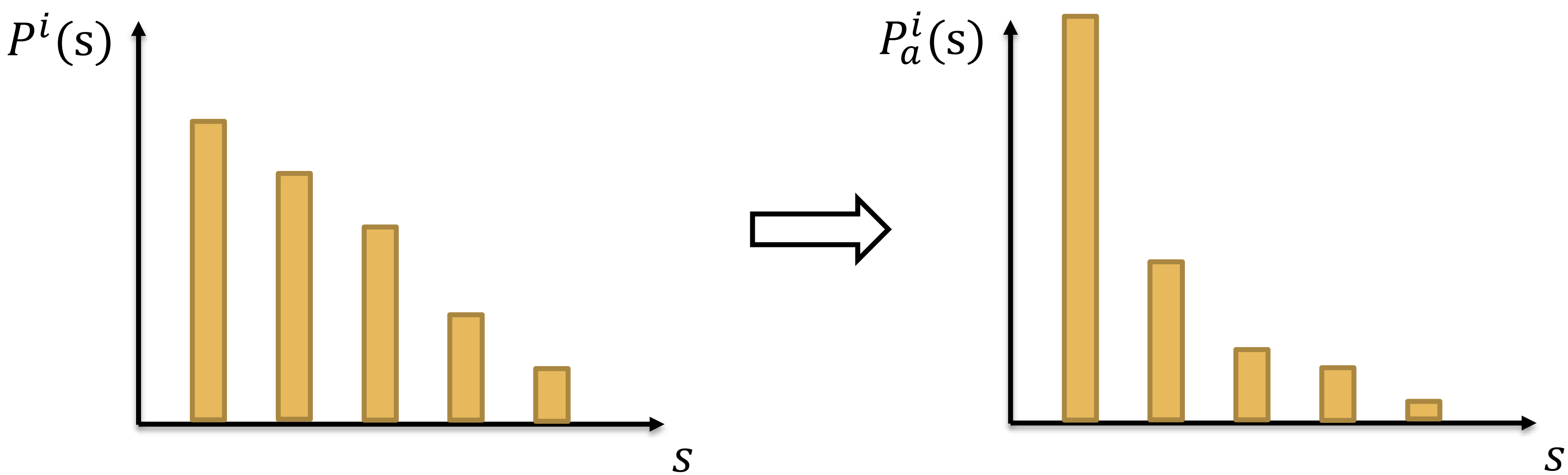
- Initiating events → failure probabilities of system components
- Intermediate and top events → conditional probability tables

Step 3: Specification of actions

Parameters of actions:

- Impact on the prior and conditional probabilities
- Annualized cost

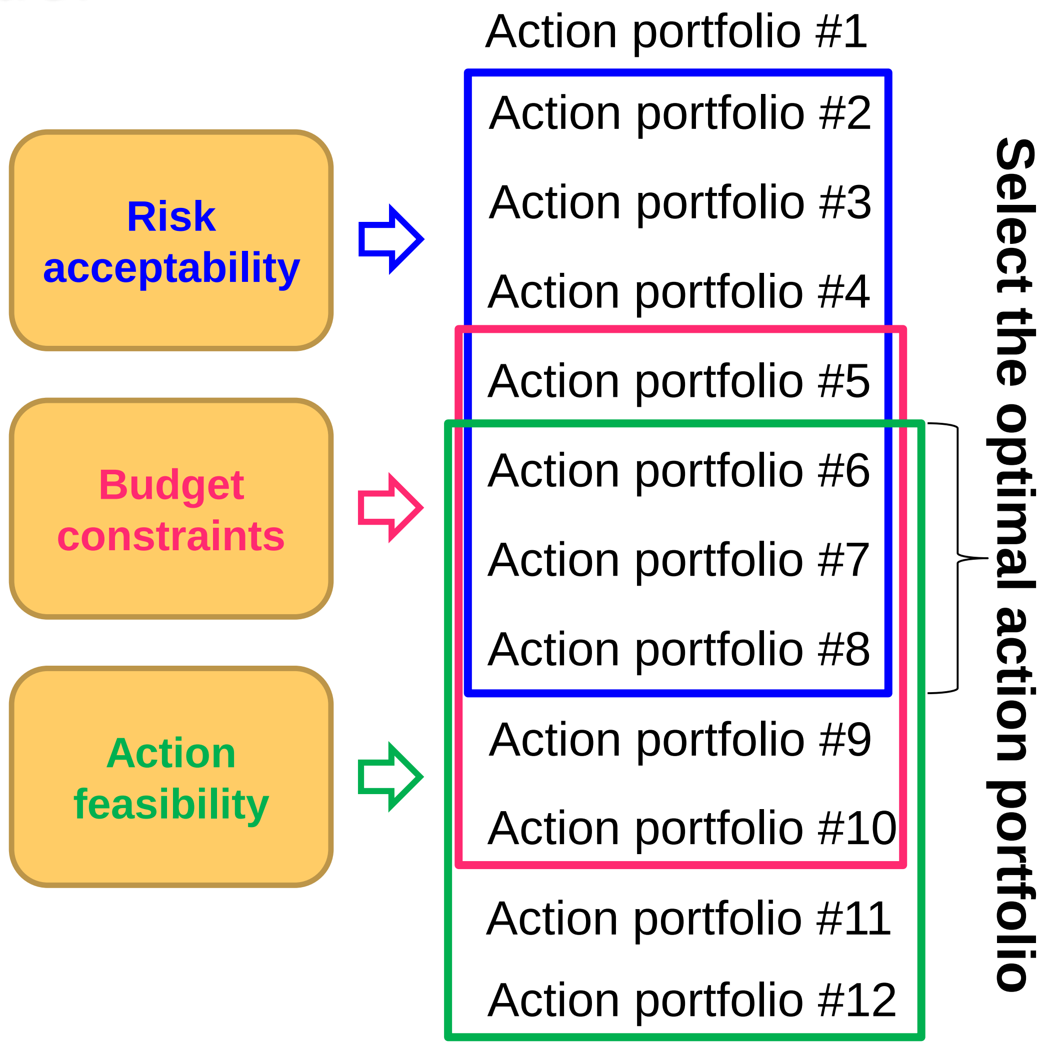
Action a for event i modifies the probability of occurrence of state s.



Step 4: Optimization model

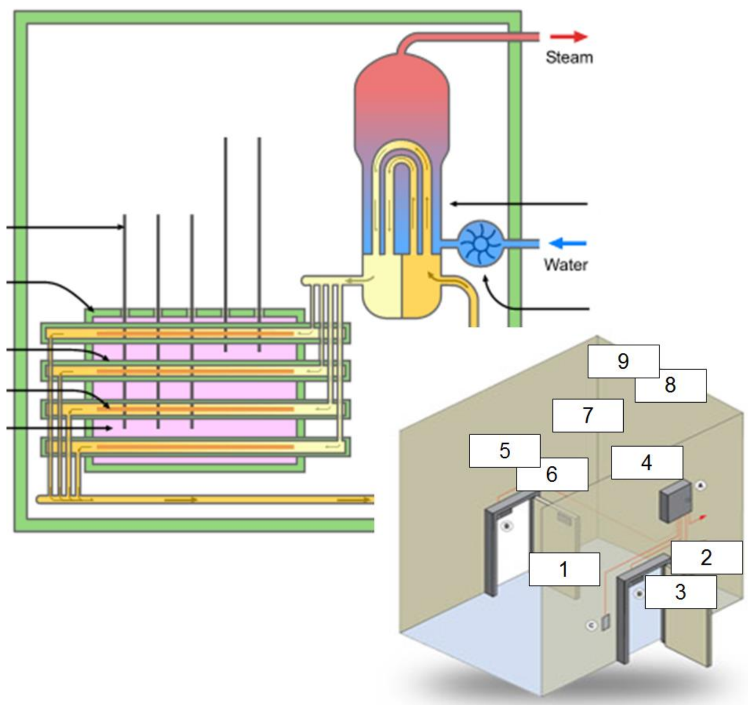
Implicit enumeration algorithm to identify the optimal portfolios of safety actions.

The resulting portfolios are globally optimal: they minimize the failure risk of target events (instead of selecting actions that target the riskiness of the single components).



Illustrative example: CANDU airlock system

The Airlock System (AS) keeps the pressure of the inner side of the reactor vault lower than the outer side to avoid the dispersion of contaminants out of the reactor bay.

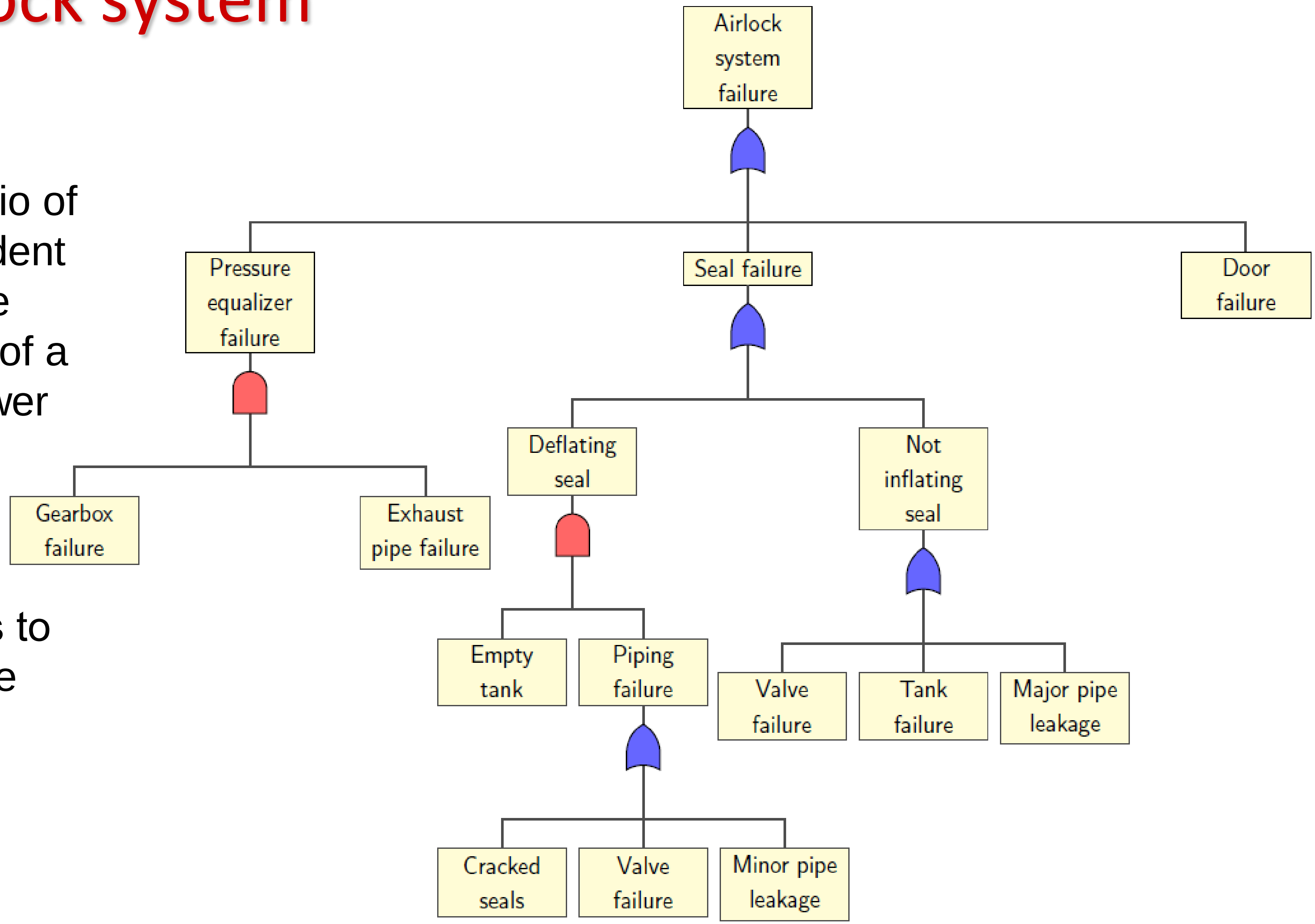


	Basic Failure Events	ID Code
1	Pressure equalizer valve failure	V1
2	Doors failure	D1
3	Seal failure	S1
4	Gearbox failure	G1
5	Minor pipe leakages	P1
6	Major pipe leakages	P2
7	Exhaust pipe failure	E1
8	Empty tank	T1
9	Tank failure	T2

Lee A., Lu L., "*Petri Net Modeling for Probabilistic Safety Assessment and its Application in the Air Lock System of a CANDU Nuclear Power Plant*", Procedia Engineering, 2012 International Symposium on Safety Science and Technology, Volume 25, pp.11-20, 2012.

CANDU airlock system

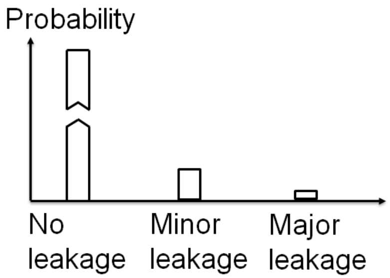
Fault Tree (FT) for analyzing the scenario of a Design Basis Accident which occurred in the Airlock System (AS) of a CANDU Nuclear Power Plant in 2011.



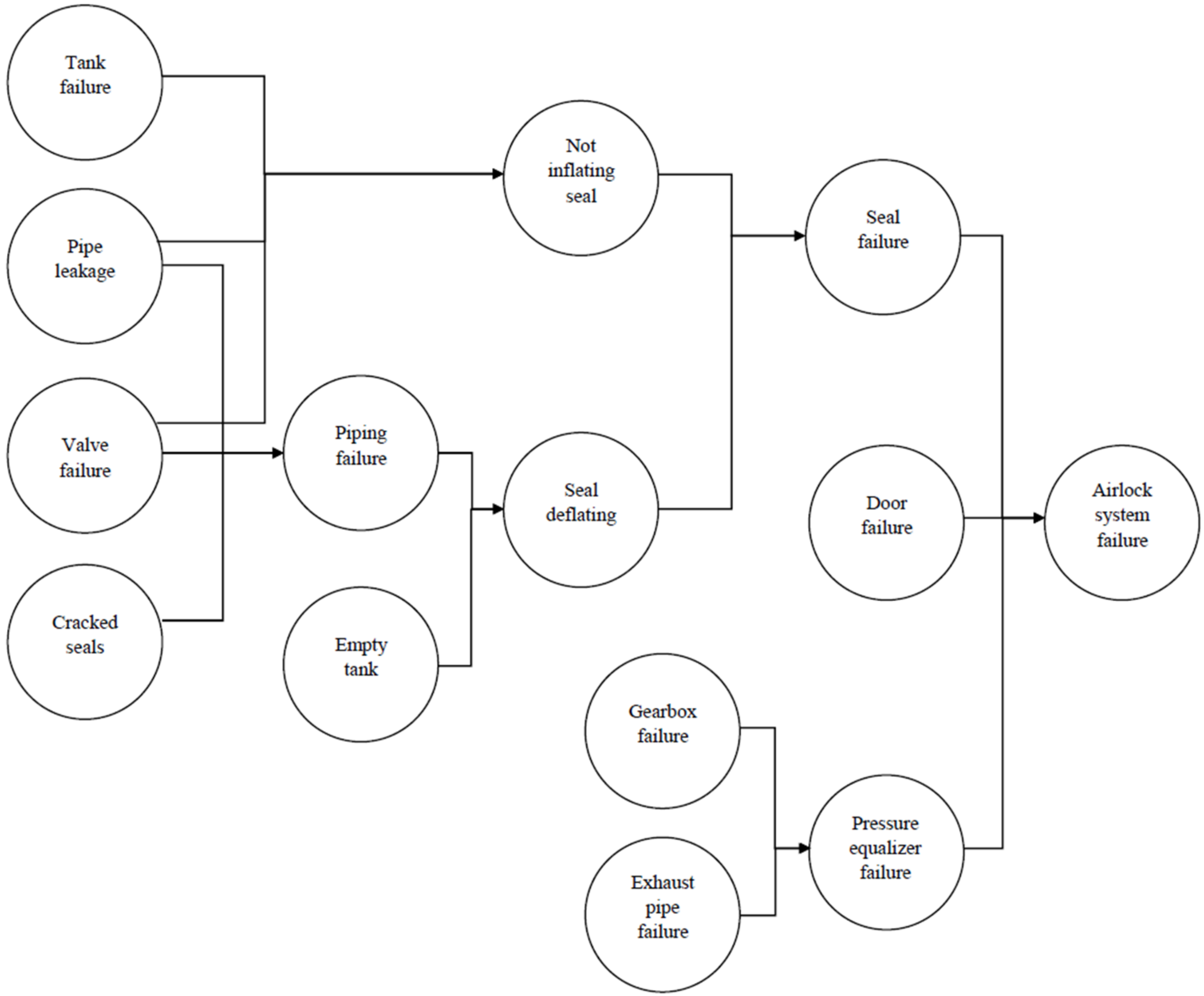
Top event = "AS fails to maintain the pressure boundary".

***Reference**: Di Maio F., Baronchelli S., Zio E., Hierarchical differential evolution for minimal cut sets identification: Application to nuclear safety systems, European Journal of Operational Research 238, pp. 645-652 (2014).*

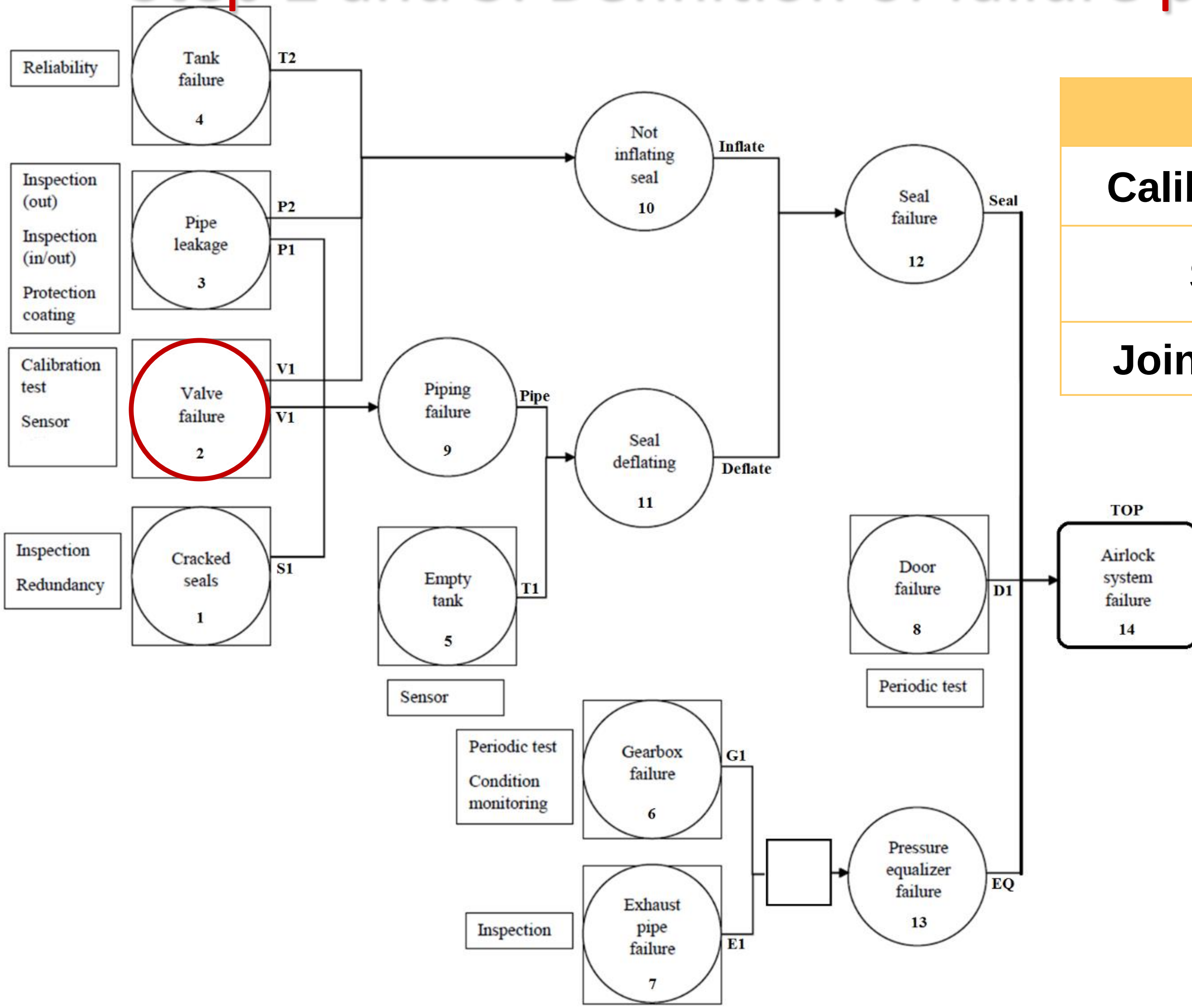
Step 1: Airlock system failure modeling



Multi-state description of pipe leakage event



Step 2 and 3: Definition of failure probabilities



Valve failure

Action		C	RRR
Calibration test	a_1	30	10^{-1}
Sensor	a_2	40	10^{-2}
Joined actions	a_3	60	10^{-4}

$$P^2_{a_1}(s=1) = 10^{-4} \cdot 10^{-1}$$

$$P^2_{a_2}(s=1) = 10^{-4} \cdot 10^{-2}$$

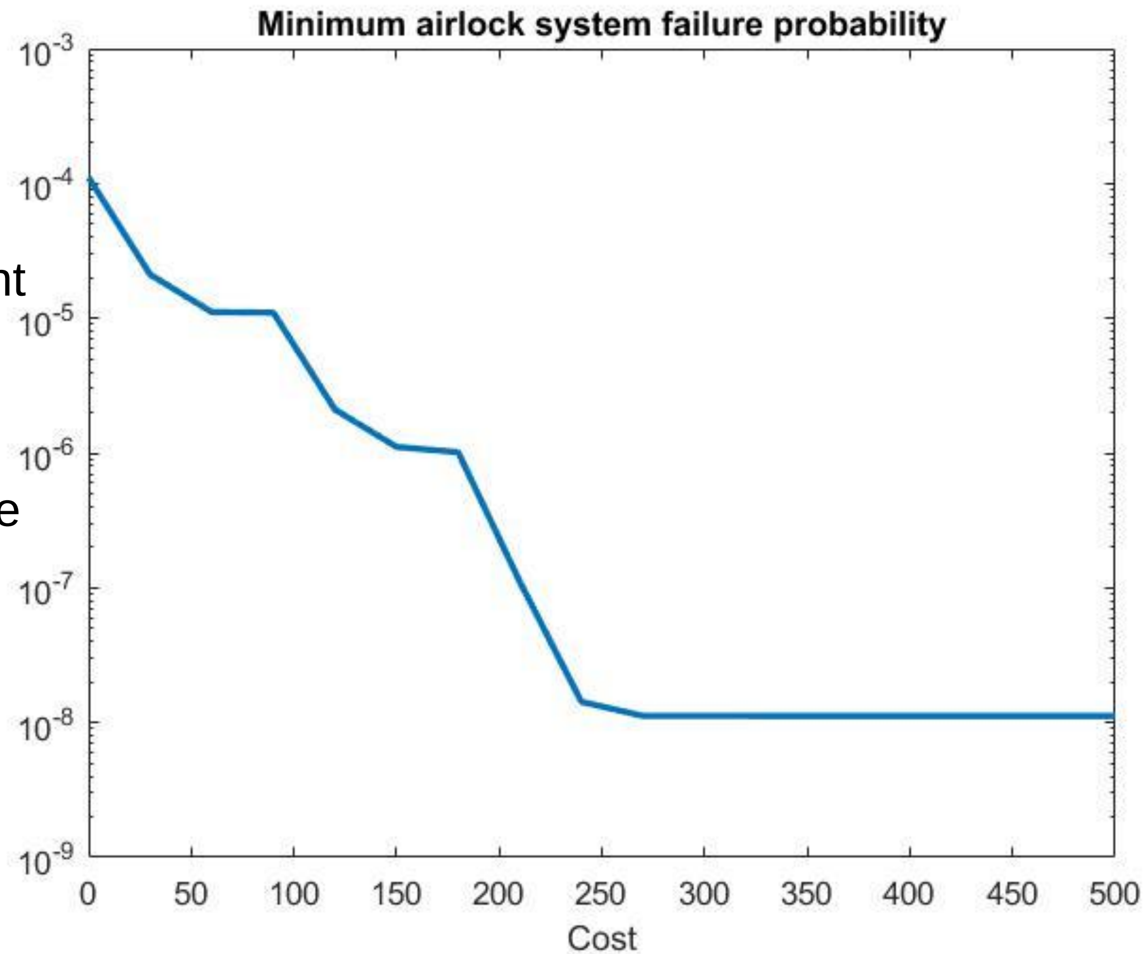
$$P^2_{a_3}(s=1) = 10^{-4} \cdot 10^{-4}$$

Risk Reduction Rate (RRR)

Step 4: Optimization results

Airlock failure probability for the optimal portfolio of actions for different budget levels.

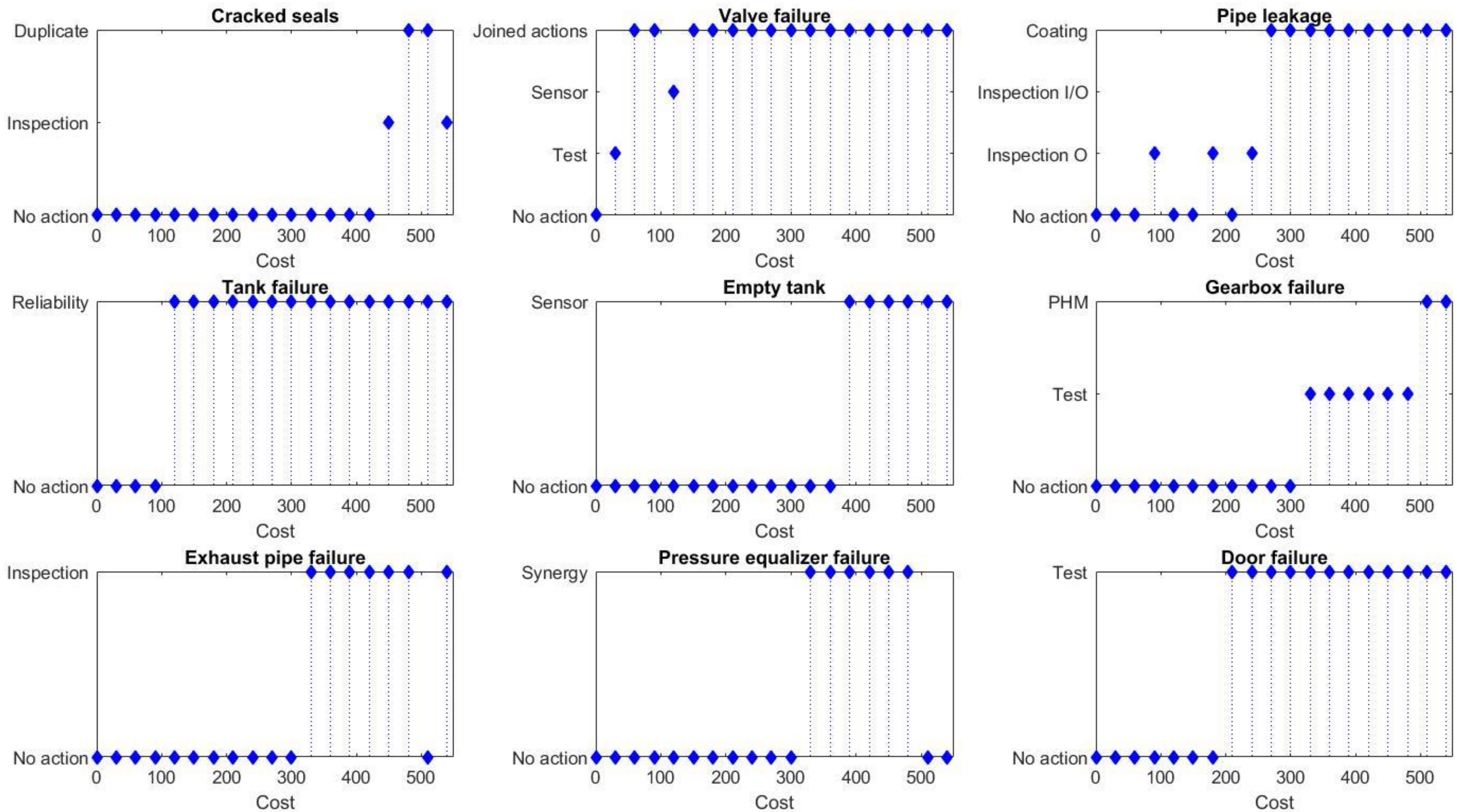
Bigger budget → more effective actions → lower residual risk of failure of the airlock system.



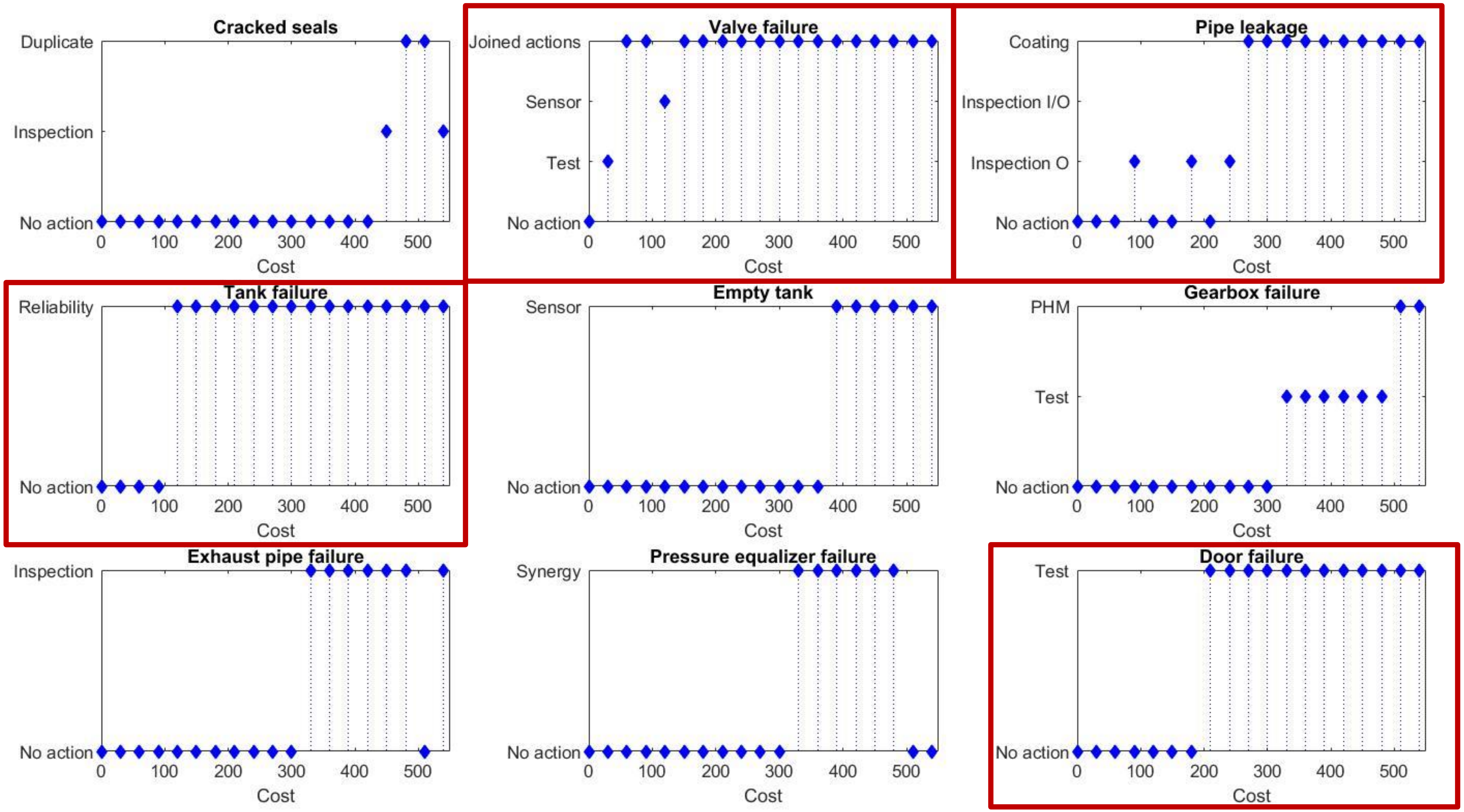
Aalto University
School of Science

POLITECNICO DI MILANO

Step 4: Optimization results



Step 4: Optimization results



Application of RRW approach

The application of this approach leads to the following issues

Iteration	Most risky event	Issue
$t = 1$	Valve failure	There are two possible actions: which one should the experts select?
$t = 2$	Tank failure	The only applicable action is very expensive: could it be that many inexpensive actions have a higher impact on risk reduction?
$t = 3$	Valve failure Door failure	If limited budget: which component should be improved first?
$t = 4$	Valve failure	If the experts apply a second action, do the joined actions have the same characteristics as two separate actions?

Application of Risk Importance Measures (RIMs)

Limitations of using RIMs (such as RRW)

- They cannot be applied in case of **multi-state and multi-objective failure scenarios** → they account only a unique target event
- Actions can be applied to **initiating events only** → not accounting for **synergies** of joined actions
- They do not account for **feasibility and budget constraints**
- They do not necessarily lead to the **global optimal portfolio of actions** because the procedure implies assumptions and expert opinions which strongly affect the decisions at the following iterations

Future research

- Accommodate **imprecise information** about event probabilities and action impacts
- Formulate and solve **dynamic Defense-in-Depth** models in the designing of safety actions (e.g. fire scenarios in a Nuclear Power Plant)
- Ongoing collaboration with an industrial partner with interests in optimization for **occupational safety** and other partners in energy field

Aalto University
School of Science

POLITECNICO DI MILANO

Thank you for your attention!

Alessandro Mancuso

System Analysis Laboratory, School of Science, Aalto University, Finland

Laboratory of Signal and Risk Analysis, Politecnico di Milano, Italy

alessandro.mancuso@aalto.fi