Portfolio optimization of safety measures for reducing risks in nuclear systems

A. Mancuso [*1,2], M. Compare[2,3], A. Salo[1] and E. Zio[2,3,4]

[1]Department of Mathematics and Systems Analysis, Aalto University, Finland
[2]Dipartimento di Energia, Politecnico di Milano, Italy
[3]Aramis s.r.l., Milano, Italy
[4]Chair on Systems Science and Energetic Challenge, Fondation EDF, Ecole Central Supelec, France

Abstract

In the framework of Probabilistic Risk Assessment (PRA), we develop a method to support the selection of cost-effective portfolios of safety measures. This method provides a systemic approach to determining the optimal portfolio of safety measures that minimizes the risk of the system and thus provides an alternative to using risk importance measures for guiding the selection of safety measures. We represent combinations of events leading to system failure with Bayesian Belief Networks (BBNs) which can be derived from traditional Fault Trees (FTs) and are capable of encoding event dependencies and multi-state failure behaviours. We also develop a computationally efficient enumeration algorithm to identify which combinations (portfolios) of safety measures minimize the risk of failure at different costs of implementing the safety measures. The method is illustrated by revisiting an earlier case study concerning the airlock system of a CANDU Nuclear Power Plant (NPP). The comparison of results with those of choosing safety measures based on risk importance measures shows that our approach leads to considerably lower residual risk at different cost levels.

Keywords: Bayesian Belief Networks, Portfolio Optimization, Risk Analysis, Safety barriers, Risk Importance Measures

[*]Corresponding author. Tel.: +358 465704346. E-mail address: alessandro.mancuso@aalto.fi (A. Mancuso)

Nomenclature

V set of nodes

N number of nodes

$V^L \subset V$ set of leaf nodes

$V^D \subset V$ set of dependent nodes

$V^T \subset V$ set of target nodes

$V^A \subseteq V$ set of nodes at which safety measures can be implemented

E set of arcs

V^i_- set of predecessors of node $i \in V$

d^i depth of node $i \in V$

$\mathcal{A}^i$ set of possible safety measures at node $i \in V^A$

$z^i_a \in \{0, 1\}$ binary decision variable for indicating safety measure $a \in \mathcal{A}^i$

$\mathbf{X}^i$ random variable representing the uncertainty in the state of the event at node $i \in V$

$\mathcal{S}^i$ set of states of the event at node $i \in V$

$\mathcal{P}_{X^i}(s)$ probability of the event that node $i \in V^L$ is in state $s \in \mathcal{S}^i$

$\mathcal{P}_{X^i_a}(s)$ probability of the event that node $i \in V^L$ is in state $s \in \mathcal{S}^i$ given the implementation of safety measure $a \in \mathcal{A}^i$

$\mathcal{Q}_{X^i}(s)$ total probability of the event that node $i \in V$ is in state $s \in \mathcal{S}^i$

$u^t(s)$ disutility function of state $s \in \mathcal{S}^t$ at node $t \in V$

$\mathcal{U}^t(s)$ expected disutility of state $s \in \mathcal{S}^t$ at node $t \in V$

$R_a(s)$ Risk Reduction Rate of safety measure $a \in \mathcal{A}^i$ in state $s \in \mathcal{S}^i$

c_a cost of safety measure $a \in \mathcal{A}^i$

Λ time periods

r annualized discount rate

1 Introduction

In the nuclear industry, Probabilistic Risk Assessment (PRA) is used for identifying the risk importance of events or components [1]. For quantifying importance, Risk Importance Measures (RIMs), such as Risk Reduction Worth (RRW), Fussel-Vesely (FV), Risk Achievement Worth (RAW), are used to rank the component failure events, whereafter the available budget for system safety improvements ([2], [3]) is allocated based on this ranking. This leads to an iterative procedure in which the most risky components are identified sequentially and safety measures are then applied to reduce their failure probabilities [1]. The procedure is repeated until the budget for safety measures is depleted or the risk becomes acceptable with respect to a given predefined criterion [4].

However, the resulting portfolio of safety measures may not be optimal, because the safety measures for the identified risk-important components are chosen one at a time, while systemic cost and feasibility constraints are considered only later. To address this issue, Zio and Podofillini [5] propose an approach based on genetic algorithms to find optimal inspection periods of system components with respect to (i) cost reduction, (ii) increase in system reliability and (iii) reduction of the mutual differences among the importance values of the components. Even so, this approach does not ensure that the portfolios of safety measures are cost-efficient in terms of reducing the risk of the system most.

Building on the principles of cost-benefit analysis, Vesely [6] develops a method to reallocate resources so that the relative cost expended on an activity or requirement is equal to its relative risk importance. This approach evaluates single activities and consequently does not analyze all the combinations (portfolios) of events leading to system failure. As a result, the identified strategies can be suboptimal.

In the framework of Portfolio Decision Analysis (PDA, [7]), Toppila and Salo [8] propose a portfolio optimization approach in which coherent Fault Trees [9] are used to model the system reliability and to solve the redundancy allocation problem [10], accounting also for the uncertainties in the occurrence probabilities of the basic events. However, this approach focuses mainly on modelling how the risk reduction portfolios impact the probability of system failure in order to determine when optimal portfolios lead to biggest improvements in system reliability at different cost levels.

As pointed out also by Toppila and Salo [8], using FTs for risk analysis has some limitations. Indeed, in spite of the clear visual representation of the analyzed combinations of events leading to system failure ([11], [12]), they are not suitable for describing multi-state component behaviours (e.g., "No leakage", "Minor leakage" and "Major leakage" for a component leakage failure, [13], [14]).

In this paper, we propose a PRA-based decision support methodology to identify the optimal portfolio of safety measures that minimizes the residual system risk while accounting for feasibility and budget constraints. The methodology represents the combinations of events

leading to system failure as BBNs ([15], [16]), which overcome the limitations of FTs by offering the possibility of modelling multi-state events and extending the concepts of AND/OR gates.

The approach can be readily deployed by mapping FTs into BBNs [17] in which the BBN nodes represent events of the FT and the arcs represent causal dependencies among them. The occurrence probabilities of the basic events, and the conditional probability tables of the intermediate events and top event, can be either inferred by statistical analysis or elicited from experts, depending on the available knowledge, information and data.

The rest of the paper is structured as follows. Section 2 presents the methodology, i.e., the BBN representation, the optimization formulation and its implementation as an enumeration algorithm. Section 3 revisits the case study concerning the airlock system of a CANDU NPP [18] and gives a comparison with the selection of safety measures based on RIMs. Section 4 discusses the potential of the proposed method further. Finally, Section 5 concludes the paper and outlines extensions for future research.

2 Problem formulation

We assume that the FT has already been converted into the corresponding BBN, for instance by the method proposed by Khakzad et al. [17]. Formally, a BBN is a directed acyclic graph consisting of:

- Nodes $V = \{1, ..., N\}$, shown as circles, represent the FT random events whose combinations can lead to system failure. More specifically, when the FT is converted into the BBN, some FT events can be merged to the same node; in general, there is no one-to-one correspondence between FT events and BBN nodes [17]. The target nodes for the risk analysis are indicated by the set $V^T \subset V$ and are shown as rounded squares. The set V^T includes the node associated with the top event of the FT [9], but it can contain other nodes which represent possible failures that deserve attention in risk analysis.

- Directed arcs $E \subseteq \{(i,j)|i,j \in V,\ i \neq j\}$ indicate conditional dependencies among nodes. Specifically, the arc $(j,i) \in E$ which connects node $j \in V$ to node $i \in V$ indicates that the event at node i is conditionally dependent on the event at node j.

The immediate follower nodes of $i \in V$ form the set $V_+^i = \{j|(i,j) \in E\}$, whereas its immediate predecessor nodes are in the set $V_-^i = \{j|(j,i) \in E\}$. Thus, all nodes can be partitioned into the set of *leaf nodes* $V^L = \{i \in V|V_-^i = \emptyset\}$ and its complement set of *dependent nodes* $V^D = V \backslash V^L = \{i \in V|V_-^i \neq \emptyset\}$.

A path is a sequence of nodes $(i_1, i_2, ..., i_\eta)$, $\eta > 1$ such that $(i_j, i_{j+1}) \in E,\ j < \eta$. Because the BBN is acyclic, there is no path $(i_1, i_2, ..., i_\eta)$, $\eta > 1$ such that $(i_j, i_{j+1}) \in E, j < \eta$ and $i_1 = i_\eta$.

For every node $i \in V$, its depth in the network can be calculated recursively by

$$d^i = \begin{cases} 0, & V_-^i = \emptyset \\ 1 + max_{j \in V_-^i} d^j, & V_-^i \neq \emptyset \end{cases}. \tag{1}$$

In our methodology, it is possible to apply safety measures at a set of action nodes $V^A \subseteq V$ at which the probability distribution for random events can be modified. Specifically, at each action node, there is a decision on which of a finite number of alternative safety measure(s) will be applied, if any. The nodes V^A are indicated by a square over the circle.

Formally, at node $i \in V^A$, the set of alternative safety measures is $\mathcal{A}^i = \{1, ..., |\mathcal{A}^i|\}$, where $|\cdot|$ is the cardinality of the set. In general, the safety measures differ in terms of their impact on risk reduction and cost of implementation.

Specifically, the choice on the safety measure at node $i \in V^A$ is indicated by the binary decision variable z_a^i, which is 1 if $a \in \mathcal{A}^i$ is applied and 0 if not. Thus, the portfolio of safety measures $A \subseteq \mathsf{X}_{i \in V^A} \mathcal{A}^i$ is defined by the binary vectors $\mathbf{z}^i = [z_a^i], \ \forall a \in \mathcal{A}^i$, where $\mathsf{X}_{i \in V^A}$ indicates the Cartesian product of sets $\mathcal{A}^i$. There are no safety measures available for nodes $i \in V \backslash V^A$: this is modelled by $\mathcal{A}^i = \emptyset$ so that $|\mathcal{A}^i| = 0$.

Figure 2 illustrates an example of a BBN, where $V^L = \{1, 2, 3, 4, 5, 6, 7, 8\}$, $V^D = \{9, 10, 11, 12, 13, 14\}$, $V^T = 14$ and safety measures can be applied at nodes $i \in V^A = \{1, 2, 3, 4, 5, 6, 7, 8, 13\}$. For instance, if there are three possible safety measures at nodes $i \in V^A$, then one possible portfolio of safety measures is $A = \{a_2^1, a_1^2, a_3^3, a_1^4, a_3^5, a_2^6, a_1^7, a_2^8, a_3^{13}\}$, where the superscript and the subscript indicate the node and the safety measure index, respectively. Thus, the portfolio A is uniquely defined by the binary vectors

$$\mathbf{z}^i = [1, 0, 0], \quad i \in \{2, 4, 7\}$$
$$\mathbf{z}^i = [0, 1, 0], \quad i \in \{1, 6, 8\}$$
$$\mathbf{z}^i = [0, 0, 1], \quad i \in \{3, 5, 13\}.$$

We define the binary vector $\mathbf{z}$ as the concatenation of vectors $\mathbf{z}^i, \ \forall i \in V^A$ such that

$$z_k = \begin{cases} z_k^{i^*}, & i^* = \min\{j | j \in V^A\}, \ k = 1, 2, ..., |\mathcal{A}^{i^*}| \\ z_{k-q}^{j^*}, & k = |\mathcal{A}^{i^*}| + 1, ..., \sum_{i \in V^A} |\mathcal{A}^i|, \end{cases} \tag{2}$$

where

$$j^* = \min\{j \in V^A | \sum_{i=1}^{j} |\mathcal{A}^i| \geq k\}, \tag{3}$$

$$q = \sum_{i=1}^{j^*-1} |\mathcal{A}^i|. \tag{4}$$

Thus, the relation between $\mathbf{z}$ and the portfolio A is a bijection. In the previous example, the vector $\mathbf{z}$ for the portfolio A is

$$\mathbf{z} = [0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1].$$

The size of the binary vector $\mathbf{z}$ is $m = \sum_{i \in V^A} |\mathcal{A}^i|$.

2.1 Characterization of conditional probability tables

The conditional probability distributions extend the concept of the AND/OR gates in the FT. This gives more flexibility than FTs for modelling how combinations of events can lead to system failure. For example, Figure 1 shows a generic FT characterized by an AND gate and its corresponding BBN obtained with the methodology proposed by Khakzad et al. [17].

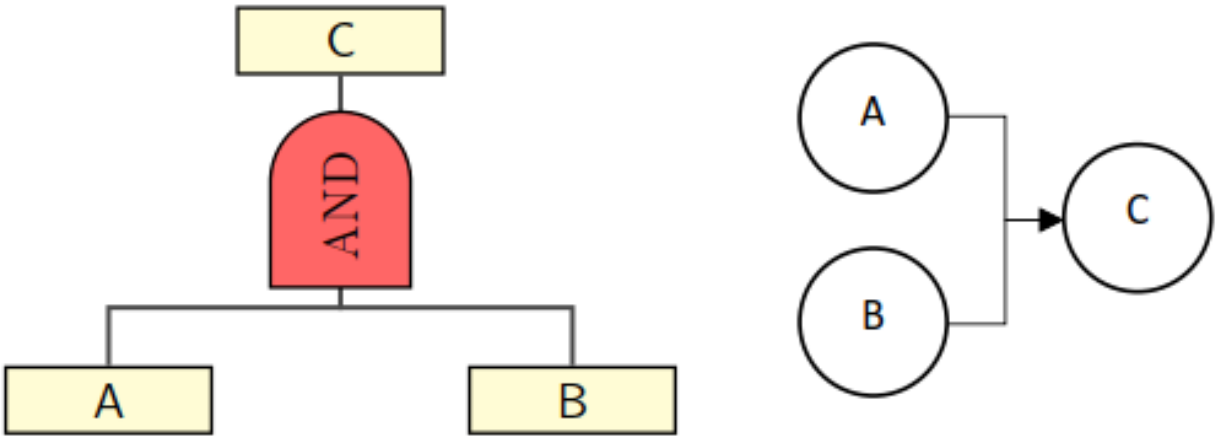


Figure 1: Correspondence between FT (left) and BBN (right).

The rules provided by the AND gate in Figure 1 are reported on the left side in Table 1. This information leads to the conditional probability table of the BBN. Specifically, the right side in Table 1 relies on the BBN in Figure 1 reflecting the logic of the AND gate. However, in contrast to the binary logic of the FT, the BBN makes it possible to specify the probability distribution. For instance, in the right side in Table 1 the event C occurs with probability 98 % if the events A and B occur simultaneously, whereas the probability is reduced to 3 % if either A or B does not occur and to 1 % if none of them occurs.

Table 1: Conditional probability tables for FT (left) and BBN (right).

$\mathcal{P}_{XC}$		C	$\overline{C}$
A	B	1	0
	$\overline{B}$	0	1
$\overline{A}$	B	0	1
	$\overline{B}$	0	1

$\mathcal{P}_{XC}$		C	$\overline{C}$
A	B	0.98	0.02
	$\overline{B}$	0.03	0.97
$\overline{A}$	B	0.03	0.97
	$\overline{B}$	0.01	0.99

Conditional probabilities can be derived from expert judgements and statistical analyses. When the conditional probability tables are elicited from experts, systematic approaches can

be adopted to reduce the number of statements needed. For instance, the noisy-OR model ([19], [20]) or the β-factor model ([21], [22]) can be used for this purpose.

2.2 Optimization model

The impact of a safety measure on what combination of events causes system failure depends on the severity of the failure and how effective the safety measure is in counteracting this combination.

Let $\mathbf{X}^i$ be the random variable representing the uncertainty in the state of event at node $i \in V$. The realization s of $\mathbf{X}^i$ belongs to the set of states $\mathcal{S}^i = \{0, ..., |\mathcal{S}^i|\}$, where state $s = 0$ indicates that the event at node $i \in V$ does not occur whereas states $s > 0$ refer to events of increasing magnitude of failure and thus increasing severity of consequences [9]. For example, in Figure 2 the different states of node "Pipe leakage" ($i = 3$) are: "No pipe leakage" ($s = 0$), "Minor pipe leakage" ($s = 1$), "Major pipe leakage" ($s = 2$).

Uncertainty about the realization of $\mathbf{X}^i$ of the event at node $i \in V^L$ is modelled through the probability mass distribution $\mathcal{P}_{X^i}(s) = p(\{\mathbf{X}^i = s\}) \geq 0$ such that

$$\sum_{s \in \mathcal{S}^i} \mathcal{P}_{X^i}(s) = 1, \ \forall i \in V^L. \tag{5}$$

At leaf nodes $i \in V^L \cap V^A$ where safety measures can be applied, applying a safety measure $a \in \mathcal{A}^i$ modifies the probability distribution by turning $\mathcal{P}_{X^i}(s)$ into $\mathcal{P}_{X^i_a}(s)$, where

$$\sum_{s \in \mathcal{S}^i} \mathcal{P}_{X^i_a}(s) = 1, \quad \forall a \in \mathcal{A}^i. \tag{6}$$

Without losing generality, we can assume that the safety measures at node $i \in V^A$ are mutually exclusive. This implies that at most one safety measure can be selected from set $\mathcal{A}^i$ so that the following inequality holds

$$\sum_{a \in \mathcal{A}^i} z^i_a \leq 1, \quad \forall i \in V^A. \tag{7}$$

Thus, the probability that the event at node $i \in V^L \cap V^A$ is in state $s \in \mathcal{S}^i$ is

$$\mathcal{Q}_{X^i}(s) = \sum_{a \in \mathcal{A}^i} z^i_a \, \mathcal{P}_{X^i_a}(s). \tag{8}$$

At every dependent node $i \in V^D$, the probability $\mathcal{P}_{X^i}(s)$ is conditional on the states of the random variables at its predecessor nodes. To model this relationship, we define the random variable $\mathbf{X}^i_-$ as the $|V^i_-|$-dimensional vector composed of the random variables $\mathbf{X}^j$, $\forall j \in V^i_-$.

Let $\mathcal{S}^i_-$ be the set of the Cartesian product of all the sets of states $\mathcal{S}^j$, $j \in V^j_-$. Then, a possible realization of $\mathbf{X}^i_-$ is indicated by the vector $\mathbf{x}^i \in \mathcal{S}^i_-$, whose j-th entry x^i_j represents the

realization of the corresponding random variable $\mathbf{X}^j$, $j \in V^i_-$. Then, the conditional probability of state $s \in \mathcal{S}^i$ of the event at node $i \in V^D \cap V^A$, given $\mathbf{x}^i \in \mathcal{S}^i_-$, is

$$\mathcal{Q}_{X^i|\mathbf{x}^i}(s) = \sum_{a \in \mathcal{A}^i} z^i_a \, \mathcal{P}_{X^i_a|\mathbf{x}^i}(s) \tag{9}$$

where $\mathcal{P}_{X^i_a|\mathbf{x}^i}(s)$ is the conditional probability of state $s \in \mathcal{S}^i$ of the event at node $i \in V^D \cap V^A$, given the realization $\mathbf{x}^i$ of its predecessors and that the safety measure $a \in \mathcal{A}^i$ is applied to mitigate the event at node $i \in V^D \cap V^A$.

The total probability of state $s \in \mathcal{S}^i$ of the event at node $i \in V^D \cap V^A$ can now be expressed recursively as

$$\mathcal{Q}_{X^i}(s) = \sum_{\mathbf{x}^i \in \mathcal{S}^i_-} \left[\sum_{a \in \mathcal{A}^i} z^i_a \, \mathcal{P}_{X^i_a|\mathbf{x}^i}(s) \right] \prod_{j \in V^i_-} \mathcal{Q}_{X^j}(x^i_j), \tag{10}$$

where the first summation is taken over all possible realizations $\mathbf{x}^i \in \mathcal{S}^i_-$. Here the total probability $\mathcal{Q}_{X^i}(s)$ is a multiplicative function of the safety measures that have been applied along the paths leading from the leaf nodes to $i \in V^D$. Note that for leaf nodes, the term $\mathcal{Q}_{X^j}(x^i_j)$ on the right side is obtained from (8).

As mentioned in Section 1, the objective of the analysis is to evaluate the risk at the target nodes $t \in V^T$ for different impacts of the portfolio of safety measures. The risk at node $t \in V^T$ is not acceptable if the probability $\mathcal{P}_{X^t}(s)$ is greater than the accepted threshold for at least one state $s \in \{1, ..., \mathcal{S}^t\}$. We assume that the larger the value of the realized state $\mathbf{X}^i = s$, the larger the magnitude of failure, then the smaller the probability threshold.

The expected disutility assigned to the target node $t \in V^T$ given the portfolio $\mathbf{z}$ is

$$\mathcal{U}^t(\mathbf{z}) = \sum_{s \in \mathcal{S}^t} \mathcal{Q}_{X^t}(s) \; u^t(s) \tag{11}$$

where $u^t(\cdot)$ is the disutility function for quantifying the severity of state $s \in \mathcal{S}^t$ [24]. Namely, $u^t(s) = 0$ if state $s \in \mathcal{S}^t$ refers to an event of negligible consequences, whereas $u^t(|S^t|) = 100$. If $|\mathcal{S}^t| > 2$, then the other intermediate states $s \in \mathcal{S}^t \backslash \{0, |S^t|\}$ can be assigned disutilities $u^t(s) \in]0, 100[$ by expert judgements, with reference to the enclosing points $u^t(0)$ and $u^t(|S^t|)$.

Estimates for $u^t(s)$, $\forall s \in \mathcal{S}^t$ can be elicited through trade-off weighing approaches SMART [23], SWING [24] or SMARTS [25] by treating the states $s \in \mathcal{S}^t$ as alternatives. If the target node $t \in V^T$ represents a binary event, the goal is to minimize the total probability $\mathcal{Q}_{X^t}(1)$ by setting $u^t(0) = 0$ and $u^t(1) = 100$.

Finally, different safety measures $a \in \mathcal{A}^i$ have different costs c_a: the optimization model accounts for the overall cost of the portfolio, which must not exceed the available budget B.

Let $m = \sum_{i \in V^A} |\mathcal{A}^i|$ be the size of the binary vector $\mathbf{z}$, the selection of safety measures for a single target node $t \in V^T$ is formalized as the following portfolio optimization problem

$$\mathbf{z}^* = \arg \min_{\mathbf{z} \subseteq \{0,1\}^m} \mathcal{U}^t(\mathbf{z}) \tag{12}$$

$$\mathcal{Q}_{X^i}(s) = \sum_{a \in \mathcal{A}^i} z_a^i \, \mathcal{P}_{X_a^i}(s) \quad \forall i \in V^L \cap V^A \tag{13}$$

$$\mathcal{Q}_{X^i}(s) = \sum_{\mathbf{x}_-^i \in \mathcal{S}_-^i} \left[\sum_{a \in \mathcal{A}^i} z_a^i \, \mathcal{P}_{X_a^i|\mathbf{x}^i}(s) \right] \prod_{j \in V_-^i} \mathcal{Q}_{X^j}(x_j^i) \quad \forall i \in V^D \cap V^A \tag{14}$$

subject to the constraints

$$\sum_{a \in \mathcal{A}^i} z_a^i \leq 1, \quad \forall i \in V^A \tag{15}$$

$$\sum_{i \in V^A} \sum_{a \in \mathcal{A}^i} z_a^i \, c_a \leq B \tag{16}$$

$$\mathbf{z}^i \in \{0,1\}^{|\mathcal{A}^i|} \quad \forall i \in V^A. \tag{17}$$

The calculation of the total probabilities $\mathcal{Q}_{X^i}(s)$ starts from the leaf nodes $i \in V^L$ and proceeds to those at the dependent nodes $i \in V^D$ by increasing the node depth d^i in (1). This is necessary because the calculation of the total probability $\mathcal{Q}_{X^i}(s)$ requires the total probabilities $\mathcal{Q}_{X^j}(s)$ of all the predecessors $j \in V_-^i$.

It is possible to introduce additional constraints which specify requirements of the system. For instance, with reference to Figure 2, if the safety measures for reducing the probability of "Gearbox failure" ($i = 6$) and "Exhaust pipe failure" ($i = 7$) are mutually exclusive, the following constraint holds

$$\sum_{a \in \mathcal{A}^6} z_a^6 + \sum_{a \in \mathcal{A}^7} z_a^7 \leq 1. \tag{18}$$

On the other hand, if at least one safety measure at nodes $i = 6$ and $i = 7$ must be applied, the corresponding constraint is

$$\sum_{a \in \mathcal{A}^6} z_a^6 + \sum_{a \in \mathcal{A}^7} z_a^7 \geq 1. \tag{19}$$

The same safety measure can impact different nodes or several safety measures must be applied simultaneously. If a safety measure a impacts two different nodes $i, j \in V^A$, then this measure must be included in both sets $\mathcal{A}^i$ and $\mathcal{A}^j$, making it necessary to introduce the constraint

$$z_a^i = z_a^j. \tag{20}$$

Furthermore, to avoid the double-counting of the cost c_a of such safety measure a, this cost can be fully allocated to the safety measure $a \in \mathcal{A}^i$ and set the cost of the safety measure $a \in \mathcal{A}^j$ to zero.

If two different safety measures $a \in \mathcal{A}^i$ and $a' \in \mathcal{A}^j$ must be applied simultaneously (i.e., safety measure $a \in \mathcal{A}^i$ can be applied if and only if safety measure $a' \in \mathcal{A}^j$ is applied too), the corresponding constraint is

$$z_a^i = z_{a'}^j. \tag{21}$$

Such additional constraints limit the set of feasible solutions and, thus, affect the resulting optimal portfolio of safety measures.

2.3 Optimization algorithm

For identifying the optimal portfolio of safety measures, we have developed the implicit enumeration algorithm in Appendix, based on Liesiö [26]. While the algorithm is computationally viable, its computational time depends on the number of nodes of the BBN and the amount of alternative safety measures per node.

The algorithm identifies the optimal portfolio $\mathbf{z}^*$ by first discarding the non-feasible solutions and, then, by evaluating the ones minimizing the expected disutility $\mathcal{U}^t$ of the single target node $t \in V^T$. Although the detailed algorithm is presented for the single-objective problem ($|V^T| = 1$), we note that it can be readily extended to multiple target nodes ($|V^T| > 1$). To this aim, we propose two different approaches.

First, according to the traditional risk analysis approach, the experts can introduce additional constraints so that the total probability $\mathcal{Q}^t(s)$ of states $s \in \mathcal{S}^t \backslash 0$ must not exceed the acceptable threshold $\epsilon^t(s)$ such that

$$\mathcal{Q}^t(s) \leq \epsilon^t(s), \quad \forall t \in V^T. \tag{22}$$

The values of $\epsilon^t(s)$ are usually provided by regulatory committees for NPP applications, for instance the United States Nuclear Regulatory Commission. The constraints must be fulfilled so that the risk of each target node is acceptable. However, it is also possible that the constraints limit the set of feasible solutions so much that no portfolios are feasible. By applying this approach, the problem would still be modelled as a single-objective optimization.

On the other hand, a multi-objective optimization problem would account for the expected disutility $\mathcal{U}^t$ of all the target nodes $t \in V^T$. This way, the optimal portfolio of safety measures would be selected among the Pareto optimal frontier, i.e. the set of non dominated portfolios of safety measures [27]. Specifically, let $t_1 \in V^T$ and $t_2 \in V^T$ be two target nodes whose expected disutilities are $\mathcal{U}^{t_1}$ and $\mathcal{U}^{t_2}$. In risk analysis there is often no explicit preference structure between the nodes. In this case, it is helpful to identify the entire Pareto optimal frontier, whose dominance condition between two portfolios $\mathbf{z}'$ and $\mathbf{z}''$ is defined by

$$\mathbf{z}' \succ \mathbf{z}'' \Leftrightarrow \begin{cases} \mathcal{U}^{t_1}(\mathbf{z}') \leq \mathcal{U}^{t_1}(\mathbf{z}'') \ \wedge \ \mathcal{U}^{t_2}(\mathbf{z}') < \mathcal{U}^{t_2}(\mathbf{z}'') \\ \mathcal{U}^{t_1}(\mathbf{z}') < \mathcal{U}^{t_1}(\mathbf{z}'') \ \wedge \ \mathcal{U}^{t_2}(\mathbf{z}') \leq \mathcal{U}^{t_2}(\mathbf{z}'') \end{cases}, \tag{23}$$

where $\mathcal{U}^t(\mathbf{z})$ represents the expected disutility at node $t \in V$ given by the portfolio $\mathbf{z}$.

3 CANDU NPP airlock system case study

We illustrate our methodology by revisiting the Design Basis Accident (DBA) that occurred in the airlock system of a CANDU NPP in 2011 ([18], [28]). The Airlock System (AS) is a safety system which keeps the pressure of the inner side of the reactor vault lower than the outer side. This pressure difference prevents the dispersion of contaminants from the reactor

bay in case of failure. Specifically, the AS consists of a vessel in the containment wall of the reactor vault and its doors allow the operators to access the vault for inspection. One door opens towards the inside, the other towards the outside.

At least one airlock door must be closed to guarantee the negative pressure drop. Each door is closed by a latch and by seals which are inflated by the air system. In case of a failure, the inflation of the seals must be switched to the back-up air supply tank. A pressure equalizer system, which can be activated only once the door latch is detected in closed position, is designed to equalize the pressure between the reactor bay and the service side and, therefore, to control the air flow between these two areas.

The target node represents the event that the single door cannot be tightened so that the airlock system fails to maintain the pressure boundary (Appendix 7.2, [18]). For simplicity, we do not replicate the same FT for the second door of the airlock system.

Possible causes for the occurrence of this target node are:

- Failure of the pressure equalizer system: This event is due to the combination of the gear box failure (which does not allow vents to open and close on-demand) and the failure to close the exhaust pipe (which prevents the equalizer from reaching the desired pressure level).

- Door failure: The door fails to close because the latches are not locked.

- Sealing system failure: This event can be caused by either (i) a failure in inflating the seals (which is due to a failure to open the valve controlling the inflation, a major pipe leakage spreading out the inflating air or a failure to engage the back-up tank) or (ii) continuous air deflating (which requires that (i) the back-up tank is already empty and can no longer compensate the air deflating and that (ii) there is a failure in the inflating air piping system). The piping failure can be caused by a crack in the seal, a pipe leakage or a valve failure.

The FT in Appendix 7.2 is transformed into the BBN in Figure 2 in which every leaf node corresponds to a basic event of the FT, except for the two events "Minor pipe leakage" and "Major pipe leakage", which are combined into the joint event "Pipe leakage" with three states: "No leakage", "Minor leakage" and "Major leakage". In particular, the events "Minor pipe leakage" and "Major pipe leakage" are not independent. This would be difficult to model in a FT, whereas a BBN can handle this situation by combining the events into one single node defined by different states.

The BBN resembles the top-down structure of the FT, with arcs connecting consequent events to model the failure scenarios. Statistical analyses and expert opinions can be used to define the prior probabilities and the conditional probability tables of the BBN. These tables also capture the rules of the AND/OR gates of FT.

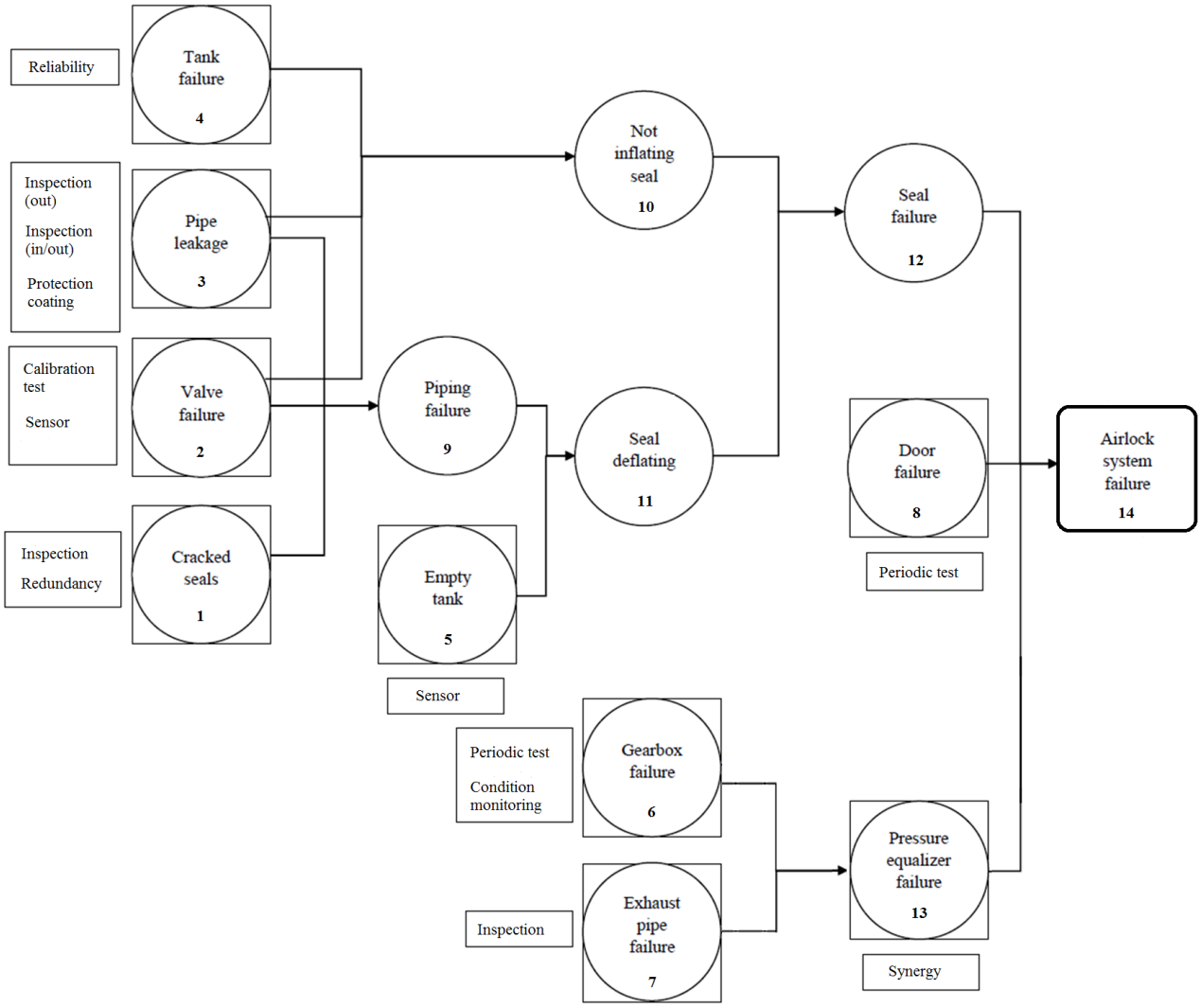


Figure 2: BBN for the airlock system failure.

Table 2 lists the safety measures $a^i_j, i \in V^A = \{1, 2, 3, 4, 5, 6, 7, 8, 13\}, j \in \{1, 2, ..., |\mathcal{A}^i|\}$ that can be applied to the events at nodes $i \in V^A$ to mitigate the event at the target node $t = 14$. Although most safety measures apply to leaf nodes, our approach can accommodate situations in which safety measures are applied at nodes whose depth is $d^i > 1$.

Specifically, we consider the safety measure "Synergy" ($a^{13}_1 \in \mathcal{A}^{13}$) applied to mitigate the event "Pressure equalizer failure" ($i = 13$) at the second level $d^{13} = 2$. This safety measure represents the combination of safety measures "Periodic test" ($a^6_1 \in \mathcal{A}^6$) and "Inspection plan" ($a^7_1 \in \mathcal{A}^7$), such that

$$\begin{aligned} 2z_{a^{13}_1} &\leq z_{a^6_1} + z_{a^7_1} \\ z_{a^{13}_1} &\geq z_{a^6_1} + z_{a^7_1} - 1. \end{aligned} \tag{24}$$

The synergy does not reduce risks, but saves costs by $c^{13}_1 = -30$ k€ for joined inspections at the gearbox and the exhaust pipe. We define the cost of the safety measure $a^i_j \in \mathcal{A}^i$ as $c^i_j = c_{a^i_j}$

(fourth column in Table 2).

Furthermore, the possibility to take several alternative safety measures simultaneously at the same node can be captured by explicitly modelling different combinations of safety measures. For example, consider the safety measure "Joined actions" ($a_3^2 \in \mathcal{A}^2$) which represents a combination of the safety measures "Calibration test" ($a_1^2 \in \mathcal{A}^2$) and "Sensor" ($a_2^2 \in \mathcal{A}^2$) at the node "Valve failure" ($i = 2$) such that the optimization model can select either one of the two separate safety measures or both. To this aim, the safety measure "Joined actions" is modelled as an additional safety measure, which accounts for the joint impact on the probability of "Valve failure" and the cost of the combined safety measures "Calibration test" and "Sensor". This additional safety measure avoids the need to account for the same probabilities multiple times and circumvents the limitation of applying a single safety measure at each node.

In this example, we simplify the data elicitation process by assigning Risk Reduction Rates $R_a(s)$ to every safety measure $a \in \mathcal{A}^i$. These safety measures modify the occurrence probability of the state $s \in \mathcal{S}^i \backslash 0$ of the event at node $i \in V^A$ so that

$$\mathcal{P}_{X_a^i}(s) = \mathcal{P}_{X^i}(s) \cdot R_a(s). \tag{25}$$

In general, the Risk Reduction Rates $R_a(s)$ can depend on the states s, but they can be equal for all $s \in \mathcal{S}^i$. Illustrative values of the Risk Reduction Rates are shown in the fifth and sixth columns of Table 2.

Finally, the cost of a safety measure (fourth column in Table 2) can be due to large initial capital investments or the accumulation of periodic expenses over the life cycle. To compare portfolios of safety measures, the cost of a safety measure can be discounted over the life cycle. In this respect, the annualized cost of a safety measure $a \in \mathcal{A}^i$ is calculated over the set Λ of time periods as

$$c_a = \sum_{\lambda \in \Lambda} \frac{c_a^\lambda}{(1+r)^\lambda}, \tag{26}$$

where c_a^λ represents the cost of safety measure $a \in \mathcal{A}^i$ at period $\lambda \in \Lambda$ and r is the discounted rate to account for the life cycle of the system [29].

For instance, in Table 2, we consider three different safety measures for reducing the probability of "Pipe leakage" ($i = 3$): "Outer inspection" ($a_1^3 \in \mathcal{A}^3$), "Inner and outer inspection" ($a_2^3 \in \mathcal{A}^3$) and "Protection coating" ($a_3^3 \in \mathcal{A}^3$). The first two involve planned inspections over $\Lambda = \{0, 1, 2, 3\}$ time periods, whereas the last one is an asset investment over the same planning horizon. If the two inspections per period cost $c_{a_1^3}^\lambda = 4$ k€/inspection and $c_{a_2^3}^\lambda = 6$ k€/inspection, the discounted costs of these two safety measures using an annualized rate $r = 0.05$, are

$$c_1^3 = 8 + \frac{8}{1.05} + \frac{8}{1.05^2} + \frac{8}{1.05^3} = 29.8 \approx 30\text{k€} \tag{27}$$

$$c_2^3 = 12 + \frac{12}{1.05} + \frac{12}{1.05^2} + \frac{12}{1.05^3} = 44.7 \approx 45\text{k€}. \tag{28}$$

On the other hand, the safety measure "Protection coating" has an initial expense of 60 k€ and a further maintenance intervention of 12 k€ at the third time period. Thus, the annualized cost of this safety measure is

$$c_3^3 = 60 + \frac{12}{1.05^3} = 70.3 \approx 70\text{k€}. \tag{29}$$

Illustrative annualized costs of the safety measures are reported in Table 2.

Table 2: Parameters of the safety measures.

Node	**Index**	**Safety measure**	c_a[k€]	$R_a(1)$	$R_a(2)$
Cracked seals	a_1^1	Inspection plan	60	10^{-3}	-
	a_2^1	Duplicating	80	10^{-4}	-
Valve failure	a_1^2	Calibration test	30	10^{-1}	-
	a_2^2	Sensor	40	10^{-2}	-
	a_3^2	Joined actions	60	10^{-4}	-
Pipe leakage	a_1^3	Outer inspection	30	10^{-1}	$10^{-1.5}$
	a_2^3	Inner and outer inspection	45	10^{-2}	$10^{-2.5}$
	a_3^3	Protection coating	70	10^{-3}	10^{-3}
Tank failure	a_1^4	Improving reliability	80	10^{-4}	-
Empty tank	a_1^5	Level sensor	60	10^{-3}	-
Gearbox failure	a_1^6	Periodic test	40	10^{-2}	-
	a_2^6	Condition monitoring	100	10^{-5}	-
Exhaust pipe failure	a_1^7	Inspection plan	40	10^{-2}	-
Door failure	a_1^8	Periodic test	60	10^{-4}	-
Pressure equalizer failure	a_1^{13}	Synergy	-30	1	-

The optimization model in Section 2.2 determines the optimal portfolios of safety measures that minimize the risk of the target node. Solutions have been found for different values B of the budget constraint (horizontal axis in Figure 3 and Figure 4).

Figure 3 shows the minimum probability of the airlock system failure that can be obtained by applying the optimal portfolio of safety measures, Figure 4 shows the optimal safety measure for every action node $i \in V^A$ in Figure 2 as a function of the available budget.

From Figure 3, we see that the minimum probability of airlock system failure remains practically the same for $B \geq 230$ k€ whereafter the risk reduction due to additional safety measures becomes negligible. As shown in Figure 4, if the budget is at least 230 k€, the optimal portfolio already contains the inspection of the door, the joined actions on the valve and the

reliability improvement of the tank. These events are directly linked to the target node by OR gates; thus, reducing their failure probabilities significantly reduces the probability of the airlock system failure. In contrast, the effects of other safety measures become negligible.

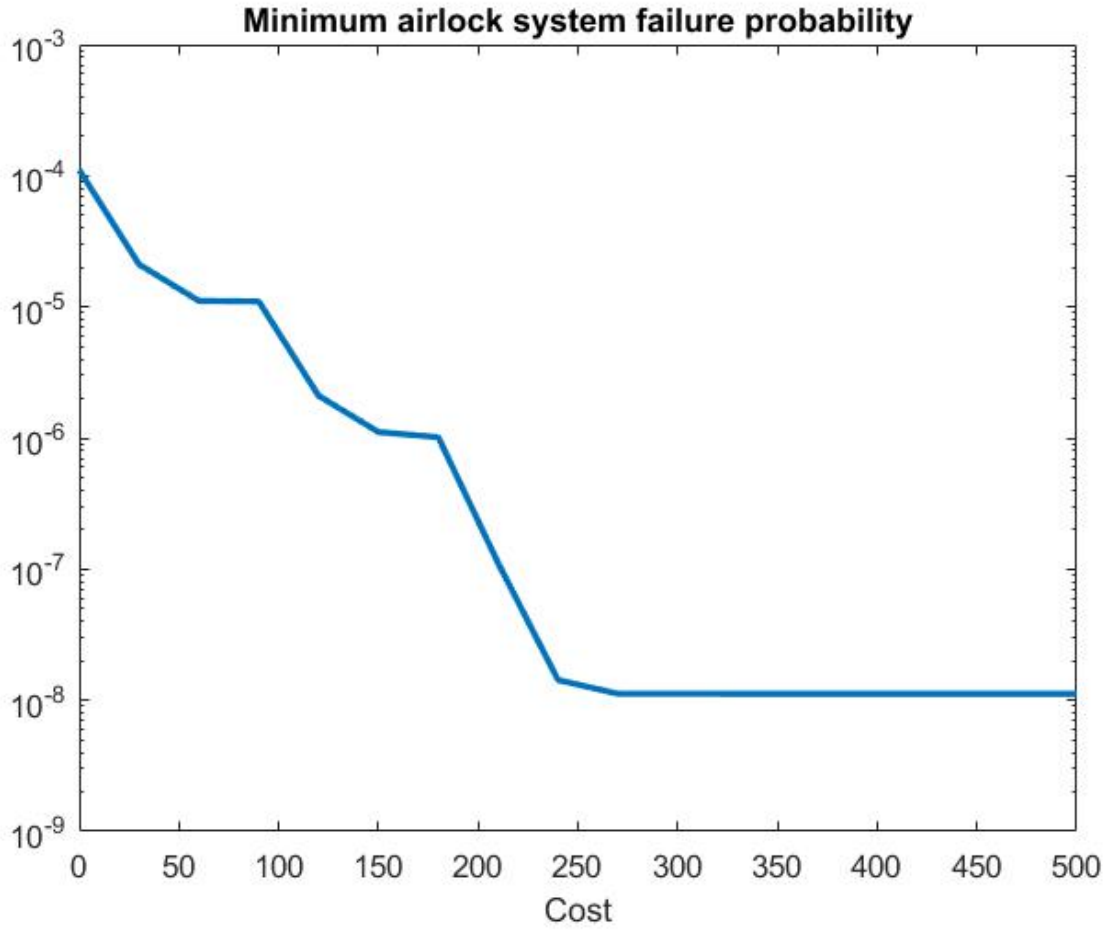


Figure 3: Probability of airlock system failure.

If the budget is low, safety measures should be applied to limit the events "Valve failure" and "Pipe leakage" because they impact two different nodes, "Piping failure" and "Not inflating seals". The safety measure "Synergy" ($a_1^{13} \in \mathcal{A}^{13}$) is applied only if "Periodic test" ($a_1^6 \in \mathcal{A}^6$) and "Inspection plan" ($a_1^7 \in \mathcal{A}^7$) also belong to the optimal portfolio, as modelled in (24).

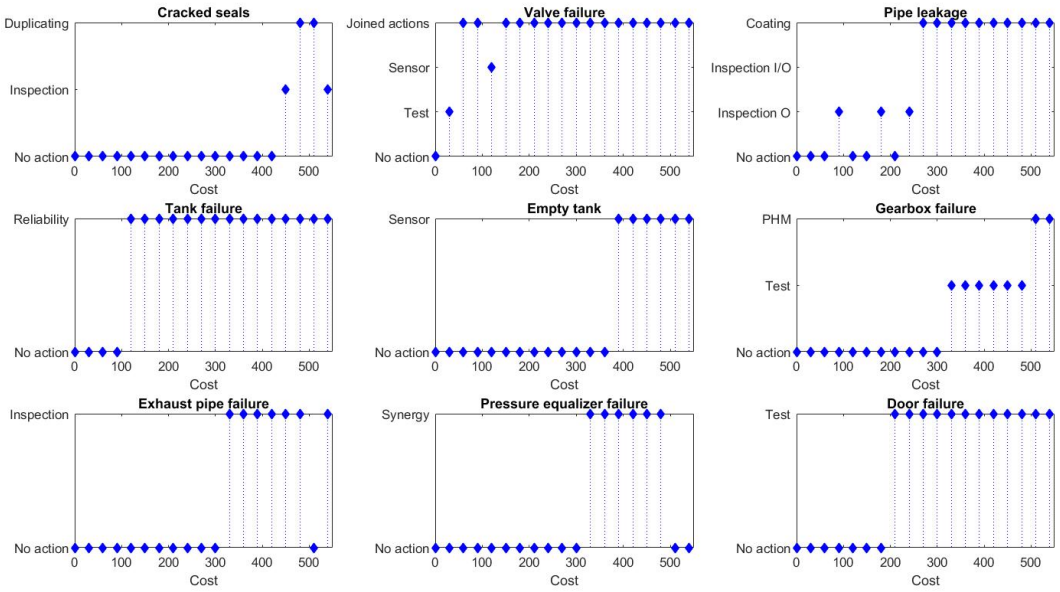


Figure 4: Optimal safety measure per event.

The portfolios of safety measures in Figure 4 are globally optimal in the sense that they minimize the failure probability of the airlock system while accounting for feasibility and budget constraints, instead of selecting safety measures that target the riskiness of the single events.

3.1 Comparison with a Risk Reduction Worth-based procedure

Risk Reduction Worth (RRW) is a risk importance measure which quantifies the maximum risk reduction that can be attained by setting the probability $\mathcal{P}_{X^i}(s), s > 0$ at node $i \in V^A$ to zero (see [2], [3] and [4] for details). This measure only applies to binary FTs, in which $\mathcal{S}^i = \{0, 1\}, \forall i \in V$ in our framework. Thus, it is necessary to apply small changes to the example in Section 3.

Once the components which contribute most to the improvement are identified, the expert can iteratively select safety measures to be applied. Namely, at iteration $\tau = 1$, the RRW values are computed for every node $i \in V^A$ as

$$RRW_\tau^i = \frac{\mathcal{W}_\tau^t}{\mathcal{W}_\tau^{t|i}}, \tag{30}$$

where $\mathcal{W}_\tau^t$ is the risk of the realization of the event $\mathbf{X}^t = 1$ at the target node $t \in V^T$ (i.e., the node related to the event of "Airlock system failure") and $\mathcal{W}_\tau^{t|i}$ is the risk of the realization $\mathbf{X}^t = 1$ of the target node $t \in V^T$ assuming $\mathcal{P}_{X^i}(0) = 1$, i.e. the realizations $\mathbf{X}^i \geq 1$ of the event at node $i \in V^A$ have been eliminated. We evaluate the risk $\mathcal{W}^t$ of the target node by the expected disutility $\mathcal{U}^t$ in (11). On this basis, at iteration $\tau = 1$, the node i_τ^* is selected so that

$$i_\tau^* = \arg\max_{i \in V^L} RRW_\tau^i, \tag{31}$$

whereafter experts decide which one out of appropriate safety measure(s) will be applied to reduce the risk of the event $i^*_\tau \in V^L \cap V^A$.

This procedure can be repeated at iteration $\tau = 2$ to determine the node $i^*_{\tau=2}$, which has the most risk reduction potential, given that a safety measure has been applied at node $i^*_{\tau=1}$. Then, the procedure is iterated until the budget has been depleted or the residual risk of the target node has been reduced to an acceptable level.

We illustrate this approach by analyzing the airlock system. At each iteration τ, we calculate the values of RRW for nodes $i \in V^A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ of which safety measures can be applied (Figure 2). We do not consider the safety measure "Synergy" ($a^{13}_1 \in \mathcal{A}^{13}$), because $R_{a^{13}_1}(1) = 1$, i.e. it does not have any additional impact on risk with respect to the two safety measures a^6_1 and a^7_1 that lead to this synergy.

At iteration $\tau = 1$, "Valve failure" ($i = 2$) has the largest RRW value

$$RRW_1 = [\approx 1; \approx 10; \approx 1; 1.01; \approx 1; \approx 1; \approx 1; 1.009]. \tag{32}$$

At node "Valve failure" ($i = 2$), two possible safety measures can reduce the risk of the target node. If the safety measure "Sensor" ($a^2_2 \in \mathcal{A}^2$) is chosen to prevent "Valve failure", the RRW values at iteration $\tau = 2$ are

$$RRW_2 = [\approx 1; 1.09; \approx 1; 5.76; \approx 1; \approx 1; \approx 1; 1.1]. \tag{33}$$

Continuing, after the safety measure "Sensor" to reduce the probability of "Valve failure" ($i = 2$) has been applied, the event "Tank failure" ($i = 4$) has the most potential for risk reduction. At this node, the only safety measure "Improving reliability" ($a^4_1 \in \mathcal{A}^4$) is also one of the most expensive, meaning that most of the available budget will be used, so that less expensive safety measures cannot be applied.

At iteration $\tau = 3$, after the safety measure to prevent "Tank failure" has been applied, we calculate the RRW values

$$RRW_3 = [\approx 1; 1.9; 1.05; \approx 1; \approx 1; \approx 1; \approx 1; 1.9]. \tag{34}$$

The events "Valve failure" ($i = 2$) and "Door failure" ($i = 8$) have the highest RRW values, in particular $RRW^2_3 = RRW^8_3$.

If the safety measure "Sensor" ($a^2_2 \in \mathcal{A}^2$) is applied to mitigate the event "Valve failure", the safety measure "Periodic test" ($a^8_1 \in \mathcal{A}^8$) is applied to prevent the event "Door failure". This way, at iteration $\tau = 4$, this approach would lead again to safety measures on the event "Valve failure" ($i = 2$), given that

$$RRW_4 = [\approx 1; 10.9; 1.01; \approx 1; \approx 1; \approx 1; \approx 1; \approx 1]. \tag{35}$$

If a second safety measure is applied to reduce the risk of this event, the joined actions may not have the same parameters of the two separate safety measures. Table 2 shows that

$$R_{a^2_3}(1) \neq R_{a^2_1}(1) \cdot R_{a^2_2}(1) \tag{36}$$

$$c_3^2 \neq c_1^2 + c_2^2. \tag{37}$$

Thus, if both safety measures at node "Valve failure" ($i = 2$) are applied, the solution would change, because the synergy in their Risk Reduction Rates would modify the RRW values at the iteration where the first safety measure has been applied ($\tau = 1$). Moreover, unlike our methodology, RIM-based procedures do not account for the eventual cost saving given by the combination of the safety measures "Inspection plan" ($a_1^6 \in \mathcal{A}^6$) and "Periodic test" ($a_1^7 \in \mathcal{A}^7$).

4 Discussion

The case study highlights one of the main advantages of framing the problem of selection of safety measures through PDA. The model does not target the riskiness of the single events; rather, it identifies the optimal portfolio of safety measures for the *overall system* and thus overcomes the limitations of taking decisions based on the iterative computation of RIMs and the choice of safety measures one-by-one.

Moreover, the BBN model of the system failure makes it possible to generalize the concepts of AND/OR gates. The impacts of the safety measures are modelled by updating the probability distributions of the affected nodes in the BBN. As a result, structural changes to the system, most notably those that correspond to the introduction/removal of nodes or dependencies between the nodes, call for revisions to the model itself. Specifically, the introduction/removal of dependencies call for changes in the dimensions and parameters of the conditional probability tables. In contrast, changes resulting from the introduction/removal of new nodes makes it necessary to introduce/remove these nodes and to elicit/revise the corresponding probability tables, too.

The framework is flexible in that multiple states at every node can be modelled. For example, consider the event "Pipe leakage" ($i = 3$) in Figure 2. The states of the leakage can be modelled as "No leakage", "Minor leakage" and "Major leakage" and even further states can be introduced as needed. Thus, the system representation is more realistic, although it increases the effort in the elicitation of the conditional probability tables.

On the other hand, RIM-based procedures are limited in that they cannot be applied in case of multi-state events or multiple target nodes. In fact, they are based on the definition of a single target node, while our methodology can accommodate multiple target nodes as described in Section 2.2.

Furthermore, RIM-based procedures apply to binary FTs in which safety measures can be applied to basic events only without accounting for synergies of joined safety measures. As shown in the preceding example, feasibility constraints or costs are considered only after the procedure has already selected the event that seemingly offers the most potential for risk reduction of the system failure: this could lead to an infeasible or cost-inefficient portfolio of safety measures. For example, the budget could be run out after few expensive safety measures,

while it could be the case that combinations of less expensive safety measures would lead to reduce the risk of the target node more.

Cost-benefit analyses based on the ratio between the RIM and the cost of the safety measure can also lead to infeasible or cost-inefficient portfolios of safety measures, because RIMs evaluate the riskiness of the events while cost is a parameter of the safety measure. For this reason, a cost-benefit analysis would support safety measures which have minimal cost in one-by-one comparisons.

In summary, this example illustrates that RIM-based procedures, such as those based on RRW, do not necessarily lead to an optimal solution, because at each iteration the importance measures are dependent on the previous decisions. Furthermore, the procedure involves assumptions and expert judgements, which can affect the decisions at the following iterations and the resulting portfolio of safety measures.

First, the RIM-based procedure does not select a specific safety measure; rather, the experts choose the most appropriate one(s) in view of the parameters of the safety measure parameters (annualized cost and impact on risk reduction) and the available budget. Second, different RIMs could give different and even conflicting indications to the experts [4]. Finally, the iteration $\tau = 3$ in this example highlights a further pitfall of a RIM-based procedure: the experts need support for selecting events which should be improved first. Our PDA framework addresses these issues explicitly.

If budget is $B = 350$ k€, the portfolios of safety measures for the two methodologies are in Table 3. The last row in Table 3 shows the probability of the event "Airlock system failure" for both solutions. The solution resulting from the RRW-based procedure depends on the authors' decisions at each iteration.

Table 3: Optimal set of safety measures for the two methodologies.

Node	**RRW approach**	**Portfolio optimization**
Cracked seals	Duplicating	-
Valve failure	Sensor Calibration test	Sensor Calibration test
Pipe leakage	Protection coating	Protection coating
Tank failure	Improving reliability	Improving reliability
Empty tank	-	-
Gearbox failure	-	Periodic test
Exhaust pipe failure	-	Inspection plan
Door failure	Periodic test	Periodic test
$\mathcal{Q}_{X^{14}}(1)$	$1.4173 \cdot 10^{-8}$	$1.1201 \cdot 10^{-8}$

While safety measures are applied in both methodologies, there are also significant differences due to the lack of systemic view of the RRW-based procedure. For example, at iteration $\tau = 6$ the RRW-based procedure identifies "Cracked seals" ($i = 1$) as the most risky event so that safety measure "Duplicating" ($a_2^1 \in \mathcal{A}^1$) is applied. On the other hand, the portfolio optimization recognizes that safety measures to prevent "Gearbox failure" ($i = 6$) and "Exhaust pipe failure" ($i = 7$) would reduce the risk of "Airlock system failure" at the same cost. Moreover, for the budget $B = 350$ k€, our solution reduces the risk of "Airlock system failure" to a level which is 21% less than the solution based on RRW (last row in Table 3). Note that RRW has been adopted as a reference for the comparison, but similar issues can be expected with the use of other RIMs as well.

In industries such as nuclear and aerospace, PRA models contain several thousands of components to which safety measures can be applied in order to reduce the probability of accident scenarios. In these cases, the standard approach based on RIMs is computationally straightforward in that the potentially most important components are first identified, albeit without analyzing how effective the available safety measures or combinations thereof are in mitigating the probability of accident scenarios. By design, the PDA approach is computationally more demanding, but it does account for the impact of the available safety measures while analyzing the relative importance of the components.

The PDA approach can be utilized in several ways for large systems. For instance, the experts can first employ RIMs to select computationally manageable portfolios consisting of the most risky components and then apply the PDA approach to make cost-effective decisions on the components within these pre-selected portfolios. The experts can also analyze portfolios

consisting of similar or comparable components to generate guidelines as to what kinds of safety measures are most cost-efficient for these components. Furthermore, complex PSA models are typically hierarchically structured and can be decomposed into several indenture levels. Then, the PDA approach can be used iteratively to first select the optimal portfolios of systems at the highest indenture levels and to determine corresponding risk reduction rates and costs. These solutions can be converted into requirements for the portfolio selection at the following lower indenture levels. Future research will focus on the computational and modelling issues arising from the application of the PDA approach to large-scale complex systems.

5 Conclusion and future research

In this paper, we have developed a methodology to support the selection of cost-efficient portfolios of safety measures in high-risk installations. The problem has been framed within the Portfolio Decision Analysis to support the selection of safety measures that improve the safety of the system cost-efficiently. The feasibility of the method has been illustrated with an example concerning an Airlock System in a CANDU NPP.

There are various opportunities for improving and extending this method. Specifically, one limitation of the methodology can be the effort in getting sufficient information to determine the failure probabilities and the conditional probability tables. This suggests two topics for further work. On one hand, the optimization model could be extended to account for the imprecision and uncertainty stemming from incomplete datasets or the qualitative statements provided by the experts. For example, the expert may provide imprecise values of both Risk Reduction Rates and costs of the safety measures. Such imprecision and uncertainty must be properly represented and propagated throughout the optimization model to obtain robust solutions. On the other hand, methods to facilitate the elicitation of parameters need to be developed so that experts need not to answer many and complex questions, which could introduce biases as well.

A further possibility is to extend the proposed methodology to time-dependent systems, for example to the analysis of fire scenarios [30]. In this case, the modelling of failure scenarios and impact of safety measures become more complicated. Techniques of Integrated Deterministic and Probabilistic Safety Assessment [31] could be used to address these issues.

6 Acknowledgements

The research has been supported by The Finnish Research Programme on Nuclear Power Plant Safety 2015-2018.

7 Appendix

7.1 Algorithm for selecting the optimal portfolio of safety measures

The algorithm determines the optimal portfolio $\mathbf{z}^*$ for the objective function $\mathcal{U}_*^t = \mathcal{U}^t(\mathbf{z}^*)$. Every portfolio of safety measures corresponds to a binary vector $\mathbf{z} = [z_1, ..., z_m]$ which is the concatenation of vectors $\mathbf{z}^i,\ \forall i \in V^A$ as described in (2). The size of the binary vector $\mathbf{z}$ is $m = \sum_{i \in V^A} |\mathcal{A}^i|$.

The model also accounts for the objective function $\mathcal{U}^t(\cdot)$, the budget and the feasibility constraints. In particular, the set of feasible portfolios is defined by a set of linear inequalities, whose coefficients are recorded in matrix $R \in \mathbb{R}^{\mathcal{L} \times m}$ ($r_j^l = [R]_{lj}$) and vector $\mathbf{b} = [b^1, ..., b^{\mathcal{L}}] \in \mathbb{R}^{\mathcal{L}}$. The set of feasible portfolios is

$$Z_F = \{\mathbf{z} \in \{0,1\}^m | R\,\mathbf{z} \leq \mathbf{b}\} \tag{38}$$

where $\leq$ holds component-wise.

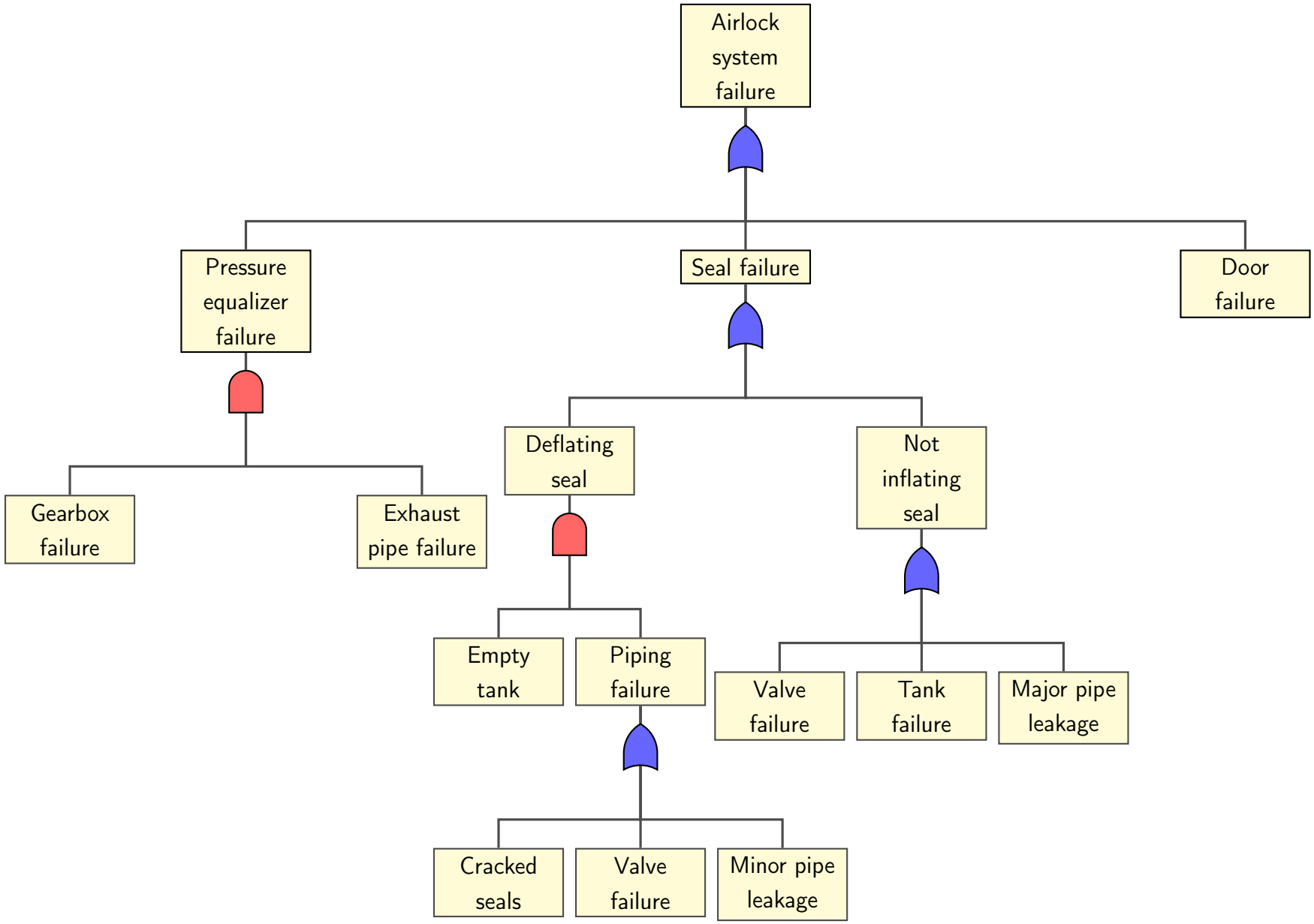
In addition to the constraints which ensure the uniqueness of the safety measure at each

node in (15), the set Z_F accounts for feasibility and budget constraints in (16).

Data: $\mathcal{U}^t(\cdot)$, R, $\mathbf{b}$, $\epsilon^i(s)$
Result: $\mathbf{z}^*$, $\mathcal{U}^t_*$
$\mathbf{z} = [0, ..., 0]^T$, $k \leftarrow 1$, $\mathbf{z}_* \leftarrow \emptyset$, $\mathcal{U}^t_* \leftarrow \infty$;
if $\boldsymbol{z} \in Z_F$ **then**
  $\mathbf{z}^* \leftarrow \mathbf{z}$, $\mathcal{U}^t_* \leftarrow \mathcal{U}^t(\mathbf{z})$;
end
Loop A: **while** $k > 0$ **do**
  Loop B: **while** $k \leq m$ **do**
    $z_k \leftarrow 1$;
    if $\boldsymbol{z} \in Z_F$ and $\mathcal{U}^t(\boldsymbol{z}) < \mathcal{U}^t_*$ **then**
      $\mathbf{z}^* \leftarrow \mathbf{z}$, $\mathcal{U}^t_* \leftarrow \mathcal{U}^t(\mathbf{z})$;
    end
    if $\sum_{j=1}^{k} z_j \, r_j^l + \sum_{j=k+1}^{m} \min\{0, r_j^l\} > b^l \, \forall l = 1, ..., \mathcal{L}$ **then**
      Break *Loop B*
    end
    $k \leftarrow k + 1$;
  end
  $z_m \leftarrow 0$;
  $k \leftarrow \max\left(\{j | z_j = 1\} \cup \{0\}\right)$;
  if $k > 0$ **then**
    $z_k \leftarrow 0$;
    $k \leftarrow k + 1$
  end
end

Algorithm 1: The implicit enumeration algorithm.

7.2 Airlock system Fault Tree



References

[1] Aven T., Baraldi P., Flage R., Zio E., *Uncertainty in Risk Assessment: The Representation and Treatment of Uncertainties by Probabilistic and Non-Probabilistic Methods*, John Wiley & Sons, New York (2014).

[2] Kuo W., Zhu X., *Importance Measures in Reliability, Risk and Optimization: Principles and Applications*, John Wiley & Sons, New York (2012).

[3] Zio E. *Computational Methods for Reliability and Risk Analysis*, World Scientific Publishing, Singapore (2011).

[4] Cheok M.C., Parry G.W., Sherry R.R., *Use of importance measures in risk-informed regulatory applications*, Reliability Engineering and System Safety 60, pp. 213-226 (1998).

[5] Zio E., Podofillini L., *Importance measures and genetic algorithms for designing a risk-informed optimally balanced system*, Reliability Engineering and System Safety 92, pp. 1435-1447 (2007).

[6] Vesely W.E., *Principles of resource-effectiveness and regulatory-effectiveness for risk-informed applications: Reducing burdens by improving effectiveness*, Reliability Engineering and System Safety 63, pp. 283-292 (1999).

[7] Salo A., Keisler J., Morton A., Eds. *Portfolio Decision Analysis – Improved Methods for Resource Allocation*, International Series in Operations Research & Management Science, Vol. 162, Springer-Verlag (2011).

[8] Toppila A., Salo A. *Selection of risk reduction portfolios under interval-valued probabilities*, Reliability Engineering and System Safety 163, pp. 69-78 (2017).

[9] Zio E. *An Introduction to the Basics of Reliability and Risk Analysis*, World Scientific Publishing, Singapore (2007).

[10] Prasad V.R., Kuo W., *Reliability optimization of coherent systems*, IEEE Transactions on Reliability 49, pp. 323-330 (2000).

[11] Couronneau J.C., Tripathi A., *Implementation of the new approach of risk analysis in France*, Proceedings of the 41st International Petroleum Conference, Bratislava, Slovakia (2003).

[12] Markowski A.S., Kotynia A., *"Bow-tie" model in layer of protection analysis*, Process Safety and Environmental Protection 89, pp. 205-213 (2011).

[13] Baraldi, P., Compare, M., Despujols, A., Lair, W., Zio, E., *A practical analysis of the degradation of a nuclear component with field data*, Safety, Reliability and Risk Analysis: Beyond the Horizon - Proceedings of the European Safety and Reliability Conference, ESREL 2013, pp. 1009-1014 (2014).

[14] Veeramany A., Pandey M.D., *Reliability analysis of nuclear piping system using semi-Markov process model*, Annals of Nuclear Energy 38, pp. 1133-1139 (2011).

[15] Jensen F., *Bayesian Networks and Decision Graphs*, Springer-Verlag, New York (2001).

[16] Weber P., Median-Oliva G., Iung B., *Overview on Bayesian networks application for dependability, risk analysis and maintenance areas*, Engineering Applications of Artificial Intelligence 25, pp.671-682 (2012).

[17] 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, pp. 46-53 (2013).

[18] 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).

[19] Käki A., Salo A., Talluri S., *Disruptions in supply networks: a proabilistic risk assessment approach*, Journal of Business Logistics 36, pp. 273-287 (2015).

[20] Pearl J., *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan Kaufmann Publishers, San Mateo (1988).

[21] Fleming K.N., *A reliability model for common mode failures in redundant safety systems*, Proceedings of the Sixth Annual Pittsburgh Conference On Modeling and Simulations, Instrument Society of America, Pittsburgh (1975).

[22] Modarres M., *Risk Analysis in Engineering: Techniques, Tools and Trends*, CRC Press, Boca Raton (2006).

[23] Edwards W., *How to use multiattribute utility measurement for social decision making*, IEEE Transactions on Systems, Man and Cybernetics 7, pp. 326-340 (1977).

[24] Von Winterfeldt D., Edwards W., *Decision Analysis and Behavioural Research*, UK: Cambridge University Press, Cambridge (1986).

[25] Edwards W., Barron F.H., *SMARTS and SMARTER: Improved simple methods for multiattribute utility measurement*, Organizational Behaviour and Human Decision Processes 60, pp. 306-325 (1994).

[26] Liesiö J., *Measurable multiattribute value functions for portfolio decision analysis*, Decision Analysis 11, pp. 1-20 (2014).

[27] Liesiö J., Mild P., Salo A., *Robust portfolio modeling with incomplete cost information and project interdependencies*, European Journal of Operational Research 190, pp. 679-695 (2008).

[28] 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 25, pp. 11-20 (2012).

[29] Luenberger D.G., *Investment Science*, Oxford University Press, Oxford (1997).

[30] Lennon T., Moore D., *The natural fire safety concept – full scale tests at Cardington*, Fire Safety Journal 38, pp. 623–643 (2003).

[31] Zio E., *Integrated deterministic and probabilistic safety analysis: Concepts, challenges, research directions*, Nuclear Engineering and Design, pp.1-7 (2014).